AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Western District of Texas, Midland Division on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
7:26-cv-00075	3/4/2026	Western District of Texas, Midland Division

PLAINTIFF	DEFENDANT
MOBILITY IP HOLDINGS, INC.	APPLE INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	8,151,345	4/3/2012	
2	8,548,924	10/1/2013	
3	8,766,772	7/1/2014	
4	8,933,807	1/13/2015	
5	10,235,513	3/19/2019	
6	10,706,412	7/7/2020	
7	10,762,187	9/1/2020	

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

APPLE 1002

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.
15/372,317	03/19/2019	10235513	116546-613CT17	6203

27189 7590 02/27/2019

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;
NEOLOGY, INC., Poway, CA;
Manfred Rietzler, Marktoberdorf, GERMANY;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Doc Code: MFEE.C.AD PTO/SB/47-EFS

Document Description: Maintenance Fee Address Change

FEE ADDRESS INDICATION FORM			
Application Number	15372317	Art Unit	2685
Filing Date	07-Dec-2016	Examiner Name	VAN TRIEU
First Name Inventor	Francisco Martinez de Velasco Cortina	Attorney Doc. Number	116546-613CT17

INSTRUCTIONS: In order for the fee address identified on this form to be effective, the issue fee must have been paid for the application listed on this form. Only an address represented by a customer number can be established as the fee address for maintenance fee purposes (hereafter, fee address). A fee address should be established when correspondence related to maintenance fees should be mailed to a different address than the correspondence address for the application. For more information on customer numbers, see the Manual of Patent Examining Procedure (MPEP) § 403.

Please recognize as the Fee Address under the provisions of 37 CFR 1.363 the address associated with:

Customer Number:	27189 PROCOPIO, CORY, HARGREAVES & SAVITCH LLP 525 B STREET SUITE 2200 SAN DIEGO CA 92101 UNITED STATES 6192381900 docketing@procopio.com

Signature :

I certify, in accordance with 37 CFR 1.4(d)(4) that I am an attorney or agent registered to practice before the Patent and Trademark Office who has filed and has been granted power of attorney in this application.

Signature	/Mark W. Catanese/	**Date**	01-24-2019
Name	Mark William Catanese	**Registration Number**	64279

Electronic Patent Application Fee Transmittal

Application Number:	15372317
Filing Date:	07-Dec-2016
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT17

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY APPL ISSUE FEE	1501	1	1000	1000
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**1000**

Electronic Acknowledgement Receipt	
EFS ID:	34951824
Application Number:	15372317
International Application Number:	
Confirmation Number:	6203
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT17
Receipt Date:	24-JAN-2019
Filing Date:	07-DEC-2016
Time Stamp:	17:51:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1000
RAM confirmation Number	012519INTEFSW17514200
Deposit Account	502075
Authorized User	Helen Glenister
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.20 (Post Issuance fees) 37 CFR 1.21 (Miscellaneous fees and charges)	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	Web85b.pdf	46536 c37187b87fcf801547e48c6912fd771c398fb6bb	no	2
Warnings:					
Information:					
2	Maintenance Fee Address Change	web85feeaddress.pdf	33159 7441c0efa4a017241335db74f9a8ad2e3c760ab8	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31840 1efc6bd8fb14509e9a53ac00056f2f186b1b10d1	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	111535		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: IFEE PTOL/85B-EFS

Document Description: Issue Fee Payment (PTO-85B)

Issue Fee Transmittal Form

Application Number	Filing Date	First Named Inventor	Atty. Docket No.	Confirmation No.
15372317	07-Dec-2016	Francisco Martinez de Velas	116546-613CT17	6203

TITLE OF INVENTION :

SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

Entity Status	Application Type	Art Unit	Class - Subclass	EXAMINER
Regular Undiscounted	Utility under 35 USC 111(a)	2685	572700	VAN TRIEU

Issue Fee Due	Publication Due	Total Fee(s) Due	Date Due	Prev. Paid Fee
$1000	$0	$1000	29-Jan-2019	$0

1.Change of Correspondence Address and/or Indication Of Fee Address (37 CFR 1.33 & 1.363)

Current Correspondence Address:	Current Indicated Fee Address :
27189 PROCOPIO, CORY, HARGREAVES & SAVITCH LLP 525 B STREET SUITE 2200 SAN DIEGO CA 92101 UNITED STATES 6192381900 PTONotifications@procopio.com	
☐ Change of correspondence address requested, system generated AIA/122-EFS form attached	☒ Fee Address indication requested, system generated SB/47-EFS form attached

2.Entity Status

Change in Entity Status

○ Applicant certifying micro entity status; system generated Micro Entity certification form attached. See 37 CFR 1.29.
Note: Absent a valid certification of micro entity status, issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment. If this box is checked, you will be prompted to choose a micro entity status on the gross income basis (37 CFR 1.29(a)) or the institution of higher education basis (37 CFR 1.29(d)), and make the applicable certification online.

○ 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.

Doc Code: IFEE PTOL/85B-EFS

Document Description: Issue Fee Payment (PTO-85B)

3.The Following Fee(s) Are Submitted:

☒ Issue Fee

☐ I authorize USPTO to apply my previously paid issue fee to the current fees due

☐ Publication Fee

☐ The Director is hereby authorized to apply my previously paid issue fee to the current fee due and to charge deficient fees to Deposit Account Number _____

☐ Advance Order - # of copies _____

☒ If i**n addition to** the payment of the issue fee amount submitted with this form, there are any discrepancies in any amount(s) due, the Director is authorized to charge any deficiency, or credit any overpayment, to Deposit Account Number 502075 . The **issue fee must be submitted** with this form. **If payment of the issue fee does not accompany this form, checking this box and providing a deposit account number will NOT be effective to satisfy full payment of the fee(s) due.**

4.Firm and/or Attorney Names To Be Printed

NOTE: If no name is listed, no name will be printed
For printing on the patent front page, list to be displayed as entered

1. PROCOPIO
2. MARK W. CATANESE
3. NOEL C. GILLESPIE

5.Assignee Name(s) and Residence Data To Be Printed

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.

Name	City	State	Country	Category
Neology, Inc.	San Diego	CALIFORNIA	united states	corporation

6.Signature

I certify, in accordance with 37 CFR 1.4(d)(4) that I am an attorney or agent registered to practice before the Patent and Trademark Office who has filed and has been granted power of attorney in this application. I also certify that this Fee(s) Transmittal form is being transmitted to the USPTO via EFS-WEB on the date indicated below.

Signature	/Mark W. Catanese/	**Date**	01-24-2019
Name	Mark William Catanese	**Registration Number**	64279

WEB IFEE 1.0

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 10/29/2018

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: 10/29/2018

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,317	12/07/2016	Francisco Martinez de Velasco Cortina	116546-613CT17	6203

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	01/29/2019

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

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

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

27189 7590 10/29/2018

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

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,317	12/07/2016	Francisco Martinez de Velasco Cortina	116546-613CT17	6203

TITLE OF INVENTION: SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	01/29/2019

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRIEU, VAN THANH	2685	340-572700

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

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

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1_____
2_____
3_____

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

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

4a. Fees submitted: ❑Issue Fee ❑Publication Fee (if required) ❑Advance Order - # of Copies _____

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

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

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

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,317	12/07/2016	Francisco Martinez de Velasco Cortina	116546-613CT17	6203

27189 7590 10/29/2018

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: 10/29/2018

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

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

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

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 15/372,317	Applicant(s) Martinez de Velasco Cortina et al.	
	Examiner VAN T TRIEU	Art Unit 2685	AIA 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 response after the Final filed on 08/29/2018.
   ☐ 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 1-26 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

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

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

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/VAN T TRIEU/
Primary Examiner, Art Unit 2685 10/22/2018

DETAILED ACTION

EXAMINER'S AMENDMENT

1. The application has been amended as follows: In the Specification filed on 12/07/2016, page 1, first paragraph, line 2, after the year "2013" insert --- now Patent Number. 9,558,385, issued on 01/31/2017, ---.

Allowable Subject Matter

2. The following is an examiner's statement of reasons for allowance: the prior arts fails to teaching and/or suggesting of a mobile device, comprising a processor configured to:

receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,

compare the received biometric data with the biometric information stored in the memory, and

transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric data matches the stored biometric information; and

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

3. Any inquiry concerning this communication or earlier communications from examiner should be directed to primary examiner craft is **Van Trieu** whose telephone number is (571) 2722972. 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

10/22/2018

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/372,317	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	VAN T TRIEU	2685

CPC - Searched*		
Symbol	Date	Examiner
G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06C20/20, G06C20/206, G06C20/40, G06C20/401, G06C20/405	1/30/17	vt
G08B13/2402, G08B13/2417	1/30/17	vt

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06C20/20, G06C20/206, G06C20/40, G06C20/401, G06C20/405, and the results text limited - see attached search history printout.	1/30/17	vt
G08B13/2402, G08B13/2417, and the results text limited - see attached search history printout.	1/30/17	vt
Update Search	6/19/17	vt
Update Search	2/1/18	vt
Update Search	7/5/18	vt
Update Search	10/22/2018	vt

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/372,317	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	VAN T TRIEU	2685

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
	Text search for claimed subject matter in EAST US Patent and PG Publication databases. See attached search history printout.	10/22/2018	vt

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/372,317	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	VAN T TRIEU	2685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

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

CLAIM		DATE								
Final	Original	01/30/2017	06/19/2017	02/01/2018	07/05/2018	10/22/2018				
1	1	✓	✓	✓	✓	=				
2	2	✓	✓	✓	✓	=				
3	3	✓	✓	✓	✓	=				
4	4	✓	✓	✓	✓	=				
5	5	✓	✓	✓	✓	=				
6	6	✓	✓	✓	✓	=				
7	7	✓	✓	✓	✓	=				
8	8	✓	✓	✓	✓	=				
11	9	✓	✓	✓	✓	=				
12	10	✓	✓	✓	✓	=				
13	11	✓	✓	✓	✓	=				
14	12	✓	✓	✓	✓	=				
15	13	✓	✓	✓	✓	=				
16	14	✓	✓	✓	✓	=				
19	15	✓	✓	✓	✓	=				
20	16	✓	✓	✓	✓	=				
21	17	✓	✓	✓	✓	=				
22	18	✓	✓	✓	✓	=				
23	19	✓	✓	✓	✓	=				
24	20	✓	✓	✓	✓	=				
9	21			✓	✓	=				
17	22			✓	✓	=				
25	23			✓	✓	=				
10	24			✓	✓	=				
18	25			✓	✓	=				
26	26			✓	✓	=				

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/372,317	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	VAN T TRIEU	2685

CPC							
Symbol						**Type**	**Version**
G06F	/	21	/	35		F	2013-01-01
H04W	/	4	/	80		I	2018-02-01
G06F	/	21	/	34		I	2013-01-01
G06F	/	21	/	32		I	2013-01-01
G06F	/	21	/	31		I	2013-01-01
G06K	/	19	/	0723		I	2013-01-01
G06K	/	19	/	07758		I	2013-01-01
G06K	/	19	/	10		I	2013-01-01
G06K	/	7	/	0008		A	2013-01-01
G06K	/	19	/	0776		A	2013-01-01
G06K	/	19	/	07764		A	2013-01-01
G07C	/	9	/	00087		A	2013-01-01
G06Q	/	2220	/	00		A	2013-01-01
H04W	/	12	/	06		A	2013-01-01
H04W	/	12	/	08		A	2013-01-01
H04L	/	63	/	0861		A	2013-01-01

CPC Combination Sets								
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	26	
/VAN T TRIEU/ Primary Examiner, Art Unit 2685	22 October 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	12

U.S. Patent and Trademark Office — Part of Paper No.: 20181022

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/372,317	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	VAN T TRIEU	2685

INTERNATIONAL CLASSIFICATION				
CLAIMED				
G06F	/	21	/	31

NON-CLAIMED				
	/		/	

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	26	
/VAN T TRIEU/ Primary Examiner, Art Unit 2685	22 October 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	12

U.S. Patent and Trademark Office — Part of Paper No.: 20181022

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15/372,317	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	VAN T TRIEU	2685

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

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	12	10	23	19										
2	2	13	11	24	20										
3	3	14	12	9	21										
4	4	15	13	17	22										
5	5	16	14	25	23										
6	6	19	15	10	24										
7	7	20	16	18	25										
8	8	21	17	26	26										
11	9	22	18												

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	26	
/VAN T TRIEU/ Primary Examiner, Art Unit 2685	22 October 2018	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	12

U.S. Patent and Trademark Office — Part of Paper No.: 20181022

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. 6203

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
15/372,317	12/07/2016	340	2685	116546-613CT17

APPLICANTS
NEOLOGY, INC., Poway, CA;

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

**** CONTINUING DATA **************************** /V.T.T/
This application is a CON of 14/084,565 11/19/2013 PAT 9558385
which is a CON of 13/350,665 01/13/2012 PAT 8587436
which is a CON of 13/175,768 07/01/2011 PAT 8237568
which is a CON of 12/688,666 01/15/2010 PAT 8004410
which is a CON of 11/279,912 04/17/2006 PAT 7671746
which is a CON of 10/615,026 07/09/2003 PAT 7081819
which claims benefit of 60/394,241 07/09/2002

**** FOREIGN APPLICATIONS **************************** /V.T.T/

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****
12/15/2016

Foreign Priority claimed ❑ Yes ☑ No 35 USC 119(a-d) conditions met ❑ Yes ☑ No Verified and Acknowledged /VAN THANH TRIEU/ Examiner's Signature	❑ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	24	20	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 IDENTIFICATION SOLUTIONS

FILING FEE RECEIVED		
2080	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).

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	14985	(emit$4 or obtain$3 or receiv$3 or send$3 or transmit$4) near9 (biometric or eye$4 or face or facial or fingerprint) near9 (point near2 sale or POI or counter or check$4 or pay$3 or shopping or store or department)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 12:43
L2	241858	(cellular or handheld or mobile or PDA or portable or reader or scan$4) near9 (biometric or eye$4 or face or facial or fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 12:44
L3	55722	(compar$5 or different or match$3 or unmatch$3) near9 (biometric or eye$4 or face or facial or fingerprint) near9 (database or disc or memor$3 or recorded or stored or previous$2)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 12:45
L4	20874	(1 or 2) same (Bluetooth or IEEE or RFID or short or tag)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 12:47
L5	650	1 and 2 and 3 and 4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 12:47
L6	30	5 not @AY > "2003"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 12:48
L7	6	(("7081819") or ("7671746") or ("8004410") or ("8587436") or ("20030131247") or ("20040059923")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2018/10/22 12:50
L8	0	6 and 7	US-PGPUB; USPAT	OR	ON	2018/10/22 12:50
L9	0	5 and 7	US-PGPUB; USPAT	OR	ON	2018/10/22 12:50

L10	2	7 and 1 and 2 and 3	US-PGPUB; USPAT	OR	ON	2018/10/22 12:50
L11	2	10 and (Bluetooth or IEEE or RFID or short or tag)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 12:53
L12	78979	(G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06G20/20, G06G20/206, G06G20/40, G06G20/401, G06G20/405, G08B13/2402, G08B13/2417).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 12:55
L13	9	12 and 6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 12:55
L14	2	12 and 7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:03
L15	0	13 and 14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:03
L16	381314	(transaction or account or bank or payment or statement) near9 (point near2 sale or POI or counter or check$4 or pay$3 or shopping or store or department)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:05
L17	7	16 and 13	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:05
L18	0	16 and 14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:06
L19	2	12 and 11	US-PGPUB; USPAT; USOCR;	OR	ON	2018/10/22 13:06

			FPRS; EPO; JPO; DERWENT; IBM_TDB			
L20	77406	(demand$3 or inquir$3 or request$3) near7 (database or memor$3 or POS or storage or recorded or system) near6 (transaction or account or bank or payment or statement)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:09
L21	4	20 and (17 or 19)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:10
L22	3928	(cellular or handheld or mobile or PDA or portable) near9 20	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:18
L23	0	22 and (17 or 19)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:18
L24	0	22 and 7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:18
L25	0	22 and 6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:19
L33	108027	(cellular or handheld or mobile or PDA or portable) with "32"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/10/22 13:21
L45	2	7 and (transaction or bank or receipt$3) near9 (POS or sale)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:41

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

L26	26138	(G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06G20/20, G06G20/206, G06G20/40, G06G20/401, G06G20/405, G08B13/2402, G08B13/2417).CPC.	US-PGPUB; USPAT	OR	ON	2018/10/22 13:19
L27	10322	(emit$4 or obtain$3 or receiv$3 or send$3 or transmit$4) near9 (biometric or eye$4 or face or facial or fingerprint) near9 (point near2 sale or POI or counter or check$4 or pay$3 or shopping or store or department)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:19
L28	160235	(cellular or handheld or mobile or PDA or portable or reader or scan$4) near9 (biometric or eye$4 or face or facial or fingerprint)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:19
L29	38932	(compar$5 or different or match$3 or unmatch$3) near9 (biometric or eye$4 or face or facial or fingerprint) near9 (database or disc or memor$3 or recorded or stored or previous$2)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:20
L31	1830	27 and 28 and 29 and (Bluetooth or IEEE or RFID or short or tag)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:20
L32	61925	(demand$3 or inquir$3 or request$3) near7 (database or memor$3 or POS or storage or recorded or system) near6 (transaction or account or bank or payment or statement)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:21
L34	86054	(cellular or handheld or mobile or PDA or portable) with "32"	US-PGPUB; USPAT	OR	ON	2018/10/22 13:22
L35	177	31 and 34	US-PGPUB; USPAT	OR	ON	2018/10/22 13:22
L36	19	26 and 35	US-PGPUB; USPAT	OR	ON	2018/10/22 13:22
L37	3	36 not @AY > "2003"	US-PGPUB; USPAT	OR	ON	2018/10/22 13:24
L38	276126	(transaction or account or bank or payment or statement) near9 (point near2 sale or POI or counter or check$4 or pay$3 or shopping or store or department)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:24
L39	3	37 and 38	US-PGPUB; USPAT	OR	ON	2018/10/22 13:25
L40	268631	(demand$3 or inquir$3 or request$3) near9 (transaction or account or bank or receipt$3)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:38
L41	2	40 and 39	US-PGPUB; USPAT	OR	ON	2018/10/22 13:38
L42	3	39 and (transaction or account or bank or receipt$3)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:39
L43	3	39 and (transaction or bank or receipt$3)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:39

L44	0	39 and (transaction or bank or receipt$3) near9 (POS or sale)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:40
L47	2	39 and (POS or counter or sale)	US-PGPUB; USPAT	OR	ON	2018/10/22 13:42

10/ 22/ 2018 2:21:52 PM

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 15/372,317	Filing Date 12/07/2016	☐ 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

		(Column 1)		(Column 2)	(Column 3)		
	08/29/2018	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	* 26	Minus	** 26	= 0	X $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)		
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	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
ANTHONY WILLIAMS

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.
15/372,317	12-07-2016	Francisco Martinez de Velasco Cortina	116546-613CT17	6203

EXAMINER	
TRIEU, VAN THANH	

SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

ART UNIT	PAPER NUMBER
2685	

SUBMISSION DATE	DELIVERY MODE
August 29, 2018	EFS WEB

RESPONSE TO FINAL OFFICE ACTION WITH REQUEST TO WITHDRAW OF FINAL OFFICE ACTION

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

Dear Sir:

In response to the Final Office Action mailed on July 16, 2018, ("Final Office Action") Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following Amendment and Remarks, where:

Listing of the Claims begin on page 2 of this paper.

Summary of Communication with Examiner begins on page 7 of this paper.

Remarks begin on page 8 of this paper.

SUMMARY OF COMMUNICATION WITH EXAMINER

Applicant thanks Examiner Trieu for the courtesy extended during the telephonic communication conducted in the present application on August 27, 2018 with Mark Catanese ("Telephone Call"). During the Telephone Call, Applicant and Examiner discussed the availability of U.S. Pat. Pub. No. 2004/0059923 ("ShamRao") as a prior art reference under 35 USC §102(a)(2) in view of the effective filing date of the present application and as set forth in the Applicant's Amendment and Response to Non-Final Office Action filed on April 4, 2018 ("Non-Final Office Action Response"). During the Telephone Call the Examiner agreed to reconsider the availability of the ShamRao as prior art to the present application and consider withdrawing the present Final Office Action and Applicant agreed to file the request in writing. The substance of those discussions is reflected in the remarks below.

REMARKS

The present amendment is in response to the Final Office Action dated July 16, 2018. In view of the above listing of the claims and the following remarks, Applicant respectfully requests reconsideration and allowance of all pending claims.

A. Claim Status

With this Response, claims 1- 26 are pending in the application. Claims 1, 9, and 15 are the independent claims.

A. Request for Withdrawal of Finality

Applicant respectfully requests that the finality of the Final Office Action should be withdrawn because the Office has failed to consider the patentability arguments presented in the Non-Final Office Action Response and erroneously rejected the claims in view ShamRao, which is not available as prior art to the present application. The incorrect application of ShamRao as prior art precludes the Office Action from addressing the merits of the argument presented concerning one of the presented independent claims. Further, since ShamRao is not available as prior art, any rejection of the claims would necessarily be new grounds of rejections that are not necessitate by amendments made by the Applicant, as the previous Non-Final Office Action Response was filed without amendment.

MPEP 706.07(d) states that "[i]f, on request by applicant for reconsideration, the primary examiner finds the final rejection to have been premature, he or she should withdraw the finality of the rejection." An office action is final, "except where the examiner introduces a new ground of rejection that is neither necessitated by applicant's amendment of the claims, nor based on information submitted in an information disclosure statement filed during the period set forth in 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p)." *MPEP 706.07(a)*.

In the present application, on February 9, 2018, Applicant received a Non-Final Office Action rejecting claims 1-23 under 35 U.S.C. §102(a)(2) as anticipated by ShamRao.

In response, Applicant filed the Non-Final Office Action Response explaining that ShamRao has a filing date of September 25, 2002, which is after filing date of July 9, 2002 for provisional application No. 60/394,241 from which the present application claims

priority. Since ShamRao is not entitled to any other effective filing date (as explained in the Non-Final Office Action Response and set forth below), Applicant argued that ShamRao is not available as prior art under 35 U.S.C. §102(a)(2).

In response, Applicant received the current, outstanding Final Office Action which fails to take note of or in any way address Applicant's detailed explanation that ShamRao is not available as prior art. MPEP 707.07(f) explains that "[w]here the requirements are traversed, or suspension thereof requested, the examiner should make proper reference thereto in his or her action on the amendment." Here, while the Office Action repeated the previous rejections, it fails to address that ShamRao is not prior art and is not entitled to any other effective filing date. For example, in the "Response to Arguments" section on pages 11-12 of the Final Office Action, the Office does not make any reference to the Applicant's arguments that ShamRao is not prior art, and instead merely argues that US App. No. 09/992,109 ("the '109 application") is related to ShamRao and discloses the claimed features (a point Applicant does not concede as set forth in the Non-Final Office Action Response). However, as explained in the Non-Final Office Action Response (and restated below), ShamRao is not a continuing application to is entitled to claim benefit as a continuing application of the '109 application, and thus is not entitled to the filing data of the '109 application. Thus, the final Office Action is deficient because the Office failed to satisfy the requirements of MPEP § 707.07(f), and Applicant respectfully submit that the outstanding Final Office Action is improper.

Further, to the extent that the Office seeks to reject the claims using the '109 application, Applicant respectfully submits that any such rejection would necessarily be a new ground of rejection that is not predicated on amendments made by the Applicant. As stated above, a final action is premature where the examiner introduces a new ground of rejection that is not necessitated by applicant's amendment of the claims. Since Applicant filed the Non-Final Office Action Response without amendment to the claims, any subsequent action would not qualify as a final office action unless such rejections are based on information submitted in an information disclosure statement.

In view of the foregoing, Applicants respectfully request withdrawal of the finality of the outstanding Final Office Action and further request allowance of the claims, or at least a new non-final office action that addresses the merits of claims.

B. Claim Rejections – 35 USC § 102

Claims 1-26 are rejected under 35 U.S.C. §102(a)(2) as being anticipated by U.S. Pat. Pub. No. 2004/0059923 ("ShamRao"). Applicant respectfully traverses all of the rejections and submits that, for at least the reasons set forth in this paper and as explained in the Non-Final Office Action Response, the cited reference does not anticipate the claims because the cited reference is not available as prior art to the present application and fails to teach or suggest each feature of at least Claims 1, 9, and 15 as presented herein.

As explained in the Non-Final Office Action Response, Applicant respectfully re-submits that ShamRao is not available as prior art to the present application. Under 35 U.S.C. §102(a)(2), "[a] person shall be entitled to a patent unless . . . (2) the claimed invention was described in . . . an application for patent published or deemed published under section 122(b), in which the patent application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention." *See also, M.P.E.P. § 2152.* Here, ShamRao was filed on September 25, 2002. Whereas, the present application claims priority to provisional application No. 60/394,241 filed on July 9, 2002. Since the present application was effectively filed before the filing data of ShamRao, ShamRao does not qualify as prior art under 35 U.S.C. § 102(a) (2).

However, the Office argued that ShamRao claims priority to the '109 application filed on November 6, 2001 ("the '109 application"). *Office Action, pp. 2 and 11-12.* Applicant respectfully disagrees and re-submits that ShamRao does not claim priority to the '109 application, and thus is not entitled to the effective filing date of November 6, 2001.

Applicant notes that 37 C.F.R. §1.78(d)(2) provides the requirements for claiming the benefit of a prior filed nonprovisional application. Section 1.78(d)(2) requires, in part:

> (2) ***any nonprovisional application***, international application designating the United States, or international design application designating the United States that claims the benefit of one or more prior-filed nonprovisional applications, international applications designating the United States, or international design applications designating the United States ***must contain or be amended to contain a reference to each such prior-filed application***, identifying it by application number (consisting of the series code and serial number), international application number and international filing date, or international registration number and filing date under § 1.1023. If the later-filed application is a nonprovisional application, the reference

> required by this paragraph must be included in an application data sheet (§ 1.76(b)(5)). ***The reference also must identify the relationship of the applications, namely, whether the later-filed application is a continuation, divisional, or continuation-in-part of the prior-filed nonprovisional application,*** international application, or international design application.

(emphasis added).

Furthermore, M.P.E.P. §211.02(I) explains that "[t]hat the Office may ***not recognize any benefit claim*** where, for example, there is ***no indication of the relationship between the nonprovisional applications***, or no indication of an intermediate nonprovisional application that is directly claiming the benefit of a provisional application." (emphasis added). For applications filed before September 16, 2012 (as is the case with ShamRao), M.P.E.P. §211.02(II) provides that "an example of a proper benefit claim is 'this application ***is a continuation*** of prior Application No. —, filed —.' A benefit claim that merely states that 'this application ***claims the benefit of Application No. —, filed —" does not comply*** with 35 U.S.C. 120 and 37 CFR 1.78, since the relationship between the applications is not stated." (emphasis added). Therefore, for a nonprovisional application to claim benefit from, and thus an effective filing data of, a prior filed nonprovisional application, the nonprovisional application ***must identify the relationship*** between the applications. Where a relationship is not identified the Office will not recognize a benefit claim to the prior application.

In this case, paragraph [0001] of ShamRao states "[t]his application is related to Ser. No. 09/992,207 . . . , Ser. No. 09/992,113 . . . , Ser. No. 09/992,115 . . . , , and Ser. No. 09/992,109 . . . , all of which were filed on Nov. 6, 2001 and all share common inventorship, the contents of which are hereby expressly incorporated-by-reference." ShamRao merely states that it "***is related to***" the earlier filed applications. As explained above, merely stating the application "***claims the benefit of***" an earlier filed application is not sufficient to establish a priority claim, and here ShamRao fails to even state that much and instead merely states that it is related to other applications. *See, e.g.,* M.P.E.P. §211.02(II). Furthermore, there is no evidence that the Office has recognized that ShamRao is entitled to the effective filing data of November 6, 2001, since, for example, the front page of the ShamRao publication states only that it was "(22) Filed: [on] Sep. 25, 2002" and is silent as to any other filing dates. Additionally, the PAIR also fails to identify any continuity data or relationships to prior filed applications. *See,*

https://portal.uspto.gov/pair/PublicPair (searching for Application Number 10/255,264). Therefore, the Office does not recognize that ShamRao is entitled to any filing date other than September 25, 2002. Since the present application was effectively filed before any possible filing data of ShamRao, ShamRao does not qualify as prior art under 35 U.S.C. § 102(a)(2).

Accordingly, Applicant respectfully submits that the Final Office Action fails to establish each and every feature of claim 1 is disclosed in the prior art. Therefore, claim 1 is patentable and Applicant respectfully requests this rejection be withdrawn.

Independent claims 9 and 15 recite features similar to claim 1. Thus for at least the same reasons, Applicant respectfully submits prior art also fails to disclose or suggest all of the features of claims 9 and 15. Accordingly, Applicant requests the rejections be withdrawn.

Dependent claims 2-8, 10-14, and 16-23 depend directly or indirectly from one of independent claims 1, 9, and 15. As dependent claims inherit their patentability from their respective independent claim, the other dependent claims are allowable for at least their dependence on an allowable claim and their respective additional novel features. Accordingly, Applicant requests these rejections be withdrawn.

C. Claim Rejections – 35 U.S.C. § 103

Claims 24-26 stand rejected under 35 U.S.C. § 103 as being unpatentable over ShamRao as applied to claim 1, and in further view of U.S. Pub. No. 2003/0131247 ("Cannon"). Applicant respectfully traverses all of the rejections and submits that, for at least the reasons set forth in this paper, the cited references do not render the claims as obvious because the cited reference fails to disclose each feature of at least claims 1, 19, and 22 as presented herein.

Dependent claims 24-26 depend directly or indirectly from one of independent claims 1, 9, and 15. As dependent claims inherit their patentability from their respective independent claim, the other dependent claims are allowable for at least their dependence on an allowable claim and their respective additional novel features.

Applicant respectfully submits that Cannon has not been argued in the Office Action to and do not cure the deficiencies of ShamRao with respect to claims 1, 9, and 15.

Applicant respectfully submits that Cannon fails to teach or suggest at least the features discussed above in connection with claims 1, 9, and 15. Thus, Applicant respectfully submits that independent Claims 1, 9, and 15 define patentable subject matter over ShamRao in view of Cannon.

Accordingly, in view of the limitations as recited in independent claims 1, 9, and 15, and in view of the additional limitations as recited in dependent claims 24-26, Applicant respectfully submits that the dependent claims are allowable for at least the reasons discussed above and their respective additional novel features. Although Applicant has not discussed specific features of all of the dependent claims in this response, Applicant does not necessarily agree with the characterizations and assessments made in the Office Action with respect to the dependent claims. Thus, Applicant respectfully submits that dependent claims 24-26 are allowable.

CONCLUSION

For all the foregoing reasons, allowance of all pending claims 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: August 29, 2018

/Mark W. Catanese/
Mark W. Catanese
Reg. No. 64,279
Customer No. 27189

PROCOPIO CORY HARGREAVES & SAVITCH LLP
525 B Street
Suite 2200
San Diego, CA 92101
Tel 6192381900
Fax 6192350398
docketing@procopio.com

Electronic Acknowledgement Receipt	
EFS ID:	33575573
Application Number:	15372317
International Application Number:	
Confirmation Number:	6203
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT17
Receipt Date:	29-AUG-2018
Filing Date:	07-DEC-2016
Time Stamp:	17:03:51
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		116546-613CT17_Resp_to_FOA_July_16__2018_as_filed_08_29_2018.PDF	83250 271c0e1824b8fa3aeb2cd71268cb56f981a86bda	yes	15

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Response After Final Action	1	1
	Claims	2	6
	Applicant summary of interview with examiner	7	7
	Applicant Arguments/Remarks Made in an Amendment	8	15
Warnings:			
Information:			
	Total Files Size (in bytes):	83250	

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.

LISTING OF THE CLAIMS

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

a biometric input device configured to receive biometric data;

a short range radio frequency circuit;

memory configured to store biometric information for identifying an individual associated with transaction information;

a processor coupled with the memory and the biometric input device, the processor configured to:

receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,

receive the biometric data from the biometric input device,

compare the received biometric data with the biometric information stored in the memory, and

transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric data matches the stored biometric information; and

a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor.

2. (Original) The mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet.

3. (Original) The mobile device of claim 1, wherein the biometric input device is a fingerprint scanner.

4. (Previously Presented) The mobile device of claim 1, wherein the processor is further configured to transmit the received biometric data or the stored biometric information with the transaction information.

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

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

7. (Original) The mobile device of claim 1, further comprising memory configured to store the transaction information.

8. (Original) The mobile device of claims 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

9. (Previously Presented) A cellular telephone, comprising:

a fingerprint scanner configured to receive fingerprint data;

a short range radio frequency circuit;

memory configured to store fingerprint information for identifying an individual associated with transaction information;

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,

receive the fingerprint data from the fingerprint scanner,

compare the received fingerprint data with the fingerprint information stored in the memory, and

transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received fingerprint data matches the stored fingerprint information; and

a mobile device body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

10. (Previously Presented) The cellular telephone of claim 9, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.

11. (Original) The cellular telephone of claim 9, wherein the transaction information is account information.

12. (Original) The cellular telephone of claim 9, wherein the transaction information is credit card information.

13. (Original) The cellular telephone of claim 9, further comprising memory configured to store the transaction information.

14. (Original) The cellular telephone of claims 13, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

15. (Previously Presented) A cellular telephone, comprising:

cellular circuitry;

a fingerprint scanner configured to receive fingerprint data;

a short range radio frequency circuit;

a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information;

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal from a point of sale terminal via the cellular circuitry, the signal comprising a request to access the memory and retrieve the transaction information,

receive the fingerprint data from the fingerprint scanner,

compare the received fingerprint data with the fingerprint information stored in the memory, and

transmit the transaction information to a remote location using the cellular circuitry when the received fingerprint data matches the stored fingerprint information; and

a cellular telephone body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

16. (Previously Presented) The cellular telephone of claim 15, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.

17. (Original) The cellular telephone of claim 15, wherein the transaction information is account information.

18. (Original) The cellular telephone of claim 15, wherein the transaction information is credit card information.

19. (Original) The cellular telephone of claim 15, further comprising memory configured to store the transaction information.

20. (Original) The cellular telephone of claims 19, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

21. (Previously Presented) The mobile device of claim 1, wherein the processor is configured to compare the received biometric data with the biometric information stored in the memory in response to receiving the request to retrieve the transaction information.

22. (Previously Presented) The cellular telephone of claim 9, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

23. (Previously Presented) The cellular telephone of claim 15, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

24. (Previously Presented) The mobile device of claim 1, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

25. (Previously Presented) The cellular telephone of claim 9, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

26. (Previously Presented) The cellular telephone of claim 15, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

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.
15/372,317	12/07/2016	Francisco Martinez de Velasco Cortina	116546-613CT17	6203

27189 7590 07/16/2018

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

EXAMINER
TRIEU, VAN THANH

ART UNIT	PAPER NUMBER
2685	

NOTIFICATION DATE	DELIVERY MODE
07/16/2018	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. 15/372,317	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 *04/19/2018*.

☐ 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) *1-26* 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) *1-26* 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: _____.

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 1-23 are rejected under 35 U.S.C. 102(e) as being anticipated by **Shamrao** [US 2004/0059923] with a priority application Serial No. 09/992,109 filed on 11/06/2001.

Claim 1, the claimed a mobile device (the portable biometric authentication PBA 10, Fig. 1), comprising: a biometric input device configured to receive biometric data (the PBAS to scan and store person biometrics data in a storage mechanism 52 such as RAM, ROM memories, Figs. 2, 3, par [0024, 0025, 0032, 0033, 0039, 0040]); a short range radio frequency circuit (the Bluetooth communications and/or IEEE 802.11, Figs. 1, pars [0036-0038]);

memory (the storage 52 such as RAM, ROM memories, Fig. 2, pars [0032, 0033]) configured to store biometric information for identifying an individual associated with transaction information (the biometric, authentication and transaction data information, Figs. 2, 3, pars [0042, 0044, 0052, 0059]):

a processor (the PBA 10 with a CPU and processing steps 104, 106, 118 Figs. 1,2,5) coupled with the memory and the biometric input device, the processor configured to: receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the

transaction information (the CPU processing a request to scan his/her biometric 104, comparing, storing and to send the biometric data information to perform a transaction at the point of sale POP via Bluetooth or IEEE 802.11, Figs. 2, 3, 5 steps 104, 106, 110, pars [0031, 0036-0038, 0054-0056]);

receive the biometric information data from the biometric input device (Figs. 2, 5), compare the received biometric information data with the biometric information stored in the memory (the comparing of biometric data, Figs. 2, 3, 5 steps 104,106, pars [0024, 0044, 0054]), and

transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric information data matches the stored biometric information (the portable biometric authentication PBA 10 communicates biometric data information with the point of sale POP via Bluetooth or IEEE 812.11, Figs. 2, 3, 5 step 110, pars [0036-0038, 0054-0056]);

and a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor (the PBA 10 or PDA 129, Figs. 1,2, 6).

Claim 2, the mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet (the cellular mobile phones or notebook computers, pars [0034, 0036]).

Claim 3, the mobile device of claim 1, wherein the biometric input device is a fingerprint scanner (pars [0036, 0084]).

Claim 4, the mobile device of claim 1, wherein the processor is further configured to transmit the received biometric information data or the stored biometric information with the transaction information (the biometric information with transactions, as cited in respect to claim 1 above).

Claim 5, the mobile device of claim 1, wherein the transaction information is account information (the variety transactions include monetary transaction, pars [0011,0044, 0052]).

Claim 6, the mobile device of claim 1, wherein the transaction information is credit card information (the smart credit card transaction, Fig. 4, par [0052]).

Claim 7, the mobile device of claim 1, further comprising memory configured to store the transaction information (the storage 52, Fig. 2).

Claim 8, the mobile device of claims 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (the storage mechanism 52 such as RAOM, ROM memories, as cited in respect to claim 1 above, Figs. 2-4, pars [0032,0033]).

Claim 9, the claim a cellular telephone, comprising: a fingerprint scanner configured to receive fingerprint information data: a short range radio frequency circuit;
memory configured to store fingerprint information for identifying an individual associated with transaction information; a processor coupled with the memory and the fingerprint scanner, the processor configured to:
receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information, receive the fingerprint information data from the fingerprint scanner, compare the received fingerprint information data with the fingerprint information stored in the memory, and transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received fingerprint information data matches the stored fingerprint information: and a mobile device body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor (as cited in respect to claims 1,2 and 3 above).

Claim 10, the cellular telephone of claim 9, wherein the processor is further configured to transmit the received fingerprint information data or the stored fingerprint information with the transaction information (as cited in respect to claims 4 and 9 above).

Claim 11, the cellular telephone of claim 9, wherein the transaction information is account information (as cited in respect to claims 5 and 9 above).

Claim 12, the cellular telephone of claim 9, wherein the transaction information is credit card information (as cited in respect to claims 6 and 9 above).

Claim 13, the cellular telephone of claim 9, further comprising memory configured to store the transaction information (as cited in respect to claims 7 and 9 above).

Claim 14, the cellular telephone of claims 13, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (as cited in respect to claims 8 and 13 above).

Claim 15, the claimed a cellular telephone, comprising: cellular circuitry; a fingerprint scanner configured to receive fingerprint information data: a short range radio frequency circuit; a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information; a processor coupled with the memory and the fingerprint scanner, the processor configured to: receive a signal from a point of sale terminal via the cellular circuitry, the signal comprising a request to access the memory and retrieve the transaction information, receive the fingerprint information data from the fingerprint scanner, compare the received fingerprint information data with the fingerprint information stored in the memory, and transmit the transaction information to a remote location using the cellular circuitry when

the received fingerprint information data matches the stored fingerprint information: and a cellular telephone body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor (as cited in respect to claims, 1, 2, 3, 9 above).

Claim 16, the cellular telephone of claim 15, wherein the processor is further configured to transmit the received fingerprint information data or the stored fingerprint information with the transaction information (as cited in respect to claims 4 and 15 above).

Claim 17, the cellular telephone of claim 15, wherein the transaction information is account information (as cited in respect to claims 5 and 15 above).

Claim 18, the cellular telephone of claim 15, wherein the transaction information is credit card information (as cited in respect to claims 6 and 15 above).

Claim 19, the cellular telephone of claim 15, further comprising memory configured to store the transaction information (as cited in respect to claims 7 and 15 above).

Claim 20, the cellular telephone of claims 19, wherein the memory configured to store the biometric information and the memory configured to store the

transaction information are the same memory (as cited in respect to claims 8 and 19 above).

Claim 21, the mobile device of claim 1, wherein the processor is configured to compare the received biometric data with the biometric information stored in the memory in response to receiving the request to retrieve the transaction information (as cited in respect to claims 1, 8 and 19 above, par [0084]).

Claim 22, the cellular telephone of claim 9, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information (as cited in respect to claims 1, 9 and 19 above, the fingerprint scanner 172, see Figs. 7, 8).

Claim 23, the cellular telephone of claim 15, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information (as cited in respect to claims 1, 9, 22 above and including the authentication for accessing or retrieving monetary transaction, see Figs. 5, 7, 8).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims the examiner presumes that the subject matter of the various claims was commonly owned as of the effective filing date of the claimed invention(s) absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and effective filing dates of each claim that was not commonly owned as of the effective filing date of the later invention in order for the examiner to consider the applicability of 35 U.S.C. 102(b)(2)(C) for any potential 35 U.S.C. 102(a)(2) prior art against the later invention.

2. Claims 24-26 are rejected under 35 U.S.C. 103 as being unpatentable over **Shamrao** [US 2004/0059923] as applied to claim 1 above, and further in view of **Cannon** [US 2003/0131247]

Claim 24, **Shamrao** fails to disclose the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz. However, **Shamrao** discloses the portable PBA 10 includes a Bluetooth and/or IEEE 802.11 for communications, Figs. 2-5, pars [0036-0038]).

Cannon suggests that the wireless transceiver biometric device 100 includes the step of correlating the identity to the purchased media and storing rights relating to

the correlation. The method also includes the step of receiving the purchased media in a secure output device. The method also includes the steps of establishing the identity in the secure output device using the biometric device and determining if the identity matches the stored rights. If the identity matches the stored rights, the method also includes the step of allowing the output of the purchased media from the secure output device (Figs. 1,2, par [0009]). The biometric device 100 use Bluetooth 500 or IEEE 802.11 wireless technology for communication over the frequency about 20 MHz, see Figs. 1,4-6, pars [0031,0039, 0043, 0069]). Therefore, it would have been obvious to one skill in the art before the effective file date of the invention to utilize the frequency range about 20 MHz of **Cannon** for the portable PBA of **Shamrao** since both systems using the short range Bluetooth and/or IEEE 82.11 wireless technology for short range communications. Wherein the Bluetooth radio is built into a small microchip and operates in a globally available frequency band ensuring communication compatibility worldwide, see page 14 of [US 09/992,109].

Claim 25, the cellular telephone of claim 9, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz (as discussed between **Shamrao** and **Cannon** in respect to claim 24 above).

Claim 26, the cellular telephone of claim 15, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz (as discussed between **Shamrao** and **Cannon** in respect to claim 24 above).

Response to the Arguments

3. In response to the arguments filed on 04/19/2018 as following:

Applicant's arguments:

(A) Any possible filing data of ShamRao, ShamRao does not qualify as prior art under 35 U.S.C. § 102(a)(2).

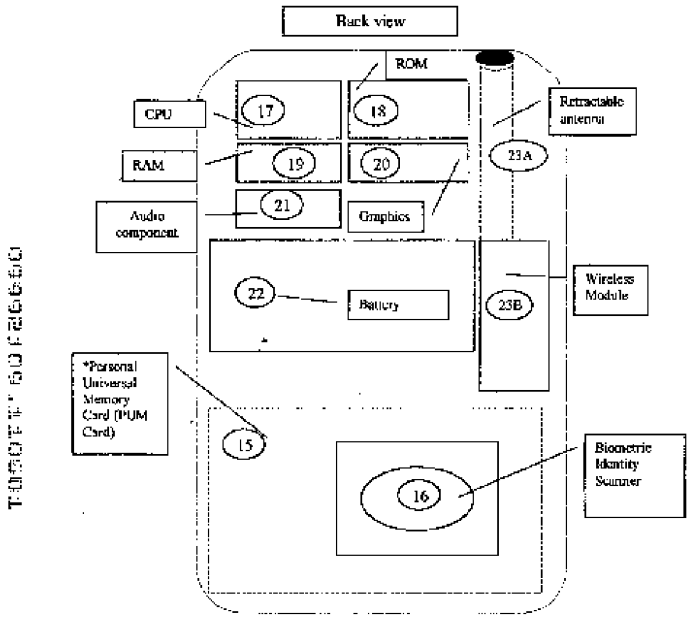
Furthermore, in the event that the publications of Application Numbers 09/992,207; 09/992,113; 09/992,115; and/or Ser. No. 09/992,109 (collectively “other applications”) are asserted against the presently presented claims, Applicant respectfully submits that these other applications do not teach or suggest all of the features of claim 1. For example, Applicant respectfully submits that the other applications do not teach or suggest at least a processor configured to “receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,” as recited in claim 1.

(B) **Cannon** has not been argued in the Office Action to and do not cure the deficiencies of **ShamRao** with respect to claims 1, 9, and 15. Applicant respectful submits that **Cannon** fails to teach or suggest at least the features discussed above in connection with claims 1, 9, and 15. Thus, Applicant respectfully submits that independent Claims 1, 9, and 15 define patentable subject matter over **ShamRao** in view of **Cannon**.

Response to the arguments:

(A) The copy of a Specification of one benefit prior US Application Number [US 09/992,109] is provided herewith, which includes a handheld wireless communication device such a PDA, cellular phone, see page 20, with biometric reader/scanner 16, the memory or PUM card 15 (see Fig. 1D, pages 3, 17) for storing of one or more customer's biometric data and a CPU 17, ROM 18, RAM 19 for processing and determining an authorization to that customer for accessing a transaction and/or other use. The handheld device also includes wireless communication module 23B such as Bluetooth and/or 802.11, see Fig. 1, pages 14, 15.

FIGURE 1D



(B) It is obviously to combine or utilize the frequency range about 20 MHz of **Cannon** for the portable PBA of **Shamrao** since both systems using the short range Bluetooth and/or IEEE 82.11 wireless technology for short range communications, without

Select Text

affecting or changing of data communications point-to-point therebetween. Wherein The Bluetooth radio is built into a small microchip and operates in a globally available frequency band ensuring communication compatibility worldwide. The Bluetooth specification has two power levels defined, see page 14 of [US 09/992,109].

Conclusion

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

Attached herewith the copy of a Specification of the Prior US Application Number [US 09/992,109] filed on 11/06/2011, as below:

HANDHELD COMPUTER SYSTEMS AND METHODS

Inventor: **Andrew Divaker ShamRao**

This application is related to Serial No. 09/992,109 entitled

5 "COMMUNICATION PROCESS FOR RETRIEVING INFORMATION FOR A COMPUTER", Serial No. entitled "CONFIGURATION-DEPENDENT DOWNLOAD PROCESS", and Serial No._____entitled "SYSTEMS AND METHODS FOR ENSURING SECURITY AND CONVENIENCE",

all of which share common inventorship and filed on the same date, the contents of which

are hereby expressly incorporated-by-reference.

BACKGROUND

The present invention relates generally to handheld computer systems. Handheld computing is a recent phenomenon and these computing devices include everything from pagers, to palm devices, to cell phones. The features carried by these devices are converging and include compactness, portability, expandability, data reception, transmission, input, and display. The handheld computing and communications industry is growing rapidly as users, particularly mobile professionals, increasingly rely on electronic management of critical personal and professional information, interaction with Internet-based information resources and mobile voice and data communications. Handheld devices such as personal digital assistants (PDAs) are small, handheld computers primarily used to write notes, record names, addresses and phone numbers, to develop an appointment calendar, and otherwise keep appointments in order. A scheduling program running separately in each of the computer and the

handheld computer maintains separate database information in data files relating to scheduled appointments and contact information.

These handheld computers often rely on the use of a stylus for data entry. The two most common methods for data entry utilizing a stylus are 1) tapping on an "on-screen software keyboard" and 2) hand writing on a pressure-sensitive layer. In the first method the electronic device displays a keyboard buttons, or other indicia on a pressure sensitive screen, and the user selects the desired option by tapping an appropriate location with the stylus. In the second method the user moves the stylus across a pressure-sensitive surface to form characters. In this latter method known as "handwriting recognition," the device recognizes the characters formed by the user on the pressure-sensitive surface. Exemplary handheld devices include products from Palm Computing, Handspring, and Windows-CE based hand held computers.

One growth driver for hand held devices is wireless communications that enable compelling applications. Digital wireless communications have become widely adopted due to declining consumer costs, expanding network coverage and the availability of extended service features such as voice and text messaging. Digital wireless technologies, which are currently

designed for voice transmission and allow only limited data transmission capabilities, are evolving towards advanced technologies enabling higher

20 data transmission rates at lower costs. Further, the development of applications for the digital delivery of consumer products and services, such as photographs, music, video games, news, books, driving directions, weather and stock quotes and trading, has accelerated as physical products and services are increasingly being replaced with bytes of data that are wirelessly transmitted.

These trends are accelerating toward the emergence of a device that integrates handheld computing applications and a broad range of communications functions. The recent push in the industry has been to create devices that can access the Internet wirelessly and allow the user to interact in a meaningful way with the information obtained from the Internet. Much of the effort has been directed at enhancing and using cellular technology to allow for communication with the Internet. This form of communication is still in its infancy, primarily because of the absence of universal standards in the mobile technology field, and the absence of bandwidth.

Current handheld products provide consumers with limited choices, typically between a simple device without expandability or the ability to be upgraded, and a complex, multi-function device that is

expensive, awkward to handle with modular attachments and difficult to use. Current devices are limited on a number of different levels. (1) Components of a device cannot be upgraded. (2) Existing devices do not possess an "open" architecture to facilitate standards in the industry and mass application development. Current handheld mobile devices initially are constructed to port proprietary software. (3) Owners of existing devices are "slaves" to their devices because of their monetary value, and because of security concerns. Much of their personal information may be stored on the device and therefore, the device becomes indispensable.

trl 15

20

While the price of these devices is decreasing steadily, it is still beyond the reach of most consumers. (4) Existing devices do not integrate functionality of PDAs and cellular and Internet telephony. One device on the market, which is not upgradeable, requires the user to purchase expensive modular attachments to make use of enhanced features. The only other alternative users have, to gain access to new features, is to purchase a new device that ports them, or allows modular attachments to achieve that end. Also, current devices and trends in the further development of them are slaves to cellular technology for communication with the Internet to conduct online wireless transactions. At this point in the infancy of wireless communication, it is inconclusive whether cellular technology or local-server technology is better.

SUMMARY

A handheld computer includes removable, replaceable, and upgradeable modules, one of which is a removable, replaceable, upgradeable, and re-writeable Personal Universal Memory card capable of receiving and storing information associated with a user from a server. The handheld computer has a motherboard having sockets to accept the replaceable, and upgradeable modules. The handheld computer also includes a card reader slot to accept the removable, replaceable, re-writeable, and upgradeable Personal Universal Memory card.

Implementations of the above aspect may include one or more of the following.

The Personal Universal Memory card can be used as an identification card for interaction with a device that requires user information. The Personal Universal Memory card can be used to customize a device to the needs of the consumer. The Personal Universal Memory card is credit-card-sized. The Personal Universal Memory card contains a cryptographic key, which protects the user's privacy during use. The Personal Universal Memory card can also be used as a credit card, debit card, or ATM card. The

cryptographic key is used to securely store the user's biometric scan on the Personal Universal Memory card for later comparison against user scans conducted for activating a user-session or for conducting transactions.

The motherboard has a sound module socket, further comprising a removable,

replaceable, and upgradeable sound module adapted to be plugged into the sound module socket. The motherboard has a graphics module socket, further comprising a removable, replaceable, and upgradeable graphics module adapted to be plugged into the graphics module socket. The motherboard has a wireless module socket, further comprising a removable, replaceable, and upgradeable wireless module adapted to be plugged into the wireless module socket. The motherboard has sockets to accept the removable, replaceable, and upgradeable central processing unit, the removable, replaceable, and upgradeable Random Access Memory module, the removable, replaceable, and

upgradeable Read Only Memory module. The motherboard also has a biometric scanner socket that receives a removable, replaceable, and upgradeable biometric scanner.

In another aspect, a computer network that includes a server wirelessly communicating with one or more wireless handheld devices includes a method of permitting a particular user to access the computer network from any of the handheld

devices. The method includes requiring that a Personal Universal Memory card be inserted into a card-reader slot on the device, requiring that the user's biometric scan matches the biometric information stored on the Personal Universal Memory card, and maintaining at the server unique customer identifiers associated with users; and maintaining at the servers unique identifiers associated with a plurality of users of the computer network establishing the user session without regard to any handheld device.

Implementation of the above method can include one or more of the following.

The method includes, at the server, using codes for user preferences sent by the device to the server to locate configuration information with matching codes; and downloading the configuration information with matching codes from the server to the selected handheld

device based on the device hardware configuration.

In another aspect, a computer program product implements, in a handheld device wirelessly coupled with a server, a method of initiating a user session with the server from the handheld device. The computer program product includes a computer-readable medium carrying executable instructions that, when executed, are capable of performing the acts of: identifying the presence of a Personal Universal Memory card in the handheld device; requesting initiation of a user session after the user has been verified as being the owner of the Personal Universal

Memory card in the device; and receiving and storing, at the handheld device, configuration information that the device allows to be downloaded to it.

Implementations of the computer program product can include executable instructions, when executed, are further capable of performing the act of initiating transmission of a requested service to the server with a service request. The executable instructions, when executed, are further capable of performing the act of receiving coded preference information associated with the authorized user of the server, the coded preference information having been generated in a process at the handheld device that includes: the server using the coded preference information to access a database maintained at the server system in order to locate the configuration information with codes that match the coded preference information associated with the user; and the handheld device downloading the configuration information to the handheld device.

The above compact, portable, wireless communication device ("device") allows the user to receive data from a local area server and transmit data to a local area server wirelessly. The device also acts as an audio and text input device to promote the user's interaction with content that has been received from the server and to facilitate text and audio

messaging. Input can occur using a keyboard on the device's touch-sensitive screen, or by voice, using the built-in microphone and speech recognition software. The display allows the user to see the received information. A speaker and head phone jack allows the user to hear information sent in audio form. The device is easily exchangeable and upgradeable using affordable replaceable components. Further, the device is adaptable to cellular technology. The user can gain access to the Internet, gain information from a remote server, or information stored on a local server by communicating with a local server, or by accessing a cellular network.

With this device, the user can set shopping list preferences to receive preference- based advertisements from local area vendors (e.g., in a mall), download games and other applications through communication with a local server (e.g., for use during wait time... or as a child-sitting device), record audio messages or convert audio input to a text file, access and surf the internet, email e-Cards, text files, audio files, download songs, access profile and preference information from a remote server, update their personal profile and preference information on their device, or on a remote server, create a new profile and preference file on the device, make telephone calls, make online payments for products and services at the vendor site, upgrade various components as needed to be able to use

applications or advanced features of the device, personalize the look of the device with different "faces," and share the device with others without compromising security. The device's use of a local area network allows for vendor to have local storage and access to their data and marketing campaigns accessed by device users.

Advantages of the invention may include one or more of the following. The

device is a wireless PDA that is small, elegant and easy to use, yet flexible enough to support a wide variety of personal preferences and professional requirements. The system provides a "generic," "open" architecture to facilitate a standard for writing wireless applications. The device is scalable, customizable, integrative, with disposable components.

The device is scalable because its components can be upgraded to handle more sophisticated web-based applications and features than the most basic version of the device can support. It is customizable because its components can be configured to suit the needs of the user. The device components are disposable because by themselves, they will be relatively inexpensive. The value of the device is determined by the sum of its components. The components are salvageable, so if one part is dysfunctional, it can be disposed of and replaced or upgraded.

Redacted

Another advantage of the device is that it is integrative because it combines functions of a Personal Digital Assistant (e.g., The Palm; see www.palm.com), with that of a messaging/email device (e.g., The BlackBerry; see www.blackberry.net), with that of phones using Internet Telephony (e.g., connect Here and Net2PhoneDirect; see www.Iconnecthere.com and www.Net2phonedirect.com). Telephony is achieved by wirelessly communicating with the Internet through a local area server. Thus, the device

provides independence from cellular telephone technology in that the device can do everything a cell phone can do without using cellular technology. However, because the device is component driven, the components can be changed and reconfigured to accommodate cellular technology when necessary.

Currently owners are "slaves" to their mobile devices because of the monetary value of the device, because all of their information is stored on the device, and because of security issues. This device berates the user because it is designed to be "slave" to the user.

As indicated above, because of its removable, replaceable, and upgradeable component-based architecture, the cost of this device is manageable and therefore, the device itself is virtually disposable. This device also does not permanently house critical user information, and therefore is disposable for this reason as well, and is useable by

5 multiple users in sequence. Critical user information is stored on a removable, replaceable, and upgradeable Personal Universal Memory Card (PUM Card), the size of a credit card that this device will accept. 1bird, three critical processes ensure the privacy and security of user information while a user is operating the device.

Thus, the device is user-dependent and will be "slave" to the user whose Personal

Jj IO Universal Memory Card is inserted into it. The three processes that ensure the privacy and security of user information are the Biometric Identity Scanning Process for authenticating that the user is the owner of the PUM Card inserted into the device, the Private Communication Process for ensuring secure transactions with the servers and other devices, and the Smart-Erase Shutdown Process for ensuring that the contents of a PUM Card left in a device are erased so its contents are not accessible by hackers.

Another advantage of the device is that it contains a Configuration-Dependent Download Process that ensures efficient operation of the device. An application will only be downloaded to a device if the device's configuration matches those required by the application for efficient operation on the device.

20 Various other features and advantages will appear from the description to

follow.

In the description, reference is made to the accompanying drawings that form a part thereof: and in which is shown by way of illustration, a specific embodiment for practicing the invention. This embodiment will be described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that structural changes may be made without departing from the scope of the invention. The following detailed description is therefore, not to be taken in a limiting sense, and the scope of the present invention is best defined by the depended claims.

BRIEF DESCRIPTION OF THE ORAWINGS

In the drawings wherein like reference numerals represent like parts:

Figs. 1A, 1B, 1C and 1D show a front view, a side view, a bottom view and a rear view of an exemplary handheld device, respectively.

Fig. 2 shows an exemplary process executed when information is being downloaded to the device of Figs. 1A-1D.

Fig. 3 shows a process to perform voice input.

Fig. 4A shows an exemplary process executed when information is being "pulled" from a server.

Fig. 4B shows an exemplary process executed when information is being "pushed" to a server.

Fig. *5* illustrates an exemplary process to update user profile and preferences. Fig. 6 shows an exemplary process executed during shut down of the device of Figs. 1A 1D.

Fig. 7 show a front view and a rear view of an exemplary Personal Universal Memory Card (PUM Card).

Fig. 8 shows an exemplary network supporting the wireless device of Figs. 1A-D

DESCRIPTION

Figs. 1A, 1B and 1C show a front view, a side view and a bottom view, respectively, of an exemplary compact, portable wireless, handheld communication device ("device"). Figure IA shows the plurality of buttons on the device, including an

5 "ON/OFF" button 1, a "DICTATE" button 3, a "KEYBOARD" button 5, a "SEND" button 6, an "INTERNET" button 7, and an "UPDATE" button 8. The device also provides a display screen 9. The device also includes a microphone port 4 and a speaker port 2. As shown in Figs. 1A, a stylus 10 is slidably stored in a recess along the right side of the device facing the user. Figure 1B shows a card-reader slot 11 into which the Personal Universal Memory Card (PUM Card) 15 (See Figure ID and Figure 7) slides. Above the PUM Card slot is a release mechanism 12 for releasing the card. The PUM

card is credit card sized and is used for storing user-produced information, such as profile information, preference information, e-mails, addresses, lists, calendar information, and so on. Fig. 1C shows an earphone plug 13 and a microphone plug 14 to receive an external earphone and/or an external microphone.

The device's value as a means of personalizing one's online and offline shopping experience is realized only when a Personalized Universal Memory Card (PUM Card) 15 is inserted into the PUM Card slot 11 on the side of the device. The user can insert the PUM Card either in a rented device, a borrowed device, or one the user owns. Once the card is inserted, and the user presses the "ON/OFF" button 1, the device powers up, and activates the antenna 24 (see Figure 1D), which facilitates wireless communication with a local server. At this point, the device prompts the user, for example, to place his index finger on the Biometric Identity Scanner 16 (See Figure 1D. Also see www.keytronic.com for a sample scanner embedded in a laptop), which matches the user's digitalized fingerprint with one stored on the PUM Card. If there is match, the user is informed that he has been identified as the owner of the PUM Card and, therefore, can use it. At this point, the device proceeds to personalize the device based on the user preferences stored on the PUM Card.

In one implementation, the card reader in the slot 11 is an internal unit mounted in a recess in the handheld computer. The reader receives the PUM card and electrical contacts on the reader connects electrical fingers that are accessible on the PUM card.

The electrical fingers support address bus signals, data bus signals, control bus signals, IO ground and power signals. These signals are communicated over the electrical fingers so that the processor of the handheld device can access memory or another processor mounted in the handheld computer.

Alternatively, in another implementation, an external reader can be used to read the PUM cards. The external reader is a small device that communicates with the

handheld computer over a communication port such as the serial bus. The user then plugs the card into this and it is then directly accessible by the handheld device.

In yet another implementation, the reader can also be a magnetic stripe reader for reading data encoded onto a magnetic strip on the PUM card. In one embodiment, the technique used for encoding magnetic cards is a "Two-Frequency, Coherent Phase

Recording" that allows for the representation of single-channe4 self-clocking serial data (F/2F). The reader can be motorized to move magnetic cards or can rely on manually moving the card, either through a

slotted reader or into an insertion-type reader. One set of preferences stored on the device is for applications the user likes to use on the device. Figure 2 describes an exemplary process 200, called the Configuration- Dependent Download Process, used by the device to download user-preferred applications from the server, while maintaining the efficiency of the device. An application will only be downloaded to a device if its configuration matches those required by the application, so as to ensure efficient operation of the device. Additional items that are downloaded include any text or audio messages sent to the user. The text messages can be viewed on the display screen 9, and the audio messages can be heard either on the speaker located at the speaker port 2, or using an earphone plugged into the earphone plug 13.

The Configuration-Dependent Download Process 200 is executed when the device is powered on. First, the user presses the on/off button (step 202). Next, the process 200 requests the users to use the Biometric Identity Scanner to authenticate his ownership of the PUM Card in device (step 204). In step 206, the Biometric Identity Scanner checks for a match between the scanned image and the one stored on the PUM Card. If the scan does not match what is on the PUM Card, the user is asked to register (step **208).** If a match is found, and the user's preferences indicate that preferred applications should be downloaded on startup, the device will send a "packet" of

information to the local server including the device hardware configuration 20 specifications, and the codes identifying user-preferred applications (step 210). The local server will look for applications whose codes match the codes for user-preferred applications; It will then see if the hardware specification requirements for these applications match the hardware configuration of the device. When the codes and configuration requirements match, the server will return only the codes for applications that the device's hardware configuration will support (step 212). In step 214, the device informs the user if some applications cannot be supported, and gives the user options to abort the download or to select from among the applications the device will support. If

5 the user opts to download applications, then the device commences the download process (step 216). If the user chooses to abort the download process, the user is given access to the main screen where he can select other options (step 218).

The device also allows for one-touch data input through voice transmission by means of pressing a button such as the "DICTATE" button 3. The process 300 for voice data input is shown in Figure 3. Pressing the "DICTATE" button (step 302) causes the device to ask the user whether he wants to create a text file or a sound file (step 304) and to execute either the audio-capture software and microphone housed in port 4 (step 306), or speech recognition software (step 308), depending

on the user's choice. The audio or text file that was created is saved on the PUM card (step 310). Next, the device asks whether the user wishes to send the saved file (step 312). If "no" the user is returned to the main screen where other options may be selected (step 314). If the user opts to do so, the device prompts the him to complete an email form (step 316) and to press the "SEND" button 6 upon completion of the form to send the requested file (step 318).

Pressing the "KEYBOARD" button 5, causes the device to launch a mini keyboard at the bottom of the touch-sensitive display 9. The key inputs can be activated with the stylus 10 used to push on the touch sensitive display screen 9. The keyboard can be used to create email text or to select preferences, create shopping lists, give feedback on a feedback form and so on. After completing each of these activities, pressing the "SEND" button 6 initiates transmission of the information to the server.

One-touch Internet access is supported through the local area server by means of pressing a button such as the "INTERNET' button 7. Pressing this button causes the device to execute communication with the Internet through a local area server. The home page loaded onto the user's device can be their custom page if they have one, or a default home page. The user will be able to surf elsewhere from that point.

Once on the Internet, the user will be able to download games, songs and other applications, send eCards, check stocks, find maps, participates in

EAST Search History

auctions, reserve travel and entertainment tickets, and access personal profile and preference information, among other activities.

The device can be used to "pull" information from a server or other device or "push" information to a server or other device over the local network or over the Internet. The process that governs information sharing from the device is called The Private Communication Process. The Private Communication Process For "Pulling" Information uses codes to identify specific kinds of information. This process is described in Figure 4A.

The Private Communication Process For "Pulling" Information is applicable, for example, when the user wants to see advertisements relevant to his shopping list. When 20 the user enters his shopping list (step 402A), each item is coded in a standardized manner, for example, shirts will have a specific code. The codes are sent to the server when the user presses the "SEND" button (step 404A). If a banner advertisement with a matching code for shirts is found on the server, that banner is "pulled" by the device and displayed for the user (step 406A). At this point, the user can access more information by clicking on the banner ad (step 408A). By using the matching-code process, the user's privacy is protected because no personal information is shared about the user, and at the same time, the user is allowed to customize his shopping experience.

The Private Communication Process For "Pushing" Information is typically used when conducting a transaction to pay for a product or service online, or when interacting with an ATM machine, or some other

device. The Private Communication Process For Online Payments is described in Figure 4B. The user accesses the Internet by pressing the "INTERNET" button (step 402B). He navigates to a transaction site such as www.paypal.com (step 404B) and follows the site's payment procedure (step 406B).

After specifying how much is to be paid, to whom, and from what account, the user is asked to authenticate that he is the owner of the PUM Card in the device by using the Biometric Identity Scanner (step 408B). Once authenticated, the user is asked to provide his password as permission to "push" personal information to a vendor from whom a product or service is being purchased (step 410B).

Besides performing transactions, the device can also be used to do Internet telephony. The sound capability supports the ability to converse with others as in a telephone call by connecting to the internet and accessing internet telephony vendors like www.net2phonedirect.com or www.iconnecthere.com.

With respect to the"UPDATE" button 8, pressing this button causes the device to execute communication with the remote servers through the local server and to download the personal profile and preference settings for the user to the PUM card on the wireless device. This process is illustrated in Figure 5. First, the user requests the

update by pressing an "UPDATE" button (step 502).

Next, the user is asked to authenticate that he is the owner of the PUM Card in the device by using the Biometric Identity Scanner (step 504). In step 3, the device checks for a connection with the local server, and in response, the local server connects with the

5 remote server behind a firewall (step 506). If the user authentication is successful, the PUM card is updated (step 508).

Pressing the "ON/OFF" button 1 at the end of a user session will initiate the Smart-Erase Shutdown Process 600 shown in Figure 6. The purpose of this process is to eliminate all traces of a user session on the device so that if it is a rental device, it will be ready for another user and the previous user's privacy will have been protected. The device has some auto shutdown features as well. If the user does not interact with it for longer than a user-specified or default amount of time, then the device will go into sleep mode. To reactivate the device from sleep mode, the user will have to go through a Biometric Identity Scan. If the device is left unused for longer than the sleep window, also specified by the user (or the default setting on the device), then the device will execute the Smart-Erase Shutdown Process.

IN step 602 of the Smart-Erase Shutdown Process 600 (Figure 6), the user presses the "ON/OFF" button to terminate the user session and

turn off the device. The device asks the user if he wants to update his profile on the main server to reflect the changes made to the PUM Card profile (step 604). A "No" response from the user (step 606) results in the device initiating step 618. A "Yes" response results in the device requesting a Biometric Identity Scan to authenticate the user's ownership of the PUM Card (step 608). If authentication fails (step 612), the device skips to step 620. After authentication (step 610), the device gives the user the options either of saving the PUM Card profile in a separate file for later review (step 614), or of overwriting the server profile (step 616). If the owner owns the device, he is asked if he wants keep the information on the device memory, and is asked to remove the PUM Card (step 618). If the device is a rental or if the owner-user opts to erase the device memory in step 618, if he owns the device, then the device memory and PUM Card, if left in the device, are erased (step 620). In step 622, the device terminates connection with the server and shuts down.

Figure ID shows an exemplary back view of the device shown in Figs. 1A-1C. Contained in the back of the device are removable and upgradeable components, including a Central Process Unit (CPU) 17, a hard drive with read-Only Memory (ROM) 18, Random-Access Memory (RAM) and Cache 19, a a graphics component 20, an audio component 21, housing compartment for batteries 22, a retractable antenna 23A

Docket 2450.4

and wireless module 23B, a housing compartment for a PUM Card 15, and the Biometric Identity Scanner 16.

The device accepts a removable, replaceable, and upgradeable Central Processing Unit (CPU) 17 used for processing information received from a local server and for processing the user s interaction with the device. The variable characteristic of this wireless CPU is its processing speed in Megahertz. One CPU can be replaced with another that possesses the same or higher processing speed, thus a1lowing the user greater 20 processing speed and power.

The device also accepts a removable, replaceable, and upgradeable components such as a hard drive 18, used for storing information received from a local server, such as application modules that a1low the user to interact with a local area server. The variable characteristic of this wireless memory component is its memory capacity, such as Read.- Only Memory (ROM). One memory component can be replaced with another that possesses the same or higher memory capacity, thus allowing the user more storage space for information downloaded from a local server.

Another component the device can accept is a removable, replaceable, and upgradeable wireless memory component used for storing information to speed up immediate access. The variable

characteristic of this wireless memory component is its memory capacity, such *as* Random Access Memory (RAM) and Cache memory I9. One memory component can be replaced with another that possesses the same or higher memory capacity, thus allowing the user more storage space for information that requires immediate access, and therefore faster access to the information.

The graphics adapter 20, used for displaying graphical information received from a local server, is another removable, replaceable, and upgradeable component. The variable characteristic of this removable graphics adapter is its power to handle complex graphics. The removable, replaceable, and upgradeable audio driver 21 allows the user to customize the driver's power to handle complex audio input, including conversion of audio input into digital format for transmission as audio or text files, or as "packets" for internet telephony, or for transmission over cellular technology.

A battery housing compartment 22 is also positioned on the back of the device to receive a battery powering the device. The battery compartment stores a rechargeable or non-rechargeable battery or batteries to power the device.

The antenna 23A is retractable; When the device is powered up, the antenna 23A extends to its full length. Conversely, when the device is shut down by means of pressing a button such as the "ON/OFF' button, the antenna 23A

retracts automatically. The wireless module 23B can be a Bluetooth module or an 802.11X module.

In Bluetooth wireless module embodiments, the Bluetooth wireless technology allows users to make effortless, wireless and instant connections between various communication devices, such as mobile phones and desktop and notebook computers.

Since it uses radio transmission, transfer of both voice and data is in real-time. The sophisticated mode of transmission adopted in the Bluetooth specification ensures protection from interference and security of data The Bluetooth radio is built into a small microchip and operates in a globally available frequency band ensuring communication compatibility worldwide. The Bluetooth specification has two power levels defined; a lower power level that covers the shorter personal area within a room, and a higher power level that can cover a medium range, such as within a home. Software controls and identity coding built into each microchip ensure that only those units preset by their owners can communicate. The Bluetooth wireless technology supports both point-to-point and point-to-multipoint connections. With the current specification, up to seven 'slave' devices can be set to communicate with a 'master' radio in one device. Several of these 'piconets' can be established and linked together in ad hoc 'scatters' to allow communication among continually flexible configurations.

All devices in the same piconet have priority synchronization, but other devices can be set to enter at any time.

The topology can best be described as a flexible, multiple piconet structure.

The Bluetooth module enables users to connect a wide range of computing and telecommunications devices easily and simply, without the need to buy, carry, or connect cables. It delivers opportunities for rapid ad hoc connections, and the possibility of automatic, unconscious, connections between devices. It will virtually eliminate the need to purchase additional or proprietary cabling to connect individual devices. Because Bluetooth wireless technology can be used for a variety of purposes, it will also potentially replace multiple cable connections via a single radio link.

For 802.11 embodiments such as 802.11b embodiments, the 802.11 standard provides MAC and PHY functionality for wireless connectivity of fixed, portable and moving stations moving at pedestrian and vehicular speeds within a local area. The IEEE 802.11 standard specifies a wireless connectivity system that standardizes access to one or more frequency bands for local area communications. For customers, the benefit is interoperability between multiple vendor products. The standard defines three physical methods as well as two types of networking. The three different physical layer methods include two using radio frequency and one using infrared. The two radio physical layers operate in 2.4 GHz :frequency

Proof of Service

range, one using :frequency hopping spread spectrum (FHSS) and the other using direct sequence spread spectrum (DSSS). The one infrared physical layer operates using baseband infrared. Over the air data rates of 1 Mbps and 2 Mbps are defined in the standard. The IEEE 802.11 standard defines two of networking, one being ad hoc networking and the other being infrastructure. An ad hoc network is a network composed sole]y of stations within mutual communication range of each other via the wireless medium. With ad hoc networking, the wireless clients communicate with t& each other without the need for a wired network or access points.

An infrastructure contains one or more access points which provide wireless clients with access to the wired network. Besides the wireless module, the device also contains a housing compartment 15 for a removable, replaceable, and upgradeable Personal Universal Memory Card (PUM Card) (see Figure 7). As described before, the PUM card is credit card sized and is used for storing user-produced information, such as profile information, preference information, e-mails, addresses, lists, calendar information, and so on. The variable characteristic of this wireless memory card is its memory capacity, such as Read-Only Memory (ROM). One memory card can be replaced with another that possesses a higher memory capacity, thus allowing the user more storage space for personal information which is used by the local area server to customize what the user experiences on the device.

The PUM card can be removed and carried like a credit card and inserted into any device capable of accepting and reading it; such as an ATM machine, parking meter, toll booth, wireless telephones, pay phones etc. This is the "universal" feature of the card. In one embodiment, the user can slide the PUM card into the device and remove it immediately thereafter. Some customers will not want to insert their card and leave it in the device for fear of forgetting it. The "swipe" method allows for their comfort. However, the device will alert them to slide it again if needed. Because the PUM card can be removed from a device and ported anywhere, Consumers do not have to carry the device with them. The device can be made available to the user at a vendor site, either for loan or rent, and the user can slid his PUM Card into the PUM Card slot and customize the device for his use. Consumers can also purchase their own devices and upgrade them as needed.

Figure 7 shows the front and back view of a PUM Card. The PUM Card can be obtained at any vendor who carries them and is available for free at its most basic level It comes with cryptographic information for transport security. Personalization of the card starts with inserting it into a device and pressing the "ON/OFF" button. When the device detects a "blank" PUM card, it initiates a registration process through which the user can personalize the card. During personalization, the user is asked to scan their fingerprint using the built-in Biometric Identity Scanner 15, and is also asked to enter various personal identification and preference information.

The PUM card can contain data that uniquely identifies the user. For example, the personalization data can include personal profile information including name, login id, password address, phone numbers, bank information, credit level etc., and consumer preference information such as preferred websites, stores, brand names, size of clothing, music, software, games, The data will also include biometric data to authenticate the user. The biometric data can include fingerprint scan, retina scan, voice identification, or other biometric data that the processor can compare against in real-time. A PUM Card can be shared by more than one user. The identities and personal profile and preference information are kept 15 separate.

Three processes that depend on a user's personal preference information stored on the PUM card are the Configuration Dependent Download Process (see Figure 2), the Private Communication Process for "Pulling" Information (see Figure 4A), and the Private Communication Process for "Pushing" Information (see Figure 4B). These processes have been described above.

As mentioned earlier, the Configuration-Dependent Download Process ensures the efficient operation of the device. This feature prompts application developers to program different versions of an application for differently configured devices, or "turn off' features for efficient use on a device, or configure modules for download that will work

efficiently on the device. Users can also purchase and "snap-on" new components such as an upgraded Read-Only memory component. Without the PUM Card, The device is virtually disposable because its utility as a tool for personalizing the wireless experience, whether it be for shopping, giving feedback, instantly receiving stock information, making travel arrangements, and so on, is limited without the PUM card. The PUM Card is the user's tool for personalized convenience in the wireless world, and processes such as the Configuration-Dependent Download Process (see Figure 2), the Private Communication Process for "Pulling" Information (see Figure 4A), and the Private Communication Process for "Pushing" Information (see Figure 4B) aid the user personalizing their experience.

Figure 8 shows an exemplary network supporting the wireless device of Figs. 1A- 1D. The network includes one or more wireless handheld devices 802 that wirelessly communicate with a local area server 810. The local area server 810 in turn communicates over a firewall with one or more remote servers **820.** The local area server 810 and the remote servers 820 communicate over a wide area network 850 such as the Internet.

The server 810 is protected by a firewall. When the firewall receives a network packet from the remote servers 820, it determines whether the transmission is authorized.

If so, the firewall examines the header within the packet to determine what encryption algorithm was used to encrypt the packet. Using this algorithm and a secret key, the firewall decrypts the data and addresses of the source and destination firewalls and sends the data to the server **810.** If both the source and destination are firewalls, the only addresses visible (i.e., unencrypted) on the network are those of the firewall. The addresses of computers on the internal networks, and, hence, the internal network topology, are hidden. This is called "virtual private networking" (VPN).

The server 810 provides a single point of integration, access, and navigation

through the multiple enterprise systems and information sources facing knowledgeable users operating the clie t handheld devices 802. The portal can additionally support services that are transaction driven. Once such service is advertising: each time the user accesses the portal, the client handheld device 802 downloads information from the server 810. The information can contain commercial messages/links or can contain downloadable software that contains codes matching those on the PUM Card. Based on user preference codes, banner advertisements

with matching codes can be displayed in the user's device. A user can click on the image and be routed to an advertiser's Web-site or retrieve more information from the server linked to the banner advertisement.

Advertisers pay for the number of advertisements accessed by users, the number of times users click on advertisements, or based on other criteria. Alternatively, the portal supports sponsorship programs, which involve providing an advertiser the right to be displayed on the face of the port or on a drop down menu for a specified period of time, usually one year or less. The portal also supports performance-based arrangements whose payments are dependent on the success of an advertising campaign, which may be measured by the number of times users visit a Web-site, purchase products or register for services. The portal can refer users to advertisers' Web-sites when they log on to the portal. Other services can be supported as well. For example, a vendor can rent space on the server to host their applications or advertisements for user access. Thus, applications will be stored on the server instead of on the handheld device, and will be accessible by users. By off-loading the storage on the server, the user minimizes the memory required on the client handheld device 802, thus enabling complex operations to run on minimal computers such as handheld computers and yet still ensures that he/she can access the application and related information anywhere anytime.

Another service is On-line Software Distribution/Rental Service. The portal can distribute its software and other software companies from its server. Additionally, the portal can rent the software so that the user pays only for the actual usage of the software. After each use, the application is erased and will be reloaded when next needed, after paying another transaction usage fee.

The device as described above is component based and its value will be determined by the sum of its removable, replaceable, and upgradeable parts, it will be a versatile instrument, the configuration of which can be customized to meet the usability needs and price point of the purchaser. The least expensive model will be virtually disposable, but reusable. As a result, vendors who purchase these devices for their customers can purchase the least expensive version with components appropriate to their price level and function they want the device to perform; vendors in malls can rent the equipment at different price levels based on the component configuration chosen by customers and the functionality they desire. The device can be used to "pull" featured sales to consumers based on their preference profile stored on their PUM card. This can take place at malls, airports, train stations, grocery stores, or at the location of any vendor. The device can be used to obtain feedback about a consumer's experience with a vendor. Further, the device can be used to collect data on behaviors and tasks that

Exhibit 1003 - Page 97

employees must complete in-house. Moreover, users who obtain these devices can purchase components separately for upgrading whatever part they want to at a price point their budget will allow to obtain the level of functionality they choose to have access to. For example, to use the telephony features of the device, the user may need to upgrade their modem and RAM components to higher levels. The disposable shell, consisting of just the screen, and buttons and other embedded components, allows users to purchase a shell of their choice at an inexpensive price and retain the components that came with the original device. Users may want to purchase a new shell because they want a different look, or because a new display technology has become available. The device can be used to conduct transactions using online transaction-vendors like www.PayPal.com. The device can be used for Internet Telephony through vendors such as www.Iconnecthere.com and www.Net2phonedirect.com. The device can be used to send instant messages to others with the device, via compressed audio files, or text based messaging.

Application developers can design applications for different levels of hardware configuration of the device and push their application for that platform and inform the user that either the more sophisticated version of their application is available, or that additional application features will become available, if they upgrade their hardware.

Portability of the device allows consumers to give feedback at the point of service provided a local server is nearby. The ability to give feedback at the point of service to an independent agency will increase the number of consumers actually giving feedback. Currently, statistics show that 9o+% of consumers do not give feedback. This amounts to many lost opportunities for vendors to address issues, which when addressed, can rescue customer confidence and loyalty.

The device supports easy data collection while satisfying privacy issues relating to personal information and preferences of the consumer. The device protects this information by reading the PUM card for preferences and then reading what advertisements are available on the local server based on a predetermined code. If the code matches, the device will "pull" the relevant ad to the device for the user to view. No personal information is sent to the local server. This same method can be used at all other electronic devices the card is used in. The device "pulls" relevant information from a device or activates a device based on synchronization of codes.

The compact, portable wireless communication device can be used in a wide range of industries, government organizations, and functions, and include, but are not limited to, the following:

Transportation and Travel Industry. More and more people travel each year, whether by rental car, plane, taxi, bus, boat, or train. The potential for

impacting the service in that industry is huge. At the most basic level, a customer will be able to give a taxi driver feedback via the device and be able to calculate the tip they should give based on the service received.

Government. Again, the implications for consumer participation in improving government services are phenomenal. Citizen participation in issues regarding legislation is also possible with this device. The device can be used in the armed forces for communication and verification of information; in the police department for verifying drivers' license information or finger prints without having to call; in schools for education...learning games can be run on the device by children, and so on.

Global Commerce. Many US companies have global operations, such as companies in the fast food industry. Understanding the preferences of local customer is a must for being successful. Many companies help large corporations establish a global Internet presence and their primary concern is whether the website caters to the local population's tastes. Consumers need access to something that is easy to use and takes very little time to give feedback. This device can help.

Advertising over the Internet has gone through many changes. All along, however, the challenge has been to target advertising to consumers who will respond to them. The core issue in this challenge is that of relevance to the consumer. This device will allow consumers to specify their preferences at the point of service, therefore, providing the information necessary to make advertising relevant to the individual. This will

Search Image

be very useful at malls where a consumer who enters the mall and specifies the categories of items s/he is looking for, can "pull" relevant advertisements from mall vendors to his or her device. The same is true of food items in a restaurant, or travel specials at airports, travel agencies, rides at theme parks, and so on. This device, combined with software, will revolutionize targeted advertising and bring value to vendors where previously that value was questionable with companies like www.DoubleClick.com.

The invention has been described herein in considerable detail in order to comply with the patent Statutes and to provide those skilled in the art with the information needed to apply the novel principles and to construct and use such specialized components as are required. However, it is to be understood that the invention can be carried out by specifically different equipment and devices, and that various modifications, both as to the equipment details and operating procedures, can be accomplished without departing from the scope of the invention itself.

---

5. **THIS ACTION IS MADE FINAL.** 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 mailing date of this final action.

6. 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: 07/05/2018

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	(("6657538") or ("20030001459") or ("20030131247") or ("20040059923") or ("20040128249")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2018/07/05 13:33
L2	11998	(cellular or handheld or mobile or PDA or portable or wireless) near9 (read$3 or scan$2 or scanning) near9 (biometric or eye$4 or faci$4 or fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 13:37
L3	15154	(cellular or handheld or mobile or PDA or portable or wireless) near9 (database or memor$5 or record$3 or stor$3) near5 (biometric or eye$4 or faci$4 or fingerprint)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 13:38
L4	2796	2 and 3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 13:39
L5	1	4 and 1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 13:39
L6	5	(("7081819") or ("7671746") or ("8004410") or ("8237568") or ("8587436")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2018/07/05 13:49
L7	5	4 and 6	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 13:53
L9	561	4 and (counter or POS or sale) with (pay$3 or payment or receipt$3 or transaction)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 13:55
L10	1	9 and (1 or 6)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 13:55
L11	1833	(4 or 1 or 6) and (RFID or tag or short or IEEE$5)	US-PGPUB; USPAT;	OR	ON	2018/07/05 13:57

			USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			
L12	1829	4 and (RFID or tag or short or IEEE$5)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 13:57
L13	6	12 and (1 or 6)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 13:57
L14	72596	(G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06C20/20, G06C20/206, G06C20/40, G06C20/401, G06C20/405, G08B13/2402, G08B13/2417).CPC.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 14:23
L15	4	14 and (1 or 6)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 14:23
L16	5	6 and fingerprint	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 16:38
L17	4	1 and fingerprint	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2018/07/05 16:39

EAST Search History (Interference)

< This search history is empty>

7/5/2018 4:49:07 PM

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372317	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	VAN TRIEU	2685

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06C20/20, G06C20/206, G06C20/40, G06C20/401, G06C20/405	1/30/17	vt
G08B13/2402, G08B13/2417	1/30/17	vt

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06C20/20, G06C20/206, G06C20/40, G06C20/401, G06C20/405, and the results text limited - see attached search history printout.	1/30/17	vt
G08B13/2402, G08B13/2417, and the results text limited - see attached search history printout.	1/30/17	vt
Update Search	6/19/17	vt
Update Search	2/1/18	vt
Update Search	7/5/18	vt

INTERFERENCE SEARCH	

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372317	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	**Art Unit**
	VAN TRIEU	2685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	01/30/2017	06/19/2017	02/01/2018	07/05/2018					
	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			✓	✓					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,317	12-07-2016	Francisco Martinez de Velasco Cortina	116546-613CT17	6203

EXAMINER	
TRIEU, VAN THANH	
ART UNIT	PAPER NUMBER
2685	
SUBMISSION DATE	DELIVERY MODE
April 19, 2018	EFS WEB

SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

AMENDMENT AND RESPONSE TO NON-FINAL OFFICE ACTION

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

Dear Sir:

In response to the Non-Final Office Action mailed on February 9, 2018, ("Office Action") Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following Amendment and Remarks, where:

Listing of the Claims begin on page 2 of this paper.

Remarks begin on page 7 of this paper.

LISTING OF THE CLAIMS

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

a biometric input device configured to receive biometric data;

a short range radio frequency circuit;

memory configured to store biometric information for identifying an individual associated with transaction information;

a processor coupled with the memory and the biometric input device, the processor configured to:

receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,

receive the biometric data from the biometric input device,

compare the received biometric data with the biometric information stored in the memory, and

transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric data matches the stored biometric information; and

a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor.

2. (Original) The mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet.

3. (Original) The mobile device of claim 1, wherein the biometric input device is a fingerprint scanner.

4. (Previously Presented) The mobile device of claim 1, wherein the processor is further configured to transmit the received biometric data or the stored biometric information with the transaction information.

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

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

7. (Original) The mobile device of claim 1, further comprising memory configured to store the transaction information.

8. (Original) The mobile device of claims 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

9. (Previously Presented) A cellular telephone, comprising:

a fingerprint scanner configured to receive fingerprint data;

a short range radio frequency circuit;

memory configured to store fingerprint information for identifying an individual associated with transaction information;

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,

receive the fingerprint data from the fingerprint scanner,

compare the received fingerprint data with the fingerprint information stored in the memory, and

transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received fingerprint data matches the stored fingerprint information; and

a mobile device body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

10. (Previously Presented) The cellular telephone of claim 9, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.

11. (Original) The cellular telephone of claim 9, wherein the transaction information is account information.

12. (Original) The cellular telephone of claim 9, wherein the transaction information is credit card information.

13. (Original) The cellular telephone of claim 9, further comprising memory configured to store the transaction information.

14. (Original) The cellular telephone of claims 13, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

15. (Previously Presented) A cellular telephone, comprising:

cellular circuitry;

a fingerprint scanner configured to receive fingerprint data;

a short range radio frequency circuit;

a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information;

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal from a point of sale terminal via the cellular circuitry, the signal comprising a request to access the memory and retrieve the transaction information,

receive the fingerprint data from the fingerprint scanner,

compare the received fingerprint data with the fingerprint information stored in the memory, and

transmit the transaction information to a remote location using the cellular circuitry when the received fingerprint data matches the stored fingerprint information; and

a cellular telephone body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

16. (Previously Presented) The cellular telephone of claim 15, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.

17. (Original) The cellular telephone of claim 15, wherein the transaction information is account information.

18. (Original) The cellular telephone of claim 15, wherein the transaction information is credit card information.

19. (Original) The cellular telephone of claim 15, further comprising memory configured to store the transaction information.

20. (Original) The cellular telephone of claims 19, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

21. (Previously Presented) The mobile device of claim 1, wherein the processor is configured to compare the received biometric data with the biometric information stored in the memory in response to receiving the request to retrieve the transaction information.

22. (Previously Presented) The cellular telephone of claim 9, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

23. (Previously Presented) The cellular telephone of claim 15, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

24. (Previously Presented) The mobile device of claim 1, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

25. (Previously Presented) The cellular telephone of claim 9, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

26. (Previously Presented) The cellular telephone of claim 15, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

REMARKS

The present amendment is in response to the Office Action dated February 9, 2018. In view of the above listing of the claims and the following remarks, Applicant respectfully requests reconsideration and allowance of all pending claims.

A. Claim Status

With this Response, claims 1- 26 are pending in the application. Claims 1, 9, and 15 are the independent claims.

B. Claim Rejections – 35 USC § 102

Claims 1-23 are rejected under 35 U.S.C. §102(a)(2) as being anticipated by U.S. Pat. Pub. No. 2004/0059923 ("ShamRao"). Applicant respectfully traverses all of the rejections and submits that, for at least the reasons set forth in this paper, the cited references do not render the claims obvious because the cited references fail to teach or suggest each feature of at least Claims 1, 9, and 15 as presented herein.

Applicant respectfully submits that ShamRao is not available as prior art to the present application. Under 35 U.S.C. §102(a)(2), "[a] person shall be entitled to a patent unless . . . (2) the claimed invention was described in . . . an application for patent published or deemed published under section 122(b), in which the patent application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention." *See also, M.P.E.P. § 2152.* Here, ShamRao was filed on September 25, 2002. Whereas, the present application claims priority to provisional application No. 60/394,241 filed on July 9, 2002. Since the present application was effectively filed before the filing data of ShamRao, ShamRao does not qualify as prior art under 35 U.S.C. § 102(a) (2).

However, the Office Action argued that ShamRao claims priority to a priority application Serial No. 09/992,109 filed on November 6, 2001 ("the '109 application"). *Office Action, p. 2.* Applicant respectfully disagrees and submits that ShamRao does not claim priority to the '109 application, and thus is not entitled to the effective filing date of November 6, 2001.

Applicant notes that 37 C.F.R. §1.78(d)(2) provides the requirements for claiming the benefit of a prior filed nonprovisional application. Section 1.78(d)(2) requires, in part:

> (2) ***any nonprovisional application***, international application designating the United States, or international design application designating the United States that claims the benefit of one or more prior-filed nonprovisional applications, international applications designating the United States, or international design applications designating the United States ***must contain***

> ***or be amended to contain a reference to each such prior-filed application***, identifying it by application number (consisting of the series code and serial number), international application number and international filing date, or international registration number and filing date under § 1.1023. If the later-filed application is a nonprovisional application, the reference required by this paragraph must be included in an application data sheet (§ 1.76(b)(5)). ***The reference also must identify the relationship of the applications, namely, whether the later-filed application is a continuation, divisional, or continuation-in-part of the prior-filed nonprovisional application,*** international application, or international design application.

(emphasis added).

Furthermore, M.P.E.P. §211.02(I) explains that "[t]hat the Office may ***not recognize any benefit claim*** where, for example, there is ***no indication of the relationship between the nonprovisional applications***, or no indication of an intermediate nonprovisional application that is directly claiming the benefit of a provisional application." (emphasis added). For applications filed before September 16, 2012 (as is the case with ShamRao), M.P.E.P. §211.02(II) provides that "an example of a proper benefit claim is 'this application ***is a continuation*** of prior Application No. —, filed —.' A benefit claim that merely states that 'this application ***claims the benefit of Application No. —, filed —" does not comply*** with 35 U.S.C. 120 and 37 CFR 1.78, since the relationship between the applications is not stated." (emphasis added). Therefore, for a nonprovisional application to claim benefit from, and thus an effective filing data of, a prior filed nonprovisional application, the nonprovisional application ***must identify the relationship*** between the applications. Where a relationship is not identified the Office will not recognize a benefit claim to the prior application.

In this case, paragraph [0001] of ShamRao states "[t]his application is related to Ser. No. 09/992,207 . . . , Ser. No. 09/992,113 . . . , Ser. No. 09/992,115 . . . , , and Ser. No. 09/992,109 . . . , all of which were filed on Nov. 6, 2001 and all share common inventorship, the contents of which are hereby expressly incorporated-by-reference." ShamRao merely states that it "***is related to***" the earlier filed applications. As explained above, merely stating the application "***claims the benefit of***" an earlier filed application is not sufficient to establish a priority claim. *See, e.g.,* M.P.E.P. §211.02(II). Furthermore, there is no evidence that the Office has recognized that ShamRao is entitled to the effective filing data of November 6, 2001, since, for example, the front page of the ShamRao publication states only that it was "(22) Filed: [on] Sep. 25, 2002" and is silent as to any other filing dates. Additionally, the PAIR also fails to identify any continuity data or relationships to prior filed applications. *See,* https://portal.uspto.gov/pair/PublicPair (searching for Application Number 10/255,264). Therefore, the Office does not recognize that ShamRao is entitled to any filing date other than September 25, 2002. Since the present application was effectively filed before

any possible filing data of ShamRao, ShamRao does not qualify as prior art under 35 U.S.C. § 102(a)(2).

Furthermore, in the event that the publications of Application Numbers 09/992,207; 09/992,113; 09/992,115; and/or Ser. No. 09/992,109 (collectively "other applications") are asserted against the presently presented claims, Applicant respectfully submits that these other applications do not teach or suggest all of the features of claim 1. For example, Applicant respectfully submits that the other applications do not teach or suggest at least a processor configured to "receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information," as recited in claim 1.

Accordingly, Applicant respectfully submits that the Office Action fails to establish each and every feature of claim 1 is disclosed in the prior art. Therefore, claim 1 is patentable and Applicant respectfully requests this rejection be withdrawn.

Independent claims 9 and 15 recite features similar to claim 1. Thus for at least the same reasons, Applicant respectfully submits prior art also fails to disclose or suggest all of the features of claims 9 and 15. Accordingly, Applicant requests the rejections be withdrawn.

Dependent claims 2-8, 10-14, and 16-23 depend directly or indirectly from one of independent claims 1, 9, and 15. As dependent claims inherit their patentability from their respective independent claim, the other dependent claims are allowable for at least their dependence on an allowable claim and their respective additional novel features. Accordingly, Applicant requests these rejections be withdrawn.

C. Claim Rejections – 35 U.S.C. § 103

Claims 24-26 stand rejected under 35 U.S.C. § 103 as being unpatentable over ShamRao as applied to claim 1, and in further view of U.S. Pub. No. 2003/0131247 ("Cannon"). Applicant respectfully traverses all of the rejections and submits that, for at least the reasons set forth in this paper, the cited references do not render the claims as obvious because the cited reference fails to disclose each feature of at least claims 1, 19, and 22 as presented herein.

Dependent claims 24-26 depend directly or indirectly from one of independent claims 1, 9, and 15. As dependent claims inherit their patentability from their respective independent claim, the other dependent claims are allowable for at least their dependence on an allowable claim and their respective additional novel features.

Applicant respectfully submits that Cannon has not been argued in the Office Action to and do not cure the deficiencies of ShamRao with respect to claims 1, 9, and 15. Applicant respectfully

submits that Cannon fails to teach or suggest at least the features discussed above in connection with claims 1, 9, and 15. Thus, Applicant respectfully submits that independent Claims 1, 9, and 15 define patentable subject matter over ShamRao in view of Cannon.

Accordingly, in view of the limitations as recited in independent claims 1, 9, and 15, and in view of the additional limitations as recited in dependent claims 24-26, Applicant respectfully submits that the dependent claims are allowable for at least the reasons discussed above and their respective additional novel features. Although Applicant has not discussed specific features of all of the dependent claims in this response, Applicant does not necessarily agree with the characterizations and assessments made in the Office Action with respect to the dependent claims. Thus, Applicant respectfully submits that dependent claims 24-26 are allowable.

CONCLUSION

For all the foregoing reasons, allowance of all pending claims 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: April 19, 2018

/Mark W. Catanese/
Mark W. Catanese
Reg. No. 64,279
Customer No. 27189

PROCOPIO CORY HARGREAVES & SAVITCH LLP
525 B Street
Suite 2200
San Diego, CA 92101
Tel 6192381900
Fax 6192350398
docketing@procopio.com

Electronic Acknowledgement Receipt	
EFS ID:	32391961
Application Number:	15372317
International Application Number:	
Confirmation Number:	6203
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT17
Receipt Date:	19-APR-2018
Filing Date:	07-DEC-2016
Time Stamp:	19:53:41
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		04_19_2018_Response_to_NFOA_116546-613CT17.PDF	81231 db5fbb567f08541ce0ed70c88e4922ba8d785442	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	11
Warnings:			
Information:			
	Total Files Size (in bytes):	81231	

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 15/372,317	Filing Date 12/07/2016	☐ 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 $80 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $420 =	
☐ 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

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	04/19/2018	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 26	Minus	** 26	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $460 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ 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.	LIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	trina riddick
*** 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.	

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.
15/372,317	12/07/2016	Francisco Martinez de Velasco Cortina	116546-613CT17	6203

27189 7590 02/09/2018

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
02/09/2018	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. 15/372,317	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 *the RCE and Amendment filed on 12/19/2017*.

☐ 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) *1-26* 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) *1-26* 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 –
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

1. Claims 1-23 are rejected under 35 U.S.C. 102(a)(2) as being anticipated by **Shamrao** [US 2004/0059923] with a priority application Serial No. 09/992,109 filed on 11/06/2001.

Claim 1, the claimed a mobile device (the portable biometric authentication PBA 10, Fig. 1), comprising: a biometric input device configured to receive biometric data (the PBAS to scan and store person biometrics data in a storage mechanism 52 such as RAM, ROM memories, Figs. 2, 3, par [0024, 0025, 0032, 0033, 0039, 0040]); a short range radio frequency circuit (the Bluetooth communications and/or IEEE 802.11, Figs. 1, pars [0036-0038]);

memory (the storage 52 such as RAM, ROM memories, Fig. 2, pars [0032, 0033]) configured to store biometric information for identifying an individual associated with transaction information (the biometric, authentication and transaction data information, Figs. 2, 3, pars [0042, 0044, 0052]):

a processor (the PBA 10 with a CPU and processing steps 104, 106, 118 Figs. 1, 2, 5) coupled with the memory and the biometric input device, the processor configured to:

receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information (the CPU processing a request to scan his/her biometric 104, comparing, storing and to send the biometric data information to perform a transaction at the point of sale POP via Bluetooth or IEEE 802.11, Figs. 2, 3, 5 steps 104, 106, 110, pars [0031, 0036-0038, 0054-0056]);

receive the biometric information data from the biometric input device (Figs. 2, 5), compare the received biometric information data with the biometric information stored in the memory (the comparing of biometric data, Figs. 2, 3, 5 steps 104,106, pars [0024, 0044, 0054]), and

transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric information data matches the stored biometric information (the portable biometric authentication PBA 10 communicates biometric data information with the point of sale POP via Bluetooth or IEEE 812.11, Figs. 2, 3, 5 step 110, pars [0036-0038, 0054-0056]);

and a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor (the PBA 10 or PDA 129, Figs. 1, 2, 6).

Claim 2, the mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet (the cellular mobile phones or notebook computers, pars [0034, 0036]).

Claim 3, the mobile device of claim 1, wherein the biometric input device is a fingerprint scanner (pars [0036, 0084]).

Claim 4, the mobile device of claim 1, wherein the processor is further configured to transmit the received biometric information data or the stored biometric information with the transaction information (the biometric information with transactions, as cited in respect to claim 1 above).

Claim 5, the mobile device of claim 1, wherein the transaction information is account information (the variety transactions include monetary transaction, pars [0011, 0044, 0052]).

Claim 6, the mobile device of claim 1, wherein the transaction information is credit card information (the smart credit card transaction, Fig. 4, par [0052]).

Claim 7, the mobile device of claim 1, further comprising memory configured to store the transaction information (the storage 52, Fig. 2).

Claim 8, the mobile device of claims 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (the storage mechanism 52 such as RAOM, ROM memories, as cited in respect to claim 1 above, Figs. 2-4, pars [0032,0033]).

Claim 9, the claim a cellular telephone, comprising: a fingerprint scanner configured to receive fingerprint information data: a short range radio frequency circuit; memory configured to store fingerprint information for identifying an individual associated with transaction information; a processor coupled with the memory and the fingerprint scanner, the processor configured to:
receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information, receive the fingerprint information data from the fingerprint scanner, compare the received fingerprint information data with the fingerprint information stored in the memory, and transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received fingerprint information data matches the stored fingerprint information: and a mobile device body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor (as cited in respect to claims 1, 2 and 3 above).

Claim 10, the cellular telephone of claim 9, wherein the processor is further configured to transmit the received fingerprint information data or the stored fingerprint information with the transaction information (as cited in respect to claims 4 and 9 above).

Claim 11, the cellular telephone of claim 9, wherein the transaction information is account information (as cited in respect to claims 5 and 9 above).

Claim 12, the cellular telephone of claim 9, wherein the transaction information is credit card information (as cited in respect to claims 6 and 9 above).

Claim 13, the cellular telephone of claim 9, further comprising memory configured to store the transaction information (as cited in respect to claims 7 and 9 above).

Claim 14, the cellular telephone of claims 13, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (as cited in respect to claims 8 and 13 above).

Claim 15, the claimed a cellular telephone, comprising: cellular circuitry; a fingerprint scanner configured to receive fingerprint information data: a short range radio frequency circuit; a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information; a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal from a point of sale terminal via the cellular circuitry, the signal comprising a request to access the memory and retrieve the transaction information,
receive the fingerprint information data from the fingerprint scanner,
compare the received fingerprint information data with the fingerprint information stored in the memory, and
transmit the transaction information to a remote location using the cellular circuitry when the received fingerprint information data matches the stored fingerprint information: and
a cellular telephone body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor (as cited in respect to claims, 1, 2, 3, 9 above).

Claim 16, the cellular telephone of claim 15, wherein the processor is further configured to transmit the received fingerprint information data or the stored fingerprint information with the transaction information (as cited in respect to claims 4 and 15 above).

Claim 17, the cellular telephone of claim 15, wherein the transaction information is account information (as cited in respect to claims 5 and 15 above).

Claim 18, the cellular telephone of claim 15, wherein the transaction information is credit card information (as cited in respect to claims 6 and 15 above).

Claim 19, the cellular telephone of claim 15, further comprising memory configured to store the transaction information (as cited in respect to claims 7 and 15 above).

Claim 20, the cellular telephone of claims 19, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (as cited in respect to claims 8 and 19 above).

Claim 21, the mobile device of claim 1, wherein the processor is configured to compare the received biometric data with the biometric information stored in the memory in response to receiving the request to retrieve the transaction information.

22. (New) The cellular telephone of claim 9, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

Claim 23, the cellular telephone of claim 15, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information (as cited in respect to claim 1 above and including the authentication for accessing or retrieving monetary transaction, see Fig. 5).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102 of this title, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims the examiner presumes that the subject matter of the various claims was commonly owned as of the effective filing date of the claimed invention(s) absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and effective filing dates of each claim that was not commonly owned as of the effective filing date of the later invention in order for the examiner to consider the applicability of 35 U.S.C. 102(b)(2)(C) for any potential 35 U.S.C. 102(a)(2) prior art against the later invention.

2. Claims 24-26 are rejected under 35 U.S.C. 103 as being unpatentable over **Shamrao** [US 2004/0059923] as applied to claim 1 above, and further in view of **Cannon** [US 2003/0131247]

Claim 24, **Shamrao** fails to disclose the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz. However, **Shamrao** discloses the portable PBA 10 includes a Bluetooth and/or IEEE 802.11 for communications, Figs. 2-5, pars [0036-0038]).

Cannon suggests that the wireless transceiver biometric device 100 includes the step of correlating the identity to the purchased media and storing rights relating to the correlation. The method also includes the step of receiving the purchased media in a secure output device. The method also includes the steps of establishing the identity in the secure output device using the biometric device and determining if the identity matches the stored rights. If the identity matches the stored rights, the method also includes the step of allowing the output of the purchased media from the secure output device (Figs. 1, 2, par [0009]). The biometric device 100 use Bluetooth 500 or IEEE 802.11 wireless technology for communication over the frequency about 20 MHz, see Figs. 1, 4-6, pars [0031, 0039, 0043, 0069]). Therefore, it would have been obvious to one skill in the art before the effective file date of the invention to utilize the frequency range about 20 MHz of **Cannon** for the portable PBA of **Shamrao** since both systems using the Bluetooth and/or IEEE 82.11 wireless technology for short range communications.

Claim 25, the cellular telephone of claim 9, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz (as discussed between **Shamrao** and **Cannon** in respect to claim 24 above).

Claim 26, the cellular telephone of claim 15, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz (as discussed between **Shamrao** and **Cannon** in respect to claim 24 above).

Conclusion

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

Ritter discloses the system and method for authenticating persons, video information of certain body features associated with a user or a user group is recorded in a point of presence (POP) or point of sale (POS). Such recorded video information is processed to derive biometric keys, which are stored in tables of a biometric server and in a SIM-card of the user. Each biometric key in the tables is assigned to a respective user. When the user inserts the SIM-card containing a personal biometric key into a communication terminal device, video information describing current body feature of the user is recorded via a video sensor that is not in the communication terminal device. The recorded current video information is then transmitted from the video sensor to the communication terminal device. To authenticate the user, the recorded current video information is processed to derive current biometric keys and compared with pre-stored biometric keys. The authenticity of the user is ensured if the comparison yield a positive result. [US 6,657,538]

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: 02/01/2018

Notice of References Cited	Application/Control No. 15/372,317	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	CPC Classification	US Classification
*	A	US-6,657,538 B1	12-2003	Ritter; Rudolf	G06F21/32	340/5.8
*	B	US-2003/0131247 A1	07-2003	Cannon, Gregory L.	G06F21/32	713/186
*	C	US-2004/0059923 A1	03-2004	ShamRao, Andrew Divaker	G06F21/32	713/186
	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	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372317	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	VAN TRIEU	2685

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06C20/20, G06C20/206, G06C20/40, G06C20/401, G06C20/405	1/30/17	vt
G08B13/2402, G08B13/2417	1/30/17	vt

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

SEARCH NOTES		
Search Notes	Date	Examiner
G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06C20/20, G06C20/206, G06C20/40, G06C20/401, G06C20/405, and the results text limited - see attached search history printout.	1/30/17	vt
G08B13/2402, G08B13/2417, and the results text limited - see attached search history printout.	1/30/17	vt
Update Search	6/19/17	vt
Update Search	2/1/18	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	147978	(cellular or handheld or mobile or PDA or portable or reader or scan$4) near9 (biometric or eye$4 or face or facial or fingerprint)	US-PGPUB; USPAT	OR	ON	2018/02/01 09:26
L2	5001	(emit$4 or obtain$3 or receiv$3 or send$3 or transmit$4) near9 (biometric or eye$4 or face or facial or fingerprint) near9 (point near2 sale or POS or counter or check$4 or pay$3)	US-PGPUB; USPAT	OR	ON	2018/02/01 09:28
L3	28232	(compar$5 or different or match$3) near9 (biometric or eye$4 or face or facial or fingerprint) near9 (memory or recorded or stored or previous$2)	US-PGPUB; USPAT	OR	ON	2018/02/01 09:30
L4	621	1 and 2 and 3 and (Bluetooth or IEEE or RFID or short or tag)	US-PGPUB; USPAT	OR	ON	2018/02/01 09:33
L5	98	4 not @AY > "2003"	US-PGPUB; USPAT	OR	ON	2018/02/01 09:33
L6	1459	(cellular or handheld or mobile or PDA or portable) near4 scan$4 near5 (biometric or eye$4 or face or facial or fingerprint)	US-PGPUB; USPAT	OR	ON	2018/02/01 09:35
L7	1	5 and 6	US-PGPUB; USPAT	OR	ON	2018/02/01 09:35
L8	1	7 and (POS or sale or receipt or pay$3 or counter)	US-PGPUB; USPAT	OR	ON	2018/02/01 09:46
L9	1	7 and (cellular or smart)	US-PGPUB; USPAT	OR	ON	2018/02/01 09:46
L10	23078	(G06F21/30, G06F21/31, G06F21/32, G06F21/34, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06C20/20, G06C20/206, G06C20/40, G06C20/401, G06C20/405, G08B13/2402, G08B13/2417).CPC.	US-PGPUB; USPAT	OR	ON	2018/02/01 09:53
L11	41	10 and 5	US-PGPUB; USPAT	OR	ON	2018/02/01 09:53
L12	1	10 and 9	US-PGPUB; USPAT	OR	ON	2018/02/01 09:53
L13	11	(("20040128249") or ("20030001459") or ("20040059923") or ("6025784") or ("7031946") or ("8237568") or ("8587436") or ("8004410") or ("7671746") or ("7081819") or ("6934861")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2018/02/01 09:57

L14	1	13 and 5	US-PGPUB; USPAT	OR	ON	2018/02/01 09:57
L15	7	13 and 6	US-PGPUB; USPAT	OR	ON	2018/02/01 09:58
L16	1186	(cellular or handheld or mobile or PDA or portable) near4 (compar$5 or match$3) near5 (biometric or eye$4 or face or facial or fingerprint)	US-PGPUB; USPAT	OR	ON	2018/02/01 10:04
L17	6	16 and 13	US-PGPUB; USPAT	OR	ON	2018/02/01 10:04
L18	2	10 and 13	US-PGPUB; USPAT	OR	ON	2018/02/01 10:09
L19	1	("6657538").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2018/02/01 10:12
L20	2	(("20020175889") or ("20030191650")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2018/02/01 10:16
L21	0	20 and 5	US-PGPUB; USPAT	OR	ON	2018/02/01 10:16
L22	0	19 and 5	US-PGPUB; USPAT	OR	ON	2018/02/01 10:22
L23	0	19 and 6	US-PGPUB; USPAT	OR	ON	2018/02/01 10:22
L24	0	19 and 1 and 2	US-PGPUB; USPAT	OR	ON	2018/02/01 10:23
L25	1	19 and 1	US-PGPUB; USPAT	OR	ON	2018/02/01 10:23
L26	1	19 and 3	US-PGPUB; USPAT	OR	ON	2018/02/01 10:23
L27	1	19 and (Bluetooth or IEEE or RFID or short or tag)	US-PGPUB; USPAT	OR	ON	2018/02/01 10:24
L28	1	19 and (POS or sale or receipt or pay$3 or counter)	US-PGPUB; USPAT	OR	ON	2018/02/01 10:24
L29	1	19 and (sale or receipt or pay$3 or counter or transaction)	US-PGPUB; USPAT	OR	ON	2018/02/01 10:58
L30	1	19 and (receipt or pay$5 or counter or transaction)	US-PGPUB; USPAT	OR	ON	2018/02/01 10:59
L31	1	("20040059923").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2018/02/01 11:56

L32	1	31 and (cellular or phone)	US-PGPUB; USPAT	OR	ON	2018/02/01 11:56
L33	1	31 and fingerprint	US-PGPUB; USPAT	OR	ON	2018/02/01 11:59
L35	0	31 and transaction near9 (account$3 or bank or sale or receipt$3)	US-PGPUB; USPAT	OR	ON	2018/02/01 12:02
L37	1	31 and transaction and (account$3 or bank or sale or receipt$3 or statement)	US-PGPUB; USPAT	OR	ON	2018/02/01 12:03
L38	7	(13 or 31) and MHz	US-PGPUB; USPAT	OR	ON	2018/02/01 12:37
L39	0	38 and 2	US-PGPUB; USPAT	OR	ON	2018/02/01 12:41
L40	8	5 and MHz	US-PGPUB; USPAT	OR	ON	2018/02/01 12:41

EAST Search History (Interference)

<This search history is empty>

2/1/2018 1:09:27 PM
C:\Users\vtrieu\Documents\EAST\Workspaces\Default EAST Workspace.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372317	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	**Art Unit**
	VAN TRIEU	2685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	01/30/2017	06/19/2017	02/01/2018						
	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			✓						

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.
15/372,317	12/07/2016	Francisco Martinez de Velasco Cortina	116546-613CT17	6203

27189 7590 12/28/2017

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
12/28/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

Applicant-Initiated Interview Summary	**Application No.**	**Applicant(s)**	
	15/372,317	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) *MARK CATANES, Reg. No. 64,279*. (4)_____.

Date of Interview: *19 December 2017*.

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: *1*.

Identification of prior art discussed: *Hoffman [US 2004/0128249]*.

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 clarifies of the invention and to propose an amendment language to present of a single portable biometric monitoring device having a plurality functions which overcomes the separated PDA and PDC units in the rejected reference. Examiner will update the search upon receiving the amendment.

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 TRIEU/ Primary Examiner, Art Unit 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.

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	15372317	Filing Date	2016-12-07	Docket Number (if applicable)	116546-613CT17	Art Unit	2685
First Named Inventor	Francisco Martinez De Velasco Cortina			Examiner Name	TRIEU, Van Thanh		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☒ Amendment/Reply
- ☐ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☒ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 502075

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

EFS - Web 2.1.15

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2017-12-19
Name	Mark W. Catanese	Registration Number	64279

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application 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.

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 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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,317	12-07-2016	Francisco Martinez de Velasco Cortina	116546-613CT17	6203

EXAMINER	
TRIEU, VAN THANH	
ART UNIT	PAPER NUMBER
2685	
SUBMISSION DATE	DELIVERY MODE
19 December 2017	EFS WEB

SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

AMENDMENT AND RESPONSE TO FINAL OFFICE ACTION WITH AMENDMENT AND REQUEST FOR CONTINUING EXAMINATION UNDER 37 C.F.R. §1.114

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

Dear Sir:

In response to the Final Office Action mailed on June 23, 2017, ("Office Action") Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following Amendment and Remarks, where:

Amendments to the Claims begin on page 2 of this paper; and

Interview Summary begins on page 8 of this paper.

Remarks begin on page 9 of this paper.

AMENDMENTS TO THE CLAIMS

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

a biometric input device configured to receive biometric data;

a short range radio frequency circuit;

memory configured to store biometric information for identifying an individual associated with transaction information[[, and]];

a processor coupled with the memory and the biometric input device, the processor configured to:

receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,

receive the biometric ~~information~~data from the biometric input device,

compare the received biometric ~~information~~data with the biometric information stored in the memory, and

transmit the transaction information to [[a]]the point of sale terminal using the short range radio frequency circuit when the received biometric ~~information~~data matches the stored biometric information; and

a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor.

2. (Original) The mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet.

3. (Original) The mobile device of claim 1, wherein the biometric input device is a fingerprint scanner.

4. (**Currently Amended**) The mobile device of claim 1, wherein the processor is further configured to transmit the received biometric ~~information~~data or the stored biometric information with the transaction information.

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

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

7. (Original) The mobile device of claim 1, further comprising memory configured to store the transaction information.

8. (Original) The mobile device of claims 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

9. (**Currently Amended**) A cellular telephone, comprising:

a fingerprint scanner configured to receive fingerprint ~~information~~data;

a short range radio frequency circuit;

memory configured to store fingerprint information for identifying an individual associated with transaction information[[, and]];

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,

receive the fingerprint ~~information~~data from the fingerprint scanner,

compare the received fingerprint ~~information~~data with the fingerprint information stored in the memory, and

transmit the transaction information to [[a]]the point of sale terminal using the short range radio frequency circuit when the received fingerprint ~~information~~data matches the stored fingerprint information; and

a mobile device body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

10. (**Currently Amended**) The cellular telephone of claim 9, wherein the processor is further configured to transmit the received fingerprint ~~information~~data or the stored fingerprint information with the transaction information.

11. (Original) The cellular telephone of claim 9, wherein the transaction information is account information.

12. (Original) The cellular telephone of claim 9, wherein the transaction information is credit card information.

13. (Original) The cellular telephone of claim 9, further comprising memory configured to store the transaction information.

14. (Original) The cellular telephone of claims 13, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

15. (**Currently Amended**) A cellular telephone, comprising:

cellular circuitry;

a fingerprint scanner configured to receive fingerprint ~~information~~data;

a short range radio frequency circuit;

a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information; [[and]]

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal from a point of sale terminal via the cellular circuitry, the signal comprising a request to access the memory and retrieve the transaction information,

receive the fingerprint ~~information~~data from the fingerprint scanner,

compare the received fingerprint ~~information~~data with the fingerprint information stored in the memory, and

transmit the transaction information to a remote location using the cellular circuitry when the received fingerprint ~~information~~data matches the stored fingerprint information; and

a cellular telephone body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

16. (**Currently Amended**) The cellular telephone of claim 15, wherein the processor is further configured to transmit the received fingerprint ~~information~~data or the stored fingerprint information with the transaction information.

17. (Original) The cellular telephone of claim 15, wherein the transaction information is account information.

18. (Original) The cellular telephone of claim 15, wherein the transaction information is credit card information.

19. (Original) The cellular telephone of claim 15, further comprising memory configured to store the transaction information.

20. (Original) The cellular telephone of claims 19, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

21. (New) The mobile device of claim 1, wherein the processor is configured to compare the received biometric data with the biometric information stored in the memory in response to receiving the request to retrieve the transaction information.

22. (New) The cellular telephone of claim 9, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

23. (New) The cellular telephone of claim 15, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

24. (New) The mobile device of claim 1, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

25. (New) The cellular telephone of claim 9, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

26. (New) The cellular telephone of claim 15, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

INTERVIEW SUMMARY

Applicant would like to thank Examiner Trieu for the courtesy extended during the telephonic interview conducted with the undersigned on December 19, 2017 ("Interview"). During the interview the nature of the rejections under §103 were discussed. Certain amendments were discussed, some of which are recited in the "Amendments to the Claims" section above. Examiner Trieu agreed that such amendments would overcome the current rejections. Further substance of the interview is captured in the following remarks.

REMARKS

The present communication is in response to the Office Action dated June 23, 2017. In the Office Action, the Examiner rejected Claims 1-20. *See Office Action, p. 1.* By this paper, Applicant has amended Claims 1, 4, 9, 10, 15, and 16 and added new Claims 21-26. Support for the amendments and new claims can be found in the specification as originally filed. For example, support can be found in at least paragraphs [0125]-[0133] and [0153]-[0162] and FIGs. 12-14 and 17 of the application as published. Applicant has not added new matter. Reconsideration and allowance are respectfully requested for all pending Claims 1-26.

A. Claim Rejections Under 35 U.S.C. §103

Claims 1-20 are rejected under 35 U.S.C. §103(a) as being anticipated by U.S. Pat. Pub. No. 2004/0128249 ("Hoffman") in view of U.S. Pat. Pub. No. 2003/0001459 ("Scott"). *See Office Action, p. 2.* Applicant respectfully traverses all of the rejections and submits that, for at least the reasons set forth in this paper, the cited references do not render the claims obvious because the cited references fail to teach or suggest each feature of at least Claims 1, 9, and 15 as presented herein.

Standard of *Prima Facie* Obviousness

The U.S. Patent and Trademark Office has the burden under §103 to establish a prima facie case of obviousness. The rationale to support a conclusion that the claim would have been obvious is that all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination yielded nothing more than predictable results to one of ordinary skill in the art. It can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. If any of these findings cannot be made, then this rationale cannot be used to support a conclusion that the claim would have been obvious to one of ordinary skill in the art. *M.P.E.P. § 2143*.

Discussion of Patentability of Claim 1

Without acquiescing to the merits of the grounds of the Examiner's rejection, and in the interest of advancing prosecution, Applicant has amended Claim 1 to recite "a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor."

In rejecting Claim 1, the Examiner appears to have characterized the PDA 1 and the DPC 22 of Hoffman as the claimed mobile device and point of sale terminal. *See Office Action, p. 2.* However, the Examiner also appears to have characterized the combination of the PDA 1 and DPC 22 of Hoffman as the claimed mobile device. *See Office Action, pp. 3, 9, and 10.* Applicant respectfully submits that the DPC 22 cannot be both the claimed point of sale terminal and part of the claimed mobile device.

However, even under the Examiner's characterization (a point that is not conceded), as discussed during the interview, Applicant submits that the cited references fail to teach or suggest a mobile device comprising "a mobile device body housing the biometric input, short range radio frequency circuit, memory, and processor," as recited in amended Claim 1. Hoffman describes that biometric samples are obtained from a person and transmitted to the DPC 22 (including the Indicator 12) via a PDA 1 "over a network 18 such as an intranet, extranet or the Internet, whether using a local area network (LAN) or a wide area network (WAN)." *Hoffman, para. [0067]; see also, e.g., id. at paras. [0116]-[0124].* Thus, as was agreed during the Interview, Hoffman fails to teach or suggest that the DCP 22 (including the Indicator 12) and PDA 1 are housed in the same device body. Accordingly, Applicant respectfully submits that Hoffman does not teach or suggest the above-identified features of amended Claim 1.

Furthermore, amended Claim 1 recites "a mobile device, comprising . . . memory configured to store biometric information for identifying an individual associated with transaction information." In rejecting this limitation, the Examiner argues "Hoffman discloses each PDA conducts one or more of the operations includes store and retrieve a unique scrip from the biometric and merchant, PIN code, see Pars [0077-0082]." *See Office Action, p. 9.* Applicant respectfully disagrees.

Paragraphs [0077]-[0087] of Hoffman are reproduced below.

[0077] The PDA is a device that gathers or contains identity information for use in authorizing scrip transactions. Each PDA conducts one or more of the following operations:

[0078] gather biometric input from a Scrip Merchant or Scrip Supporter

[0079] gather a PIN code or password from a Scrip Merchant or Scrip Supporter

[0080] secure communication between PDA and DPC using encryption

[0081] secure storage of secret encryption keys

[0082] store and retrieve a unique Scrip Merchant PDA hardware identification code

[0083] secure enclosure & components from unauthorized tampering

[0084] display information, allow parties to approve or cancel a scrip transaction

[0085] automated data scanning, such as a magnetic ink character reader, a magnetic stripe reader or a bar-code reader

[0086] store, verify, and retrieve a Scrip Merchant's digital identification code or a Scrip Beneficiary's digital identification code

[0087] allow parties to select among choices of Scrip Merchant and Scrip Supporter accounts

Thus, at best Hoffman describes the PDA 1 gathers biometric input from a Scrip Supporter and stores "secret encryption keys"; "hardware identification code"; "digital identification code", etc. However, nowhere does Hoffman describe that the PDA 1 comprises memory that stores biometric information used to identify the Scrip Supporter, which is subsequently compared to and matched with the gathered biometric input recited in paragraph [0097] of Hoffman. In contrast, Claim 1 recites "memory configured to store biometric information for identifying an individual," that is compared to and matched with biometric data received from the biometric input device as claimed.

Applicant respectfully submits that Scott does not cure the deficiencies of Hoffman with respect to amended Claim 1. Scott was cited merely to supposedly show certain features which are unrelated to the above-indicated features of amended Claim 1, and does not appear to remedy the deficiencies of Hoffman. Therefore, the combination of prior art references does not teach or suggest all of the features of amended Claim 1. Accordingly, not all of the claim limitations were known or taught by the prior art. Furthermore, the Examiner did not identify a reason, with respect to at least the above-identified limitation, that would have prompted a person of ordinary skill in the relevant field to combine or modify the elements in the way the claimed new invention does. In view of the above, Applicant respectfully submits that no prima facie case of obviousness has been established

with respect to amended Claim 1, and thus for at least these reasons the independent claim is patentable over the prior art of record.

Accordingly, for at least the reasons set forth above, Applicant respectfully submits that the cited references fail to teach or suggest all of the features of amended Claim 1. Therefore, amended Claim 1 is patentable over Hoffman and/or Scott, in combination or individually, and Applicant respectfully requests this rejection be withdrawn.

Discussion of Patentability of Remaining Independent Claims

Applicant submits that amended Claims 9 and 15 recite at least some of the patentable limitations discussed in connection with amended Claim 1 above. Thus, Applicant respectfully submits that amended Claims 9 and 15 also define patentable subject matter over the cited references. Accordingly, for at least this reason, Applicant respectfully submits that amended independent Claims 9 and 15 are allowable under 35 U.S.C. §103.

Discussion of Patentability of Dependent Claims

Applicant submits that each of the dependent Claims 2-8, 10-14, and 16-20 depends directly or indirectly on at least one of amended Claims 1, 9, and 15. Thus, dependent Claims 2-8, 10-14, and 16-20 incorporate by reference all the limitations of their respective independent claims, pursuant to 35 U.S.C. § 112(d). In view of the limitations as recited in the independent claims, and in view of the additional limitations as recited in the dependent claims, Applicant respectfully submits that the dependent claims are allowable for at least the reasons discussed above and their respective additional novel features. Although Applicant has not discussed specific features of all of the dependent claims in this response, Applicant does not necessarily agree with the characterizations and assessments made by the Examiner with respect to the dependent claims. Thus, Applicant respectfully submits that dependent Claims 2-8, 10-14, and 16-20 are allowable.

B. New Dependent Claims

New dependent Claims 21-26 have been added. Applicant submits that new dependent Claims 21-26 depend directly or indirectly on one of independent Claims 1, 9,

and 15. Thus, dependent Claims 21-26 incorporate by reference all the limitations of the independent claims from which they depend, pursuant to 35 U.S.C. § 112(d). In view of the limitations as recited in the independent claims, and in view of the additional limitations as recited in the new dependent claims, Applicant respectfully submits that the new dependent claims are allowable for at least the reasons discussed above and their respective additional novel limitations. Thus, Applicant respectfully submits that new dependent Claims 21-26 are allowable.

C. No Disclaimers or Disavowals

Although the present communication may include alterations to the application or claims, or characterizations of claim scope or referenced art, Applicant is not conceding in this application that previously pending claims are not patentable over the cited references. Rather, any alterations or characterizations are being made to facilitate expeditious prosecution of this application. Applicant reserves the right to pursue at a later date any previously pending or other broader or narrower claims that capture any subject matter supported by the present disclosure, including subject matter found to be specifically disclaimed herein or by any prior prosecution. Accordingly, reviewers of this or any parent, child or related prosecution history shall not reasonably infer that Applicant has made any disclaimers or disavowals of any subject matter supported by the present application.

CONCLUSION

For all the foregoing reasons, allowance of all pending claims 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: December 19, 2017

/Mark W. Catanese/
Mark W. Catanese
Reg. No. 64,279
Customer No. 27189

PROCOPIO CORY HARGREAVES & SAVITCH LLP
525 B Street
Suite 2200
San Diego, CA 92101
Tel 6192381900
Fax 6192350398
docketing@procopio.com

Electronic Patent Application Fee Transmittal

Application Number:	15372317
Filing Date:	07-Dec-2016
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT17

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
CLAIMS IN EXCESS OF 20	1202	6	80	480
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
RCE- 1st Request	1801	1	1200	1200
		Total in USD ($)		**3080**

Electronic Acknowledgement Receipt	
EFS ID:	31279935
Application Number:	15372317
International Application Number:	
Confirmation Number:	6203
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT17
Receipt Date:	19-DEC-2017
Filing Date:	07-DEC-2016
Time Stamp:	20:19:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$3080
RAM confirmation Number	122017INTEFSW20212900
Deposit Account	502075
Authorized User	Helen Glenister
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	12_19_2017_RCE_as_filed_116546-613CT17.PDF	1349890 e250c68f37947834945c33598cb5618476f90ffc	no	3
Warnings:					
Information:					
2		12_19_2017_Response_for_FOA_as_filed_116546-613CT17.PDF	106466 cbf6920564afcd9ee6512d536bd156829f804956	yes	14

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment Submitted/Entered with Filing of CPA/RCE	1	1
	Claims	2	7
	Applicant summary of interview with examiner	8	8
	Applicant Arguments/Remarks Made in an Amendment	9	14

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	34266 c48576c4cf1ec27fcbe40dca2289d35a7ee932d8	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1490622		

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 15/372,317	Filing Date 12/07/2016	☐ 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

		(Column 1)		(Column 2)	(Column 3)		
	12/19/2017	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	* 26	Minus	** 20	= 6	X $80 =	480
	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	**480**

		(Column 1)		(Column 2)	(Column 3)		
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	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
ANTHONY TYSON

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.
15/372,317	12/07/2016	Francisco Martinez de Velasco Cortina	116546-1108C8	6203

27189 7590 06/23/2017

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
06/23/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

Office Action Summary	Application No. 15/372,317	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 *05/02/2017*.

☐ 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) *1-20* 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) *1-20* 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 *5/2/17 & 5/2/17*.

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 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hoffman** [US 2004/0128249] in view of **Scott** [US 2003/0001459]

Claim 1, the claimed a mobile device, comprising: a biometric input device configured to receive biometric data; a short range radio frequency circuit (the portable electronic script transaction authorization device PDA 1 with PDC 22 at the point of sale receives at least one wireless biometric samples/signals 62 from the biometric sensors/scanners 2, Figs. 1, 6, pars [0039, 0054, 0089, 0113, 0129-0131]);

memory configured to store biometric information for identifying an individual associated with transaction information (the PDA 1 with DPC 22 store biometric sample/signal 62 and to retrieve the script transactions from the scrip supporter, Figs. 3, 4, pars [0040, 0041,0057, 0077, 0095, 0109, 0113]); and

a processor coupled with the memory and the biometric input device, the processor configured to: receive a signal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information, receive biometric information from the biometric input device the memory, (the DPC 22 comprised of an identicator 12 with internal execution modules 38 to wirelessly receive the biometric sample/signal 62 from the wireless biometric sensors 2 and the requested script transaction data information and then to compare a script supporter's bid biometric sample/signal 62 with previous stored biometric sample/signal from registered scrip supporters for determining whether it is matching for authentication or not, Figs. 1 -6, pars [0102, 0106, 0109, 0111, 0113, 0117, 0122, 0127]).

But **Hoffman** fails to disclose transmit the transaction information to a point of sale terminal using the short range radio frequency circuit when the received biometric information matches the stored biometric information. However, **Hoffman** discloses the PDA 1 is connected via the Internet, as is at least one Identicator 12 of the DPC 22 located at the register or point of sale, see Figs. 1, pars [0113, 0118]. TCP/IP is used to transmit messages from PDA 1 to Identicator 12. There are many different ways to connect PDA 1 to the identicator 12 of DPC 22 12 for identify the merchants and transactions, both tethered and wireless that are well understood in the industry,

including but not limited to: the Internet; an intranet; an extranet; a local area network ("LAN"); and a wide area network ("WAN"), see Fig. 1, pars [0116-0118, 0122]. **Scott** suggests that the wireless transceiver 1112 is used to conduct a secure electronic sales transaction comprising receiving biometric data from a wireless transceiver biometric device 3400, see Fig. 36, par [0174], and verifying the identity of an individual by the identification device 3604, see Fig. 36, par [0174]. The identification device 3604 is a wireless communicate to the casher register 3602 and/or other personal engaged in a transaction via the Bluetooth wireless network such as controller, processor, computer, PDA and/or cellular, see Fig. 36, 37, pars [0174, 0175, 0178]). Wherein the integrated circuit or small chip 1112 is a wireless transceiver, see Fig. 11, par [0108, lines 6-9]. Therefore, it would have been obvious to one skill in the art before the effective of the filed date to substitute the Bluetooth wireless transceiver of **Scott** for the RF communication of **Hoffman** for optimizing space and saving energy by the small/tiny IC chip wireless transceiver as one or more of the many different communication methods (**Hoffman**, pars [0116, 0118]).

Claim 2, wherein the mobile device is one of a cellphone, smartphone, or tablet (the PDA 1 connected via a cellular digital packet data modem, Figs. 1, 6, pars [0113, 0117]).

Claim 3, wherein the biometric input device is a fingerprint scanner (the scanner 2, Figs. 1, 6).

Claim 4, wherein the processor is further configured to provide the received biometric information or the stored biometric information with the transaction information (as discussed between **Hoffman** and **Scott** in respect to claim 1 above, as the DPC 22).

Claim 5, wherein the transaction information is account information (the account transactions or script accounts, Fig. 6, pars [0112, 0113]).

Claim 6, wherein the transaction information is credit card information (the debit or credit card transactions/scripts, par [0112]).

Claim 7, further comprising memory configured to store the transaction information (as discussed between **Hoffman** and **Scott** in respect to claim 1 above, as the DPC 22, Figs. 1, 6).

Claim 8, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (as discussed between **Hoffman** and **Scott** in claim 1 above as the DPC 22, Figs. 1, 6).

Claim 9, all the claimed subject matters are discussed between **Hoffman** and **Scott** in respect to the method claim 1 above.

Claim 10, herein the processor is further configured to provide the received fingerprint information or the stored fingerprint information with the transaction information (as discussed between **Hoffman** and **Scott** in respect to claim 3 above).

Claim 11, wherein the transaction information is account information (as discussed between **Hoffman** and **Scott** in respect to claim 5 above).

Claim 12, wherein the transaction information is credit card information (as discussed between **Hoffman** and **Scott** in respect to claim 6 above).

Claim 13, further comprising memory configured to store the transaction information (as discussed between **Hoffman** and **Scott** in respect to claim 7 above).

Claim 14, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (as discussed between **Hoffman** and **Scott** in respect to claim 8 above).

Claim 15, all the claimed subject matters are discussed between **Hoffman** and **Scott** in respect to the method claims 1 and 2 above.

Claim 16, wherein the processor is further configured to provide the received fingerprint information or the stored fingerprint information with the transaction information (as discussed between **Hoffman** and **Scott** in respect to claim 3 above).

Claim 17, wherein the transaction information is account information (as discussed between **Hoffman** and **Scott** in respect to claim 5 above).

Claim 18, wherein the transaction information is credit card information (as discussed between **Hoffman** and **Scott** in respect to claim 6 above).

Claim 19, further comprising memory configured to store the transaction information (as discussed between **Hoffman** and **Scott** in respect to claim 7 above).

Claim 20, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (as discussed between **Hoffman** and **Scott** in respect to claim 8 above).

Response to Arguments

2. Applicant's arguments with respect to claims 1 and 10 have been considered but are moot because the arguments do not apply to any of the references being used in the current rejection.

Applicant's arguments:

(A) The portable, or mobile device of **Hoffman** is clearly the PDA, but the PDA of **Hoffman** does not include memory configured to store the biometric: Thus, the need to combine the PDA with the DPC, which is not portable and which does store the biometric.

(B) But the claim also requires that the mobile device receive a request to access the memory and retrieve transaction information. If the PDA/DPC combo is the mobile device, then this request must come from somewhere other than the PDA/DPC. Yet the portion of **Hoffman** cited in the Action refers to communications between an identicator 12 included in the DPC and the PDA as satisfying this limitation. This is simply inconsistent: The DPC cannot be the mobile device and also generate the request that is sent to the mobile device.

(C) **Hoffman**, as noted in the Action, the transaction information is transmitted to the DPC. Also, in **Hoffman**, the transaction information is transmitted to the DPC before a determination is made as to whether the received biometric information matches the stored biometric information.

(D) The amended to indicate that mobile device, or cellular telephone, transmits the transaction information to a POS or remote location.

(E) **Hoffman** does not describe such a short range radio frequency circuit.

Response to the arguments:

(A) **Hoffman** discloses each of the PDA conducts one or more of the operations includes store and retrieve a unique scrip form the biometric and merchant, PIN code, see Pars [0077-0082]

(B) **Hoffman** discloses that the Identicator 12 of the PDC 22 determines randomly which BID processor will be used for a given electronic scrip transaction, and delegates the identification request to that BID processor. That BID processor performs a search of its biometric sample database in order to find a matching registered biometric sample, see par [0143]. The electronic Clearinghouse 14 receives or takes the ID codes, data and scrip transaction request, see par [0166]).

(C) **Hoffman** discloses once a BPID processor receives a bid biometric sample 62 and PIC for identification, the processor searches through its database, retrieving all registered biometric samples that match or correspond to that particular bid PIC. Once all corresponding registered biometric samples are retrieved, the Identicator 12 compares the bid biometric samples obtained from the electronic scrip transaction to all retrieved registered biometric samples. If a match occurs, the Identicator 12 transmits the identity of the Scrip Supporter or the Supporter ID Code to the electronic Clearinghouse 14. If no match is found, the Identicator 12 transmits a "not identified"

message back to gateway machine 26 and to the logging facility 36, see Fig. 5, par [0150].

(D) The amended claim limits are obvious met by the combination of transmitting the transactions to the register or point of sale between **Hoffman** and **Scott** as discussed above.

(E) It is obvious to combine the Bluetooth or short range communication as discussed between **Hoffman** and **Scott** for constraint space and saving energy as one of different communication methods.

Conclusion

3. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

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.

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

Seigel et al discloses the cashless and clerkless transaction system can comprise four main functional components: a point of sale terminal, identification devices, databases and a network to connect the components. A cashless and clerkless transaction can be implemented by gathering product information, gathering personal information and capturing biometric information from the individual seeking to purchase a product through wired or wireless Bluetooth or short range communication. The captured biometric information can be compared with stored biometric information to confirm a consumer's identity. [US 2003/0139984]

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: 06/19/2017

Notice of References Cited	Application/Control No. 15/372,317	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	CPC Classification	US Classification
*	A	US-2003/0001459 A1	01-2003	Scott, Walter G.	G06K9/00885	310/339
*	B	US-2003/0139984 A1	07-2003	Seigel, William G.	G06F21/10	705/28
	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	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	464286	(emit$4 or obtain$3 or receiv$3 or send$3 or transmit$4) near9 (biometric or eye$4 or face or facial or fingerprint)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:16
L2	110394	(cellular or handheld or mobile or PDA or portable or reader or scann$3) near9 (biometric or eye$4 or face or facial or fingerprint)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:17
L3	42236	1 and 2	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:18
L5	27178	3 and (Bluetooth or RFID or IEEE or short or tag)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:19
L6	1702	(compar$5 or different or match$3) near9 (bill or purchas$3 or transaction) near9 (biometric or eye$4 or face or facial or fingerprint)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:20
L7	584	5 and 6	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:21
L8	92	7 not @AY > "2003"	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:21
L10	1911	1 near9 (counter or point near2 sale or POS or check$4out)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:22
L11	13	8 and 10	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:23
L12	19387	(G06F21/30, G06F21/305, G06F21/31, G06F21/32, G06F21/35, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06C20/20, G06C20/206, G06C20/40, G06C20/401, G06C20/405, G08B13/2402, G08B13/2417).CPC.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:34
L13	2785	12 not @AY > "2003"	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:34
L14	22	8 and 13	US-PGPUB; USPAT;	OR	OFF	2017/06/19 10:34

			USOCR			
L15	1	11 and 13	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:35
L16	9	(("6025784") or ("7031946") or ("8237568") or ("8587436") or ("8004410") or ("7671746") or ("7081819") or ("6934861") or ("2013350665") or ("2014084565") or ("20040128249")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:41
L17	2	16 and 8	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:41
L18	0	17 and 10	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:42
L19	2102	(emit$4 or send$3 or transmit$4) near9 (bill or purchas$3 or transaction) near9 (Bluetooth or IEEE or "801" or RFID or short)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:44
L20	2	19 and 8	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:44
L21	0	19 and 16	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:46
L22	3	16 and (emit$4 or send$3 or transmit$4) near9 (Bluetooth or IEEE or "801" or RFID or short)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:52
L23	6	16 and (Bluetooth or IEEE or "801" or RFID or short)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:52
L24	7	16 and (counter or point near2 sale or POS or check$4out)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/06/19 10:53

EAST Search History (Interference)

<This search history is empty>

6/19/2017 10:57:12 AM
C:\Users\vtrieu\Documents\EAST\Workspaces\Default EAST Workspace (Flat Panel).wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372317	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	VAN TRIEU	2685

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/30, G06F21/31, G06F21/32, G06F21/35, G06F30/305, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06Q20/20, G06Q20/206, G06Q20/40, G06Q20/401, G06Q20/405	1/30/17	vt
G08B13/2402, G08B13/2417	1/30/17	vt

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
G06F21/30, G06F21/31, G06F21/32, G06F21/35, G06F30/305, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06Q20/20, G06Q20/206, G06Q20/40, G06Q20/401, G06Q20/405,,and the results text limited - see attached search history printout.	1/30/17	vt
G08B13/2402, G08B13/2417, and the results text limited - see attached search history printout.	1/30/17	vt
Update Search	6/19/17	vt

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372317	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	**Art Unit**
	VAN TRIEU	2685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	01/30/2017	06/19/2017							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

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	15372317
Filing Date	2016-12-07
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	2685
Examiner Name	TRIEU, VAN THANH
Attorney Docket Number	116546-1108C8

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8548927	B2	2013-10-01	Beenau et al.	
	2	8401539	B2	2013-03-19	Beenau et al.	
	3	8126449	B2	2012-02-28	Beenau et al.	
	4	8041815	B2	2011-10-18	Bahl et al.	
	5	8004410	B2	2011-08-23	Martinez de Velasco Cortina et al.	
	6	7980378	B2	2011-07-19	Jones et al.	
	7	7911643	B2	2011-03-22	Yamada et al.	
	8	7844505	B1	2010-11-30	Arneson et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	9	7671746	B2	2010-03-02	Martinez de Velasco Cortina et al.	
	10	7533809	B1	2009-05-19	Robinson et al.	
	11	7487538	B2	2009-02-03	Mok	
	12	7310734	B2	2007-12-18	Boate et al.	
	13	7225337	B2	2007-05-29	Baessler	
	14	7080819	B2	2006-07-25	Tojo	
	15	7031946	B1	2006-04-18	Tamai et al.	
	16	6975834	B1	2005-12-13	Forster	
	17	6950013	B2	2005-09-27	Scaman et al.	
	18	6894615	B2	2005-05-17	Look	
	19	6850147	B2	2005-02-01	Prokoski	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	20	6848048	B1	2005-01-25	Holmes	
	21	6793134	B2	2004-09-21	Clark	
	22	6758405	B2	2004-07-06	Look	
	23	6753759	B2	2004-06-22	Stegmaier et al.	
	24	6698653	B1	2004-03-02	Diamond et al.	
	25	6617961	B1	2003-09-09	Janssen et al.	
	26	6570487	B1	2003-05-27	Steeves	
	27	6427504	B1	2002-08-06	Janssen et al.	
	28	6388579	B1	2002-05-14	Adcox et al.	
	29	6360208	B1	2002-03-19	Ohanian et al.	
	30	6340116	B1	2002-01-22	Cecil et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	31	6334059	B1	2001-12-25	Stilp et al.	
	32	6276607	B1	2001-08-21	Sato	
	33	6275157	B1	2001-08-14	Mays et al.	
	34	6269292	B1	2001-07-31	Kokubu et al.	
	35	6268796	B1	2001-07-31	Gnadinger et al.	
	36	6211790	B1	2001-04-03	Radomsky et al.	
	37	6203952	B1	2001-03-20	O'Brien et al.	
	38	6182894	B1	2001-02-06	Hackett et al.	
	39	6175922	B1	2001-01-16	Wang	
	40	6167333	A	2000-12-26	GEHLOT et al.	
	41	6163771	A	2000-12-19	WALKER et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	42	6157333	A	2000-12-05	Louagie et al.	
	43	6140941	A	2000-10-31	Dwyer et al.	
	44	6111506	A	2000-08-29	YAP et al.	
	45	6104281	A	2000-08-15	HEINRICH et al.	
	46	6098879	A	2000-08-08	TERRANOVA STEVEN N	
	47	6073840	A	2000-06-13	MARION KENNETH O	
	48	6052068	A	2000-04-18	PRICE R et al.	
	49	6025784	A	2000-02-15	Mish	
	50	6025780	A	2000-02-15	BOWERS et al.	
	51	5974500	A	1999-10-26	MALETSKY et al.	
	52	5874896	A	1999-02-23	LOWE et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	53	5864580	A	1999-01-26	Lowe et al.	
	54	5787174	A	1998-07-28	TUTTLE JOHN R	
	55	5742618	A	1998-04-21	Lowe	
	56	5657008	A	1997-08-12	Bantli	
	57	5590197	A	1996-12-31	CHEN et al.	
	58	5552789	A	1996-09-03	Schuermann	
	59	4529870	A	1985-07-16	CHAUM DAVID	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100095130	A1	2010-04-15	Bertran et al.	
	2	20100094754	A1	2010-04-15	Bertran et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	3	20070022058	A1	2007-01-25	Labrou et al.	
	4	20060020558	A1	2006-01-26	Bonalle	
	5	20050149764	A1	2005-07-07	Bahl et al.	
	6	20030200227	A1	2003-10-23	Ressler	
	7	20030074317	A1	2003-04-17	Hofi	
	8	20020112177	A1	2002-08-15	Voltmer et al.	
	9	20020109580	A1	2002-08-15	Shreve et al.	
	10	20020089434	A1	2002-07-11	Ghazarian	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2004006165	WO	A1	2004-01-15	BNC IP SWITZERLAND GMBH		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	2	2002042076	JP	A	2002-02-08	DAINIPPON PRINTING CO LTD	Abstract	☒
	3	19608757	DE	A1	1997-09-11	BROSOW, JOERGEN	Abstract	☒
	4	10042805	DE	A1	2002-03-14	BUNDESDRUCKEREI GMBH	Abstract	☒
	5	9843104	WO	A2	1998-10-01	Price, Frederick		☐
	6	0993999	EP	A2	2000-04-19	Ford Motor Company Limited		☐
	7	0977145	EP	A2	2000-02-02	Kabushiki Kaisha Toshiba		☐

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

NON-PATENT LITERATURE DOCUMENTS [Remove]

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	RFID Handbook - Active Load Modulation, 8 pages.	
	2	MOHAMMED et al., Smart Card Technology: Past Present and Future, International Journal of The Computer, the Internet and Management, Vol. 12#1 (January - April 2004), pp. 12-22.	
	3	ATMEL, Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards, 28 pages.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	~~4~~	~~ATMEL, Atmel Smart Card ICs, Silicon solutions making smart cards smarter, 12 pages.~~	
	5	Extended European Search Report, European Patent Application No. 10182033.0, dated 13 January 2012, 7 pages.	
	6	FANCHER, Carol Hovenga. Motorola, Inc., In your pocket smartcards, IEEE SPECTRUM, February 1997, 7 pages.	
	7	RAKERS, et al. Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal of Solid-State Circuits, Vol. 36, No. 3, March 2001, 7 pages.	
	8	Japanese Office Action, Japanese Patent Application No. 2004-519130, dated 12 May 2009, 10 pages.	X
	9	ANONYMOUS, Read/write RFID offers standalone advantages, Security, August 1996; 33, 8; ProQuest, 1 page.	☐
	10	Response to Office Action filed on November 18, 2016 for US patent application no. 14/321,781.	☐
	11	US Office Action dated May 19, 2016 received in US patent application no. 14/321,781.	☐
	12	Response to Office Action filed on December 24, 2015 for US patent application no. 14/321,781.	☐
	13	US Office Action dated June 24, 2015 received in US patent application no. 14/321,781.	☐
	14	US Notice of Allowance dated July 11, 2014 received in US patent application no. 14/022,135.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	15	Response to Office Action filed on March 14, 2014 for US patent application no. 14/022,135.	☐
	16	US Office Action dated March 7, 2014 received in US patent application no. 14/022,135.	☐
	17	Response to Office Action filed on February 3, 2014 for US patent application no. 14/022,135.	☐
	18	US Office Action dated December 5, 2013 received in US patent application no. 14/022,135.	☐
	19	Appeal Brief filed February 9, 2017 for US patent application no. 14/585,057.	☐
	20	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/585,057.	☐
	21	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 9, 2016 for US patent application no. 14/585,057.	☐
	22	US Office Action dated May 9, 2016 received in US patent application no. 14/585,057.	☐
	23	Response to Office Action filed on January 7, 2016 for US patent application no. 14/585,057.	☐
	24	US Office Action dated October 7, 2015 received in US patent application no. 14/585,057.	☐
	25	US Notice of Allowance dated December 3, 2014 received in US patent application no. 14/028,469.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	26	Supplemental response to Office Action filed on October 31, 2014 for US patent application no. 14/028,469.	☐
	27	Response to Office Action filed on October 14, 2014 for US patent application no. 14/028,469.	☐
	28	US Office Action dated August 18, 2014 received in US patent application no. 14/028,469.	☐
	29	US Office Action dated July 9, 2014 received in US patent application no. 14/028,469.	☐
	30	Response to Office Action filed on June 13, 2014 for US patent application no. 14/028,469.	☐
	31	US Office Action dated April 3, 2014 received in US patent application no. 14/028,469.	☐
	32	Response to Office Action filed on March 14, 2014 for US patent application no. 14/028,469.	☐
	33	US Office Action dated March 6, 2014 received in US patent application no. 14/028,469.	☐
	34	Response to Office Action filed on February 3, 2014 for US patent application no. 14/028,469.	☐
	35	US Office Action dated December 6, 2013 received in US patent application no. 14/028,469.	☐
	36	Appeal Brief filed January 30, 2017 for US patent application no. 14/639,034.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	37	Pre-Brief Appeal Conference Decision dated July 21, 2016 and received in US patent application no. 14/639,034.	☐
	38	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on June 30, 2016 for US patent application no. 14/639,034.	☐
	39	US Office Action dated December 30, 2015 received in US patent application no. 14/639,034.	☐
	40	Response to Office Action filed on November 30, 2015 for US patent application no. 14/639,034.	☐
	41	US Office Action dated May 29, 2015 received in US patent application no. 14/639,034.	☐
	42	Response to Office Action filed on April 26, 2017 for US patent application no. 14/724,593.	☐
	43	US Office Action dated February 17, 2017 received in US patent application no. 14/724,593.	☐
	44	Pre-Brief Appeal Conference Decision dated December 12, 2016 and received in US patent application no. 14/724,593.	☐
	45	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 7, 2016 for US patent application no. 14/724,593.	☐
	46	US Office Action dated May 6, 2016 received in US patent application no. 14/724,593.	☐
	47	Response to Office Action filed on January 7, 2016 for US patent application no. 14/724,593.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	48	US Office Action dated August 4, 2015 received in US patent application no. 14/724,593.	☐
	49	Appeal Brief filed April 18, 2017 for US patent application no. 14/659,502.	☐
	50	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/659,502.	☐

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

EXAMINER SIGNATURE

Examiner Signature	/VAN T TRIEU/	Date Considered	06/18/2017

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Daniel K. Robertson/	Date (YYYY-MM-DD)	2017-05-02
Name/Print	Daniel K. Robertson	Registration Number	48077

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /V.T.T/

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. /V.T.T/

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	15372317
Filing Date	2016-12-07
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	2685
Examiner Name	TRIEU, VAN THANH
Attorney Docket Number	116546-1108C8

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					

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					

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

/V.T.T/	1	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 16, 2016 for US patent application no. 14/659,502.	
/V.T.T/	2	US Office Action dated May 16, 2016 received in US patent application no. 14/659,502.	
/V.T.T/	3	Response to Office Action filed on December 22, 2015 for US patent application no. 14/659,502.	
/V.T.T/	4	US Office Action dated June 22, 2015 received in US patent application no. 14/659,502.	

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

EXAMINER SIGNATURE

Examiner Signature	/VAN T TRIEU/	Date Considered	06/18/2017

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Daniel K. Robertson/	Date (YYYY-MM-DD)	2017-05-02
Name/Print	Daniel K. Robertson	Registration Number	48077

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/372,317	12-07-2016	Francisco Martinez de Velasco Cortina	116546-1108C8	6203

EXAMINER	
TRIEU, VAN THANH	
ART UNIT	PAPER NUMBER
2685	
SUBMISSION DATE	DELIVERY MODE
2 May 2017	EFS WEB

SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

AMENDMENT AND RESPONSE TO NON-FINAL OFFICE ACTION

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

Dear Sir:

In response to the Non-Final Office Action mailed on February 2, 2017, Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following Amendment and Remarks, where:

Amendments to the Claims begin on page 2 of this paper; and

Remarks begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

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

a biometric input device configured to receive biometric data;

a short range radio frequency [[antenna]] circuit;

memory configured to store biometric information for identifying an individual associated with transaction information, and

a processor coupled with the memory and the biometric input device, the processor configured to:

receive a signal via the short range radio frequency [[antenna]] circuit, the signal comprising a request to access the memory and retrieve the transaction information,

receive biometric information from the biometric input device,

compare the received biometric information with the biometric information stored in the memory, and

~~provide~~ transmit the transaction information to a point of sale terminal using the short range radio frequency circuit ~~in response to the access request~~ when the received biometric information matches the stored biometric information.

2. (Original) The mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet.

3. (Original) The mobile device of claim 1, wherein the biometric input device is a fingerprint scanner.

4. (Currently Amended) The mobile device of claim 1, wherein the processor is further configured to ~~provide~~ transmit the received biometric

information or the stored biometric information with the transaction information.

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

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

7. (Original) The mobile device of claim 1, further comprising memory configured to store the transaction information.

8. (Original) The mobile device of claims 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

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

a fingerprint scanner configured to receive fingerprint information;

a short range radio frequency [[antenna]] circuit;

memory configured to store fingerprint information for identifying an individual associated with transaction information, and

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal via the short range radio frequency [[antenna]] circuit, the signal comprising a request to access the memory and retrieve the transaction information,

receive fingerprint information from the fingerprint scanner,

compare the received fingerprint information with the fingerprint information stored in the memory, and

~~provide~~ transmit the transaction information to a point of sale terminal using the short range radio frequency circuit ~~in response to the access request~~ when the received fingerprint information matches the stored fingerprint information.

10. (Currently Amended) The cellular telephone of claim 9, wherein the processor is further configured to ~~provide~~ transmit the received fingerprint information or the stored fingerprint information with the transaction information.

11. (Original) The cellular telephone of claim 9, wherein the transaction information is account information.

12. (Original) The cellular telephone of claim 9, wherein the transaction information is credit card information.

13. (Original) The cellular telephone of claim 9, further comprising memory configured to store the transaction information.

14. (Original) The cellular telephone of claims 13, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

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

cellular circuitry;

a fingerprint scanner configured to receive fingerprint information;

a short range radio frequency circuit; ~~antenna and a chip, the chip comprising:~~

a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information; [[,]] and

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal via the cellular circuitry, the signal comprising a request to access the memory and retrieve the transaction information,

receive fingerprint information from the fingerprint scanner,

compare the received fingerprint information with the fingerprint information stored in the memory, and

~~provide~~ transmit the transaction information to a remote location using the cellular circuitry ~~in response to the access request~~ when the received fingerprint information matches the stored fingerprint information.

16. (Currently Amended) The cellular telephone of claim 15, wherein the processor is further configured to ~~provide~~ transmit the received fingerprint information or the stored fingerprint information with the transaction information.

17. (Original) The cellular telephone of claim 15, wherein the transaction information is account information.

18. (Original) The cellular telephone of claim 15, wherein the transaction information is credit card information.

19. (Original) The cellular telephone of claim 15, further comprising memory configured to store the transaction information.

20. (Original) The cellular telephone of claims 19, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory

REMARKS

The present amendment is in response to the Non-Final Office Action dated February 2, 2017. In view of the above listing of the claims and the following remarks, Applicant respectfully requests reconsideration and allowance of all pending claims.

A. Claim Status

Claims 1-20 are pending in the application. Claims 1-20 stand rejected. Independent claims 1, 9 and 15 and dependent claims 4, 10 and 16 have been amended. No new matter is added by these amendments.

B. Claim Rejections Under 35 U.S.C. § 102

Claims 1-20 are rejected under 35 U.S.C. 102(a)(2) as being anticipated by Hoffman [US 2004/0128249]. Applicant respectfully traverses the rejection because Hoffman does not teach each and every limitation of the claims.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987) (emphasis added). Moreover, "The identical invention must be shown in as complete detail as is contained in the ... claim." Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

Certain embodiments disclosed in the present application are directed to a mobile device that comprises a biometric input device and can store both biometric identity information and transaction information. The mobile device can also use the biometric input device for authenticating the user of the device during a transaction such as with a POS. In such a situation, the POS would request the transaction information from the mobile device. The user can provide their biometric via the biometric input device. The

mobile device can be configured to then compare the provided biometric to the stored biometric and provide the transaction information to the POS when there is a match.

Accordingly, e.g., claim 1 is directed to a "mobile device, comprising: a biometric input device configured to receive biometric data; a short range radio frequency circuit; memory configured to store biometric information for identifying an individual associated with transaction information, and a processor coupled with the memory and the biometric input device, the processor configured to: receive a signal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information, receive biometric information from the biometric input device, compare the received biometric information with the biometric information stored in the memory, and transmit the transaction information to a point of sale terminal using the short range radio frequency circuit when the received biometric information matches the stored biometric information."

It should be noted that in claims 1 and 9, the transaction information is provided via a short range radio frequency circuit, in claim 15 the transaction information is provided via cellular circuitry.

Support for, e.g., claim 1 can be found in the description of embodiment (IV) titled, "RF Communication Device and Method of Use." The description clearly shows a "mobile device" (see device 1205), "comprising: a biometric input device configured to receive biometric data" (see device 1223, which paragraph 67 notes can be included in the device 1205); "a short range radio frequency circuit" (see RF device 1222, which includes an chip and an antenna); "memory configured to store biometric information for identifying an individual associated with transaction information" (as noted in paragraph 69, biometric information, e.g., fingerprint information, can be stored), and "a processor coupled with the memory and the biometric input device, the processor configured to: receive a signal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information, receive biometric information from the biometric input device, compare the received biometric information with the biometric information stored in the memory, and transmit the transaction information to a point of sale terminal using the short range radio frequency circuit when the received biometric information matches the stored biometric information" (as noted in paragraph 67, phone 1205 can

include an ASIC configured to run an application for matching fingerprint information obtained from scanner 1223 with fingerprint information stored in memory included in device 1205; as noted in paragraph 64 the fingerprint information can be used for identification purposes; and as noted in paragraph 71, an RF reader, e.g. at a POS, can identify the user, e.g., via authentication of the user's fingerprint data per paragraph 64, and then obtain transaction information from the phone 1205).

In contrast, Hoffman discloses a system in which a Party Data Apparatus (PDA) gathers identity information that is then stored in a Data Processing Center (DPC). The PDA gathers biometric input and securely communicates the biometric information to the DPC using encryption (see, for example, para. [0106] of Hoffman). It appears that the Action is equating the combination of the PDA and the DPC with the mobile device of the claim 1. But the attempt to equate the PDA/DPC combination with the mobile device of claim 1 fails on its face. The portable, or mobile device of Hoffman is clearly the PDA, but the PDA of Hoffman does not include memory configured to store the biometric: Thus, the need to combine the PDA with the DPC, which is not portable and which does store the biometric.

But the claim also requires that the mobile device receive a request to access the memory and retrieve transaction information. If the PDA/DPC combo is the mobile device, then this request must come from somewhere other than the PDA/DPC. Yet the portion of Hoffman cited in the Action refers to communications between an identicator 12 included in the DPC and the PDA as satisfying this limitation. This is simply inconsistent: The DPC cannot be the mobile device and also generate the request that is sent to the mobile device.

Moreover the mobile device of claim 1 and the cellular telephone in claims 9 and 15 must have a short range radio frequency circuit, such as RFID or NFC. Hoffman does not describe such a short range radio frequency circuit.

Finally, claims 1, 9 and 15 have been amended to indicate that mobile device, or cellular telephone, transmits the transaction information to a POS or remote location. In Hoffman, as noted in the Action, the transaction information is transmitted to the DPC. Also, in Hoffman, the transaction information is transmitted to the DPC before a determination is made as to whether the received biometric information matches the stored biometric information. This is necessarily true since that determination is made in the DPC. Whereas in independent claims 1, 9 and 15 the transaction information is only transmitted once the

determination is made. For at least these reasons, applicant believes that independent claims 1, 9 and 15, and claims dependent thereon, are allowable.

CONCLUSION

For all the foregoing reasons, allowance of all pending claims 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: May 2, 2017

/Daniel K. Robertson/
Daniel K. Robertson
Reg. No. 48077

Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101-4469
(619) 238-1900
Customer No. 27189

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

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

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							
If you wish to add additional Foreign Patent Document citation information please click the Add button								Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	1	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 16, 2016 for US patent application no. 14/659,502.	
	2	US Office Action dated May 16, 2016 received in US patent application no. 14/659,502.	
	3	Response to Office Action filed on December 22, 2015 for US patent application no. 14/659,502.	
	4	US Office Action dated June 22, 2015 received in US patent application no. 14/659,502.	

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	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Daniel K. Robertson/	Date (YYYY-MM-DD)	2017-05-02
Name/Print	Daniel K. Robertson	Registration Number	48077

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Acknowledgement Receipt

EFS ID:	29089347
Application Number:	15372317
International Application Number:	
Confirmation Number:	6203
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Daniel K. Robertson/gloria mimi choi
Filer Authorized By:	Daniel K. Robertson
Attorney Docket Number:	116546-1108C8
Receipt Date:	02-MAY-2017
Filing Date:	07-DEC-2016
Time Stamp:	17:24:40
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		NPL_14659502_Rejections_and_Amendments.PDF	3853918 b947bc3764d64854f3bcbf7e76860e6da8c216c7	yes	104

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Non Patent Literature	1	22
	Non Patent Literature	23	24
	Non Patent Literature	25	33
	Non Patent Literature	34	63
	Non Patent Literature	64	79
	Non Patent Literature	80	104

Warnings:					
Information:					
2		Reply_to_NFOA_TBF_116546-1108C8.PDF	51897 dc06ffa592661a7b046c51006b47acb6feb85651	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	6
	Applicant Arguments/Remarks Made in an Amendment	7	11

Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	IDS_SB08_116546-1108C8.PDF	612214 b5f065123c5c01615b31224ee14be183337de750	no	4

Warnings:	
Information:	
A U.S. Patent Number Citation or a U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form for autoloading of data into USPTO systems. You may remove the form to add the required data in order to correct the Informational Message if you are citing U.S. References. If you chose not to include U.S. References, 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.	
Total Files Size (in bytes):	4518029

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	15372317
Filing Date	2016-12-07
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	2685
Examiner Name	TRIEU, VAN THANH
Attorney Docket Number	116546-1108C8

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	8548927	B2	2013-10-01	Beenau et al.	
	2	8401539	B2	2013-03-19	Beenau et al.	
	3	8126449	B2	2012-02-28	Beenau et al.	
	4	8041815	B2	2011-10-18	Bahl et al.	
	5	8004410	B2	2011-08-23	Martinez de Velasco Cortina et al.	
	6	7980378	B2	2011-07-19	Jones et al.	
	7	7911643	B2	2011-03-22	Yamada et al.	
	8	7844505	B1	2010-11-30	Arneson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	9	7671746	B2	2010-03-02	Martinez de Velasco Cortina et al.	
	10	7533809	B1	2009-05-19	Robinson et al.	
	11	7487538	B2	2009-02-03	Mok	
	12	7310734	B2	2007-12-18	Boate et al.	
	13	7225337	B2	2007-05-29	Baessler	
	14	7080819	B2	2006-07-25	Tojo	
	15	7031946	B1	2006-04-18	Tamai et al.	
	16	6975834	B1	2005-12-13	Forster	
	17	6950013	B2	2005-09-27	Scaman et al.	
	18	6894615	B2	2005-05-17	Look	
	19	6850147	B2	2005-02-01	Prokoski	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	20	6848048	B1	2005-01-25	Holmes	
	21	6793134	B2	2004-09-21	Clark	
	22	6758405	B2	2004-07-06	Look	
	23	6753759	B2	2004-06-22	Stegmaier et al.	
	24	6698653	B1	2004-03-02	Diamond et al.	
	25	6617961	B1	2003-09-09	Janssen et al.	
	26	6570487	B1	2003-05-27	Steeves	
	27	6427504	B1	2002-08-06	Janssen et al.	
	28	6388579	B1	2002-05-14	Adcox et al.	
	29	6360208	B1	2002-03-19	Ohanian et al.	
	30	6340116	B1	2002-01-22	Cecil et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	31	6334059	B1	2001-12-25	Stilp et al.	
	32	6276607	B1	2001-08-21	Sato	
	33	6275157	B1	2001-08-14	Mays et al.	
	34	6269292	B1	2001-07-31	Kokubu et al.	
	35	6268796	B1	2001-07-31	Gnadinger et al.	
	36	6211790	B1	2001-04-03	Radomsky et al.	
	37	6203952	B1	2001-03-20	O'Brien et al.	
	38	6182894	B1	2001-02-06	Hackett et al.	
	39	6175922	B1	2001-01-16	Wang	
	40	6167333	A	2000-12-26	GEHLOT et al.	
	41	6163771	A	2000-12-19	WALKER et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	42	6157333	A	2000-12-05	Louagie et al.	
	43	6140941	A	2000-10-31	Dwyer et al.	
	44	6111506	A	2000-08-29	YAP et al.	
	45	6104281	A	2000-08-15	HEINRICH et al.	
	46	6098879	A	2000-08-08	TERRANOVA STEVEN N	
	47	6073840	A	2000-06-13	MARION KENNETH O	
	48	6052068	A	2000-04-18	PRICE R et al.	
	49	6025784	A	2000-02-15	Mish	
	50	6025780	A	2000-02-15	BOWERS et al.	
	51	5974500	A	1999-10-26	MALETSKY et al.	
	52	5874896	A	1999-02-23	LOWE et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	53	5864580	A	1999-01-26	Lowe et al.	
	54	5787174	A	1998-07-28	TUTTLE JOHN R	
	55	5742618	A	1998-04-21	Lowe	
	56	5657008	A	1997-08-12	Bantli	
	57	5590197	A	1996-12-31	CHEN et al.	
	58	5552789	A	1996-09-03	Schuermann	
	59	4529870	A	1985-07-16	CHAUM DAVID	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20100095130	A1	2010-04-15	Bertran et al.	
	2	20100094754	A1	2010-04-15	Bertran et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	3	20070022058	A1	2007-01-25	Labrou et al.	
	4	20060020558	A1	2006-01-26	Bonalle	
	5	20050149764	A1	2005-07-07	Bahl et al.	
	6	20030200227	A1	2003-10-23	Ressler	
	7	20030074317	A1	2003-04-17	Hofi	
	8	20020112177	A1	2002-08-15	Voltmer et al.	
	9	20020109580	A1	2002-08-15	Shreve et al.	
	10	20020089434	A1	2002-07-11	Ghazarian	

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

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	2004006165	WO	A1	2004-01-15	BNC IP SWITZERLAND GMBH		

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	2	2002042076	JP	A	2002-02-08	DAINIPPON PRINTING CO LTD	Abstract	☒
	3	19608757	DE	A1	1997-09-11	BROSOW, JOERGEN	Abstract	☒
	4	10042805	DE	A1	2002-03-14	BUNDESDRUCKEREI GMBH	Abstract	☒
	5	9843104	WO	A2	1998-10-01	Price, Frederick		☐
	6	0993999	EP	A2	2000-04-19	Ford Motor Company Limited		☐
	7	0977145	EP	A2	2000-02-02	Kabushiki Kaisha Toshiba		☐

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T5
	1	RFID Handbook - Active Load Modulation, 8 pages.	
	2	MOHAMMED et al., Smart Card Technology: Past Present and Future, International Journal of The Computer, the Internet and Management, Vol. 12#1 (January - April 2004), pp. 12-22.	
	3	ATMEL, Understanding the Requirements of ISO/IEC 14443 for Type B Proximity Contactless Identification Cards, 28 pages.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	4	ATMEL, Atmel Smart Card ICs, Silicon solutions making smart cards smarter, 12 pages.	
	5	Extended European Search Report, European Patent Application No. 10182033.0, dated 13 January 2012, 7 pages.	
	6	FANCHER, Carol Hovenga. Motorola, Inc., In your pocket smartcards, IEEE SPECTRUM, February 1997, 7 pages.	
	7	RAKERS, et al. Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal of Solid-State Circuits, Vol. 36, No. 3, March 2001, 7 pages.	
	8	Japanese Office Action, Japanese Patent Application No. 2004-519130, dated 12 May 2009, 10 pages.	X
	9	ANONYMOUS, Read/write RFID offers standalone advantages, Security, August 1996; 33, 8; ProQuest, 1 page.	☐
	10	Response to Office Action filed on November 18, 2016 for US patent application no. 14/321,781.	☐
	11	US Office Action dated May 19, 2016 received in US patent application no. 14/321,781.	☐
	12	Response to Office Action filed on December 24, 2015 for US patent application no. 14/321,781.	☐
	13	US Office Action dated June 24, 2015 received in US patent application no. 14/321,781.	☐
	14	US Notice of Allowance dated July 11, 2014 received in US patent application no. 14/022,135.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	15	Response to Office Action filed on March 14, 2014 for US patent application no. 14/022,135.	☐
	16	US Office Action dated March 7, 2014 received in US patent application no. 14/022,135.	☐
	17	Response to Office Action filed on February 3, 2014 for US patent application no. 14/022,135.	☐
	18	US Office Action dated December 5, 2013 received in US patent application no. 14/022,135.	☐
	19	Appeal Brief filed February 9, 2017 for US patent application no. 14/585,057.	☐
	20	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/585,057.	☐
	21	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 9, 2016 for US patent application no. 14/585,057.	☐
	22	US Office Action dated May 9, 2016 received in US patent application no. 14/585,057.	☐
	23	Response to Office Action filed on January 7, 2016 for US patent application no. 14/585,057.	☐
	24	US Office Action dated October 7, 2015 received in US patent application no. 14/585,057.	☐
	25	US Notice of Allowance dated December 3, 2014 received in US patent application no. 14/028,469.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	26	Supplemental response to Office Action filed on October 31, 2014 for US patent application no. 14/028,469.	☐
	27	Response to Office Action filed on October 14, 2014 for US patent application no. 14/028,469.	☐
	28	US Office Action dated August 18, 2014 received in US patent application no. 14/028,469.	☐
	29	US Office Action dated July 9, 2014 received in US patent application no. 14/028,469.	☐
	30	Response to Office Action filed on June 13, 2014 for US patent application no. 14/028,469.	☐
	31	US Office Action dated April 3, 2014 received in US patent application no. 14/028,469.	☐
	32	Response to Office Action filed on March 14, 2014 for US patent application no. 14/028,469.	☐
	33	US Office Action dated March 6, 2014 received in US patent application no. 14/028,469.	☐
	34	Response to Office Action filed on February 3, 2014 for US patent application no. 14/028,469.	☐
	35	US Office Action dated December 6, 2013 received in US patent application no. 14/028,469.	☐
	36	Appeal Brief filed January 30, 2017 for US patent application no. 14/639,034.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	37	Pre-Brief Appeal Conference Decision dated July 21, 2016 and received in US patent application no. 14/639,034.	☐
	38	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on June 30, 2016 for US patent application no. 14/639,034.	☐
	39	US Office Action dated December 30, 2015 received in US patent application no. 14/639,034.	☐
	40	Response to Office Action filed on November 30, 2015 for US patent application no. 14/639,034.	☐
	41	US Office Action dated May 29, 2015 received in US patent application no. 14/639,034.	☐
	42	Response to Office Action filed on April 26, 2017 for US patent application no. 14/724,593.	☐
	43	US Office Action dated February 17, 2017 received in US patent application no. 14/724,593.	☐
	44	Pre-Brief Appeal Conference Decision dated December 12, 2016 and received in US patent application no. 14/724,593.	☐
	45	Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on November 7, 2016 for US patent application no. 14/724,593.	☐
	46	US Office Action dated May 6, 2016 received in US patent application no. 14/724,593.	☐
	47	Response to Office Action filed on January 7, 2016 for US patent application no. 14/724,593.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

	48	US Office Action dated August 4, 2015 received in US patent application no. 14/724,593.	☐
	49	Appeal Brief filed April 18, 2017 for US patent application no. 14/659,502.	☐
	50	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/659,502.	☐

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	15372317
	Filing Date	2016-12-07
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	2685
	Examiner Name	TRIEU, VAN THANH
	Attorney Docket Number	116546-1108C8

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Daniel K. Robertson/	Date (YYYY-MM-DD)	2017-05-02
Name/Print	Daniel K. Robertson	Registration Number	48077

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Electronic Patent Application Fee Transmittal	
Application Number:	15372317
Filing Date:	07-Dec-2016
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Daniel K. Robertson
Attorney Docket Number:	116546-1108C8
Filed as Large Entity	
Filing Fees for Utility under 35 USC 111(a)	

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

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

Electronic Acknowledgement Receipt	
EFS ID:	29089284
Application Number:	15372317
International Application Number:	
Confirmation Number:	6203
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Daniel K. Robertson/gloria mimi choi
Filer Authorized By:	Daniel K. Robertson
Attorney Docket Number:	116546-1108C8
Receipt Date:	02-MAY-2017
Filing Date:	07-DEC-2016
Time Stamp:	17:25:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$180
RAM confirmation Number	050317INTEFSW17271101
Deposit Account	502075
Authorized User	Gloria Choi
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	WO2004006165.PDF	16289266 66528ac5ebb4db401fb5fd5269b57fdd67e47757	no	94
Warnings:					
Information:					
2	Foreign Reference	JP2002042076.PDF	2759352 ec469f93bd123690356951428bba7500e4ce8935	no	9
Warnings:					
Information:					
3	Foreign Reference	DE19608757.PDF	1491667 e9e9d2697b02430fb3327a67de7035f1d2352787	no	6
Warnings:					
Information:					
4	Foreign Reference	DE10042805.PDF	12640477 824e6851f23bc447615210a3b8c3961ed53ed966	no	12
Warnings:					
Information:					
5	Foreign Reference	WO1998043104.PDF	4022652 ab309e032ae0d7b65a64908b5b4c8af433c7e840	no	38
Warnings:					
Information:					
6	Foreign Reference	EP0993999.PDF	12612799 09035172ebea24be9963f75bef4ec9c8be7778c5	no	10
Warnings:					
Information:					

7	Foreign Reference	EP0977145.PDF	5553711 53cda0831046769df8887464a086e09846a42bee	no	43
Warnings:					
Information:					
8	Non Patent Literature	NPL_RFID_Handbook_Active_Load_Modulation.PDF	724388 ae1b90b675310c6d3e359541e9991b1f751a76b4	no	8
Warnings:					
Information:					
9	Non Patent Literature	NPL_Mohammed_et_al_Smart_Card_Technology.PDF	800740 1a3f41b8d05ae2b007dbd617d4440fbed460940e	no	11
Warnings:					
Information:					
10	Non Patent Literature	NPL_Atmel_Understanding_the_Requirements.PDF	953721 609fba03ddaa4ddf268d98040918586f3cab0bea	no	28
Warnings:					
Information:					
11	Non Patent Literature	NPL_Atmel_Smart_Cards_ICs.PDF	3746166 837cd88afc736d4d727481b9680346dba943034e	no	12
Warnings:					
Information:					
12	Non Patent Literature	NPL_EESR_EP101820330.PDF	317764 7f542e8769a6cf420fb53db204636df6092c5d52	no	7
Warnings:					
Information:					
13	Non Patent Literature	NPL_Fancher_In_your_pocket_smartcards.PDF	1969305 b9269a1b51049e246d75166e113ae54d39cb90c9	no	7
Warnings:					
Information:					

14	Non Patent Literature	NPL_Rakers_Secure_Contactless_Smartcard_ASIC_with_DPA_Protection.PDF	655066 ce772b672ba90fd289cc285f25f435ee27ab3be4	no	7
Warnings:					
Information:					
15	Non Patent Literature	NPL_JP_OA_JP2004519130.PDF	1158006 ed90eedb1349386d2d829c6f67cca9097ef11edb	no	10
Warnings:					
Information:					
16	Non Patent Literature	NPL_Anonymous_ReadWrite_RFID_Offers_Standalone.PDF	173548 c0f146328abb3362dac83e497dcd7f6c3b5b49a6	no	1
Warnings:					
Information:					
17		NPL_14321781_Rejections_and_Amendments.PDF	3697373 36aec421706a841c03ac4c3b65ef9ce60ba869b4	yes	97

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Non Patent Literature	1	16
	Non Patent Literature	17	43
	Non Patent Literature	44	74
	Non Patent Literature	75	97

Warnings:					
Information:					
18		NPL_14022135_Rejections_and_Amendments.PDF	1536852 79921e073d780349bcd5776b899b8d476c82cb72	yes	45

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Non Patent Literature	1	10

	Non Patent Literature		11	17	
	Non Patent Literature		18	27	
	Non Patent Literature		28	34	
	Non Patent Literature		35	45	
Warnings:					
Information:					
19		NPL_14585057_Rejections_and_Amendments.PDF	3499096 1dc64e89387a504a23f327e389f4781426c6c214	yes	94
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Non Patent Literature		1	16	
	Non Patent Literature		17	18	
	Non Patent Literature		19	27	
	Non Patent Literature		28	56	
	Non Patent Literature		57	69	
	Non Patent Literature		70	94	
Warnings:					
Information:					
20		NPL_14028469_Rejections_and_Amendments.PDF	4322660 77ad3bf14f3aa49a053ede8b281047eb20dbe67f	yes	120
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Non Patent Literature		1	8	
	Non Patent Literature		9	16	
	Non Patent Literature		17	28	

	Non Patent Literature		29	46	
	Non Patent Literature		47	60	
	Non Patent Literature		61	68	
	Non Patent Literature		69	82	
	Non Patent Literature		83	89	
	Non Patent Literature		90	98	
	Non Patent Literature		99	106	
	Non Patent Literature		107	120	
Warnings:					
Information:					
21		NPL_14639034_Rejections_and_Amendments.PDF	3120565 d76fc6256d9d9cded3c2ae7c9abebac8fa8ac21e	yes	82
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Non Patent Literature		1	17	
	Non Patent Literature		18	19	
	Non Patent Literature		20	29	
	Non Patent Literature		30	52	
	Non Patent Literature		53	63	
	Non Patent Literature		64	82	
Warnings:					
Information:					
22		NPL_14724593_Rejections_and_Amendments.PDF	3891697 c904b0c7dc2ee6cba8ce4b97f09fd98dc08e3963	yes	106

	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Non Patent Literature		1	8	
	Non Patent Literature		9	30	
	Non Patent Literature		31	32	
	Non Patent Literature		33	41	
	Non Patent Literature		42	70	
	Non Patent Literature		71	82	
	Non Patent Literature		83	106	
Warnings:					
Information:					
23	Information Disclosure Statement (IDS) Form (SB08)	IDS_SB08_116546-1108C8.PDF	615719 78326cce9b086bfad419c03d3f33c8e545f64acc	no	15
Warnings:					
Information:					
24	Fee Worksheet (SB06)	fee-info.pdf	30563 dde2c3b6031ba05f42e60c0bb46709a1400de7e9	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	86583153		

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.

(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).

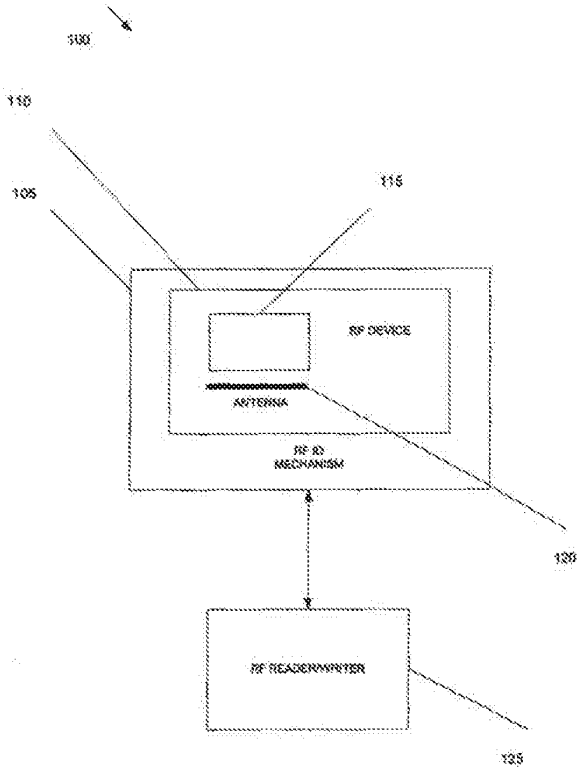
(74) Agent: **MIDGLEY, Jonathan, Lee**; Marks & Clerk, 57-60 Lincolns Inn Fields, London, WC2A 3LS (GB).

(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:

$$L_1 = 2.93 \text{K} 10^{8} H$$
$$L_2 = 6.437 \text{K} 10^{22} H$$

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.

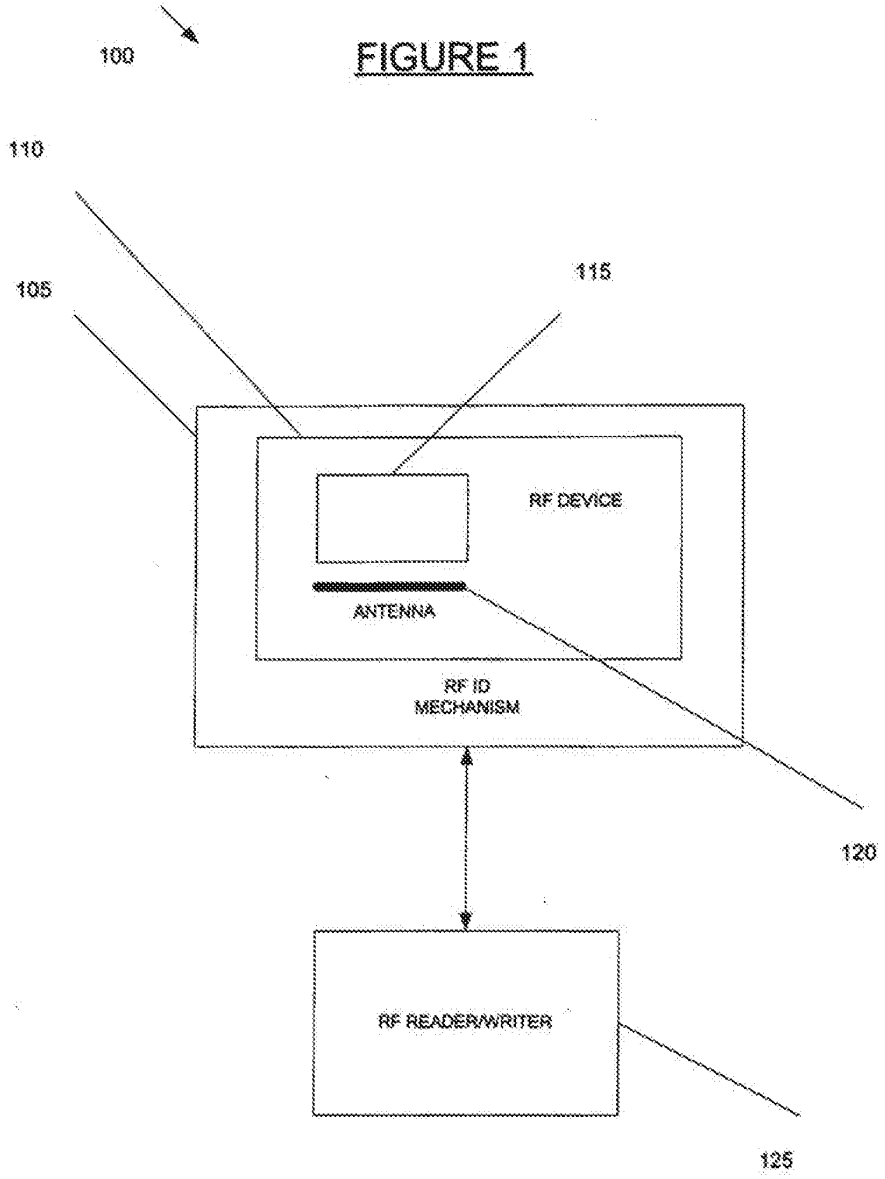

100
110
105
115
RF DEVICE
ANTENNA
RF ID
MECHANISM
120
RF READER/WRITER
125

FIGURE 1

FIGURE 2

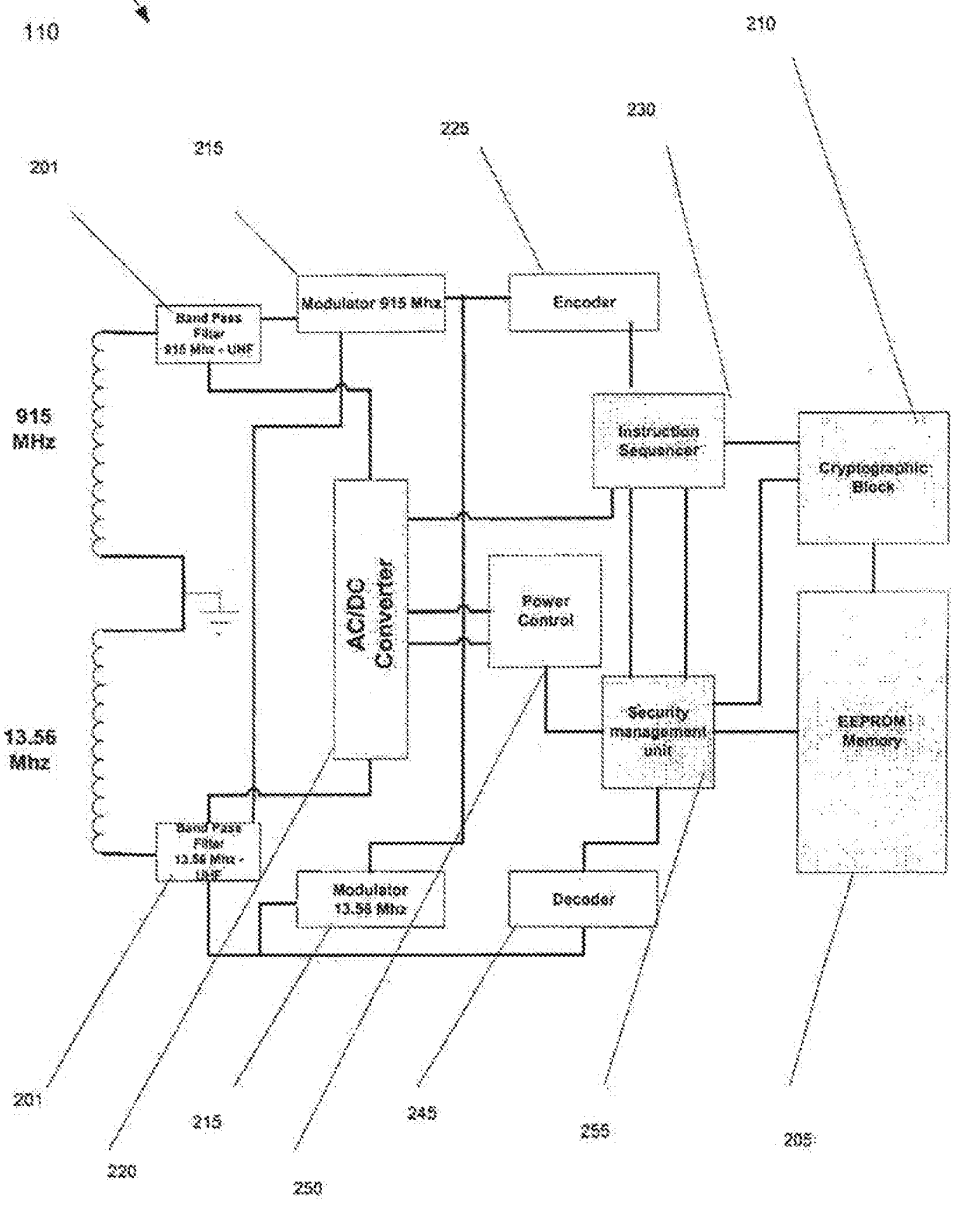

110
210
230
225
215
201
Modulator 915 Mhz
Encoder
915 MHz
Instruction Sequencer
Cryptographic Block
AC/DC Converter
Power Control
13.56 Mhz
Security management unit
EEPROM Memory
Modulator 13.56 Mhz
Decoder
201
215
245
255
205
220
250

FIGURE 3A

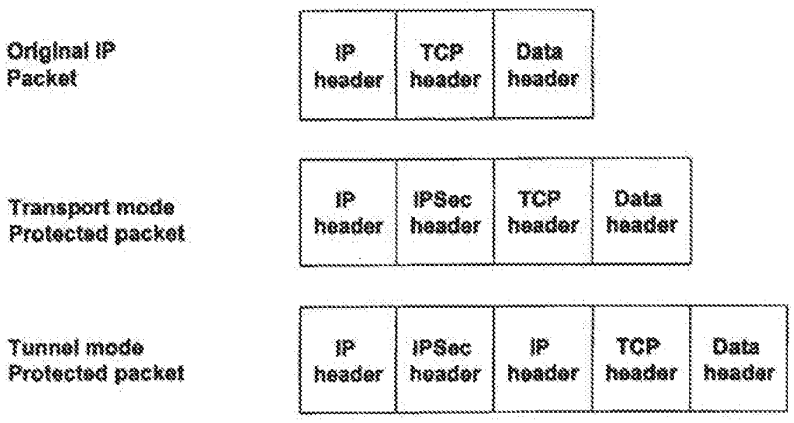
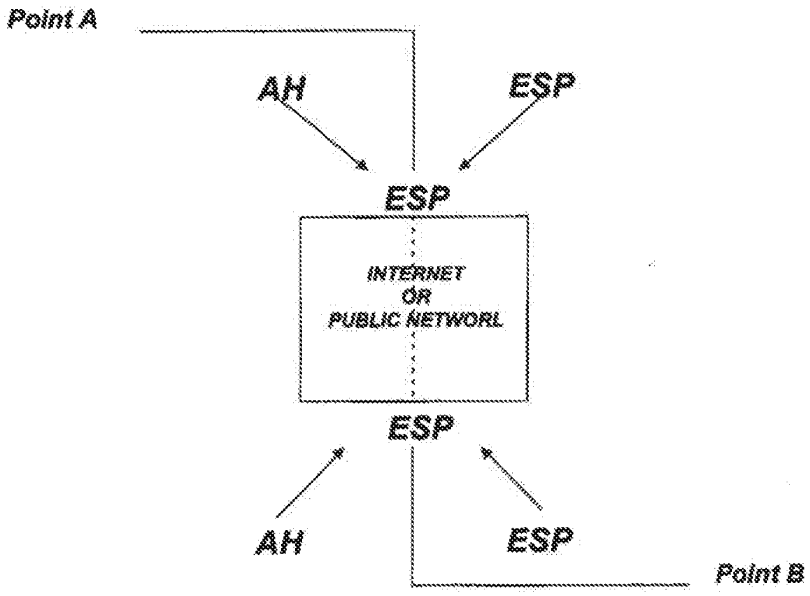

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIGURE 3B


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

400

FIGURE 4

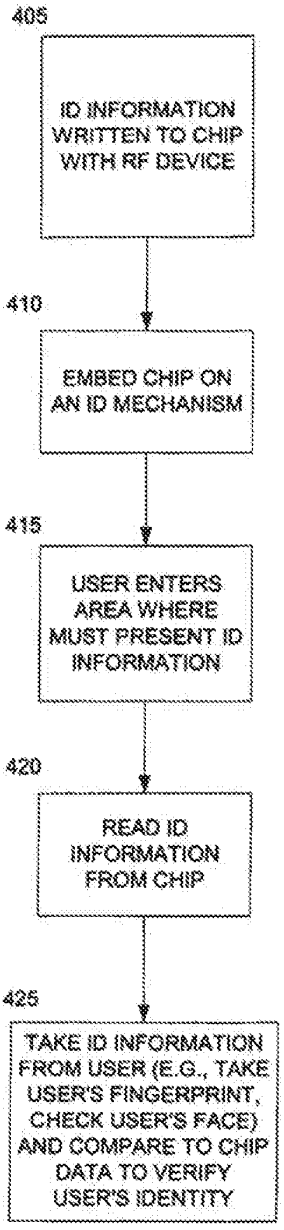

405
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
410
EMBED CHIP ON AN ID MECHANISM
415
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
420
READ ID INFORMATION FROM CHIP
425
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY

FIGURE 5

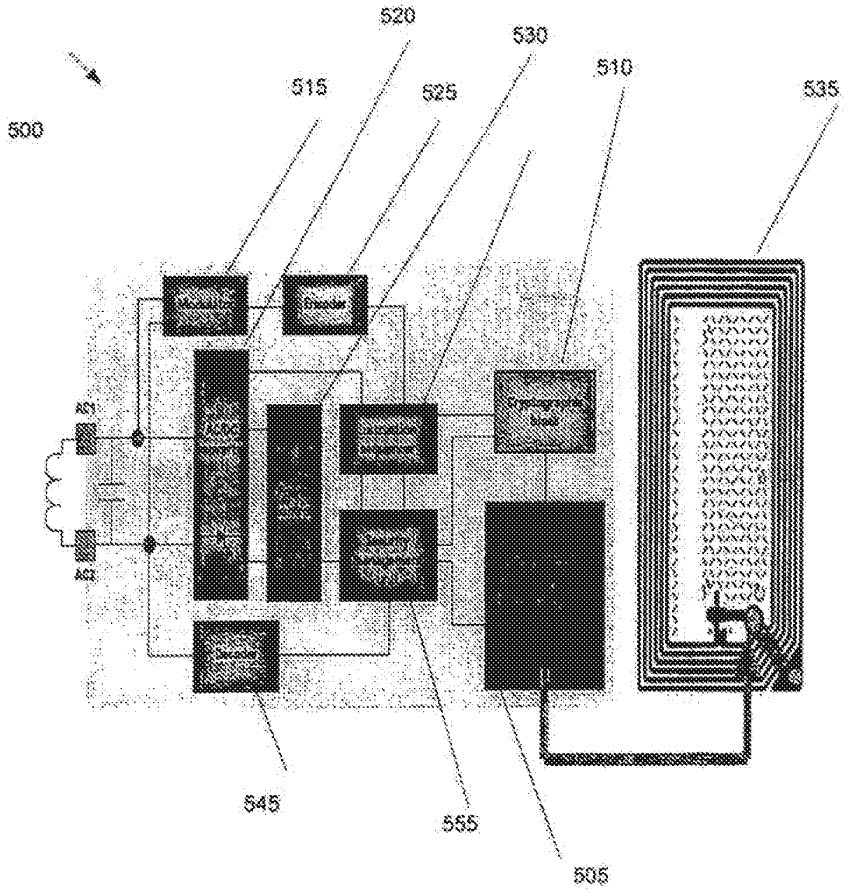


FIGURE 6

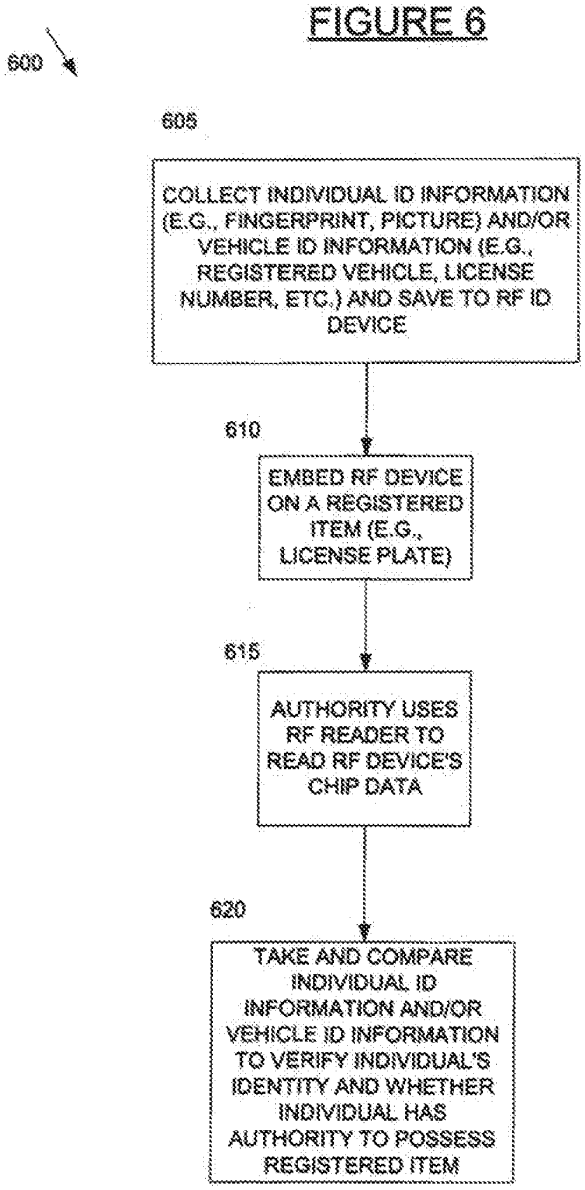

600
605
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
610
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
615
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
620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

FIGURE 7

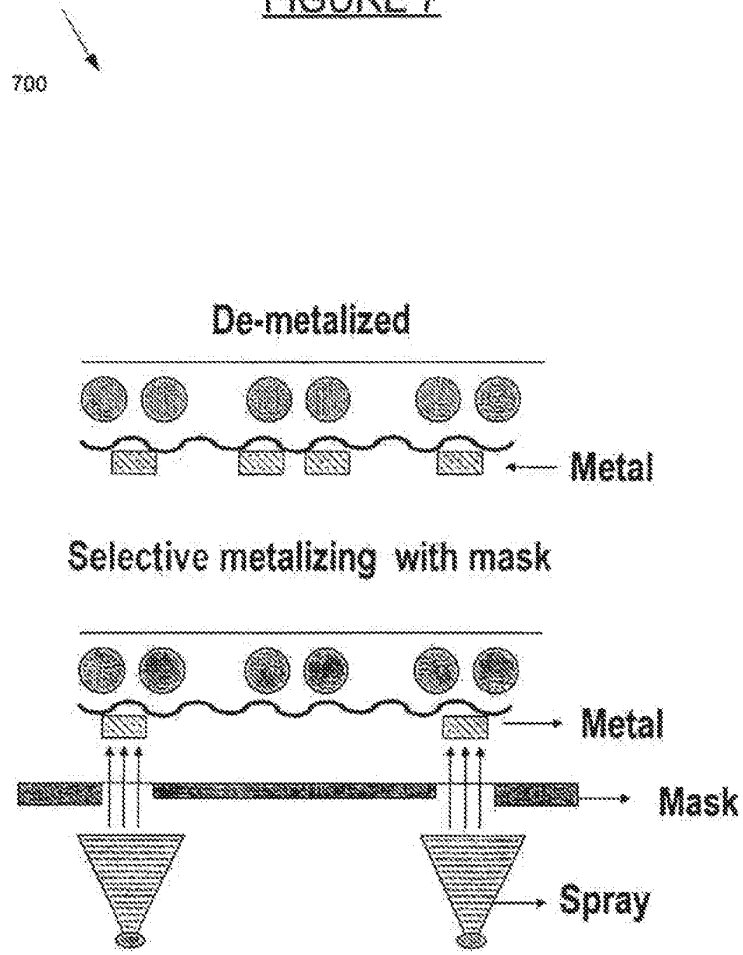

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIGURE 8

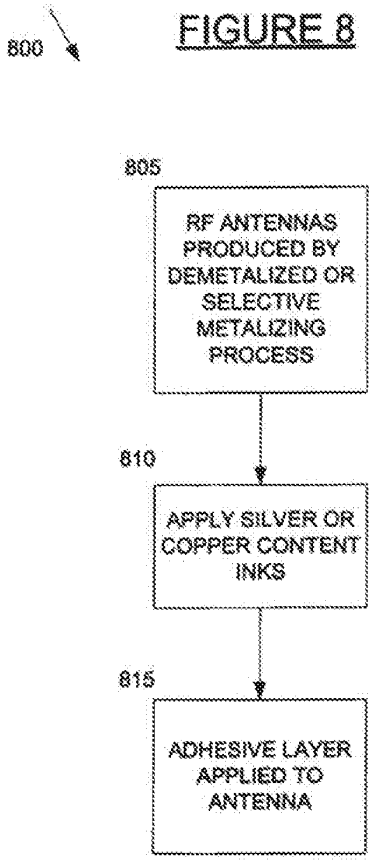

800
805
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
810
APPLY SILVER OR COPPER CONTENT INKS
815
ADHESIVE LAYER APPLIED TO ANTENNA

FIGURE 9

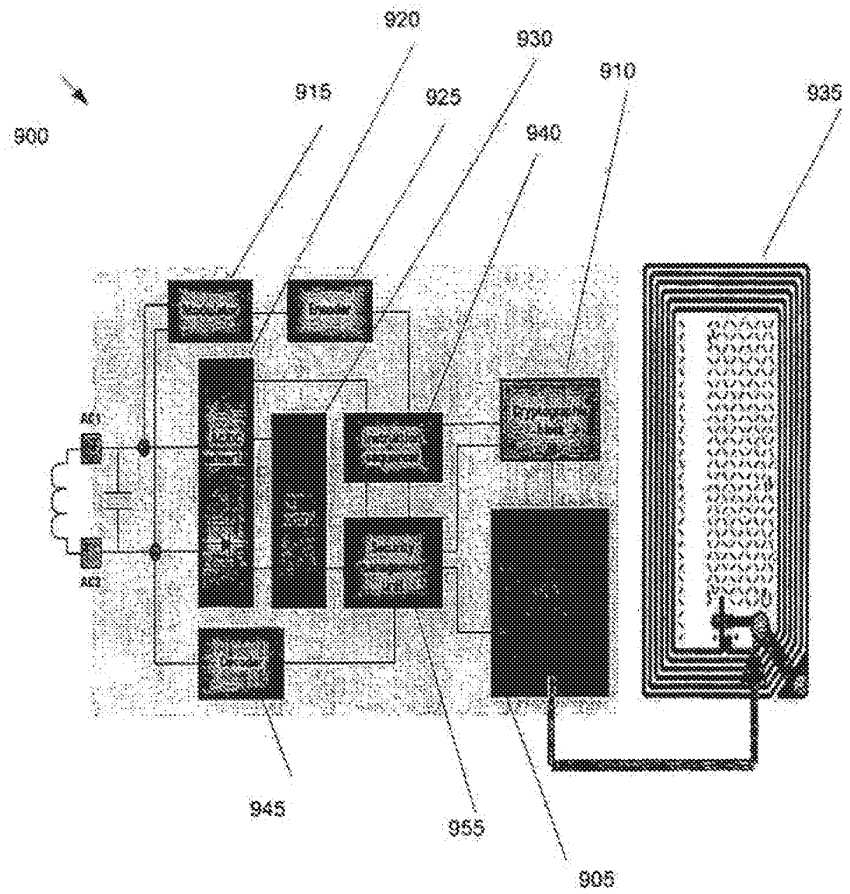


FIGURE 10

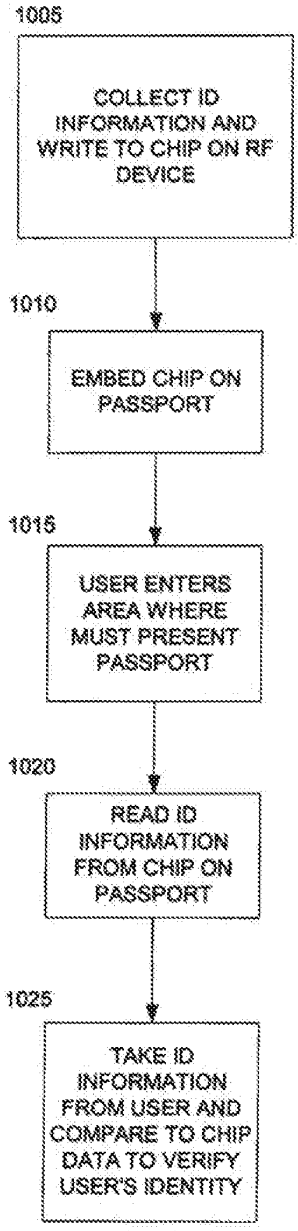

1005
COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1010
EMBED CHIP ON PASSPORT
1015
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1020
READ ID INFORMATION FROM CHIP ON PASSPORT
1025
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY

FIGURE 11

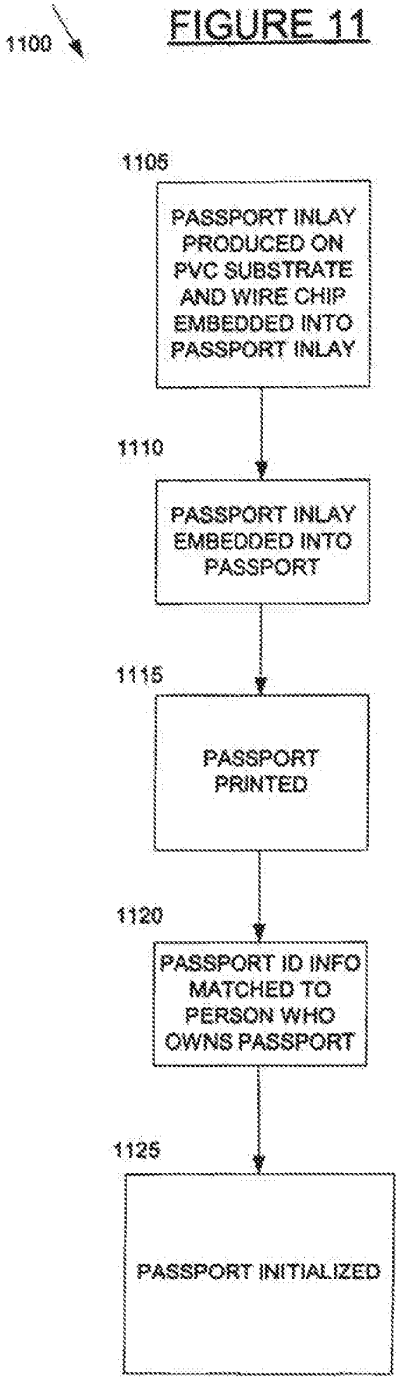

1100
1105
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1110
PASSPORT INLAY EMBEDDED INTO PASSPORT
1115
PASSPORT PRINTED
1120
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1125
PASSPORT INITIALIZED

FIGURE 12

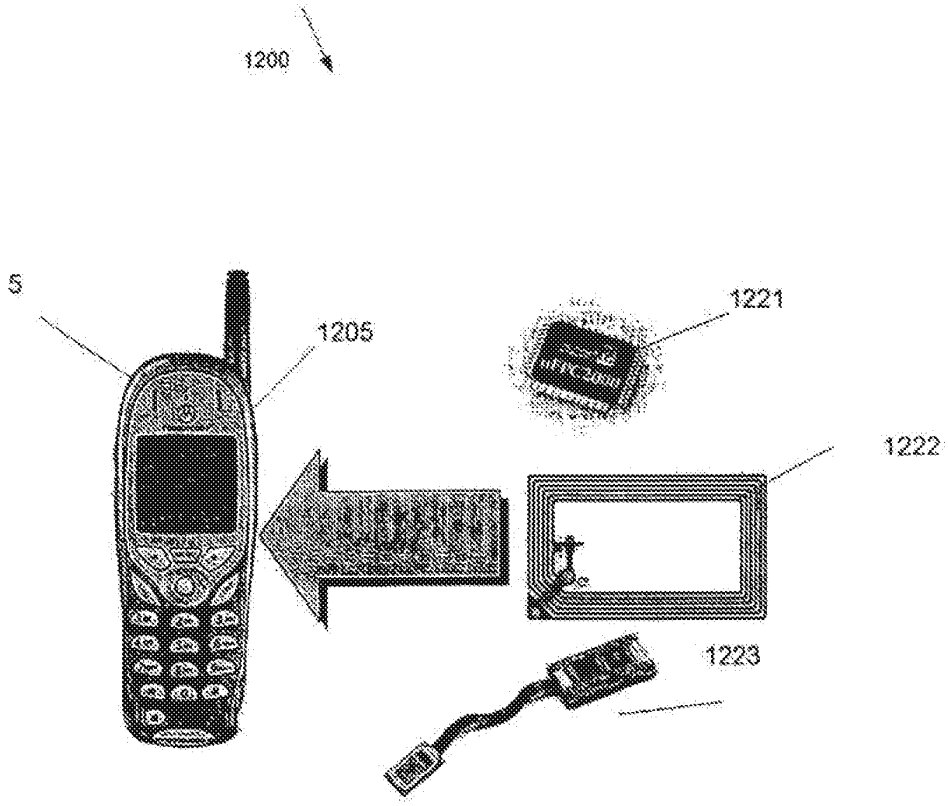


FIGURE 13

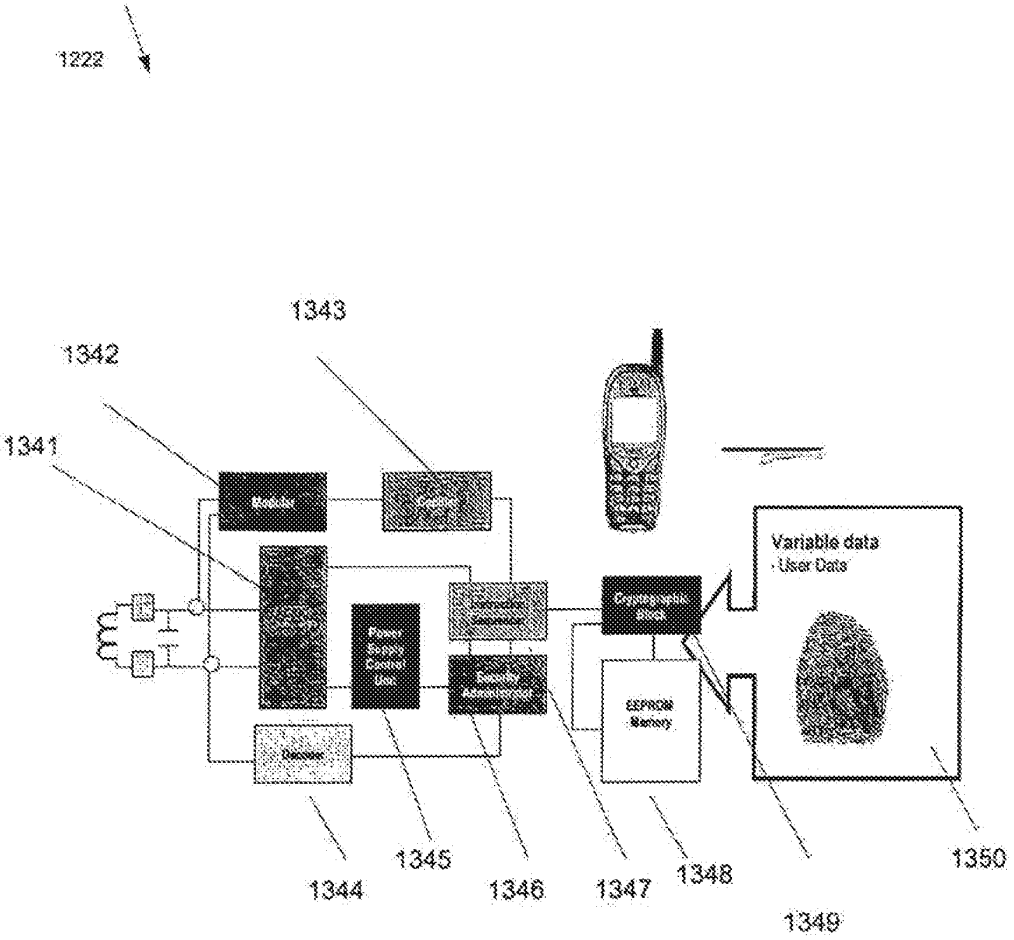

1222
1343
1342
1341
Variable data
- User Data
1344
1345
1346
1347
1348
1349
1350

FIGURE 14

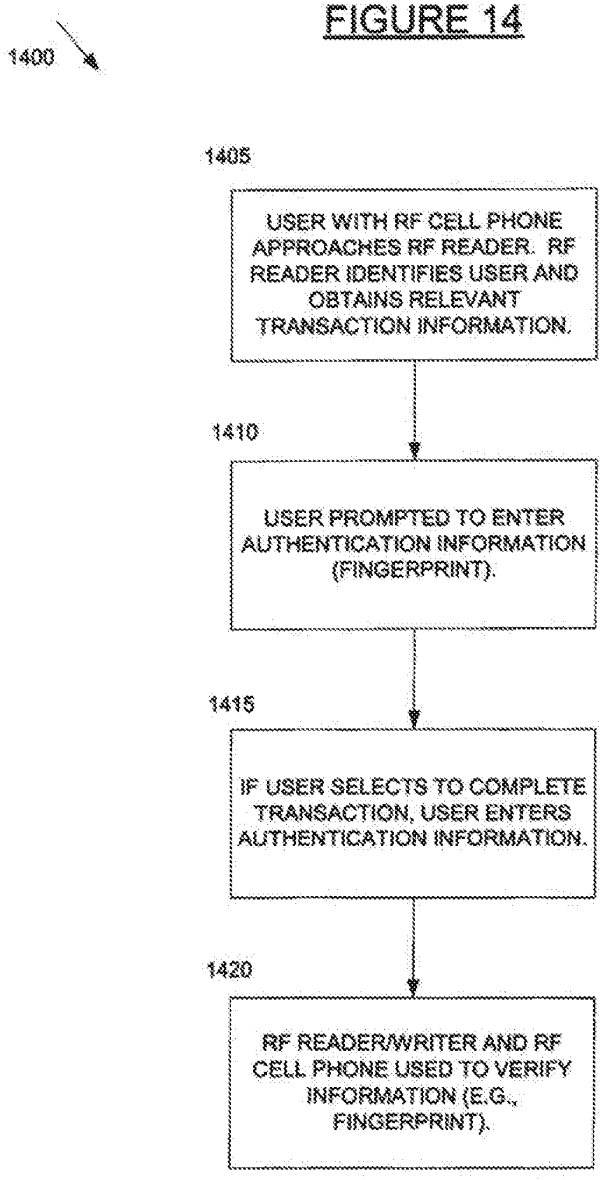

1400
1405
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION.
1410
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT).
1415
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION.
1420
RF READER/WRITER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

FIGURE 15

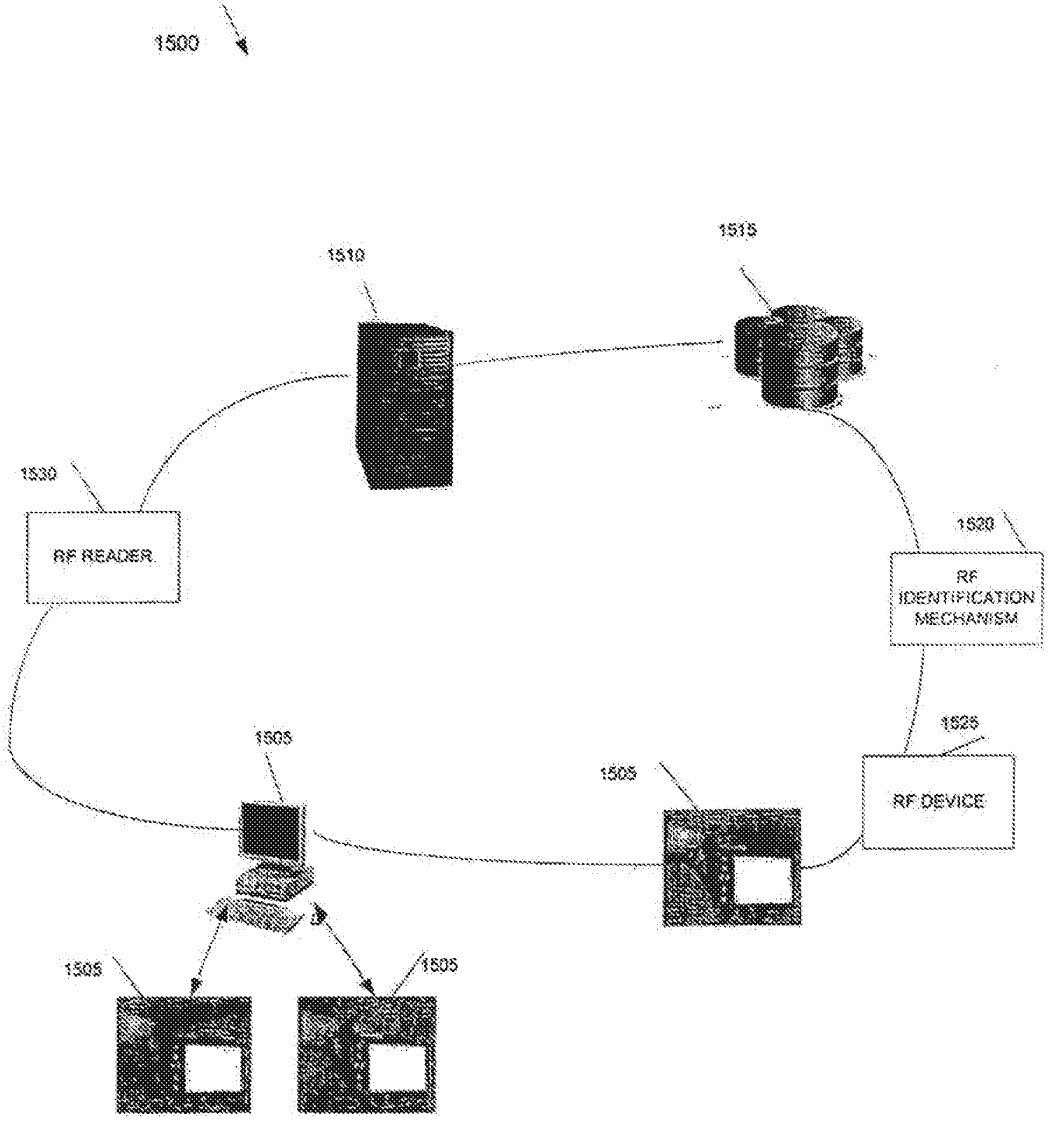

1500
1510
1515
1530
RF READER
1520
RF IDENTIFICATION MECHANISM
1525
RF DEVICE
1505
1505
1505
1505

FIGURE 16

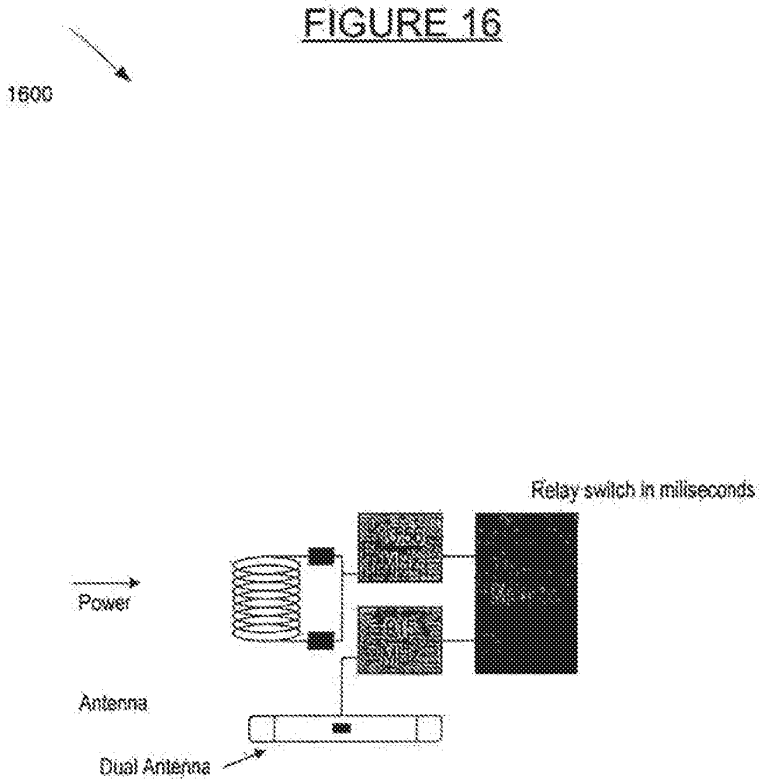

1600
Relay switch in milliseconds
Power
Antenna
Dual Antenna

FIGURE 17

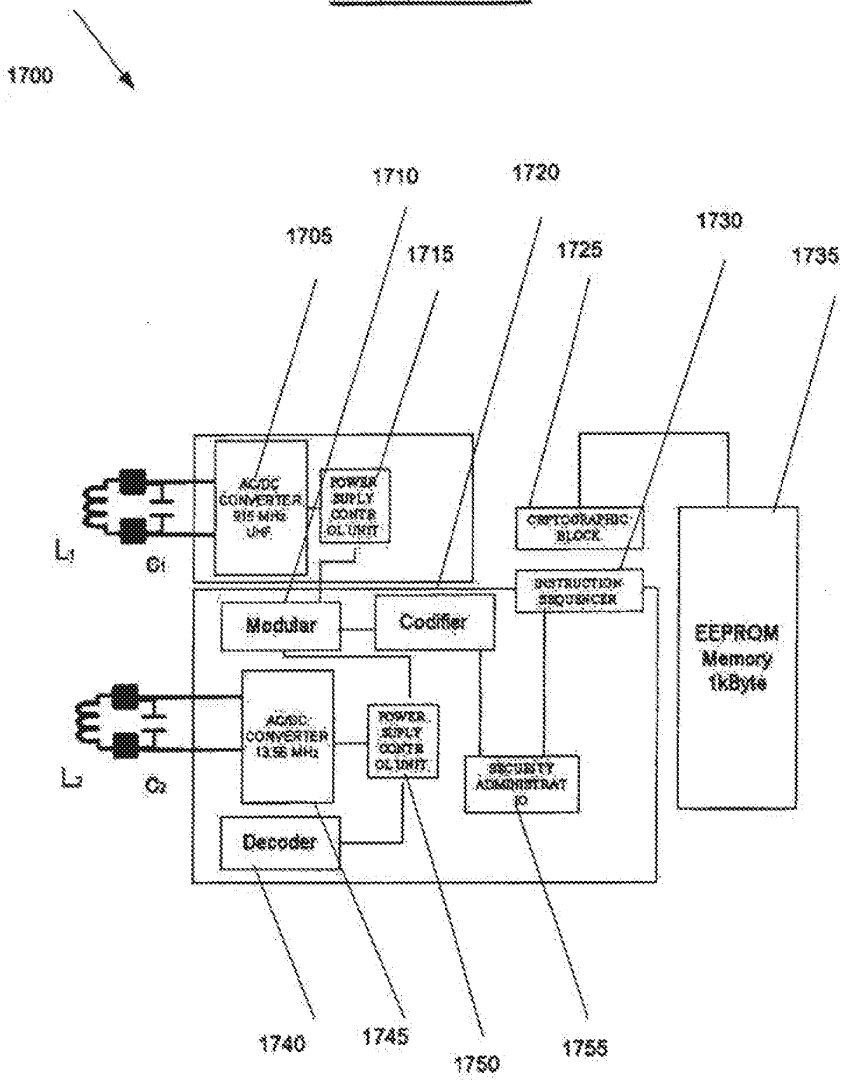

1700
1710
1720
1705
1715
1725
1730
1735
AC/DC CONVERTER
POWER SUPPLY CONTR OL UNIT
CRYPTOGRAPHIC BLOCK
INSTRUCTION SEQUENCER
Modulator
Codifier
EEPROM Memory 1kByte
AC/DC CONVERTER
POWER SUPPLY CONTR OL UNIT
SECURITY ADMINISTRAT IO
Decoder
1740
1745
1750
1755

FIGURE 18

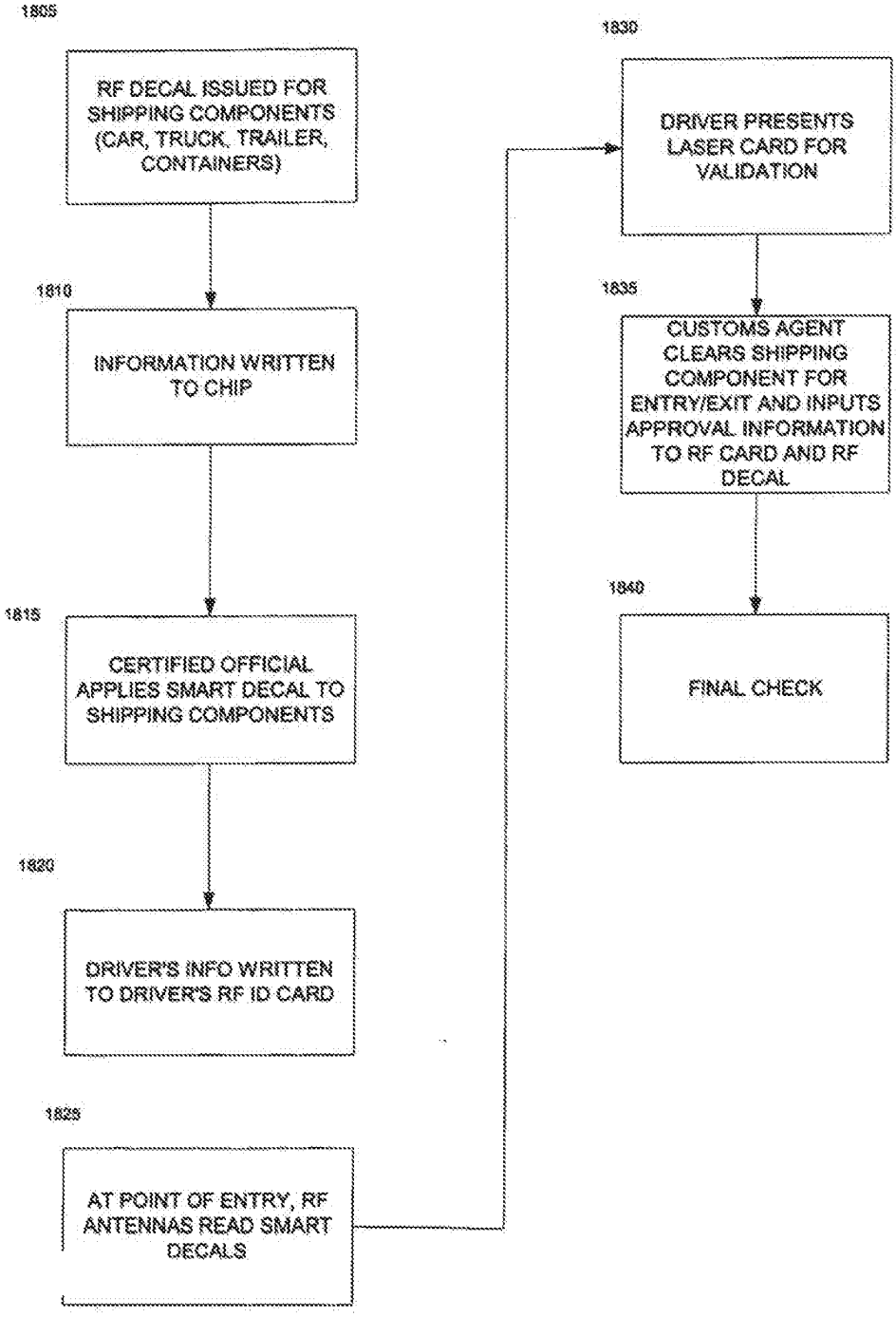

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS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

FIGURE 19

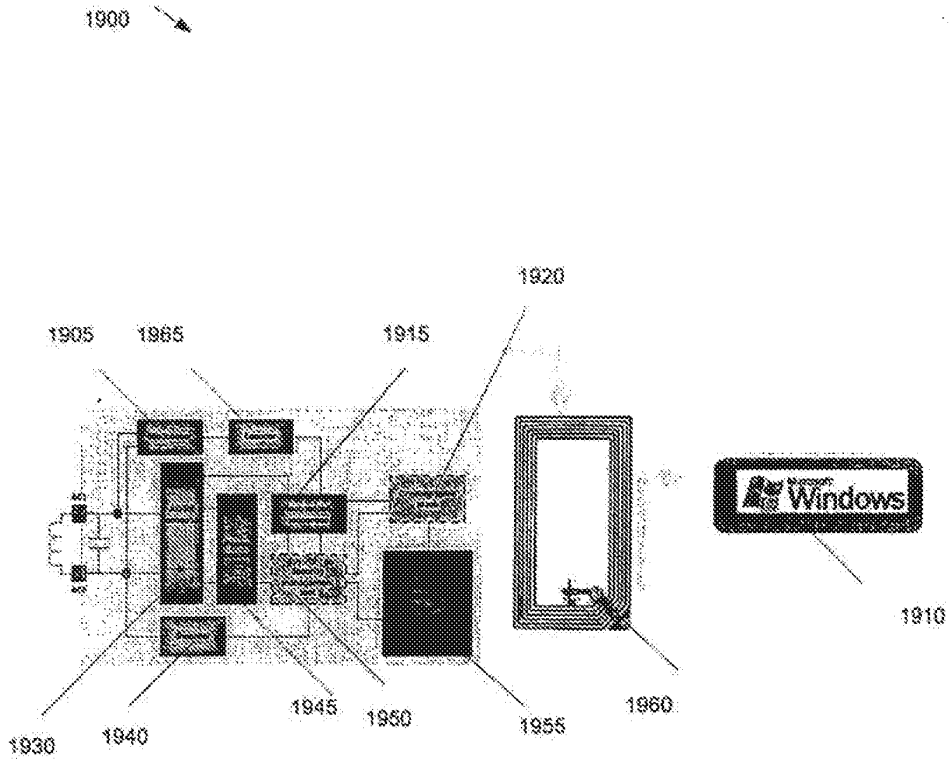
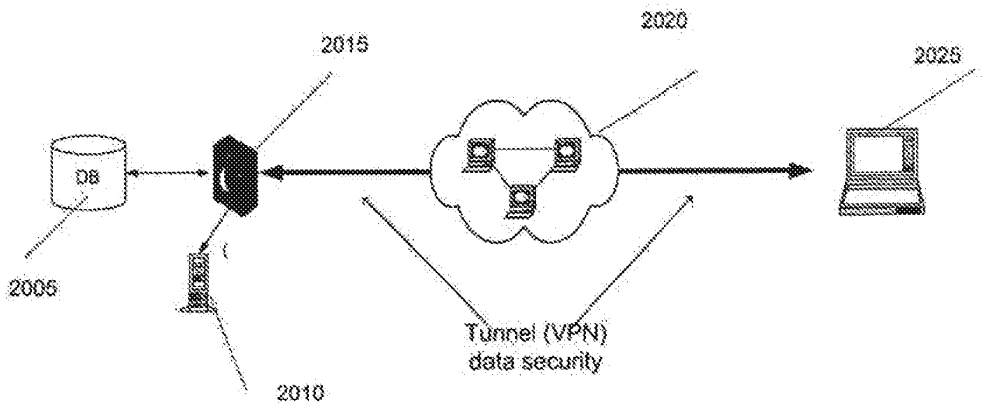

1900
1920
1905
1965
1915
Windows
1910
1930
1940
1945
1950
1955
1960

FIGURE 20



2100

FIGURE 21

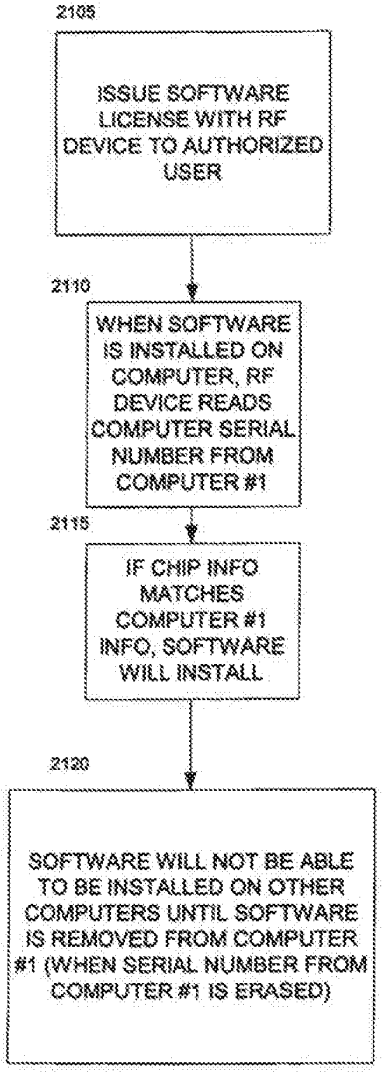


FIGURE 22

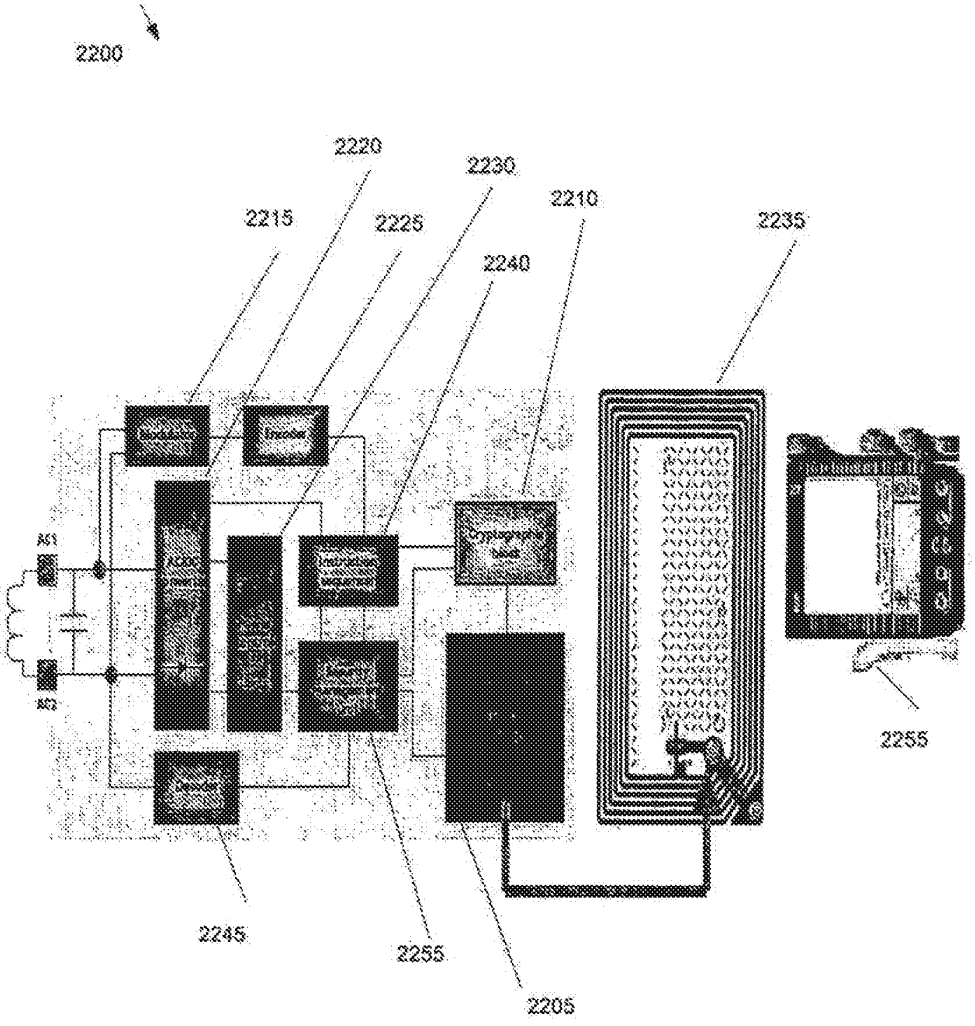
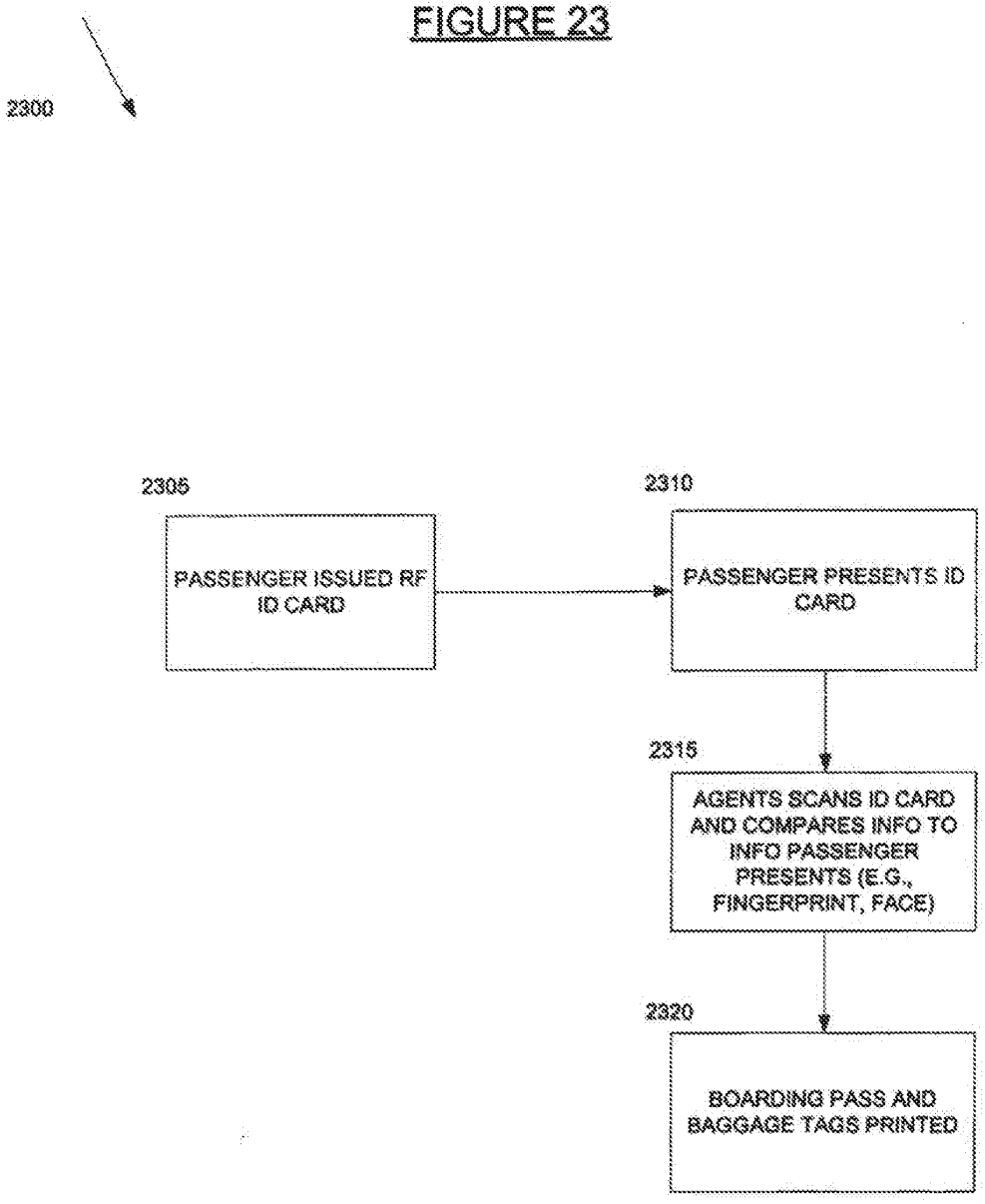


FIGURE 23


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

INTERNATIONAL SEARCH REPORT

Internat slication No
PCT/IB 03/03702

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

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, IBM-TDB, INSPEC, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

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

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

☒ Patent family members are listed in annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

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

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

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

INTERNATIONAL SEARCH REPORT

Inte l application No.
PCT/IB 03/03702

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

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

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

2. ☒ Claims Nos.: 3-48
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

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

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

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 3-48

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

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

INTERNATIONAL SEARCH REPORT

Interna plication No
PCT/IB 03/03702

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

Form PCT/ISA/210 (patent family annex) (July 1992)

Espacenet

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

NON-CONTACT DATA CARRIER AND BOOKLET THEREWITH

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

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

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

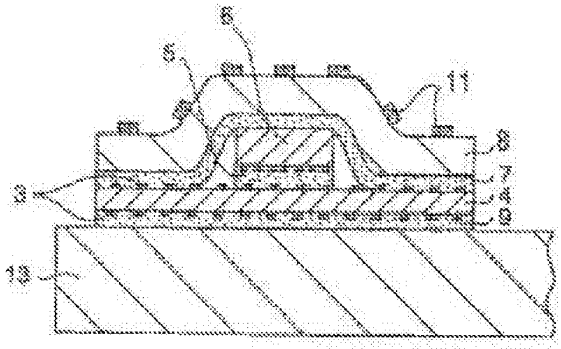
- cooperative:

Application number: JP20000220335 20000721 Global Dossier

Priority number(s): JP20000220335 20000721

Abstract of JP2002042076 (A)

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


6
5
11
8
7
4
2
3
13

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

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

審査請求　未請求　請求項の数12　ＯＬ　（全７頁）　最終頁に続く

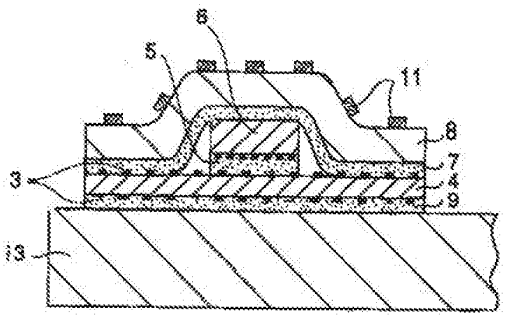
(21)出願番号　特願2000－220335(Ｐ2000－220335)
(22)出願日　平成12年７月21日(2000.7.21)

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

Ｆターム(参考)　2C005 HA01 HB02 HB09 JA20 KA06
KA37 KB05 LB20 MA01 MA10
MB01 MB06 NA09 PA01 PA14
PA18
3E040 AA07 BA07 BA16 CB01 FK05
5B035 BA03 BB09 CA01 CA23

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

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



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

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

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

【０００７】

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

【０００８】

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

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

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

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

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

【００１３】

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

【００２８】

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

【図面の簡単な説明】

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

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

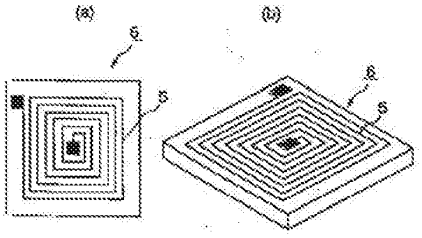
【図３】図２（ａ）のＡ－Ａ線断面図である。

【図４】本発明の非接触型データキャリアを有する冊子の一部断面図である。

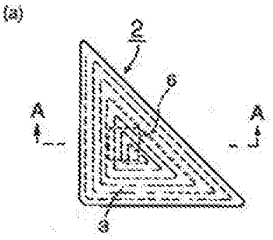
【図５】本発明の非接触型データキャリアを有する冊子の裏表紙を開いた状態を示す斜視図である。

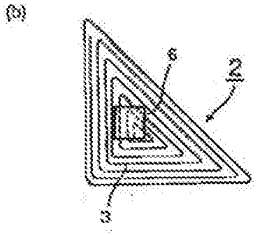
【図6】本発明の非接触型データキャリアを有する冊子の裏表紙を開いた後、本文用紙の一部をめくった状態を示す斜視図である。
【図7】本発明の非接触型データキャリアを有する冊子を閉じた状態を示す平面図である。
【図8】（a）、（b）は、それぞれ異なる形状の非接触型データキャリアを貼付する位置を示すマークが印刷されている冊子の一部切り欠き平面図である。
【符号の説明】
1　冊子
2　非接触型データキャリア
3　第1のコイルアンテナ
4　第1の基材シート
5　第2のコイルアンテナ
6　非接触型ICチップ
7　接着層
8　第2の基材シート
9　接着剤層
10　剥離紙
11　地紋印刷
12　表表紙
13　裏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

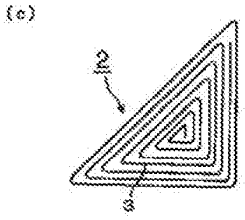
【図1】



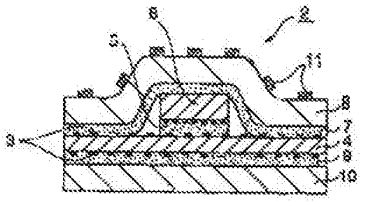
【図2】



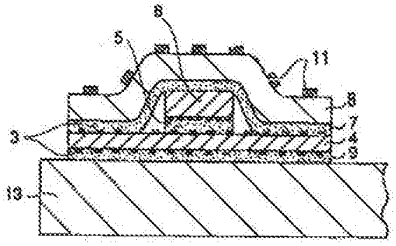




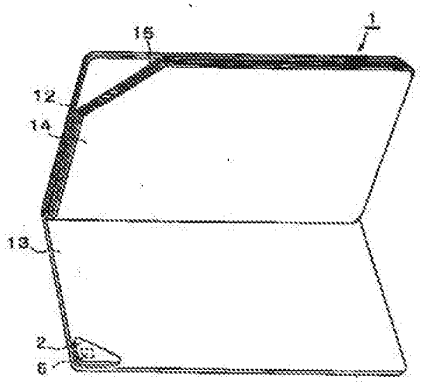
【図3】



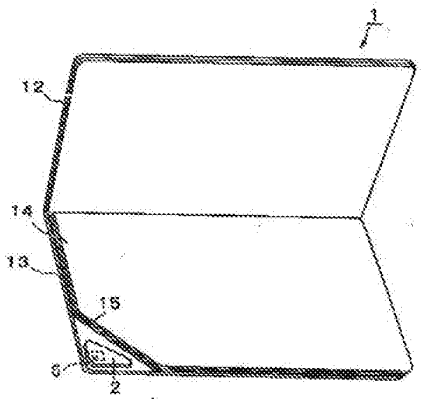
【図4】



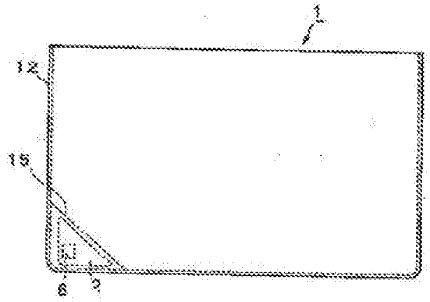
【図5】



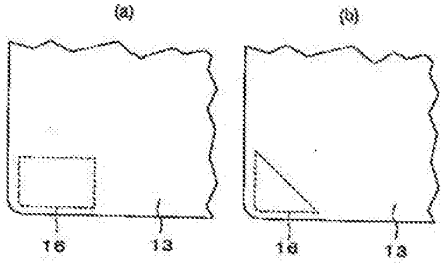
【図6】



【図7】



【図8】



フロントページの続き

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

Espacenet

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

Verfahren und Vorrichtung zur Echtheitskontrolle von Dokumenten in Form von Chipkarten

Inventor(s):

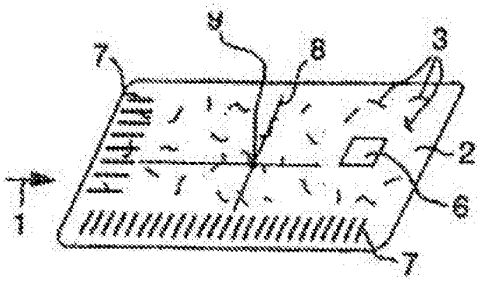
Applicant(s): BROSOW JOERGEN [AT] + (BROSOW, JOERGEN, HOF, AT)

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

Application number: DE1996108757 19960306

Priority number(s): DE1996108757 19960306 ; DE1996108233 19960304

Abstract of DE19608757 (A1)



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

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

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

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

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

DE 196 08 757 A 1

(30) Innere Priorität:
196 08 333.1 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

Beschreibung

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

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

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

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

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

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

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

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

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

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

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

Patentansprüche

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

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

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

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

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

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

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

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

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

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 198 08 757 A1
Int. Cl.⁶: G 07 D 7/00
Offenlegungstag: 11. September 1997

Fig. 1

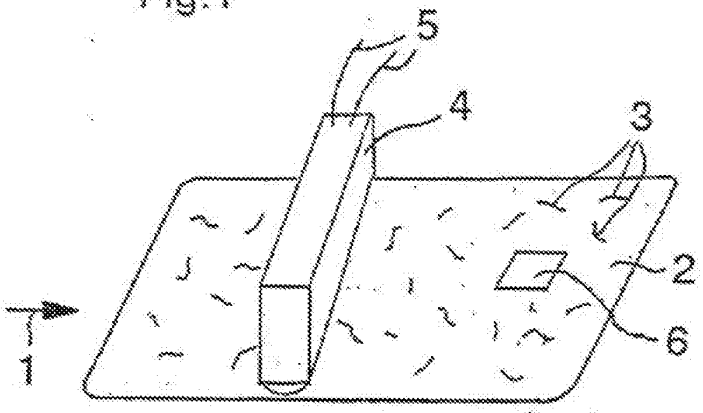
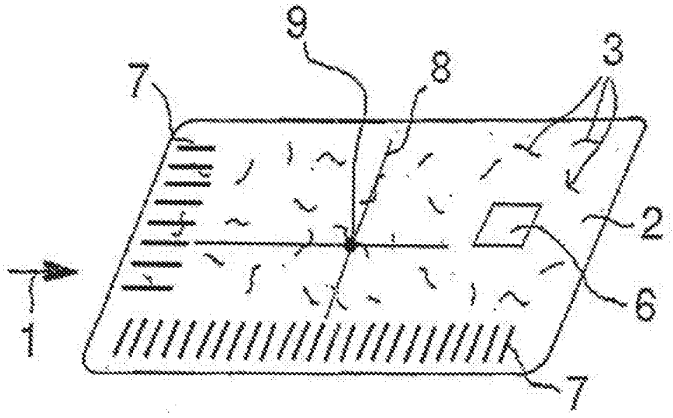


Fig. 2



Espacenet

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

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

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

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

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

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

Application number: DE2000142805 20000830

Priority number(s): DE2000142805 20000830

Abstract of DE10042805 (A1)

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

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

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

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

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

DE 100 42 805 A 1

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

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

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

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

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

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

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

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

DE 100 42 805 A 1

Beschreibung

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

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

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

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

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

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

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

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

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

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

1) Transponder

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

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

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

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

[0014] Weitere Vorteile von Transpondern sind:

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

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

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

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

1a) Befestigungsort Transponder

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

Bootslänge:

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

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

1b) Datenspeicher des Transponders

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

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

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

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

1c) Sende-/Empfangseinrichtung des Transponders

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

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

2) Lesegerät

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

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

3) Transponderpass

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

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

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

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

4) Registrierung und Markierung von Booten

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

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

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

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

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

5) Diebstahlmeldung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[0051] Derartige Interessenten sind in **Fig.** 2 als zentrale Datenbank (DB), Exekutive bzw. Zentrale der Wasserschutzpolizei (Ux), 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

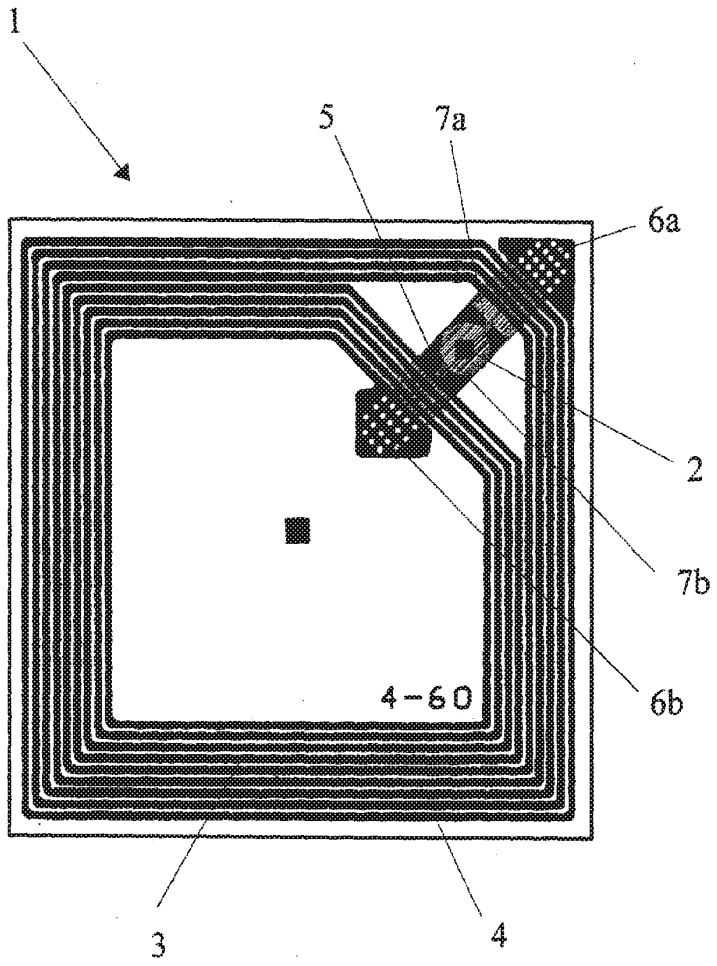


FIG. 1

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

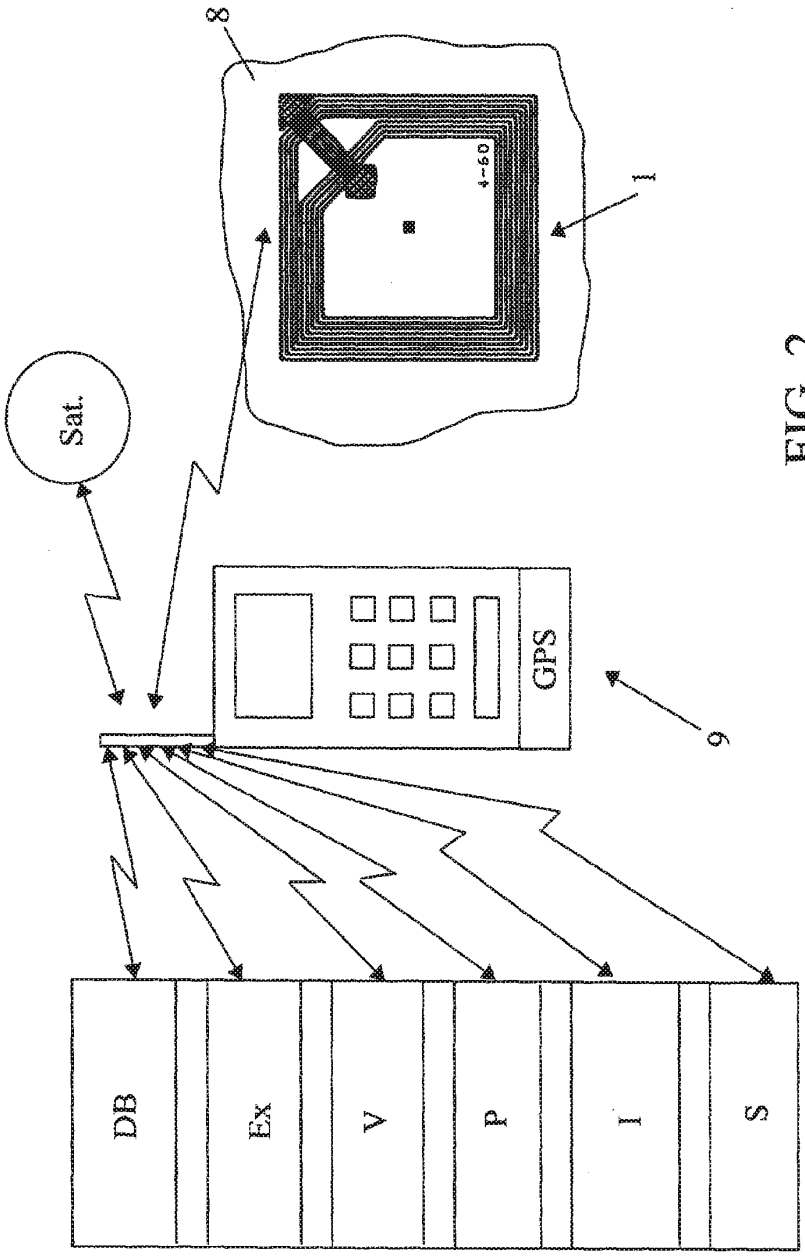


FIG. 2

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

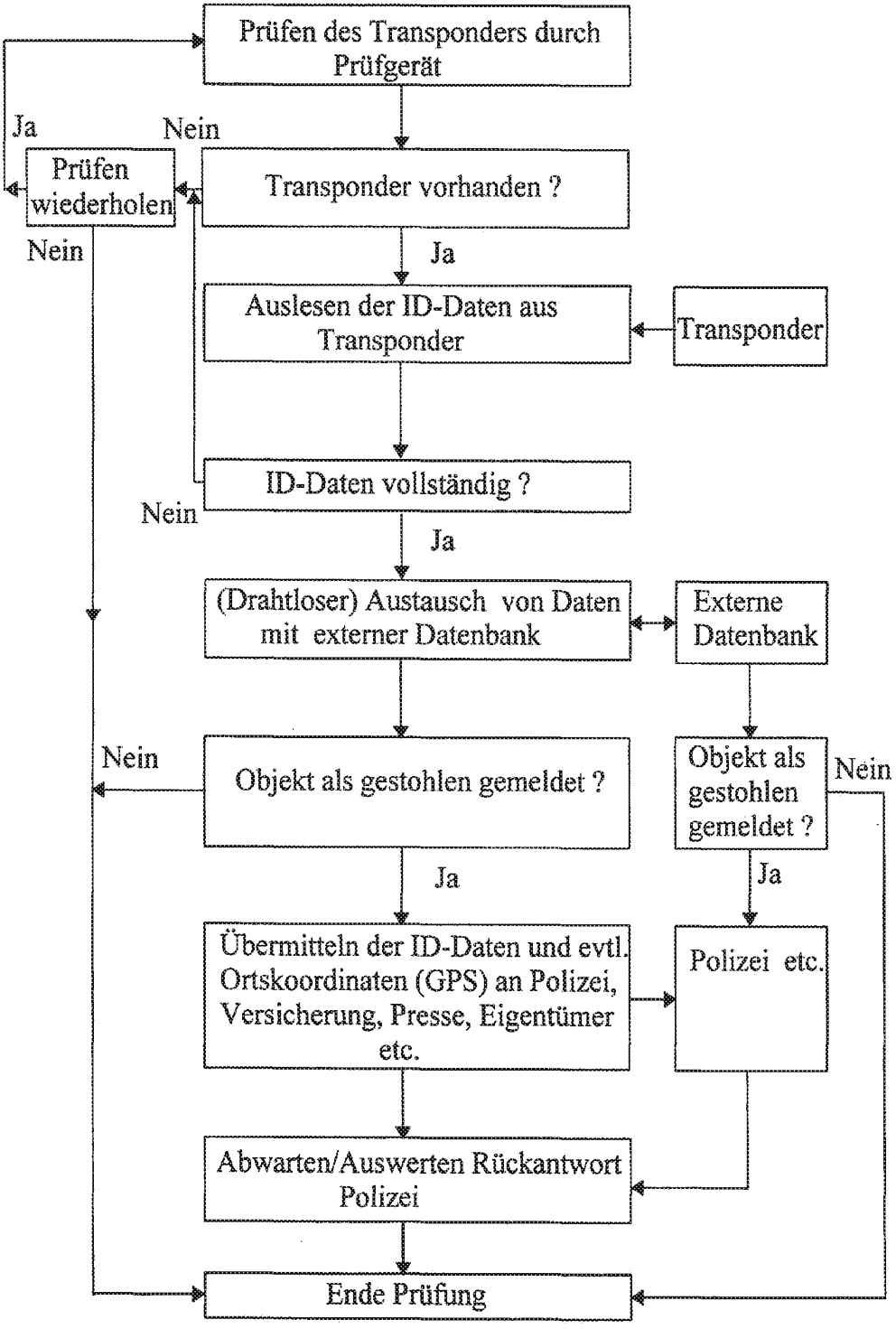


FIG. 3

101 710/436

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G01S

A2

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

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

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

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

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

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

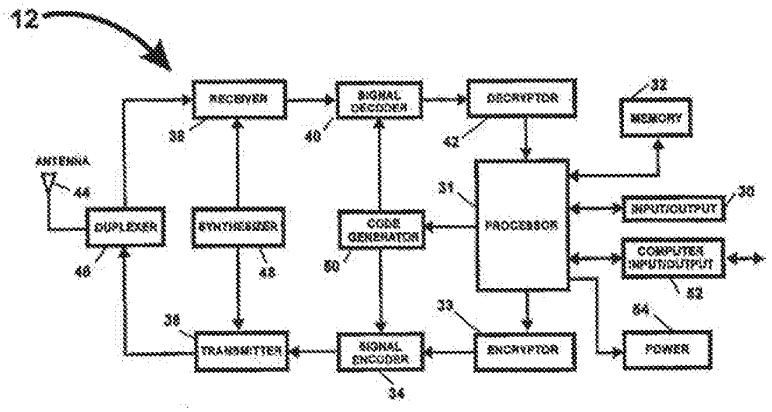
(72) Inventor: CLEVELAND, Joseph, Robert; 911 Grinnell Drive, Richardson, TX 75081 (US).

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

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

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

(54) Title: VEHICLE IDENTIFICATION SYSTEM



(57) Abstract

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

FOR THE PURPOSES OF INFORMATION ONLY

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

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

VEHICLE IDENTIFICATION SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

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

2. Description of Related Art

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

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

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

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

SUMMARY OF THE INVENTION

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

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

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

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

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

BRIEF DESCRIPTION OF THE DRAWINGS

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

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

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

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

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

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

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

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

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

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

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

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

DESCRIPTION OF THE PREFERRED EMBODIMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CLAIMS:

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

an interrogator for sending an interrogation signal;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

32. A vehicle identification tag comprising:

a memory for storing information;

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

a power supply for providing power to said transceiver.

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

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

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

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

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

37. A method for identifying mobile vehicles, comprising:

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

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

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

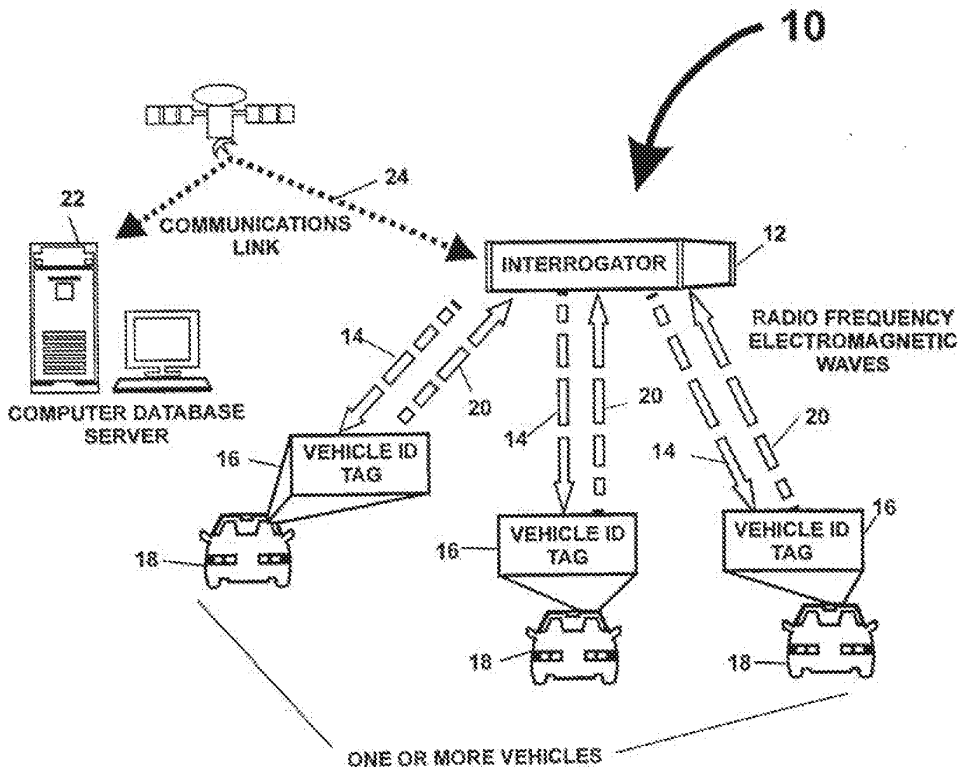

10
22
24
COMMUNICATIONS LINK
INTERROGATOR
12
RADIO FREQUENCY ELECTROMAGNETIC WAVES
14
20
COMPUTER DATABASE SERVER
VEHICLE ID TAG
16
18
ONE OR MORE VEHICLES

Figure 1

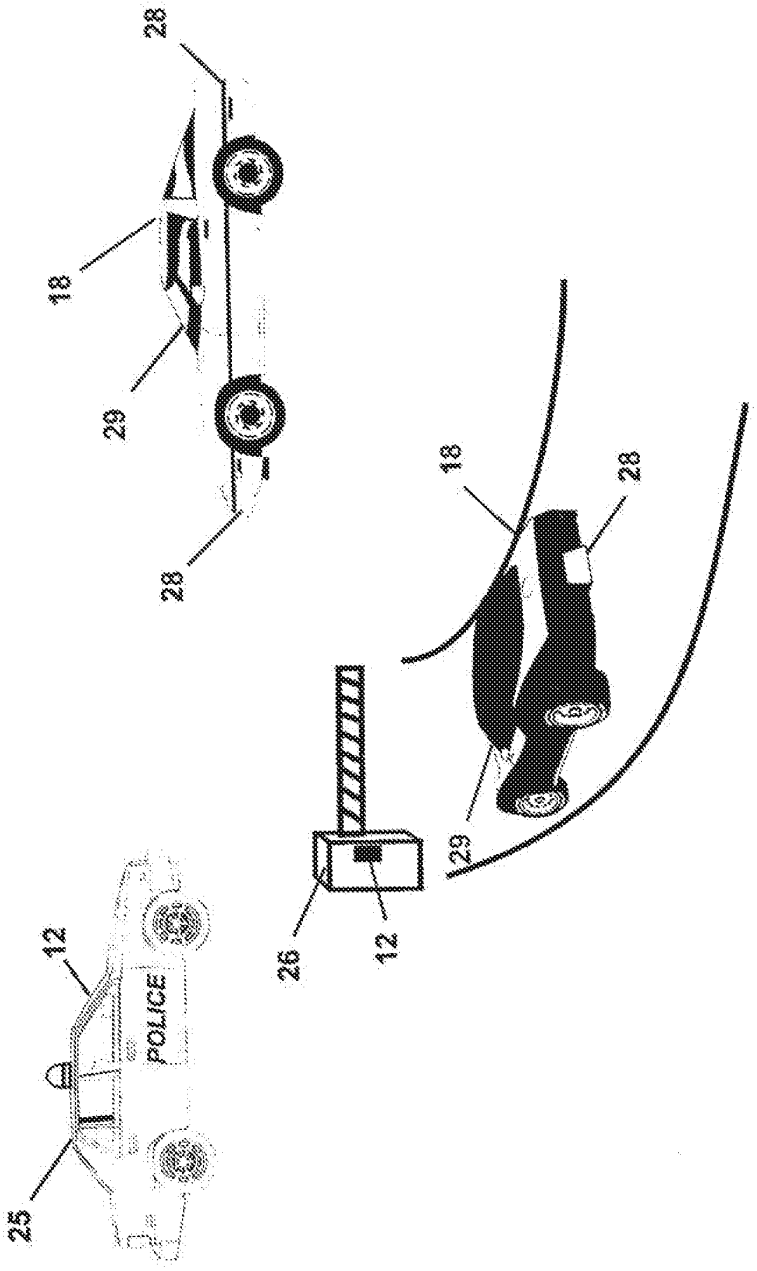


Figure 2

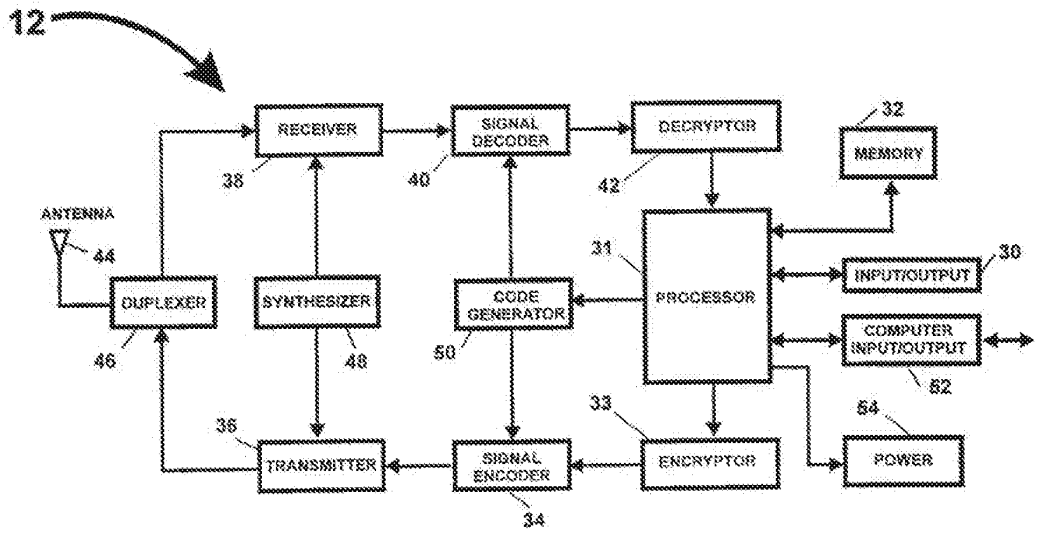

12
RECEIVER
SIGNAL DECODER
DECRYPTOR
MEMORY
32
38
40
42
ANTENNA
44
DUPLEXER
SYNTHESIZER
CODE GENERATOR
PROCESSOR
INPUT/OUTPUT
30
31
COMPUTER INPUT/OUTPUT
46
48
50
52
33
54
36
TRANSMITTER
SIGNAL ENCODER
ENCRYPTOR
POWER
34

Figure 3

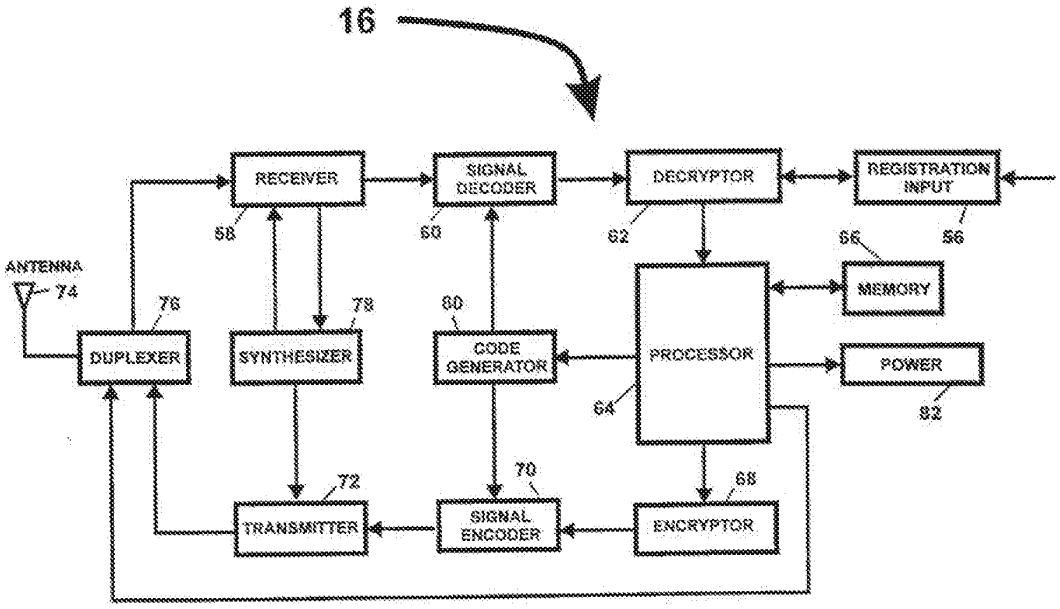

16
RECEIVER
SIGNAL DECODER
DECRYPTOR
REGISTRATION INPUT
58
60
62
56
56
ANTENNA
74
MEMORY
76
78
80
DUPLEXER
SYNTHESIZER
CODE GENERATOR
PROCESSOR
POWER
64
82
72
70
68
TRANSMITTER
SIGNAL ENCODER
ENCRYPTOR

Figure 4

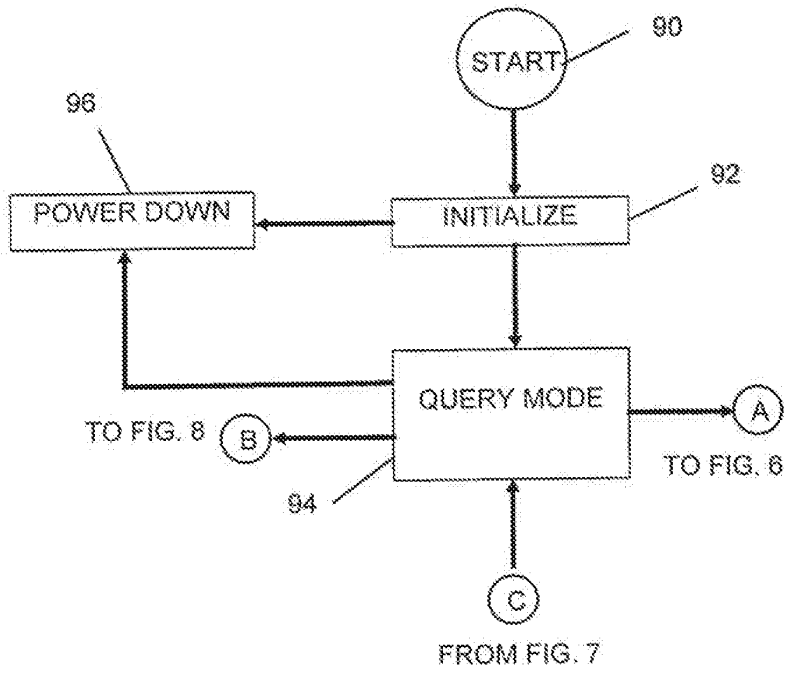

START
90
96
92
POWER DOWN
INITIALIZE
QUERY MODE
TO FIG. 8
B
A
TO FIG. 6
94
C
FROM FIG. 7

Figure 5

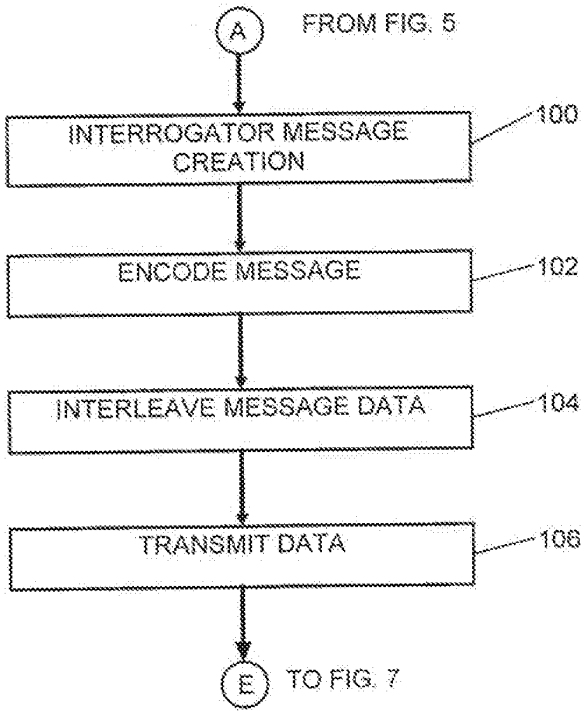

A
FROM FIG. 5
INTERROGATOR MESSAGE CREATION
100
ENCODE MESSAGE
102
INTERLEAVE MESSAGE DATA
104
TRANSMIT DATA
106
E
TO FIG. 7

Figure 6

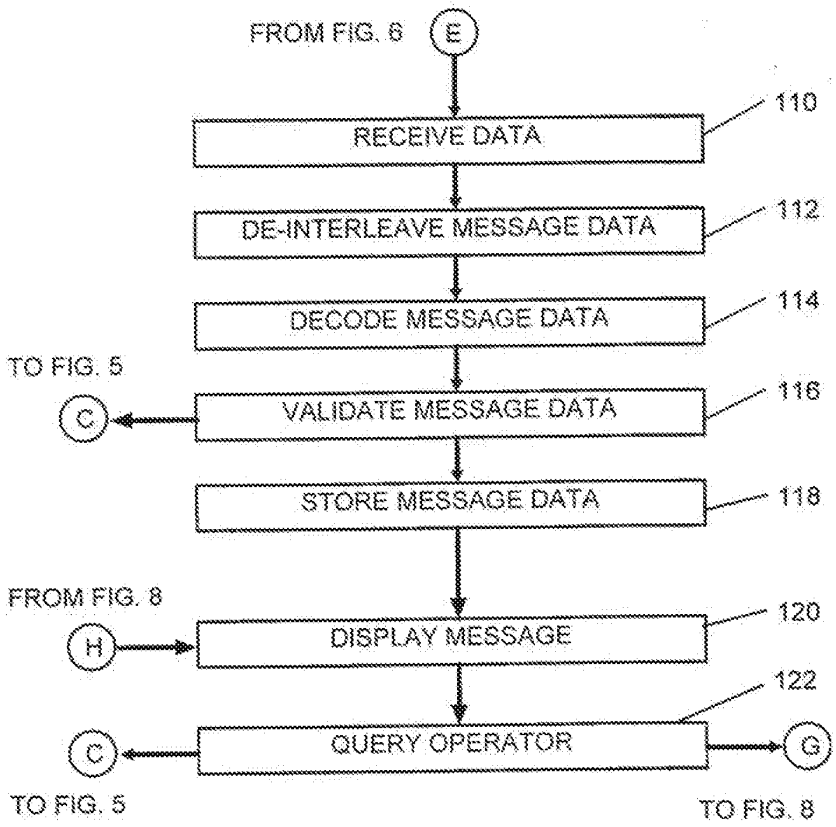

FROM FIG. 6
E
RECEIVE DATA
110
DE-INTERLEAVE MESSAGE DATA
112
DECODE MESSAGE DATA
114
TO FIG. 5
C
VALIDATE MESSAGE DATA
116
STORE MESSAGE DATA
118
FROM FIG. 8
H
DISPLAY MESSAGE
120
122
C
QUERY OPERATOR
G
TO FIG. 5
TO FIG. 8

Figure 7

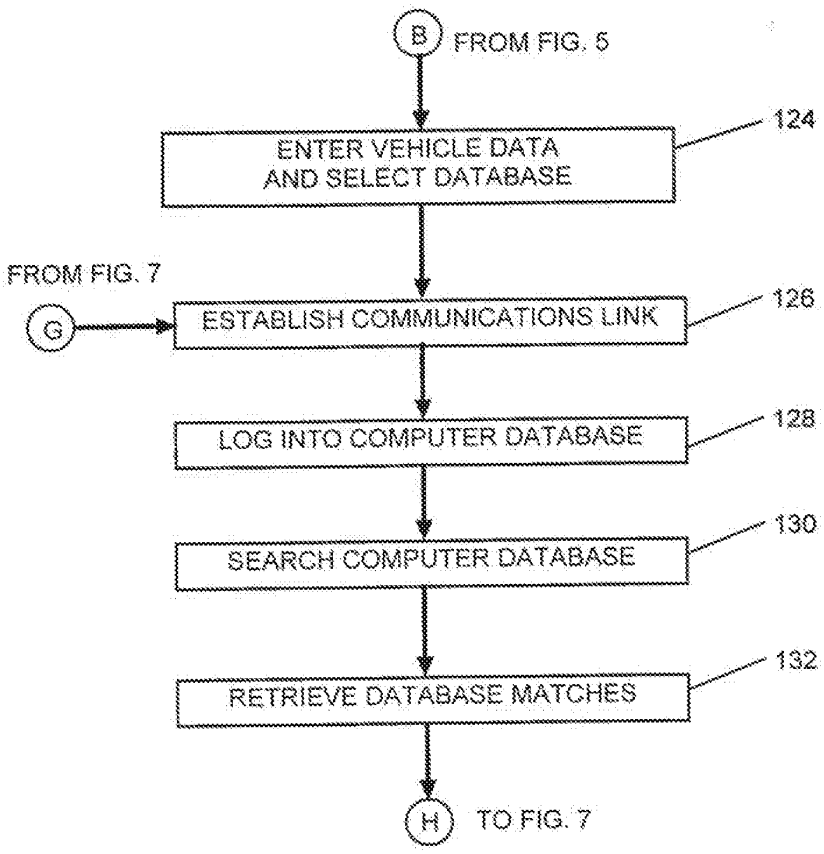

B
FROM FIG. 5
ENTER VEHICLE DATA AND SELECT DATABASE
124
FROM FIG. 7
G
ESTABLISH COMMUNICATIONS LINK
126
LOG INTO COMPUTER DATABASE
128
SEARCH COMPUTER DATABASE
130
RETRIEVE DATABASE MATCHES
132
H
TO FIG. 7

Figure 8

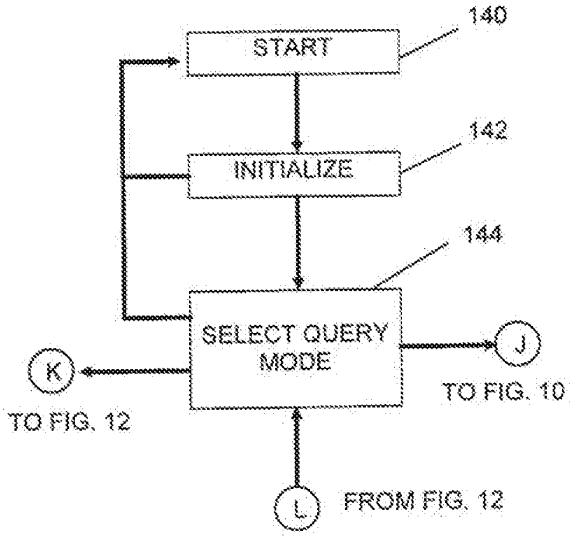

140
START
142
INITIALIZE
144
SELECT QUERY MODE
J
TO FIG. 10
K
TO FIG. 12
L
FROM FIG. 12

Figure 9

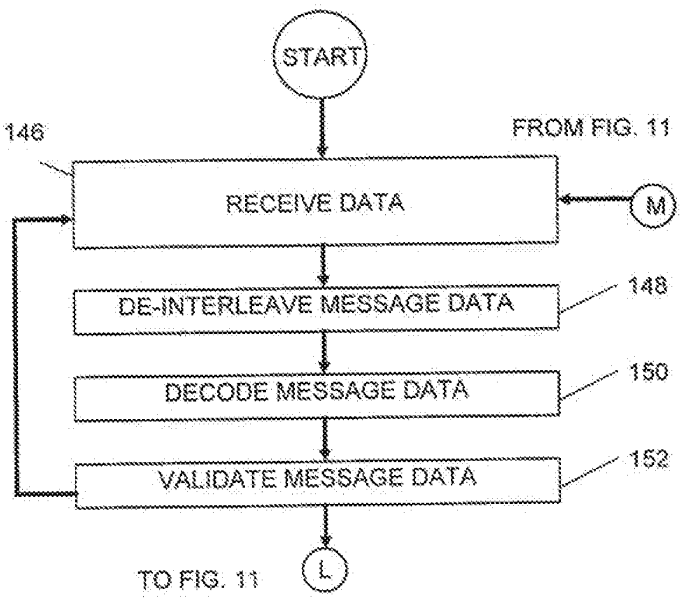

START
146
FROM FIG. 11
RECEIVE DATA
M
DE-INTERLEAVE MESSAGE DATA
148
DECODE MESSAGE DATA
150
VALIDATE MESSAGE DATA
152
TO FIG. 11
L

Figure 10

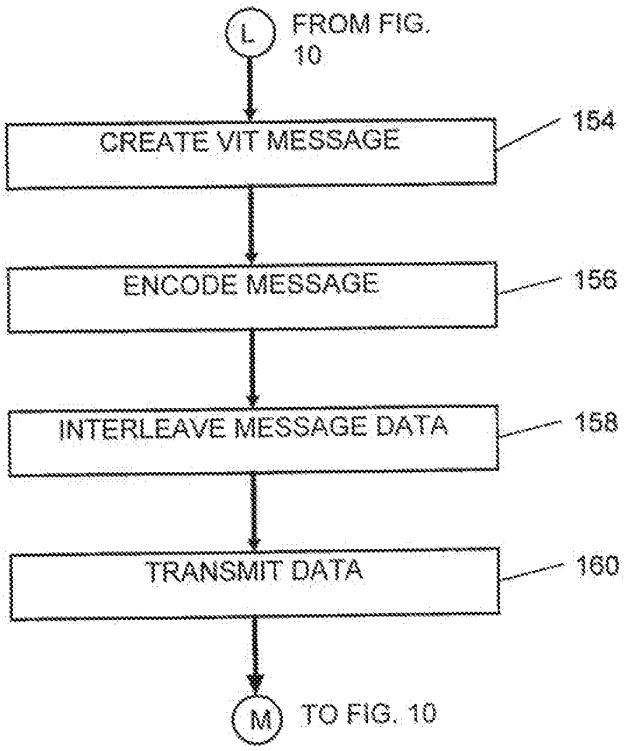

L
FROM FIG. 10
CREATE VIT MESSAGE
154
ENCODE MESSAGE
156
INTERLEAVE MESSAGE DATA
158
TRANSMIT DATA
160
M
TO FIG. 10

Figure 11

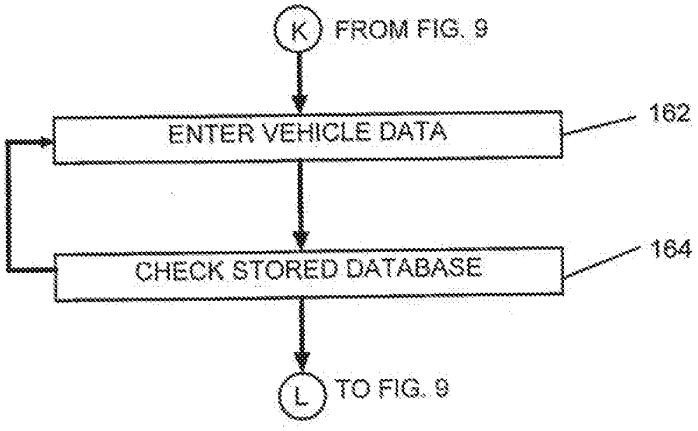

K
FROM FIG. 9
ENTER VEHICLE DATA
162
CHECK STORED DATABASE
164
L
TO FIG. 9

Figure 12

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

(11) EP 0 993 999 A2

(12) EUROPEAN PATENT APPLICATION

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

(51) Int Cl.7: **B60R 25/04**

(21) Application number: **99305339.6**

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

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

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

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

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

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

(54) Fuel pump immobilization

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

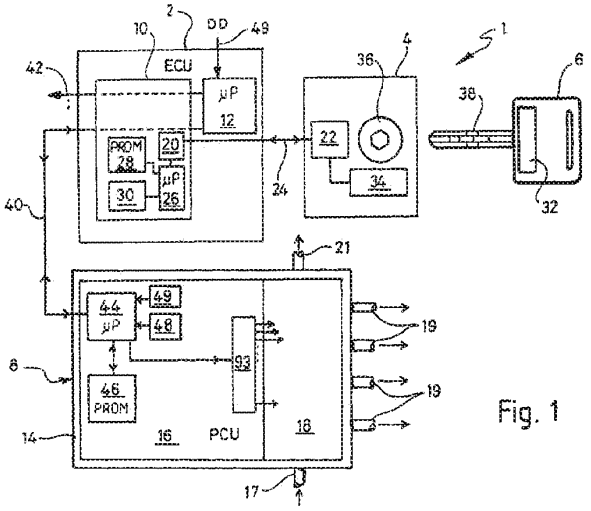


Fig. 1

EP 0 993 999 A2

Printed by Jouve, 75001 PARIS (FR)

Description

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

46.

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

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

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

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

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

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

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

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

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

Claims

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

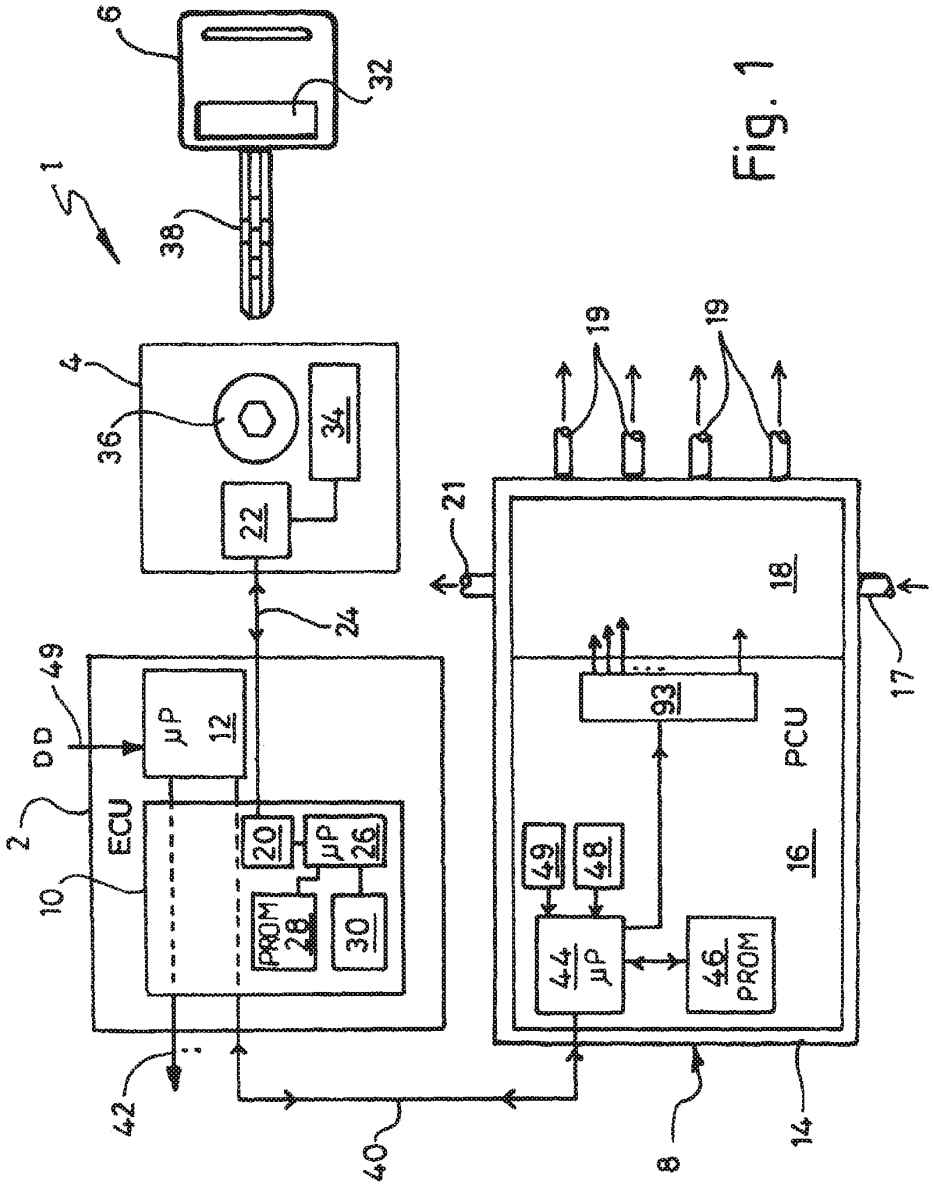

6
32
1
38
4
36
34
22
24
49
DD
2
ECU
μP
12
10
20
μP
26
PROM
28
30
42
40
8
14
21
19
19
18
17
93
PCU
16
49
48
44
μP
46
PROM

Fig. 1

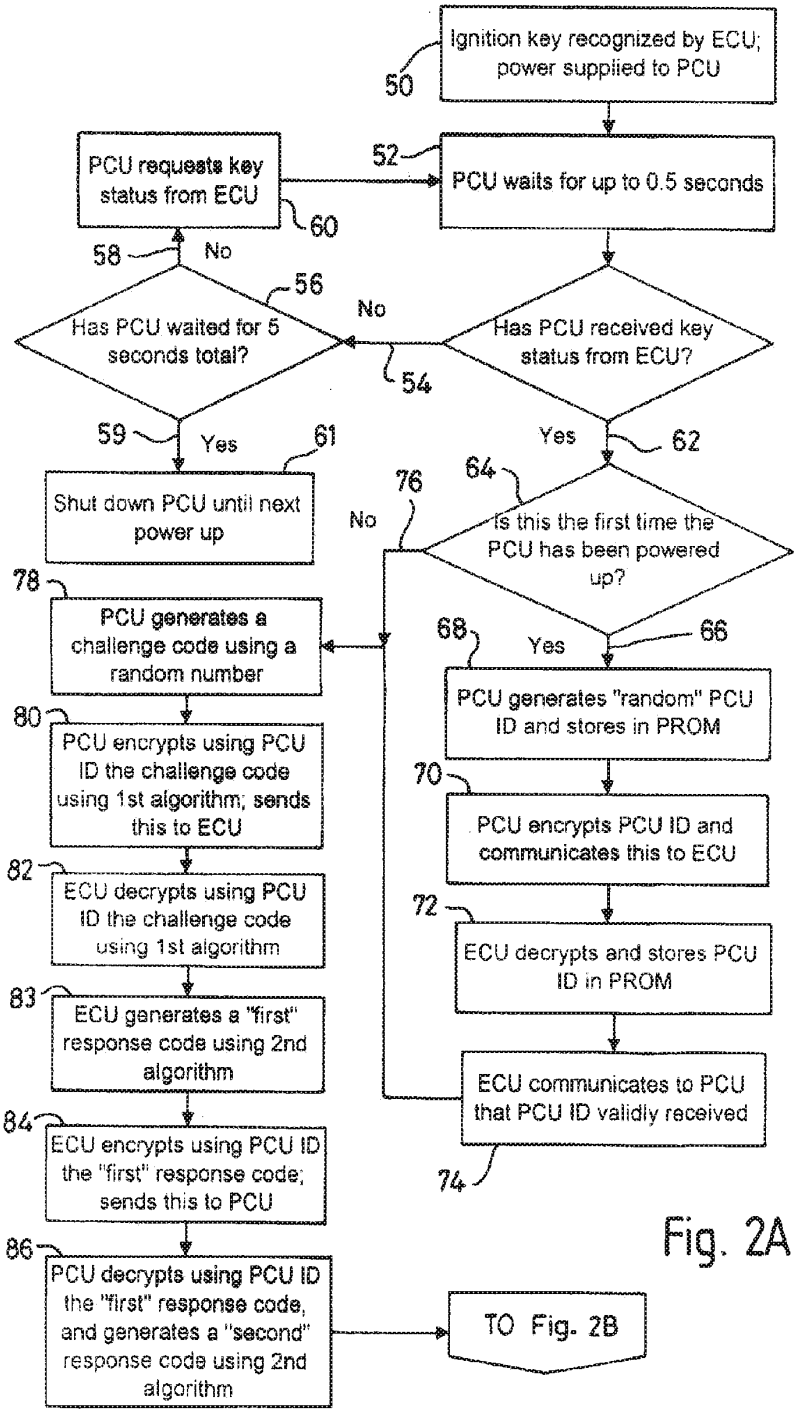

Ignition key recognized by ECU; power supplied to PCU
50
PCU requests key status from ECU
60
52
PCU waits for up to 0.5 seconds
58
No
56
Has PCU waited for 5 seconds total?
No
54
Has PCU received key status from ECU?
59
Yes
61
Yes
62
Shut down PCU until next power up
64
76
No
Is this the first time the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

Fig. 2A

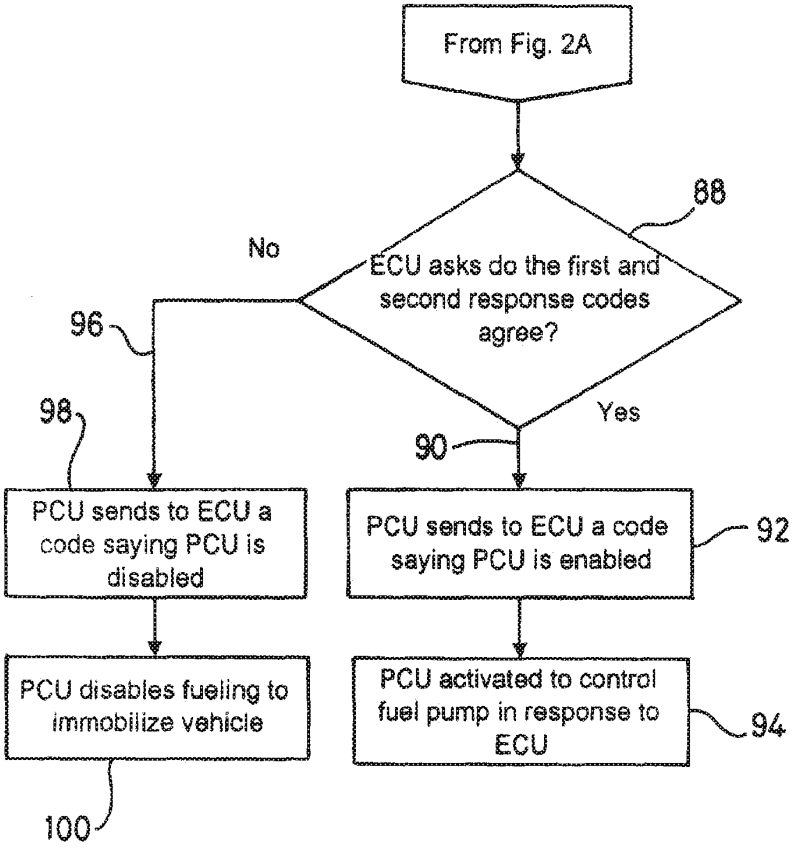

From Fig. 2A
88
ECU asks do the first and second response codes agree?
No
Yes
96
98
90
PCU sends to ECU a code saying PCU is disabled
PCU sends to ECU a code saying PCU is enabled
92
PCU disables fueling to immobilize vehicle
PCU activated to control fuel pump in response to ECU
94
100

Fig. 2B

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

(11) EP 0 977 145 A2

(12) EUROPEAN PATENT APPLICATION

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

(51) Int Cl.7: G06K 19/077

(21) Application number: 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 33693498
24.02.1999 JP 4639299

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

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

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

(54) Radio IC card

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

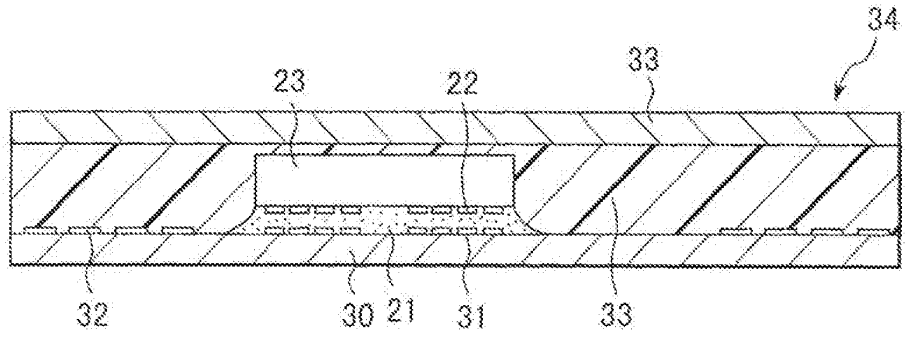


FIG. 14

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 ○ 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

$$v = -d\Phi/dt \qquad (6)$$

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

$$v = \mu \cdot S \cdot dH/dt \qquad (8)$$

[0199] An example of calculation of induction electromotive force v is shown below. Since the cavity 43 is located within the power supply coil 42, the permeability of air is approximated on the basis of that of vacuum as follows:

$$\mu = 1.25 \times 10^{-6} \text{ [H/m]} \qquad (9)$$

[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

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

[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

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

[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 line 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.

[0364] Accordingly, exchange of a cell is not required, and power consumption in the standby state of the reader/writer can be reduced to achieve energy saving. Thus, the radio IC card with simple structure can be manufactured. For example, compared to the cell-built-in type radio IC card, the energy saving ratio of power supply is 100% and no waste cell is produced.

Claims

1. A radio IC card for data communication with outside, characterized by comprising:

   a board (30) having at least two rectangular-spiral antennas (31, 32) formed thereon; and
   a semiconductor element (23) having a rectangular-spiral antenna (22) formed on a surface thereof, the semiconductor element being mounted on the board such that the antenna (22) on the semiconductor element is situated opposed to one (31) of said at least two antennas on the board (30).

2. A radio IC card according to claim 1, characterized in that said antenna (23) on the semiconductor element is formed by bonding a piece of bonding wire (27) among a plurality of electrode pads (26) formed on the surface of the semiconductor element.

3. A radio IC card according to claim 1, characterized in that the antenna (22) on the semiconductor element is formed of a metallic film.

4. A radio IC card according to claim 1, characterized in that a layer of the antenna (22) formed of a metallic film and a layer of an insulating film (21) are laminated on the surface of the semiconductor element.

5. A radio IC card according to claim 1, characterized in that said antenna (22) is provided on each of upper and lower surfaces of the semiconductor element (23).

6. A radio IC card according to claim 1, characterized in that said semiconductor element (23) is provided with a layer for formation of an electric element (29).

7. A radio IC card according to claim 1, characterized in that one (31) of the antennas formed on the board (30) has substantially the same shape as the antenna (22) formed on the semiconductor element, and the other (32) of the antennas on the board is greater in size than said one (31) of the antennas on the board.

8. A radio IC card according to claim 1, characterized in that one (31) of the antennas on the board and the other (32) of the antennas on the board are electrically connected.

9. A radio IC card according to claim 1, characterized in that one (31) of the antennas on the board and the antenna (22) on the semiconductor device are electromagnetically connected.

10. A radio IC card according to claim 1, characterized in that said antenna (22) is formed over the semiconductor element (23), with an insulating film (21) interposed.

11. A radio IC card according to claim 1, characterized in that said antenna (22) is formed over the semiconductor element (23), with a magnetic film interposed.

12. A radio IC card according to claim 1, characterized in that an insulating film (21) is formed on each of the antennas (31, 32) on the board.

13. A radio IC card according to claim 1, characterized in that an insulating film (21), in which magnetic particles are dispersed, is formed on each of the antennas (31, 32) on the board.

14. A radio IC card according to claim 1, characterized in that said semiconductor element (23) and said substrate (30) are integrally sealed with resin (25).

15. A method of manufacturing a radio IC card for data communication with outside, the method characterized by comprising the steps of:

forming a rectangular-spiral antenna (22) on a surface of a semiconductor element (23);
forming at least two rectangular-spiral antennas (31, 32) on a board (30); and
disposing the antenna (22) formed on the semiconductor element such that the antenna formed on the semiconductor element is opposed to one (31) of said antennas formed on the board.

16. A method of manufacturing a radio IC card, according to claim 15, characterized in that the antenna (22) on the surface of the semiconductor element is formed by a thin-film patterning process.

17. A method of manufacturing a radio IC card, according to claim 15, characterized in that the antenna (22) on the surface of the semiconductor element is formed by a printing process.

18. A method of manufacturing a radio IC card, according to claim 15, characterized in that the antenna (22) on the surface of the semiconductor element is formed such that a plurality of electrode pads (26) are provided on the surface of the semiconductor element and the electrode pads are connected by means of wire bonding.

19. A method of manufacturing a radio IC card, according to claim 15, characterized in that said at least two antennas (31, 32) on the board are integrally formed.

20. A method of manufacturing a radio IC card, according to claim 15, characterized in that the method includes a step of integrally sealing the semiconductor element (23) and the board (30) with resin (25).

21. A radio IC card having at least one rectangular-spiral antenna (42) and one semiconductor element (23) mounted thereon, characterized in that a cavity portion (43) is provided near the antenna and a permanent magnet (44) is movably provided within the cavity portion.

22. A radio IC card according to claim 21, characterized in that the permanent magnet (44) is movable in a direction of a central axis of the antenna (42).

23. A radio IC card according to claim 21, characterized in that the permanent magnet (44) is rotatably provided within the cavity portion (43).

24. A radio IC card according to claim 21, characterized in that the antenna (42) serves both for power supply to the semiconductor element (23) and for data communication.

25. A method of manufacturing a radio IC card for data communication with outside, the method characterized by comprising the steps of:

mounting at least one semiconductor element (23) and one rectangular-spiral antenna (41, 42) on a first casing body (40a) in which a recess portion is formed in advance;
inserting a permanent magnet (44) movably in the recess portion; and
attaching a second casing body (40b) to the first casing body provided with said at least one semiconductor element and one antenna and said permanent magnet.

26. A data reader/writer apparatus for reading/writing data from/in a radio IC card, the apparatus characterized by comprising:

a radio IC card on which at least one rectangular-spiral antenna (41, 42) and a semiconductor element (23) are mounted; and
read/write means for performing data communication with the semiconductor element mounted on the radio IC card, the read/write means having a permanent magnet (52) for inducing an electromotive force in the antenna mounted on the radio IC card by crossing a magnetic field over the antenna.

27. A radio IC card having at least one data communication antenna (41) and one semiconductor element (23) mounted thereon, characterized in that the radio IC card comprises a piezoelectric element (81) connected to the semiconductor element.

28. A radio IC card according to claim 27, characterized in that said piezoelectric element (81) is used as a board, and said at least one antenna (41) and one semiconductor element (23) are mounted on the piezoelectric element.

29. A radio IC card according to claim 27, characterized in that electrodes (92a, 92b) are provided on both sides of the piezoelectric element (91), and these electrodes are electrically connected to at least said semiconductor element (23).

30. A method of manufacturing a radio IC card for data communication with outside, the method characterized by comprising the steps of:

attaching at least one data communication antenna (41) and one semiconductor element (23) to a first casing body (80a);
attaching a piezoelectric element (81) to the first casing body (80a); and
adhering a second casing body (80b) to the first casing body (80a).

31. A method of manufacturing a radio IC card, the method characterized by comprising the steps of:

attaching at least one data communication antenna (41) and one semiconductor element (23) on a board (91) formed of a piezoelectric element; and
applying an outer coating to the board (91) on which the antenna and the semiconductor element are attached.

32. A data read/write apparatus characterized by comprising:

a radio IC card having at least one data communication antenna (41) and one semiconductor element (23) mounted thereon and including a piezoelectric element (81) connected to the semiconductor element (23); and
read/write means for performing data communication with the semiconductor element (23) by means of the antenna (41), the read/write means including a pressing mechanism (106a, 106b) for pressing the piezoelectric element (81) of the radio IC card, thereby producing an electric charge in the piezoelectric element.

33. A radio IC card for data communication with outside, characterized by comprising:

a semiconductor element (23) having a rectangular-spiral antenna (22) formed on a surface thereof;
a board (111) having at least three rectangular-spiral antennas (31, 41, 42) formed thereon such that one (31) of said at least three antennas is situated, opposed to the antenna (22) of the semiconductor element;
a cavity portion (43) provided near one (42) of the other antennas on the board; and
a permanent magnet (44) provided movably in the cavity portion.

34. A radio IC card according to claim 33, characterized in that on said board (111) there are provided:

an antenna (31) situated to be opposed to the antenna (22) on the semiconductor element (23);
a communication antenna (41) electrically connected to said antenna; and
a power supply antenna (42) electrically connected to the communication antenna (41), a magnetic flux of the permanent magnet (44) being crossed over the power supply antenna.

35. An IC card according to claim 33, characterized in that said antennas are sealed with an insulating material (113) in which magnetic particles are dispersed.

36. A method of manufacturing a radio IC card, the method characterized by comprising the steps of:

mounting at least one semiconductor element (23) and at least three rectangular-spiral antennas (31, 41, 42) on a first casing body (100a) in which a recess portion is formed in advance;
inserting a permanent magnet (44) movably in the recess portion; and
attaching a second casing body (110b) to the first casing body (110a).

37. A method of manufacturing a radio IC card according to claim 36, characterized in that the method includes the steps of:

storing the permanent magnet (44) movably in a case; and
mounting the case in the recess portion.

38. A method of manufacturing a radio IC card according to claim 36, characterized in that the first and second casing

bodies (110a, 110b) are formed of an insulating material in which magnetic particles are dispersed.

39. A radio tag for data communication with inside, characterized in that a rectangular-spiral antenna (22) is formed on a surface of a semiconductor element (23).

40. A radio tag according to claim 39, characterized in that said antenna (22) on the semiconductor element is formed by bonding a piece of bonding wire (27) among a plurality of electrode pads (26) formed on the surface of the semiconductor element.

41. A radio tag according to claim 39, characterized in that the antenna (22) on the semiconductor element is formed of a metallic film.

42. A radio tag according to claim 39, characterized in that a layer of the antenna (22) formed of a metallic film (21) and a layer of an insulating film (21) are laminated on the surface of the semiconductor element (23).

43. A radio tag according to claim 39, characterized in that said antenna (22) is provided on each of upper and lower surfaces of the semiconductor element (23).

44. A radio tag according to claim 39, characterized in that said semiconductor element (23) is provided with a layer for formation of an electric element (24).

45. A radio tag according to claim 39, characterized in that the antenna (22) is provided over the semiconductor element (23), with an insulating film (21) interposed.

46. A radio tag according to claim 39, characterized in that said antenna (22) is formed over the semiconductor element (23), with a magnetic film interposed.

47. A radio tag according to claim 39, characterized in that the antenna (22) is formed on the semiconductor element (23), with an insulating film (21) containing dispersed magnetic particles interposed.

48. A radio tag according to claim 39, characterized in that the semiconductor element (23) having the antenna (22) formed on the surface thereof is sealed with resin (25).

49. A method of manufacturing a radio tag for data communication with outside, the method characterized by comprising the steps of:

forming an insulating film (21) over a surface of a semiconductor wafer (20) on which a plurality of semiconductor elements (23) are formed;
forming rectangular-spiral antennas (22) on the insulating film at positions corresponding to the semiconductor elements; and
dicing the semiconductor elements (23) out of the semiconductor wafer (20).

50. A method of manufacturing a radio tag according to claim 49, characterized in that the antenna (22) formed on the surface of each of the semiconductor elements is formed by a thin-film patterning process.

51. A method of manufacturing a radio tag according to claim 49, characterized in that the antenna (22) formed on the surface of each of the semiconductor elements is formed by a printing process.

52. A method of manufacturing a radio tag according to claim 49, characterized in that said antenna (22) on each of the semiconductor elements is formed by bonding a piece of bonding wire among a plurality of electrode pads (26) formed on the surface of the semiconductor element.

53. A method of manufacturing a radio tag according to claim 49, characterized in that each of the semiconductor elements (23) on the surface of which the antenna is formed is sealed with resin (25).

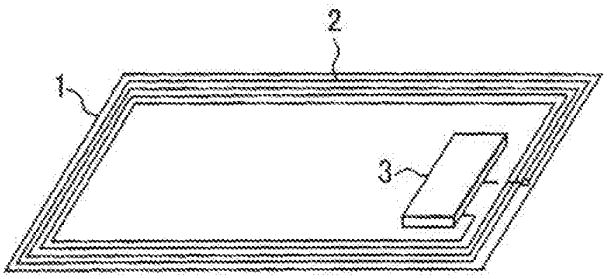


FIG. 1

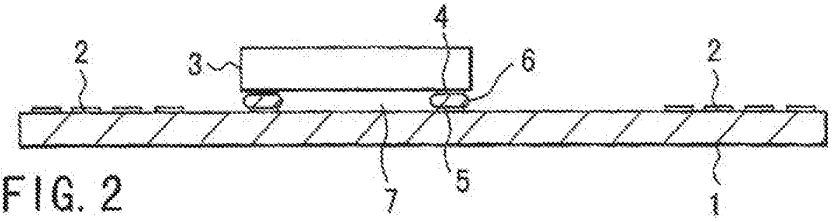


FIG. 2

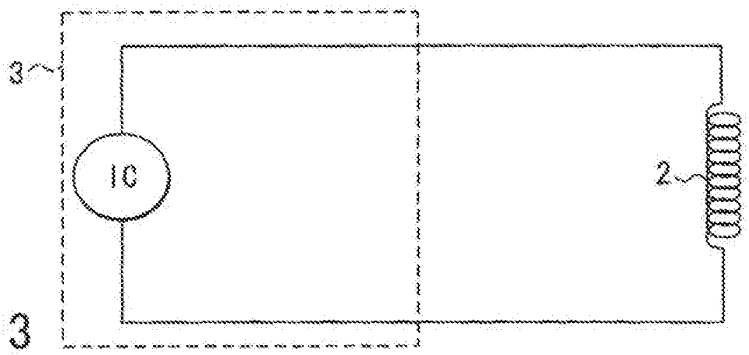


FIG. 3

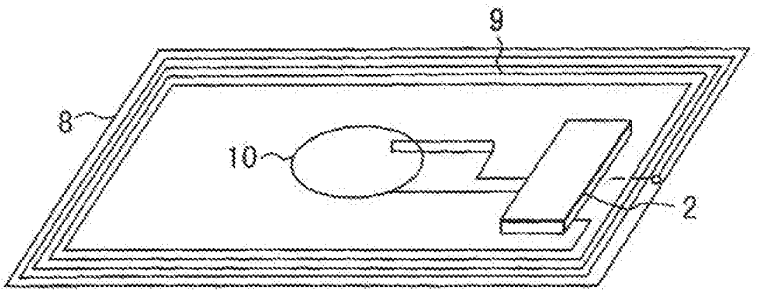


FIG. 4

FIG. 5

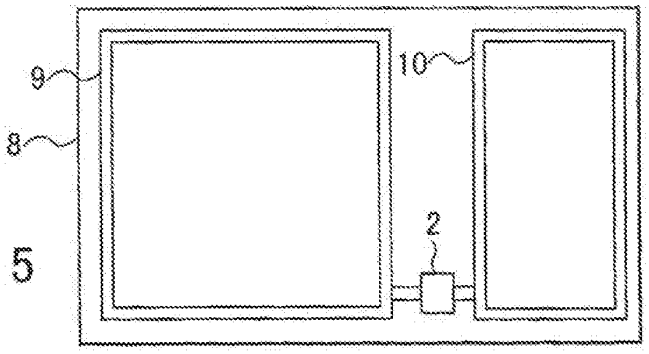


FIG. 6

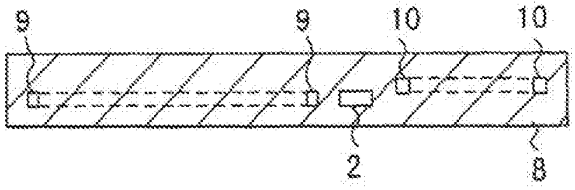


FIG. 7A

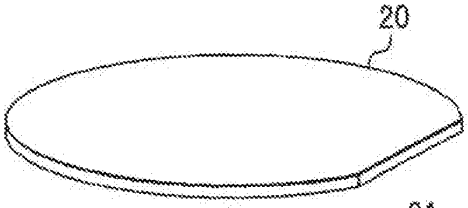


FIG. 7B

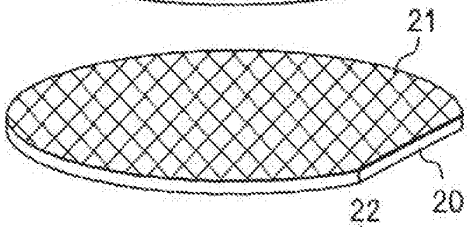


FIG. 7C

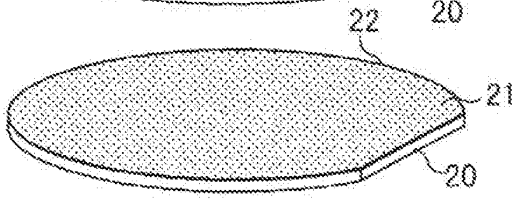
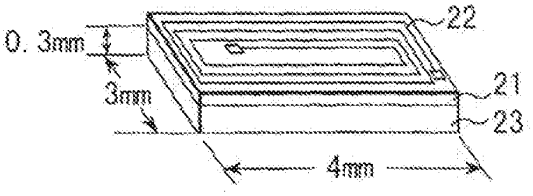


FIG. 7D



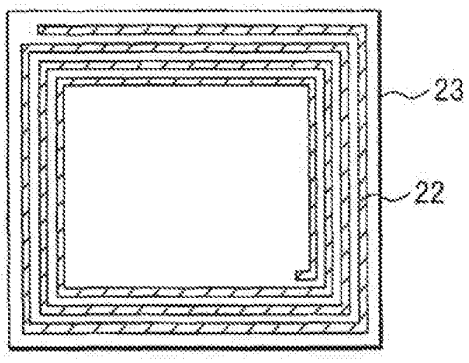


FIG. 8A

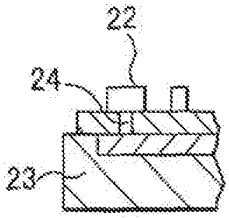


FIG. 8C

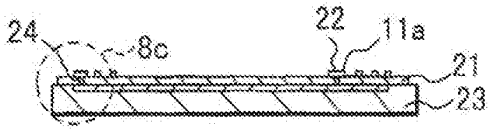


FIG. 8B

FIG. 8D

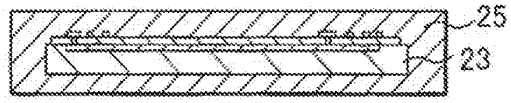


FIG. 9A

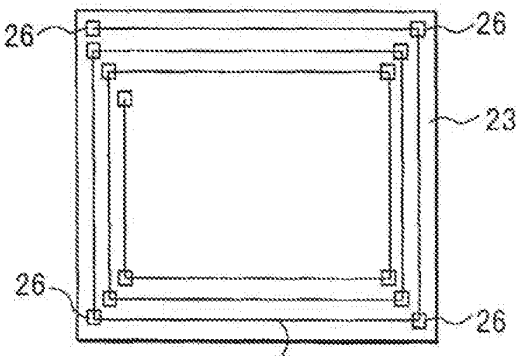


FIG. 9B

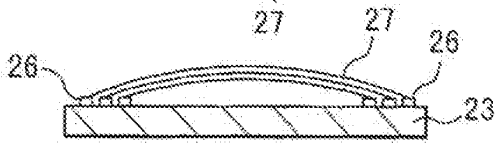


FIG. 10

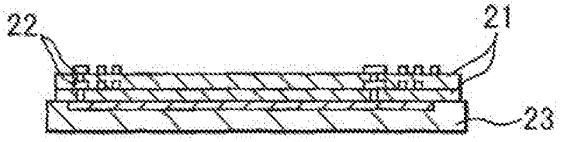


FIG. 11

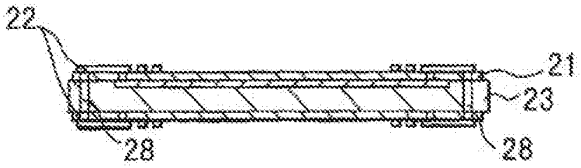


FIG. 12

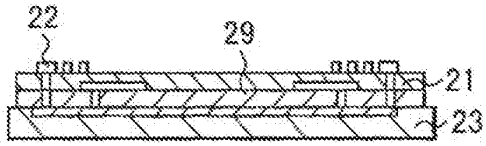


FIG. 13A

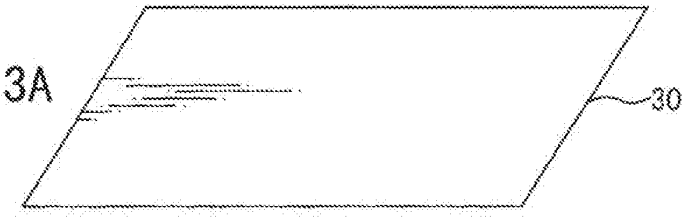


FIG. 13B

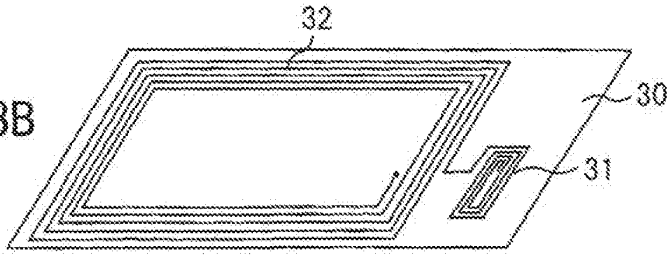
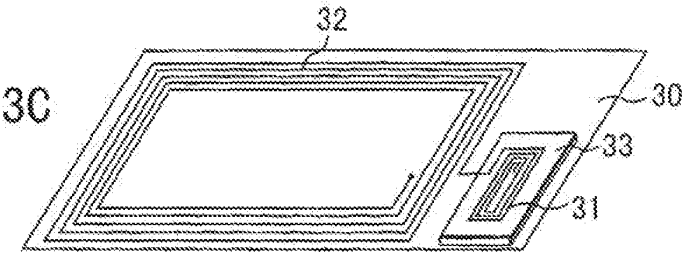


FIG. 13C



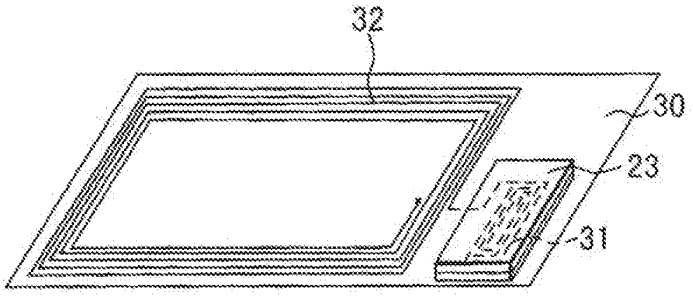


FIG. 13D

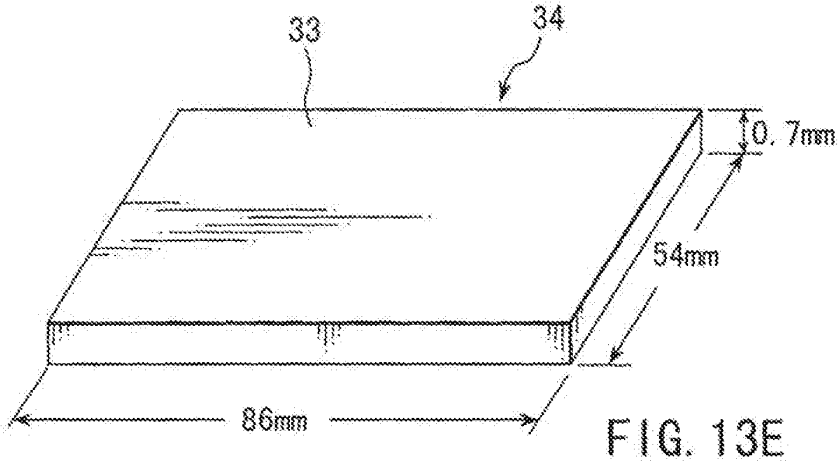


FIG. 13E

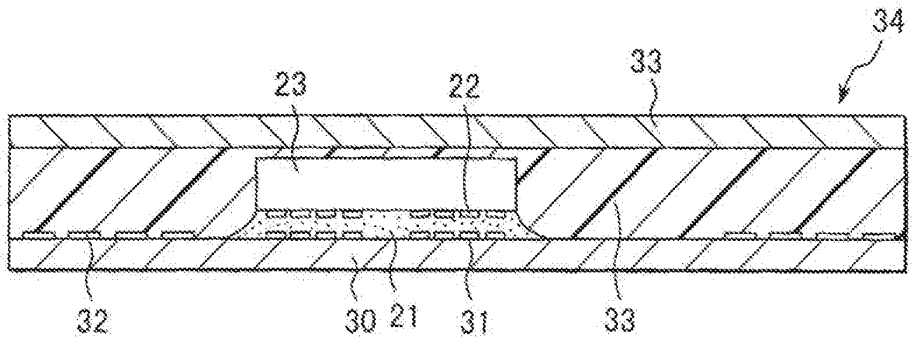


FIG. 14

FIG. 15

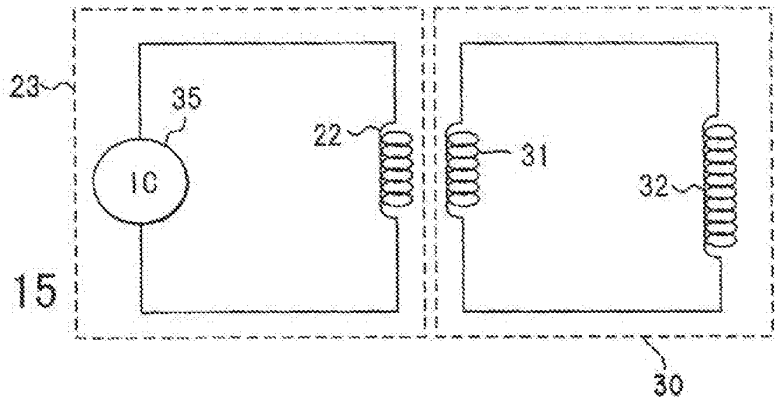


FIG. 16

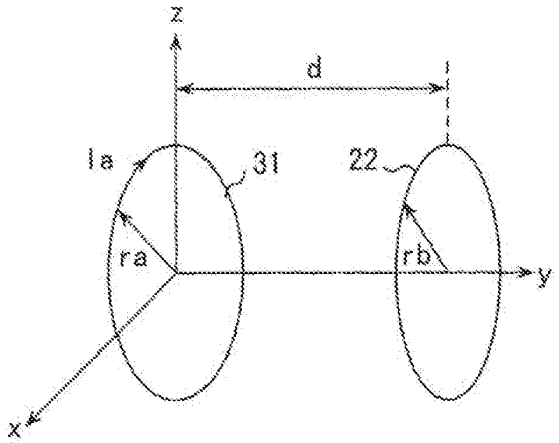


FIG. 17A

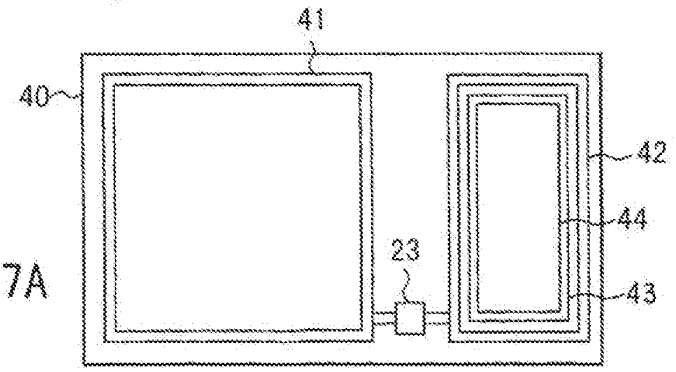
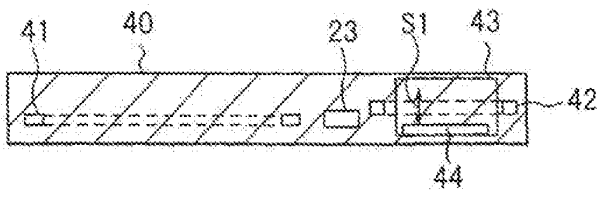


FIG. 17B



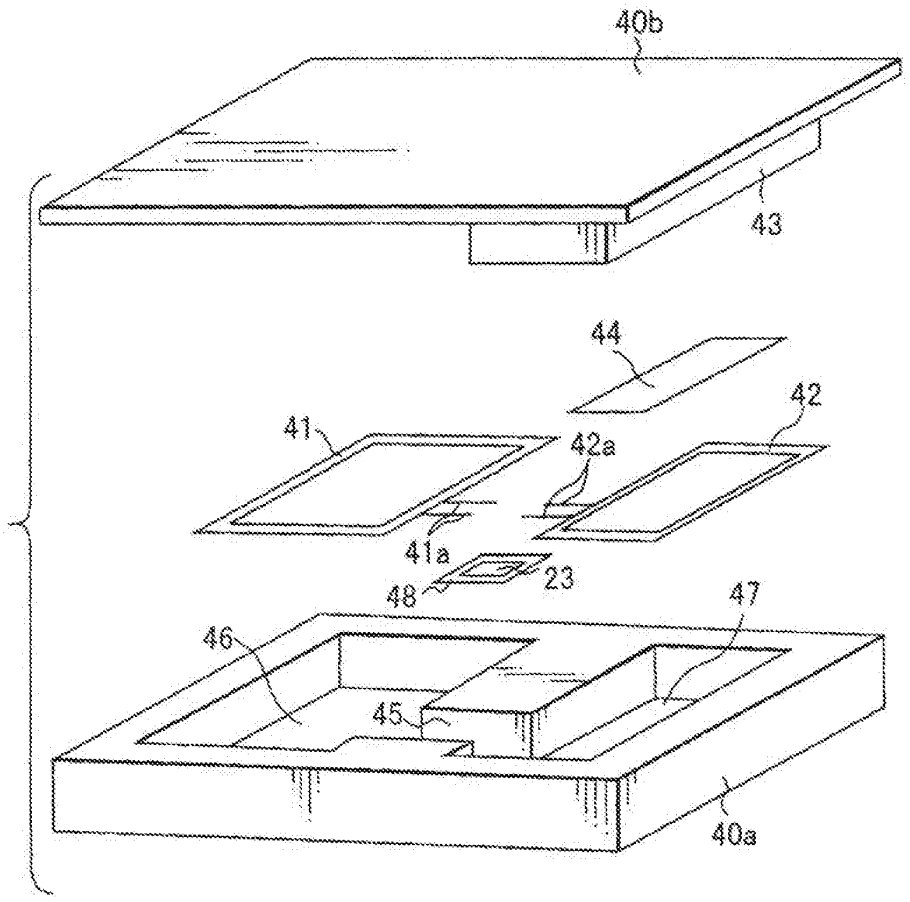


FIG. 18

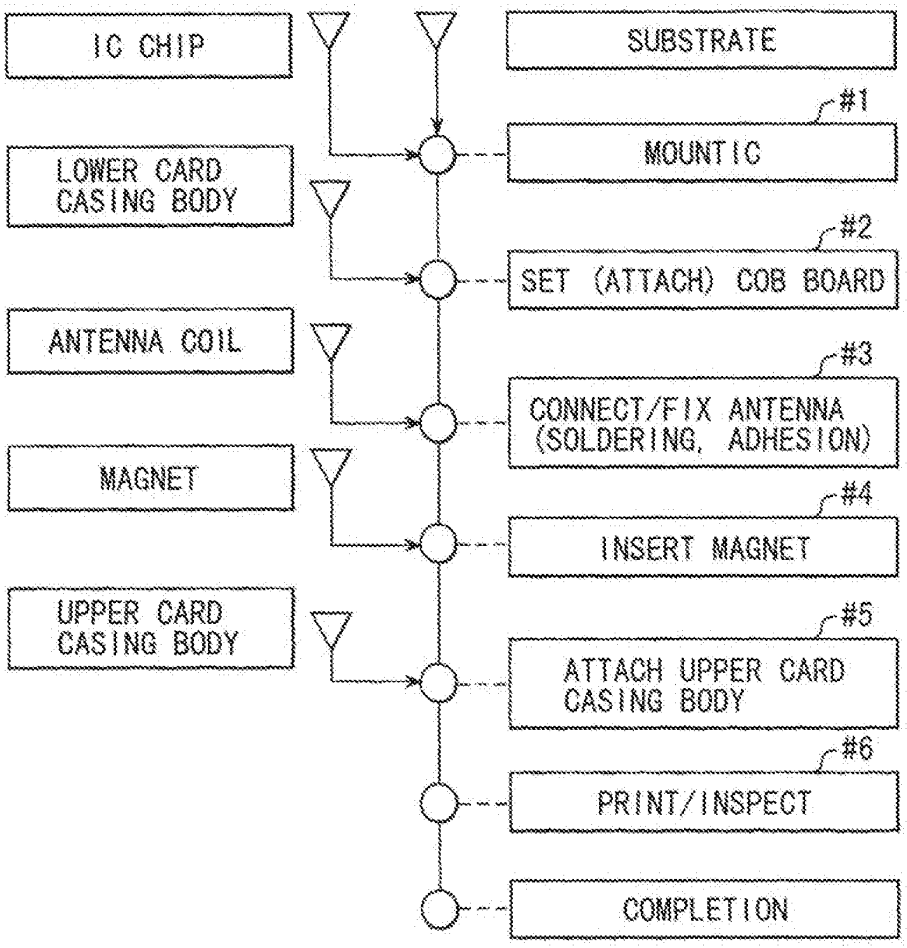

IC CHIP
LOWER CARD CASING BODY
ANTENNA COIL
MAGNET
UPPER CARD CASING BODY
SUBSTRATE
#1
MOUNT IC
#2
SET (ATTACH) COB BOARD
#3
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#4
INSERT MAGNET
#5
ATTACH UPPER CARD CASING BODY
#6
PRINT/INSPECT
COMPLETION

FIG. 19

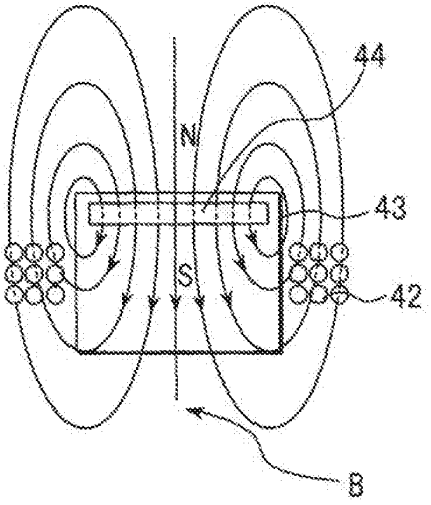


FIG. 20A

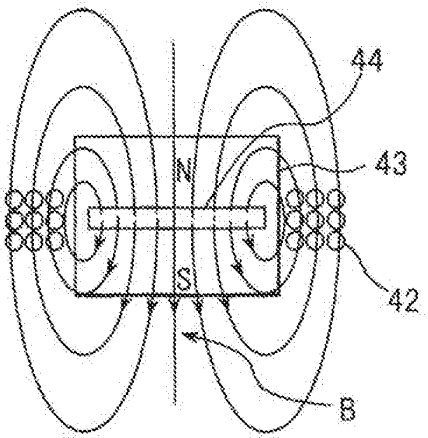


FIG. 20B

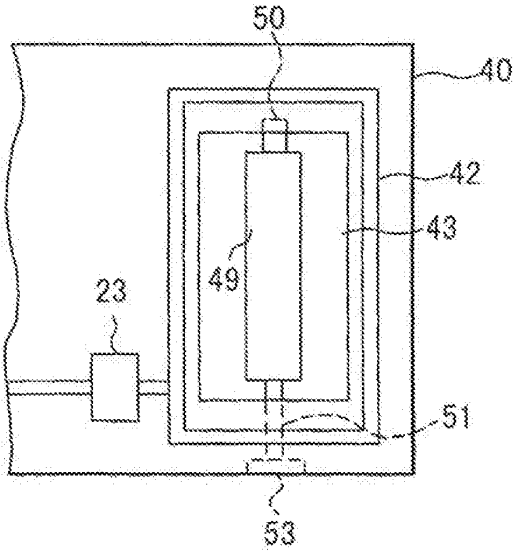


FIG. 21A

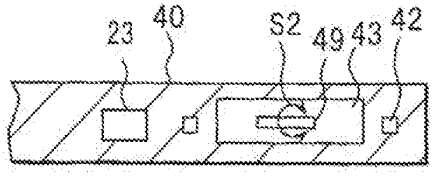


FIG. 21B

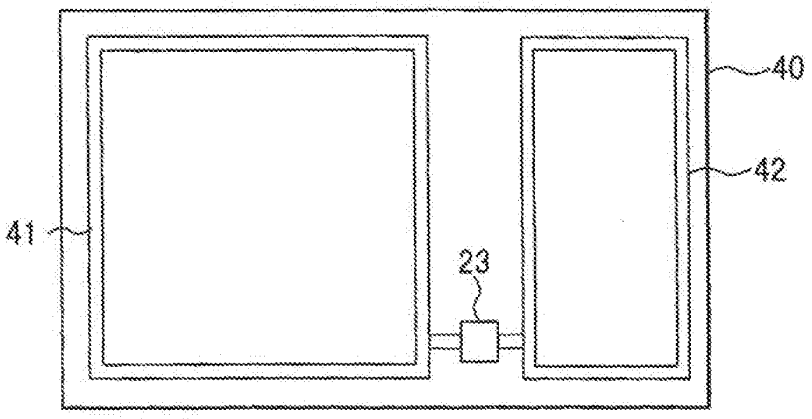


FIG. 22A

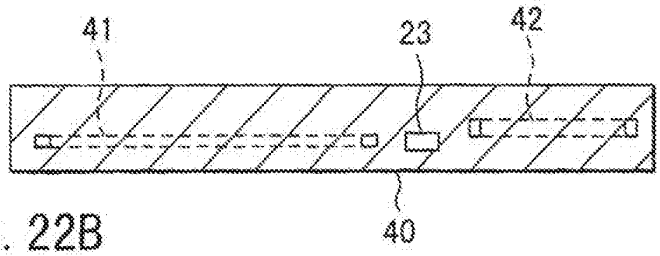


FIG. 22B

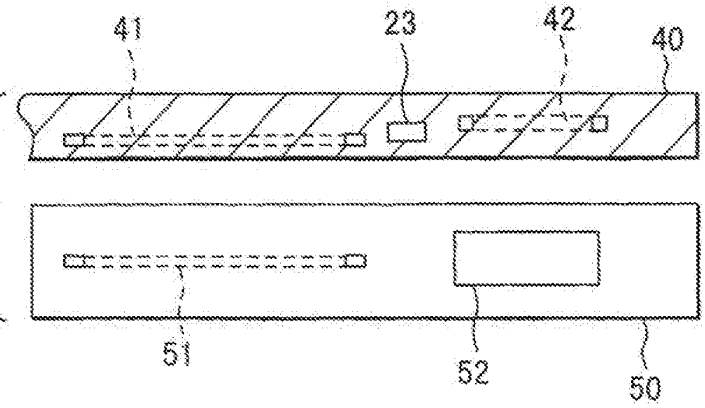


FIG. 23

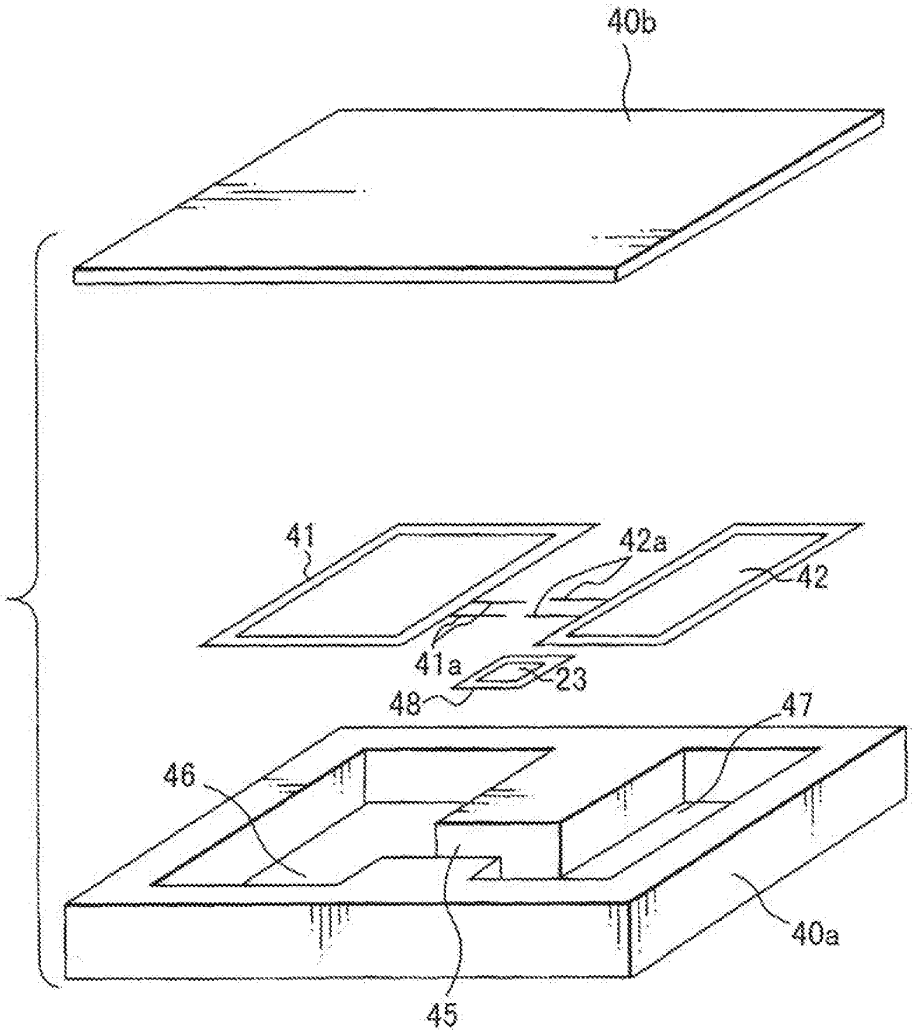


FIG. 24

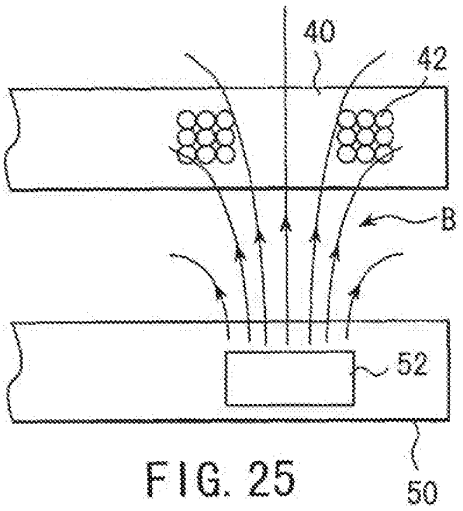


FIG. 25

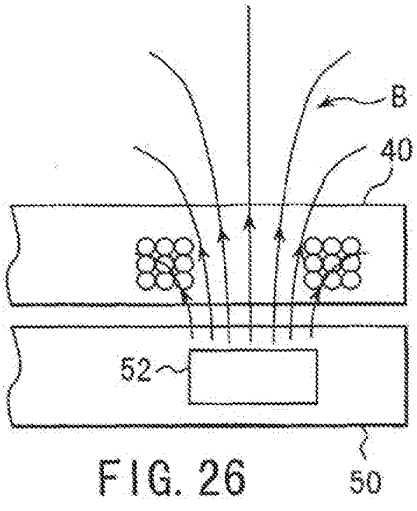


FIG. 26

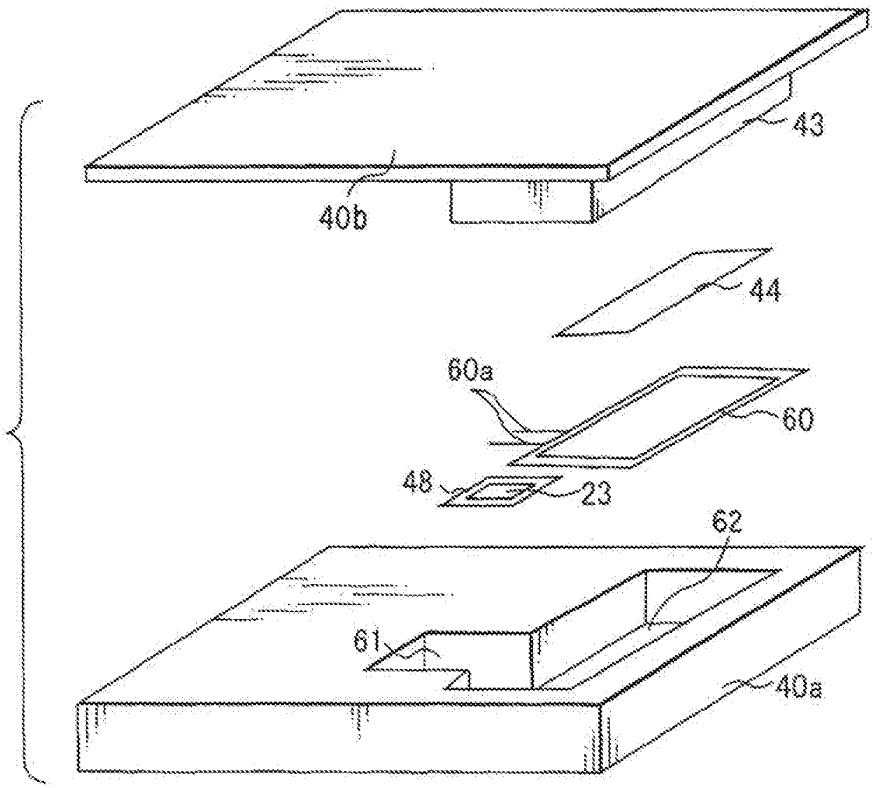


FIG. 27

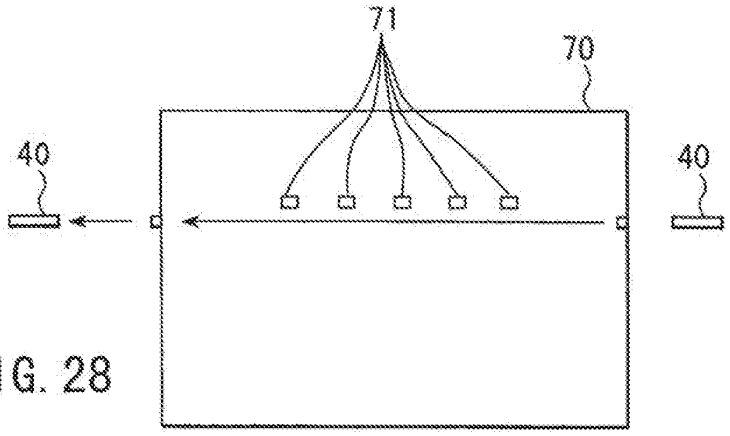


FIG. 28

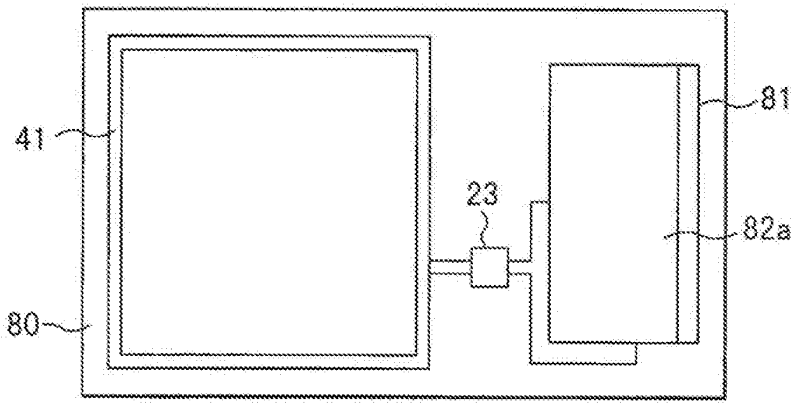


FIG. 29A

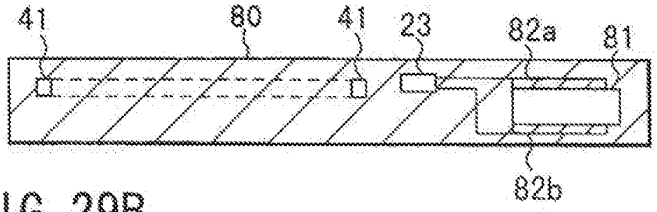


FIG. 29B

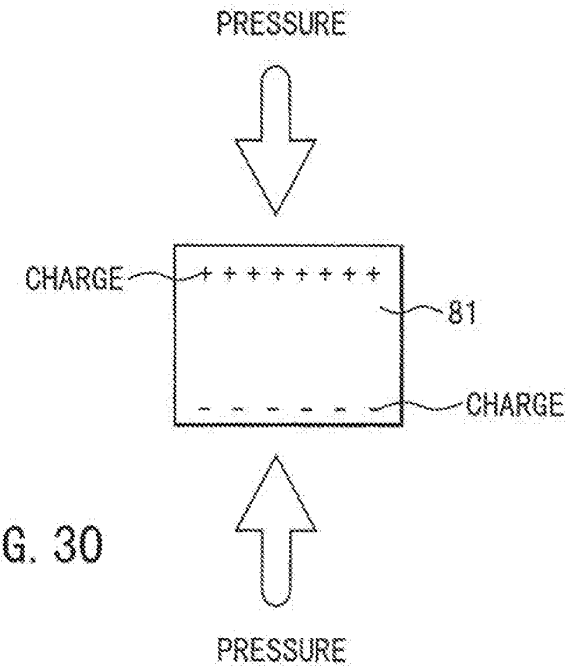


FIG. 30

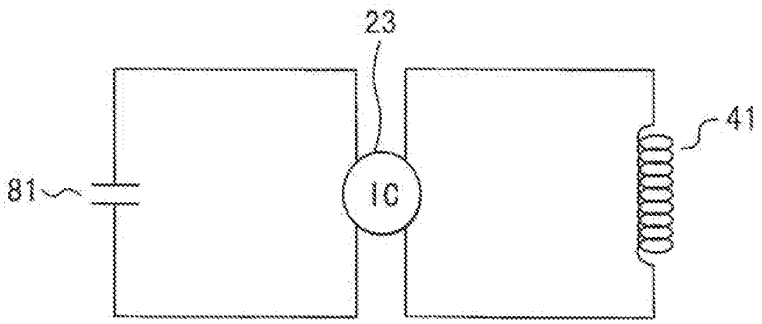


FIG. 31

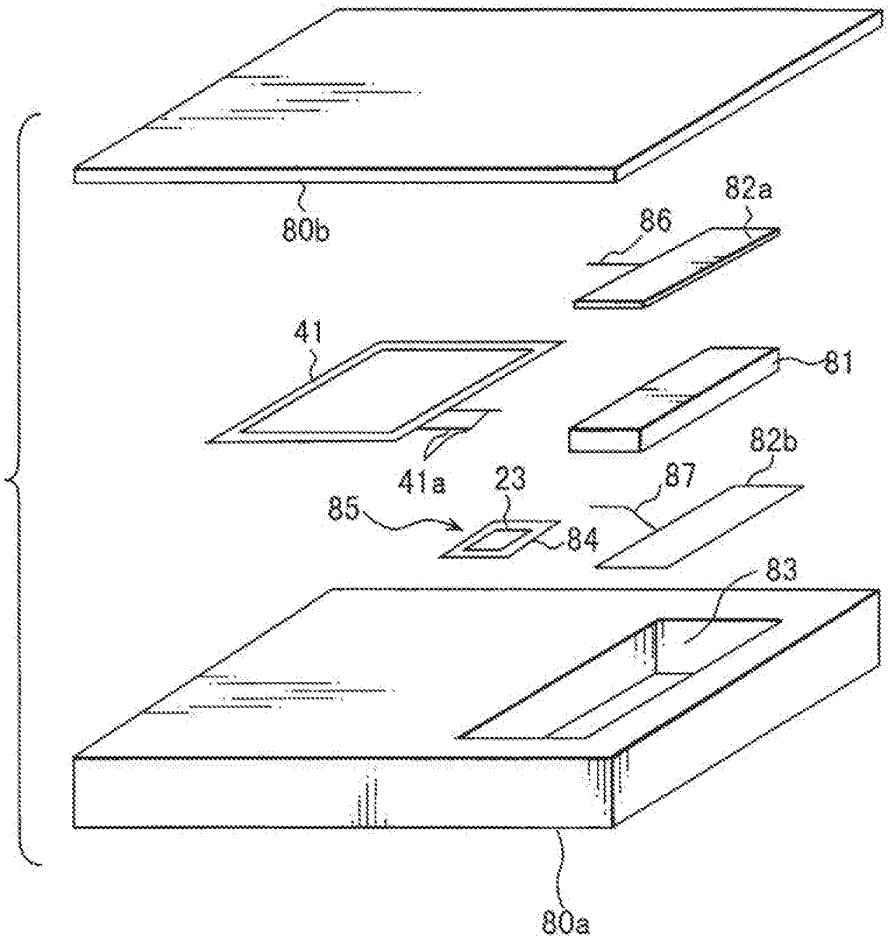


FIG. 32

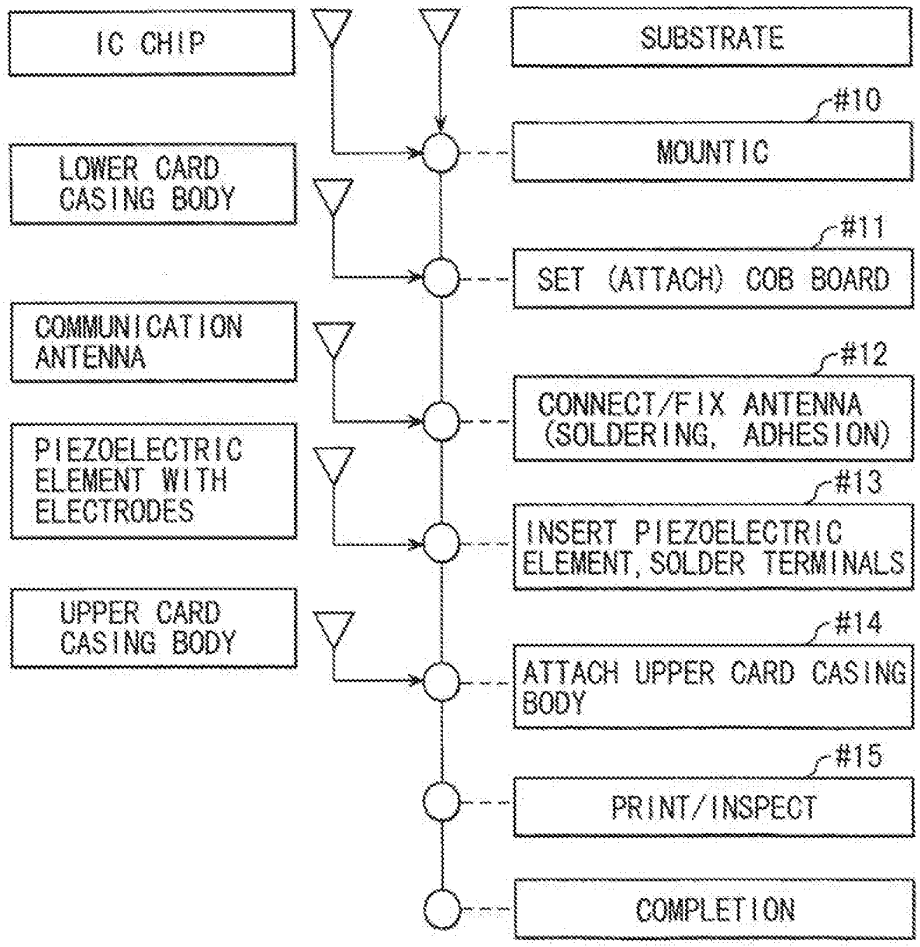

IC CHIP
LOWER CARD CASING BODY
COMMUNICATION ANTENNA
PIEZOELECTRIC ELEMENT WITH ELECTRODES
UPPER CARD CASING BODY
SUBSTRATE
#10
MOUNT IC
#11
SET (ATTACH) COB BOARD
#12
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#13
INSERT PIEZOELECTRIC ELEMENT, SOLDER TERMINALS
#14
ATTACH UPPER CARD CASING BODY
#15
PRINT/INSPECT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

FIG. 33

FIG. 34A

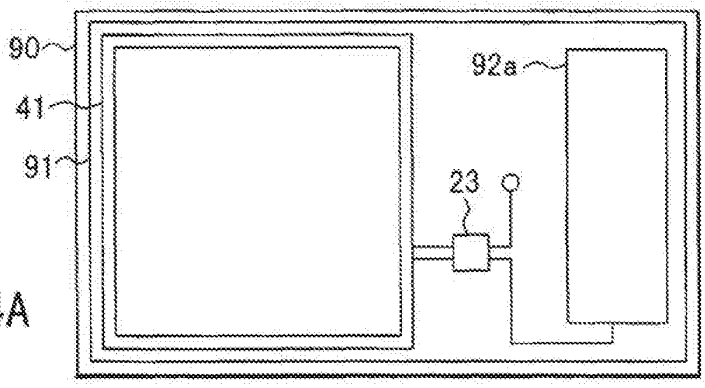


FIG. 34B

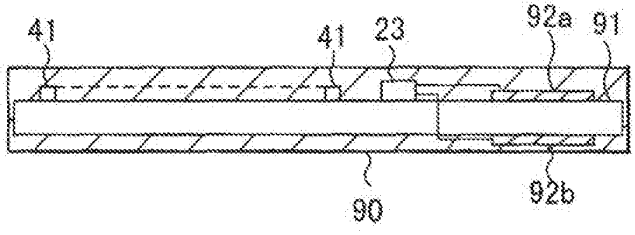
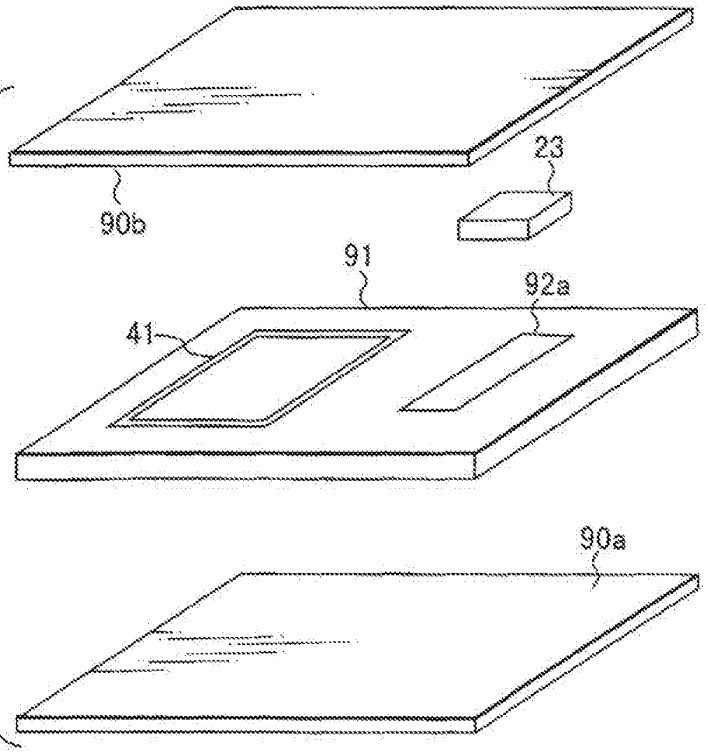


FIG. 35



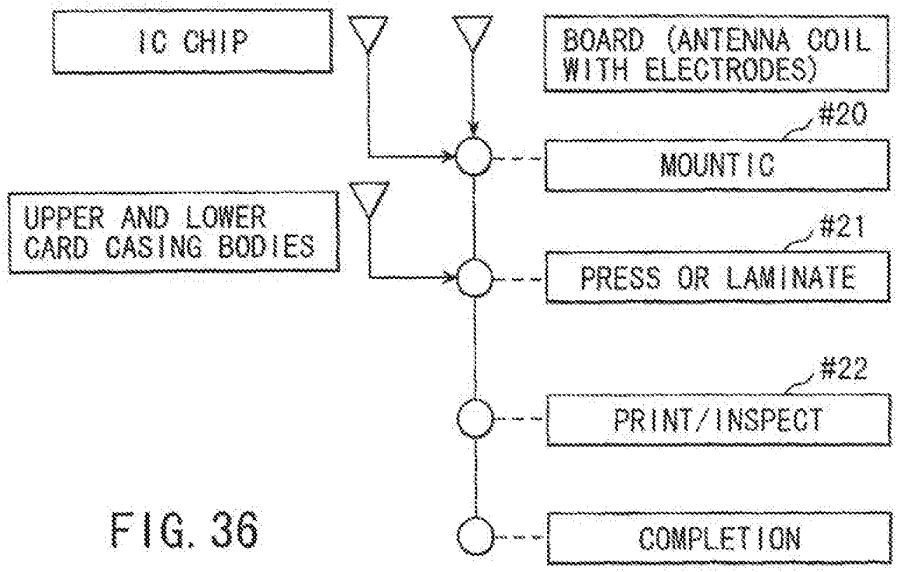


FIG. 36

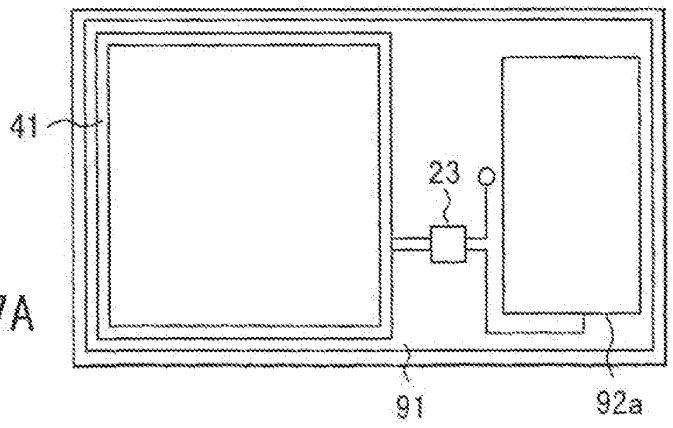


FIG. 37A

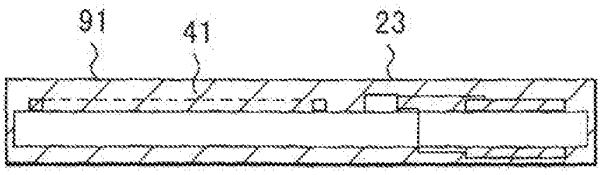


FIG. 37B

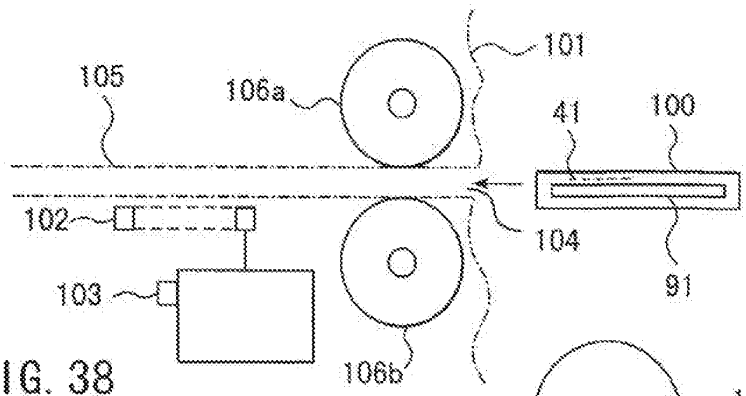


FIG. 38

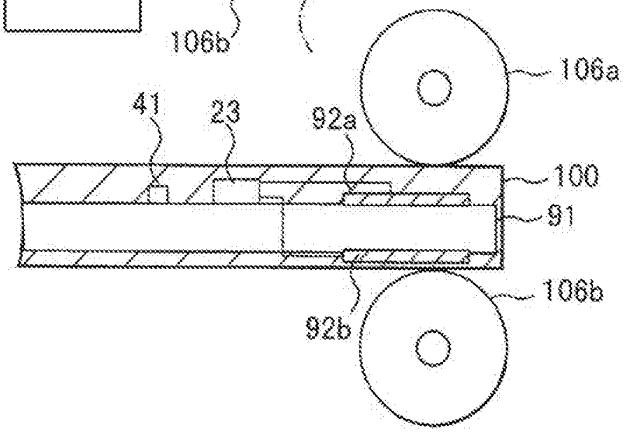


FIG. 39

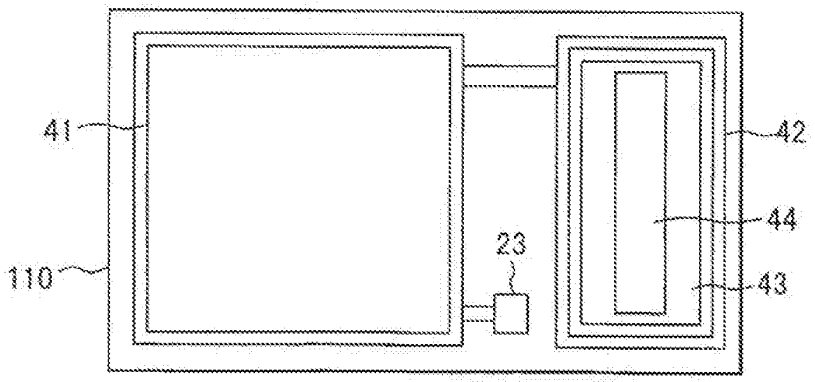


FIG. 40A

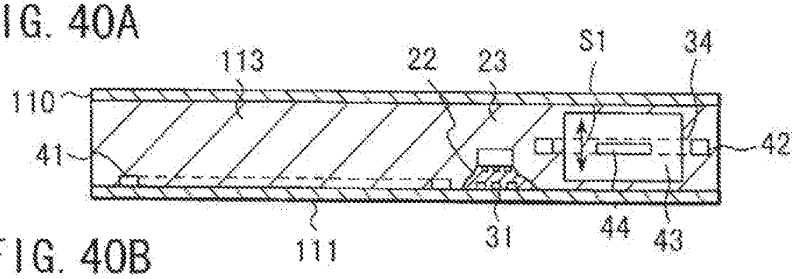


FIG. 40B

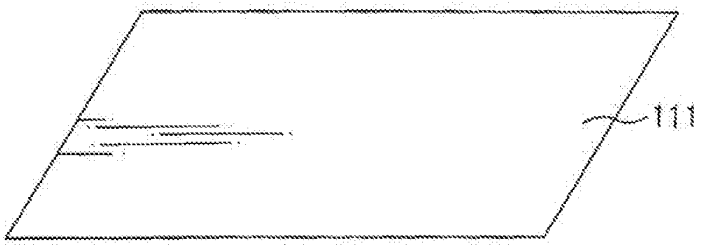


FIG. 41A

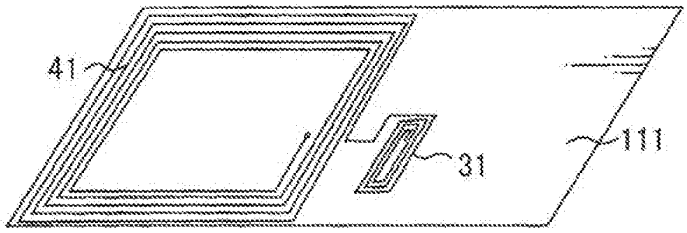


FIG. 41B

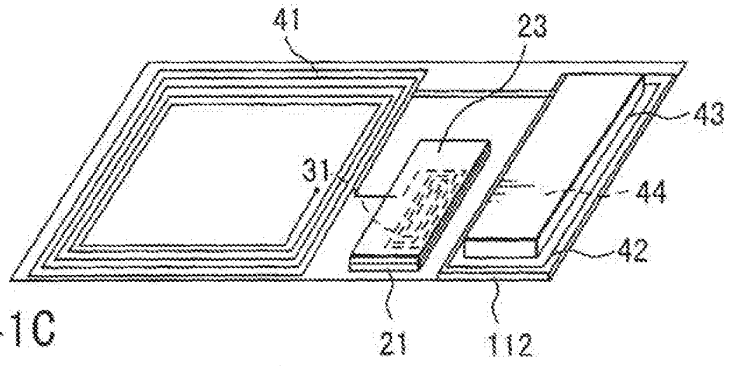


FIG. 41C

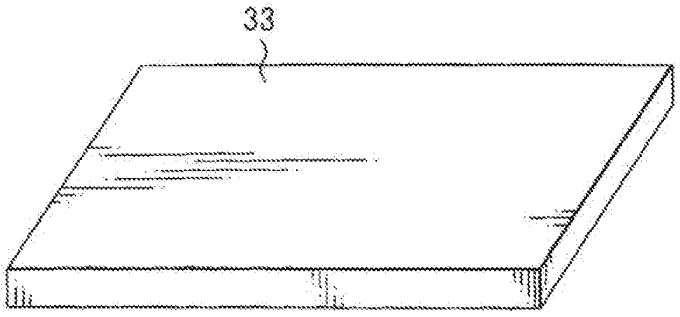
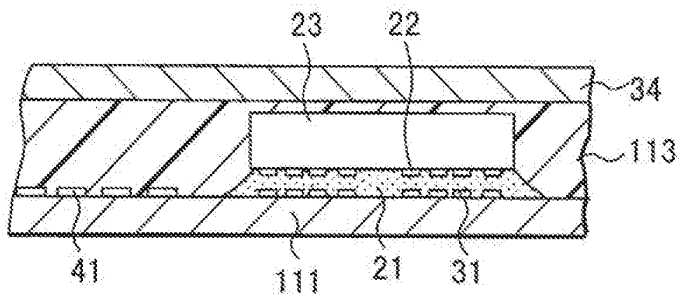


FIG. 41D

FIG. 42


23
22
34
113
41
111
21
31

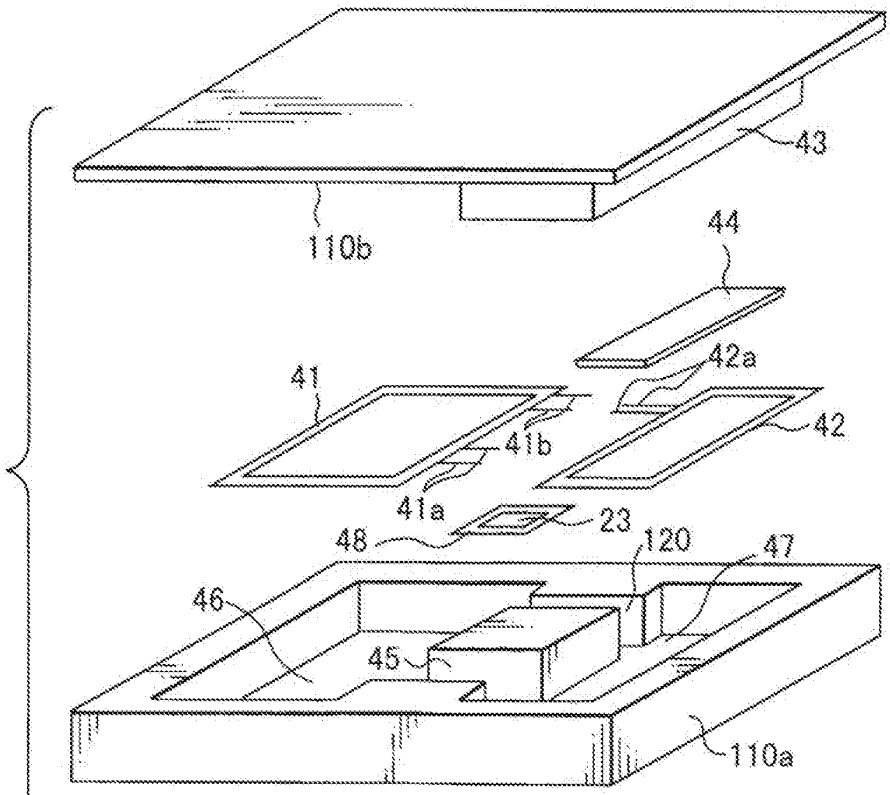

43
110b
44
42a
41
42
41b
41a
23
48
120
47
46
45
110a

FIG. 43

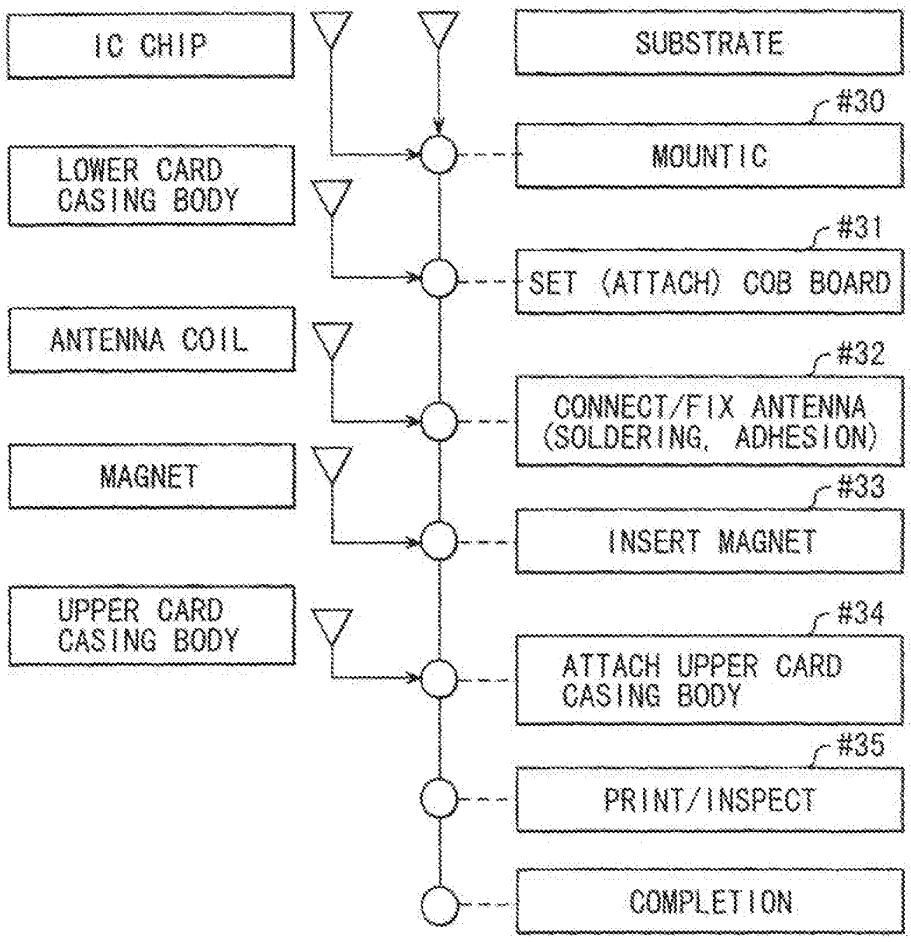

IC CHIP
LOWER CARD CASING BODY
ANTENNA COIL
MAGNET
UPPER CARD CASING BODY
SUBSTRATE
#30
MOUNT IC
#31
SET (ATTACH) COB BOARD
#32
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#33
INSERT MAGNET
#34
ATTACH UPPER CARD CASING BODY
#35
PRINT/INSPECT
COMPLETION

FIG. 44

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 15/372,317	Filing Date 12/07/2016	☐ 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	05/02/2017	(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))	* 20	Minus	** 20	= 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
PARTHENIA D. MERRILL

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
15/372,317	12/07/2016	Francisco Martinez de Velasco Cortina	116546-1108C8

CONFIRMATION NO. 6203

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

PUBLICATION NOTICE

OC000000090297289

Title:SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

Publication No.US-2017-0094516-A1
Publication Date:03/30/2017

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 (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, 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.
15/372,317	12/07/2016	Francisco Martinez de Velasco Cortina	116546-1108C8	6203

27189 7590 02/02/2017

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
02/02/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@procopio.com
PTONotifications@procopio.com

Office Action Summary	Application No. 15/372,317	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 *12/7/2016*.

☐ 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) *1-20* 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) *1-20* 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 –
>
> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

1. Claims 1-20 are rejected under 35 U.S.C. 102(a)(2) as being anticipated by **Hoffman** [US 2004/0128249].

Claim 1, the claimed a mobile device, comprising: a biometric input device configured to receive biometric data; a short range radio frequency antenna (the portable electronic script transaction authorization device PDA 1 with PDC 22 at the point of sale receives at least one wireless biometric samples/signals 62 from the biometric sensors/scanners 2, Figs. 1, 6, pars [0039, 0054, 0089, 0113, 0129-0131]);

memory configured to store biometric information for identifying an individual associated with transaction information (the PDA 1 with DPC 22 store biometric sample/signal 62 and to retrieve the script transactions from the scrip supporter, Figs. 3, 4, pars [0040, 0041, 0057, 0077, 0095, 0109, 0113]); and

a processor coupled with the memory and the biometric input device, the processor configured to: receive a signal via the short range radio frequency antenna, the signal comprising a request to access the memory and retrieve the transaction information,

receive biometric information from the biometric input device the memory, and provide the transaction information in response to the access request when the received biometric information matches the stored biometric information (the DPC 22 comprised of an identicator 12 with internal execution modules 38 to wirelessly receive the biometric sample/signal 62 from the wireless biometric sensors 2 and the requested script transaction data information and then to compare a script supporter's bid biometric sample/signal 62 with previous stored biometric sample/signal from registered scrip supporters for determining whether it is matching for authentication or not, Figs. 1-6, pars [0102, 0106, 0109, 0111, 0113, 0117, 0122, 0127]).

Claim 2, wherein the mobile device is one of a cellphone, smartphone, or tablet (the PDA 1 connected via a cellular digital packet data modem, Figs. 1, 6, pars [0113, 0117]).

Claim 3, wherein the biometric input device is a fingerprint scanner (the scanner 2, Figs. 1, 6).

Claim 4, wherein the processor is further configured to provide the received biometric information or the stored biometric information with the transaction information (as cited in respect to claim 1 above, as the DPC 22).

Claim 5, wherein the transaction information is account information (the account transactions or script accounts, Fig. 6, pars [0112, 0113]).

Claim 6, wherein the transaction information is credit card information (the debit or credit card transactions/scripts, par [0112]).

Claim 7, further comprising memory configured to store the transaction information (as cited in respect to claim 1 above, as the DPC 22, Figs. 1, 6)

Claim 8, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (as cited in claim 1 above as the DPC 22, Figs. 1, 6).

Claim 9, all the claimed subject matters are cited in respect to the method claim 1 above.

Claim 10, herein the processor is further configured to provide the received fingerprint information or the stored fingerprint information with the transaction information (as cited in respect to claim 3 above).

Claim 11, wherein the transaction information is account information (as cited in respect to claim 5 above).

Claim 12, wherein the transaction information is credit card information (as cited in respect to claim 6 above).

Claim 13, further comprising memory configured to store the transaction information (as cited in respect to claim 7 above).

Claim 14, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (as cited in respect to claim 8 above).

Claim 15, all the claimed subject matters are cited in respect to the method claims 1 and 2 above.

Claim 16, wherein the processor is further configured to provide the received fingerprint information or the stored fingerprint information with the transaction information (as cited in respect to claim 3 above).

Claim 17, wherein the transaction information is account information (as cited in respect to claim 5 above).

Claim 18, wherein the transaction information is credit card information (as cited in respect to claim 6 above).

Claim 19, further comprising memory configured to store the transaction information (as cited in respect to claim 7 above).

Claim 20, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory (as cited in respect to claim 8 above).

Conclusion

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

Haala discloses the security system, and more particularly to a crosscheck identification system which obstructs or prevents a person from negotiating a transaction with another person, group, or entity in a population, if during a crosscheck it is determined that a person's record contains questionable information. [US 6,934,861]

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: 01/30/2017

Notice of References Cited	Application/Control No. 15/372,317	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	CPC Classification	US Classification
*	A	US-6,934,861 B2	08-2005	Haala; Catherine A.	G06Q20/341	705/44
*	B	US-2004/0128249 A1	07-2004	Hoffman, Ned	G06F21/32	705/44
	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	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372317	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	**Art Unit**
	VAN TRIEU	2685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

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

CLAIM		DATE								
Final	Original	01/30/2017								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	110493	(handheld or cellular or mobile or PDA or portable or scan$5) near9 (biometric or eye$4 or face or finger)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:31
L2	456158	(obtain$4 or receiv$3 or send$3 or transmit$4) near9 (biometric or eye$4 or face or finger)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:32
L3	551549	(handheld or cellular or device or mobile or PDA or portable or scan$5 or unit) near9 (biometric or eye$4 or face or finger)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:32
L4	140811	2 and 3	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:33
L5	69933	4 and (RFID or short or Bluetooth or IEEE or tag)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:34
L6	133474	(demand$3 or inquir$3 or request$3 or retriev$3) near9 (bill or purchas$3 or transaction)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:35
L7	1369	(compar$5 or different or match$3) near9 (bill or purchas$3 or transaction) near9 (biometric or eye$4 or face or facial or finger)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:37
L8	383	5 and 6 and 7	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:37
L9	344	7 not @AY > "2003"	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:38
L10	60	8 not @AY > "2003"	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 08:39
L11	8	10 and (short$range or IEEE or "801$3")	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:08
L12	24	10 and (short$range or IEEE or "80$4")	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:10

L13	8	10 and (short$range or IEEE or "802$4")	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:10
L14	23685	(G06F21/30, G06F30/305, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06Q20/20, G06Q20/206, G06Q20/40, G06Q20/401, G06Q20/405, G08B13/2402, G08B13/2417).CPC.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:32
L15	4779	14 not @AY > "2003"	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:32
L16	4	15 and 13	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:32
L17	38	15 and 10	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:33
L18	26	(13 or 17) and (cellular or smart or tablet)	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:33
L19	5	(("7081819") or ("7671746") or ("8004410") or ("8237568") or ("8587436")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:42
L20	2	(("6025784") or ("7031946")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2017/01/30 09:51

EAST Search History (Interference)

<This search history is empty>

1/30/2017 9:52:01 AM
C:\Users\vtrieu\Documents\EAST\Workspaces\Default EAST Workspace (Flat Panel).wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	15372317	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	VAN TRIEU	2685

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/30, G06F30/305, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06Q20/20, G06Q20/206, G06Q20/40, G06Q20/401, G06Q20/405	1/30/17	vt
G08B13/2402, G08B13/2417	1/30/17	vt

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
G06F21/30, G06F30/305, G06F30/31, G06F30/32, G06F30/34, G06F30/35, G06Q20/20, G06Q20/206, G06Q20/40, G06Q20/401, G06Q20/405,,and the results text limited - see attached search history printout.	1/30/17	vt
G08B13/2402, G08B13/2417, and the results text limited - see attached search history printout.	1/30/17	vt

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

MAILED
JAN 24 2017
OFFICE OF PETITIONS

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

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 15/372,317

1. THE REQUEST FILED December 7, 2016 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 Brian W. Brown at 571-272-5338.

/Brian W. Brown/
[*Signature*]

Petitions Examiner, 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
15/372,317	12/07/2016	2876	1600	116546-1108C8	20	3

CONFIRMATION NO. 6203

FILING RECEIPT

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

OC000000087940693

Date Mailed: 12/19/2016

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

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

Applicant(s)

NEOLOGY, INC., Poway, CA;

Power of Attorney: The patent practitioners associated with Customer Number 27189

Domestic Priority data as claimed by applicant

This application is a CON of 14/084,565 11/19/2013
which is a CON of 13/350,665 01/13/2012 PAT 8587436
which is a CON of 13/175,768 07/01/2011 PAT 8237568
which is a CON of 12/688,666 01/15/2010 PAT 8004410
which is a CON of 11/279,912 04/17/2006 PAT 7671746
which is a CON of 10/615,026 07/09/2003 PAT 7081819
which claims benefit of 60/394,241 07/09/2002

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 12/15/2016

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 15/372,317**

Projected Publication Date: 03/30/2017

Non-Publication Request: No

Early Publication Request: No

Title

SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION 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: 15/372,317

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))	20 minus 20 =	*			OR	x 80 =	0.00
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	1600

APPLICATION AS AMENDED - PART II

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

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/SB/424 (12-11)

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):	116546-1108C8
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION 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), 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. An executed oath or declaration under 37 CFR 1.63 is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /Noel C. Gillespie/	Date December 7 2016
Name (Print/Typed) Noel C. Gillespie	Practitioner Registration Number 47596

Note: *Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.*

☐ *Total of_____ 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.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	Unknown
Filing Date	Herewith
First Named Inventor	Francisco Martinez de Velasco Cortina
Title	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
Art Unit	Unknown
Examiner Name	Not Yet Assigned
Attorney Docket Number	116546-1108C8

SIGNATURE of Applicant or Patent Practitioner

Signature	/Noel C. Gillespie/	Date (Optional)	
Name	Noel C. Gillespie	Registration Number	47596
Title (if Applicant is a juristic entity)	Attorney of Record		
Applicant Name (if Applicant is a juristic entity)	NEOLOGY, INC.		

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of _____ forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 27189

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

☑ The address associated with the above-mentioned Customer Number

OR

☐ The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

NEOLOGY, INC.

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature		Date (Optional)	6-25-2015
Name	FRANCISCO MARTINEZ DE VELASCO CORTINA		
Title	CEO		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Electronic Patent Application Fee Transmittal	
Application Number:	
Filing Date:	
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Noel C. Gillespie
Attorney Docket Number:	116546-1108C8
Filed as Large Entity	
Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)	

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
UTILITY APPLICATION FILING	1011	1	280	280
UTILITY SEARCH FEE	1111	1	600	600
UTILITY EXAMINATION FEE	1311	1	720	720
REQUEST FOR PRIORITIZED EXAMINATION	1817	1	4000	4000
Pages:				
Claims:				
Miscellaneous-Filing:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
PUBL. FEE- EARLY, VOLUNTARY, OR NORMAL	1504	1	0	0
PROCESSING FEE, EXCEPT PROV. APPLS.	1830	1	140	140
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**5740**

Electronic Acknowledgement Receipt	
EFS ID:	27728578
Application Number:	15372317
International Application Number:	
Confirmation Number:	6203
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Noel C. Gillespie
Filer Authorized By:	
Attorney Docket Number:	116546-1108C8
Receipt Date:	07-DEC-2016
Filing Date:	
Time Stamp:	20:45:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$5740
RAM confirmation Number	120816INTEFSW20460400
Deposit Account	502075
Authorized User	cindy guido
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	WebADS.pdf	147260 4d26032e59ed717a8587451690309df23dbabf5d	no	8
Warnings:					
Information:					
2	Drawings-only black and white line drawings	FIGURES_from_Parent.PDF	273431 ae46d4f4ed7f689e595635bcbd3f75ce39bb3f27	no	24
Warnings:					
Information:					
3	Oath or Declaration filed	Signed_Dec_Francisco_116546_1108C8.PDF	515332 b80a6d1be376dda041de6759bdc6c4f6ea7eb112	no	1
Warnings:					
Information:					
4	Oath or Declaration filed	Signed_Dec_Manfred_116546_1108C8.PDF	199284 310924149cee7f6e88a49872dfe06586a3d87d37	no	2
Warnings:					
Information:					
5		SPECIFICATION_116546_1108C8_TBF.PDF	247001 2fdb709027b175b28eb69946a74e7db08dbaae1f	yes	44

Multipart Description/PDF files in .zip description

Document Description	Start	End
Abstract	44	44
Claims	39	43
Specification	1	38

Warnings:					
Information:					
6	TrackOne Request	Track_One_Request_116546_1108C8.PDF	140434 10c28facdd2896e1baaace349bd7e4e5b664cc07	no	2
Warnings:					
Information:					
7	Power of Attorney	POA_116546_1108C8.PDF	379962 e8bc50c82c96430559fe5796dc9b80f081453e3f	no	2
Warnings:					
Information:					
8	Fee Worksheet (SB06)	fee-info.pdf	39906 8b886fb763a128559a91a4fb5793553a406b2c13	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1942610		

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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-1108C8
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION 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

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Francisco		Martinez de Velasco Cortina	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	La Jolla	State/Province	CA	Country of Residence [i]	US

Mailing Address of Inventor:

Address 1	12760 Danielson Ct.		
Address 2	Suite A		
City	Poway	State/Province	CA
Postal Code	92064	Country [i]	US

Inventor 2

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:

WEB ADS 1.0

PTO/AIA/14 (08-15)
Approved for use through 04/30/2017. 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	116546-1108C8
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION 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 IDENTIFICATION SOLUTIONS		
Attorney Docket Number	116546-1108C8	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	24	**Suggested Figure for Publication (if any)**	1

Filing By Reference:

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	27189		

PTO/AIA/14 (08-15)
Approved for use through 04/30/2017. 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	116546-1108C8
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS	

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix	Remove
Registration Number					
Prefix	**Given Name**	Middle Name	**Family Name**	Suffix	Remove
Registration Number					

Additional Representative Information blocks may be generated within this form by selecting the **Add** button.

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, 365(c), or 386(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending	Remove

Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
	Continuation of	14084565	2013-11-19

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14084565	Continuation of	13350665	2012-01-13	8587436	2013-11-19

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13350665	Continuation of	13175768	2011-07-01	8237568	2012-08-07

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13175768	Continuation of	12688666	2010-01-15	8004410	2011-08-23

Prior Application Status	Patented	Remove

Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12688666	Continuation of	11279912	2006-04-17	7671746	2010-03-02

PTO/AIA/14 (08-15)
Approved for use through 04/30/2017. 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	116546-1108C8
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS	

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	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing or 371(c) Date (YYYY-MM-DD)
10615026	Claims benefit of provisional	60394241	2002-07-09

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button.

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. When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(i)(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).

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.

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.

PTO/AIA/14 (08-15)
Approved for use through 04/30/2017. 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	116546-1108C8
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS	

Authorization or Opt-Out of Authorization to Permit Access:

When this Application Data Sheet is properly signed and filed with the application, applicant has provided written authority to permit a participating foreign intellectual property (IP) office access to the instant application-as-filed (see paragraph A in subsection 1 below) and the European Patent Office (EPO) access to any search results from the instant application (see paragraph B in subsection 1 below).

Should applicant choose not to provide an authorization identified in subsection 1 below, applicant **must opt-out** of the authorization by checking the corresponding box A or B or both in subsection 2 below.

NOTE: This section of the Application Data Sheet is **ONLY** reviewed and processed with the **INITIAL** filing of an application. After the initial filing of an application, an Application Data Sheet cannot be used to provide or rescind authorization for access by a foreign IP office(s). Instead, Form PTO/SB/39 or PTO/SB/69 must be used as appropriate.

1. Authorization to Permit Access by a Foreign Intellectual Property Office(s)

A. Priority Document Exchange (PDX) - Unless box A in subsection 2 (opt-out of authorization) is 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 State Intellectual Property Office of the People's Republic of China (SIPO), the World Intellectual Property Organization (WIPO), and any other foreign intellectual property office participating with the USPTO in a bilateral or multilateral priority document exchange agreement in which a foreign application claiming priority to the instant patent application is filed, access to: (1) the instant patent application-as-filed and its related bibliographic data, (2) any foreign or domestic application to which priority or benefit is claimed by the instant application and its related bibliographic data, and (3) the date of filing of this Authorization. See 37 CFR 1.14(h)(1).

B. Search Results from U.S. Application to EPO - Unless box B in subsection 2 (opt-out of authorization) is checked, the undersigned hereby **grants the USPTO authority** to provide the EPO access to the bibliographic data and search results from the instant patent application when a European patent application claiming priority to the instant patent application is filed. See 37 CFR 1.14(h)(2).

The applicant is reminded that the EPO's Rule 141(1) EPC (European Patent Convention) requires applicants to submit a copy of search results from the instant application without delay in a European patent application that claims priority to the instant application.

2. Opt-Out of Authorizations to Permit Access by a Foreign Intellectual Property Office(s)

☐ A. Applicant **DOES NOT** authorize the USPTO to permit a participating foreign IP office access to the instant application-as-filed. If this box is checked, the USPTO will not be providing a participating foreign IP office with any documents and information identified in subsection 1A above.

☐ B. Applicant **DOES NOT** authorize the USPTO to transmit to the EPO any search results from the instant patent application. If this box is checked, the USPTO will not be providing the EPO with search results from the instant application.

NOTE: Once the application has published or is otherwise publicly available, the USPTO may provide access to the application in accordance with 37 CFR 1.14.

PTO/AIA/14 (08-15)
Approved for use through 04/30/2017. 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	116546-1108C8
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS	

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor:	

If the Applicant is an Organization check here. ☒

Organization Name	NEOLOGY, INC.

Mailing Address Information For Applicant:

Address 1	12760 Danielson Ct.		
Address 2	Suite A		
City	Poway	**State/Province**	CA
Country[i]	US	Postal Code	92064
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button.

PTO/AIA/14 (08-15)
Approved for use through 04/30/2017. 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	116546-1108C8
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS	

Assignee Information including Non-Applicant Assignee 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.

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.

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country [i]		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button.

PTO/AIA/14 (08-15)
Approved for use through 04/30/2017. 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	116546-1108C8
	Application Number	
Title of Invention	SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS	

Signature:

NOTE: This Application Data Sheet must be signed in accordance with 37 CFR 1.33(b). **However, if this Application Data Sheet is submitted with the INITIAL filing of the application and either box A or B is not checked in subsection 2 of the "Authorization or Opt-Out of Authorization to Permit Access" section, then this form must also be signed in accordance with 37 CFR 1.14(c).**

This Application Data Sheet **must** be signed by a patent practitioner if one or more of the applicants is a **juristic entity** (e. g., corporation or association). If the applicant is two or more joint inventors, this form must be signed by a patent practitioner, **all** joint inventors who are the applicant, or one or more joint inventor-applicants who have been given power of attorney (e.g., see USPTO Form PTO/AIA/81) on behalf of **all** joint inventor-applicants.

See 37 CFR 1.4(d) for the manner of making signatures and certifications.

Signature	/Noel C. Gillespie/			Date (YYYY-MM-DD)	
First Name	Noel C.	Last Name	Gillespie	Registration Number	47596

Additional Signature may be generated within this form by selecting the Add button.

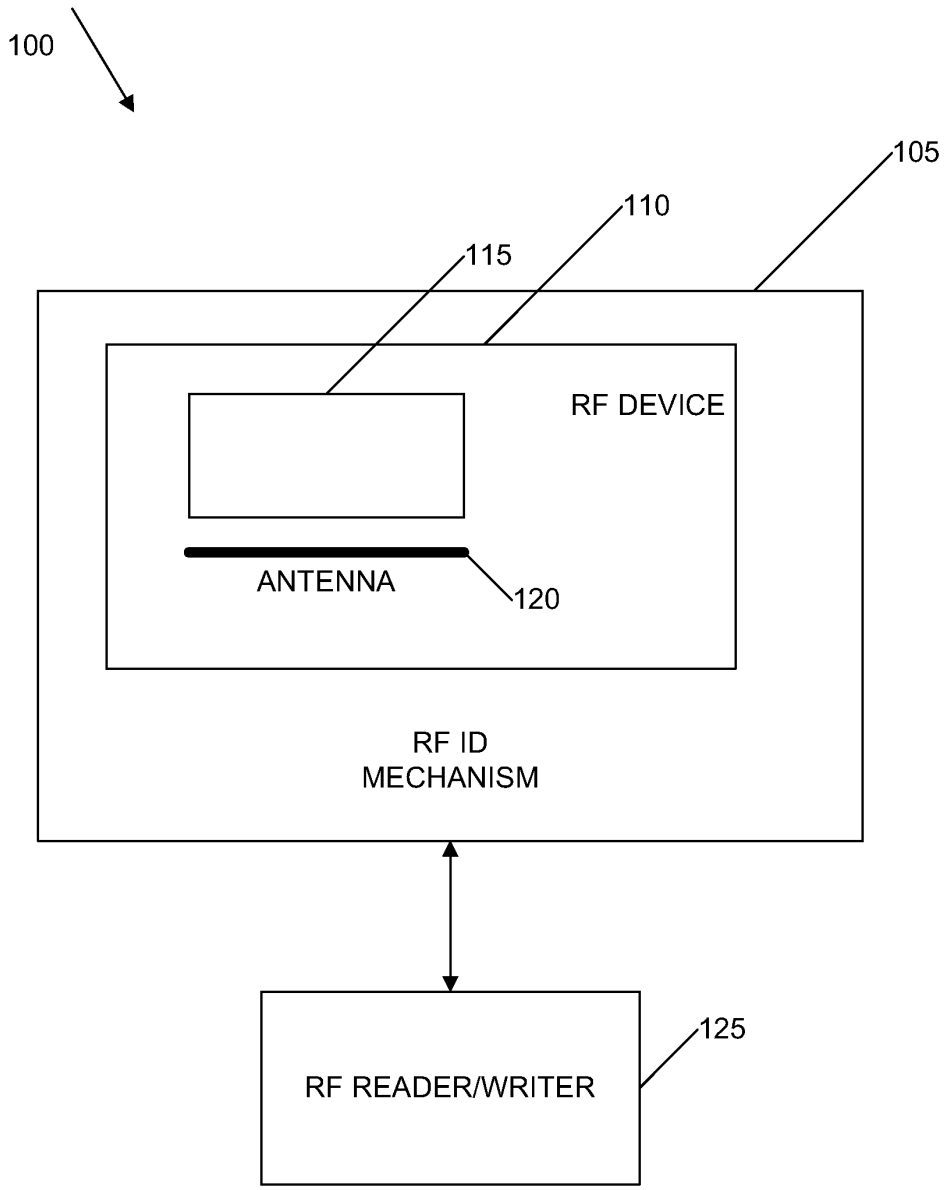

100
105
110
115
RF DEVICE
ANTENNA
120
RF ID
MECHANISM
125
RF READER/WRITER

FIG. 1

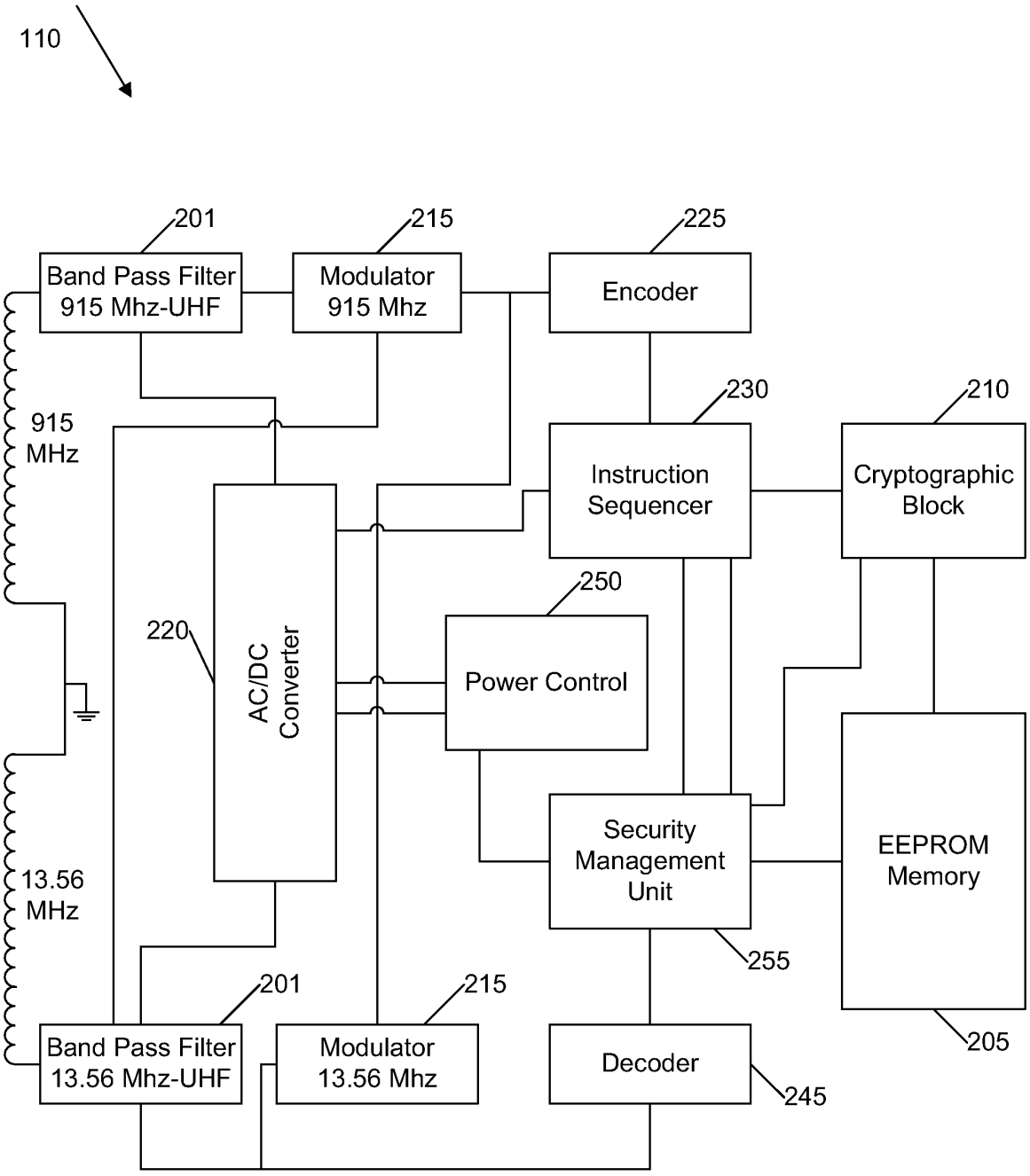

110
201
Band Pass Filter
915 Mhz-UHF
215
Modulator
915 Mhz
225
Encoder
915
MHz
230
Instruction
Sequencer
210
Cryptographic
Block
250
220
AC/DC
Converter
Power Control
13.56
MHz
Security
Management
Unit
EEPROM
Memory
255
201
215
Band Pass Filter
13.56 Mhz-UHF
Modulator
13.56 Mhz
Decoder
205
245

FIG. 2

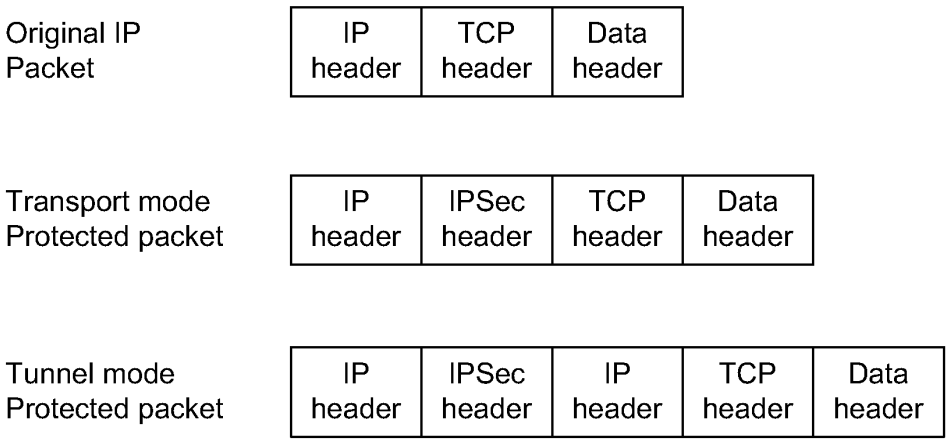

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIG. 3A

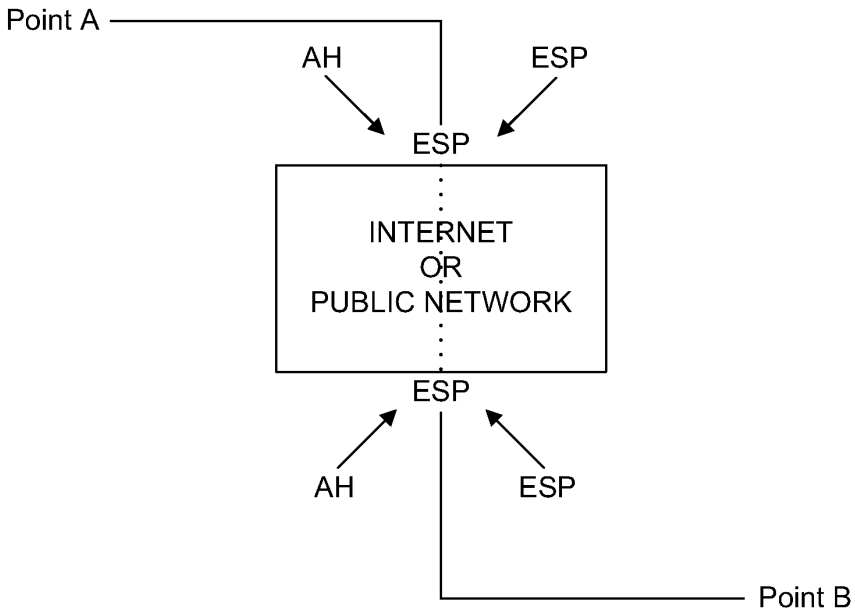

Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORK
ESP
AH
ESP
Point B

FIG. 3B

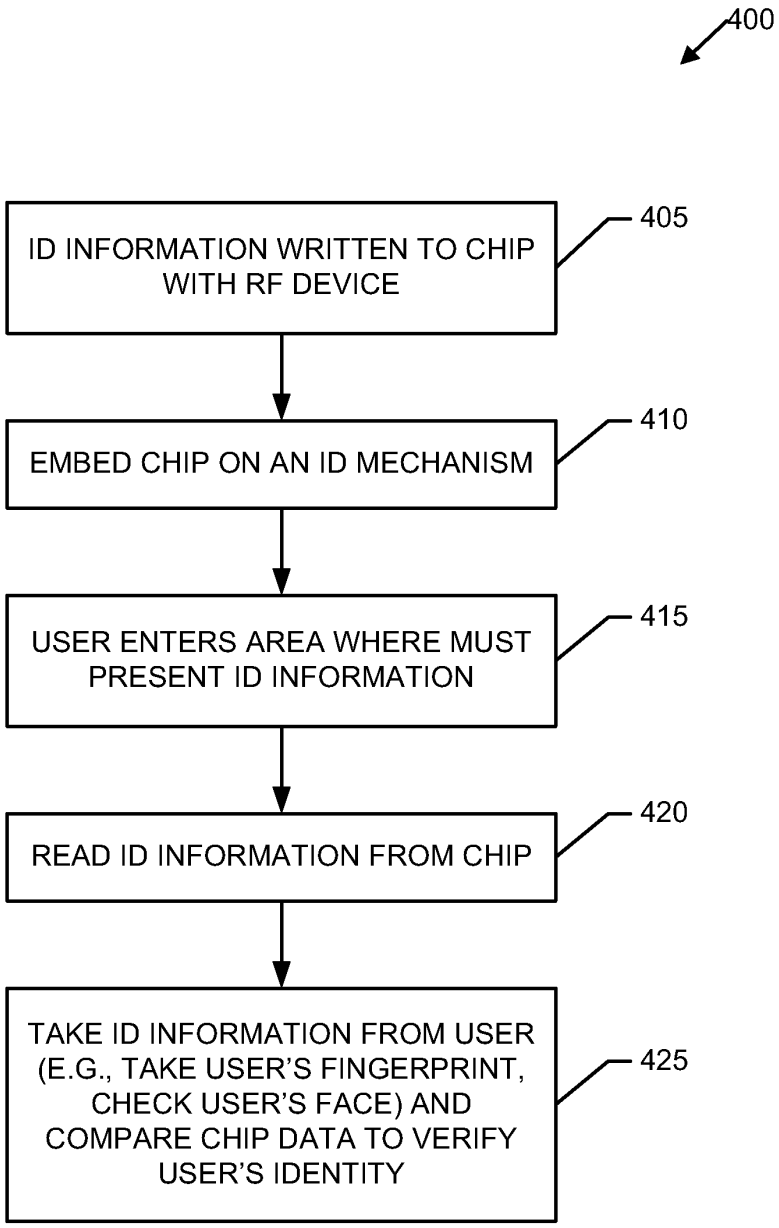

400
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
405
EMBED CHIP ON AN ID MECHANISM
410
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
415
READ ID INFORMATION FROM CHIP
420
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE CHIP DATA TO VERIFY USER'S IDENTITY
425

FIG. 4

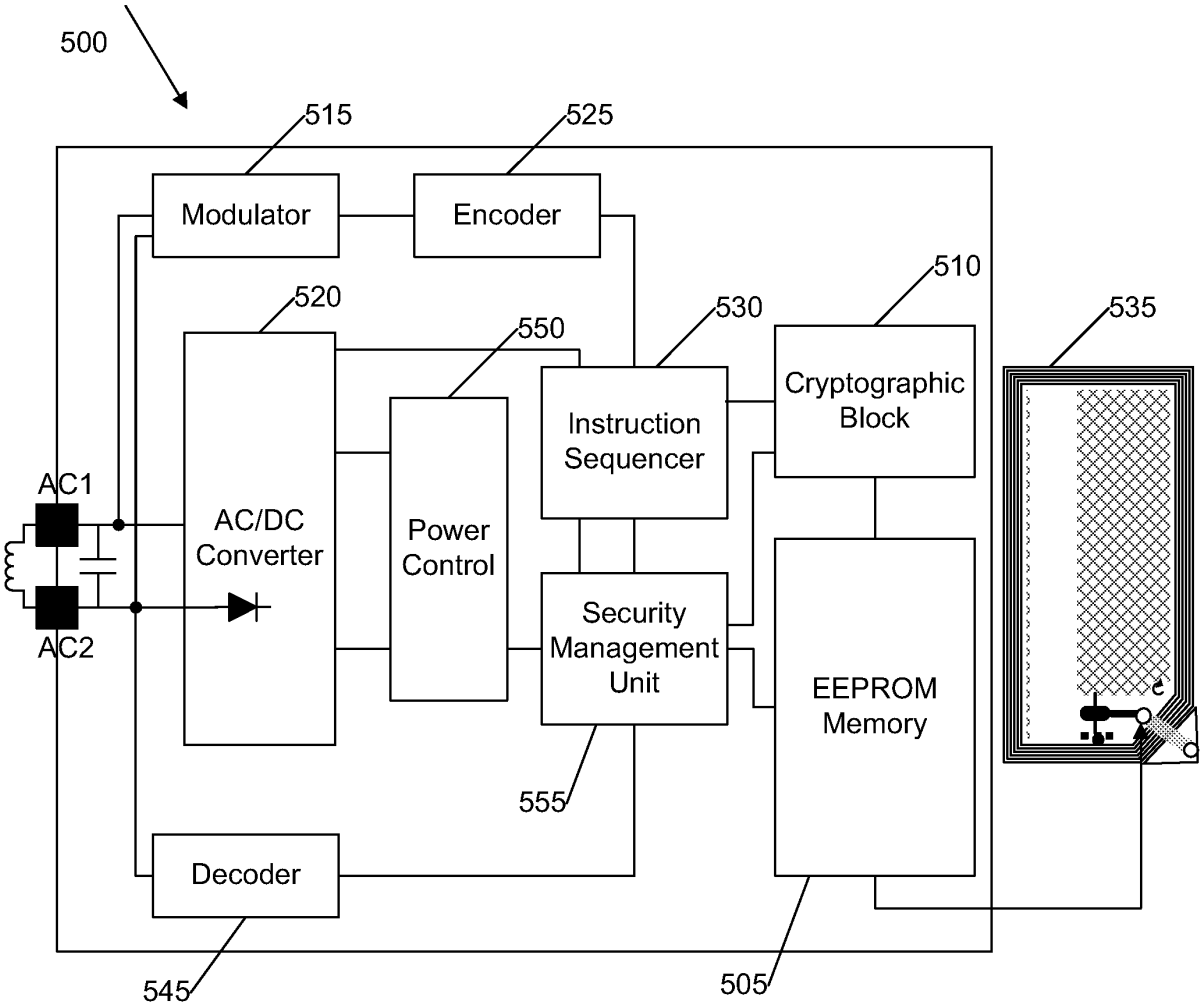

500
515
525
Modulator
Encoder
510
520
530
535
550
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
555
Decoder
545
505

FIG. 5

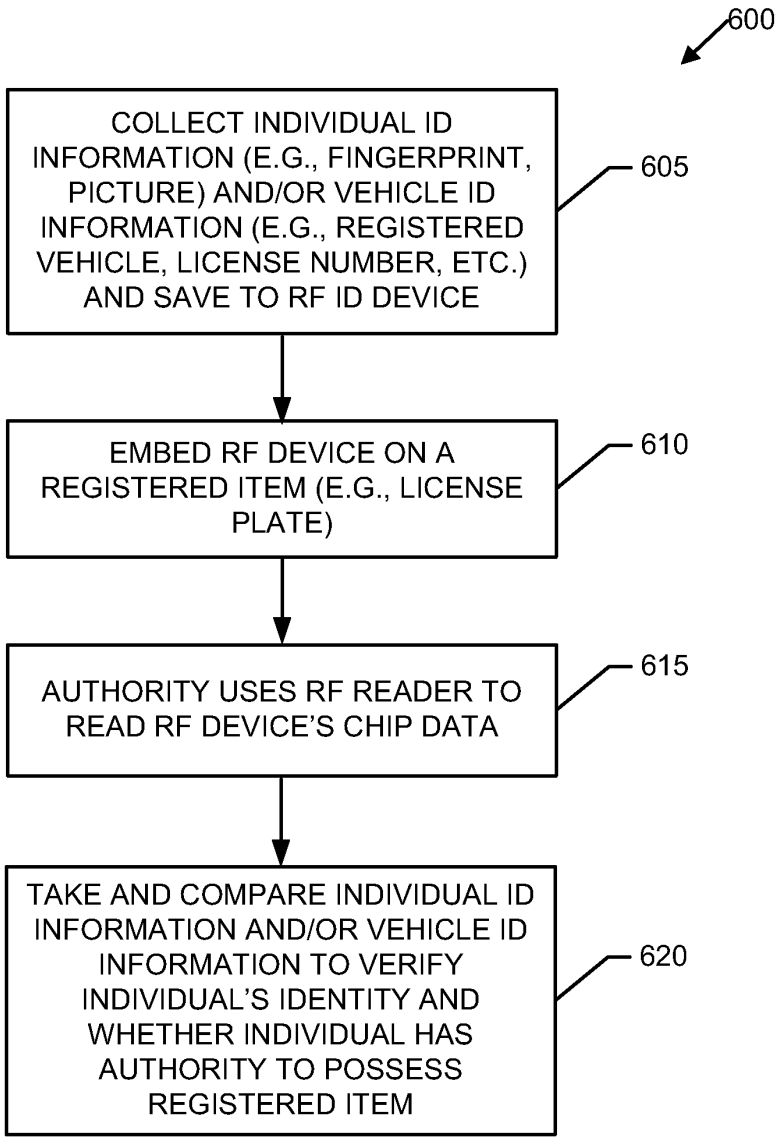

600
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
605
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
610
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
615
TAKE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

FIG. 6

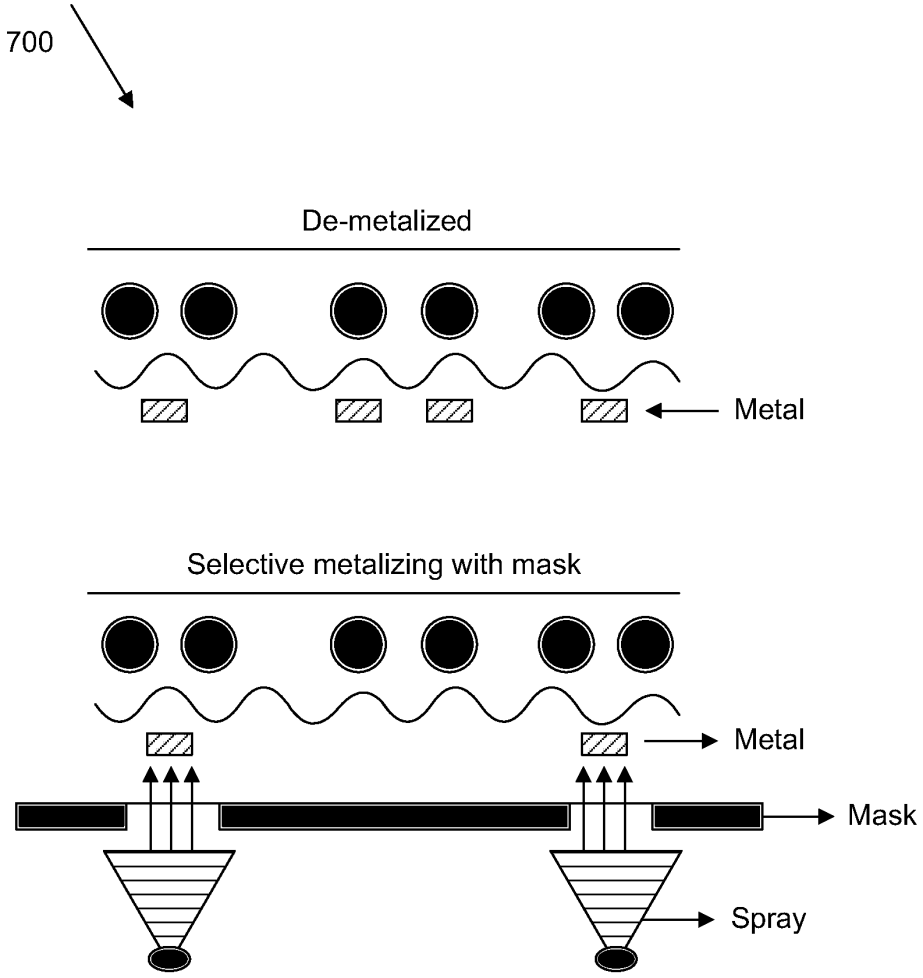

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIG. 7

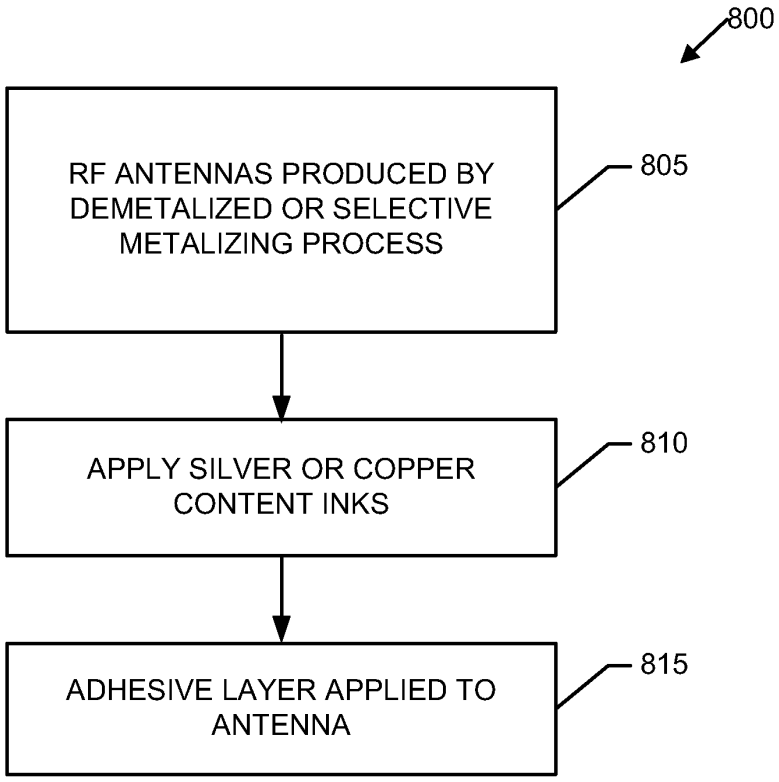

800
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
805
APPLY SILVER OR COPPER CONTENT INKS
810
ADHESIVE LAYER APPLIED TO ANTENNA
815

FIG. 8

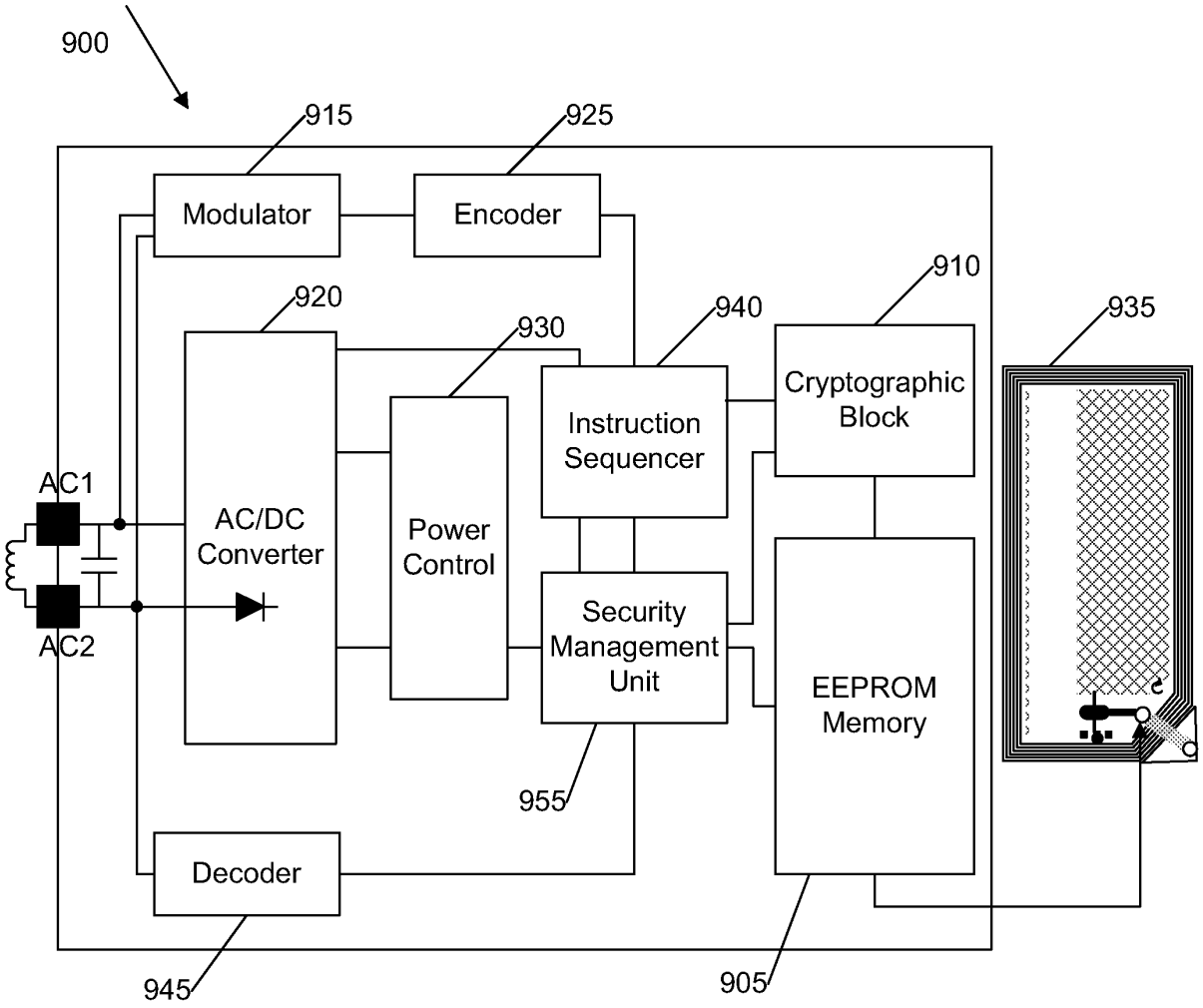

900
915
925
Modulator
Encoder
910
920
940
935
930
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
955
Decoder
945
905

FIG. 9

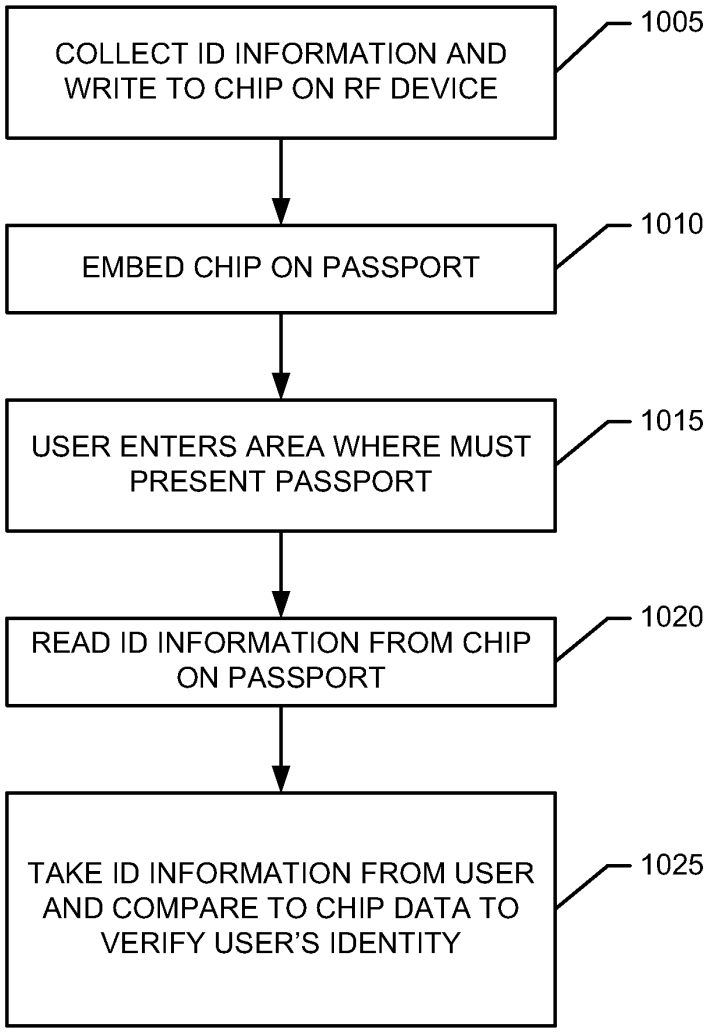

COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1005
EMBED CHIP ON PASSPORT
1010
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1015
READ ID INFORMATION FROM CHIP ON PASSPORT
1020
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY
1025

FIG. 10

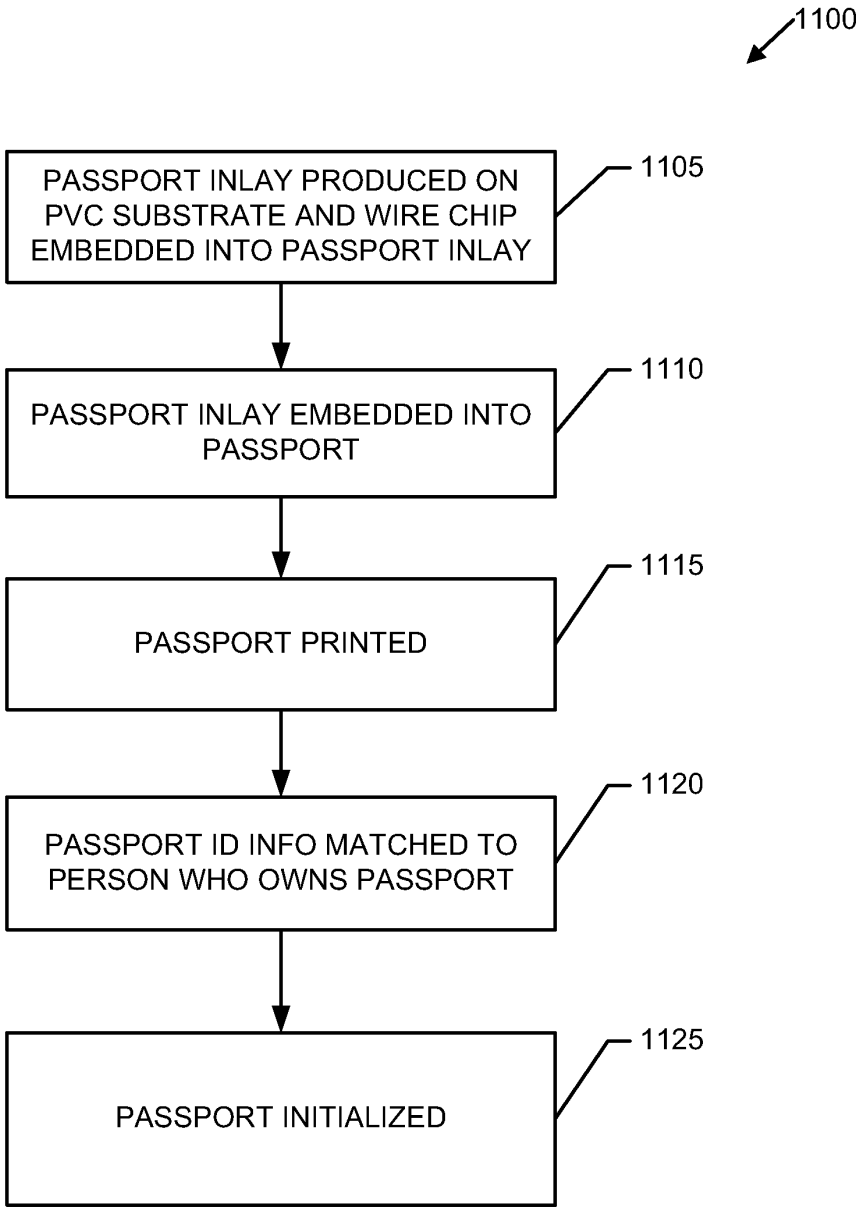

1100
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1105
PASSPORT INLAY EMBEDDED INTO PASSPORT
1110
PASSPORT PRINTED
1115
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1120
PASSPORT INITIALIZED
1125

FIG. 11

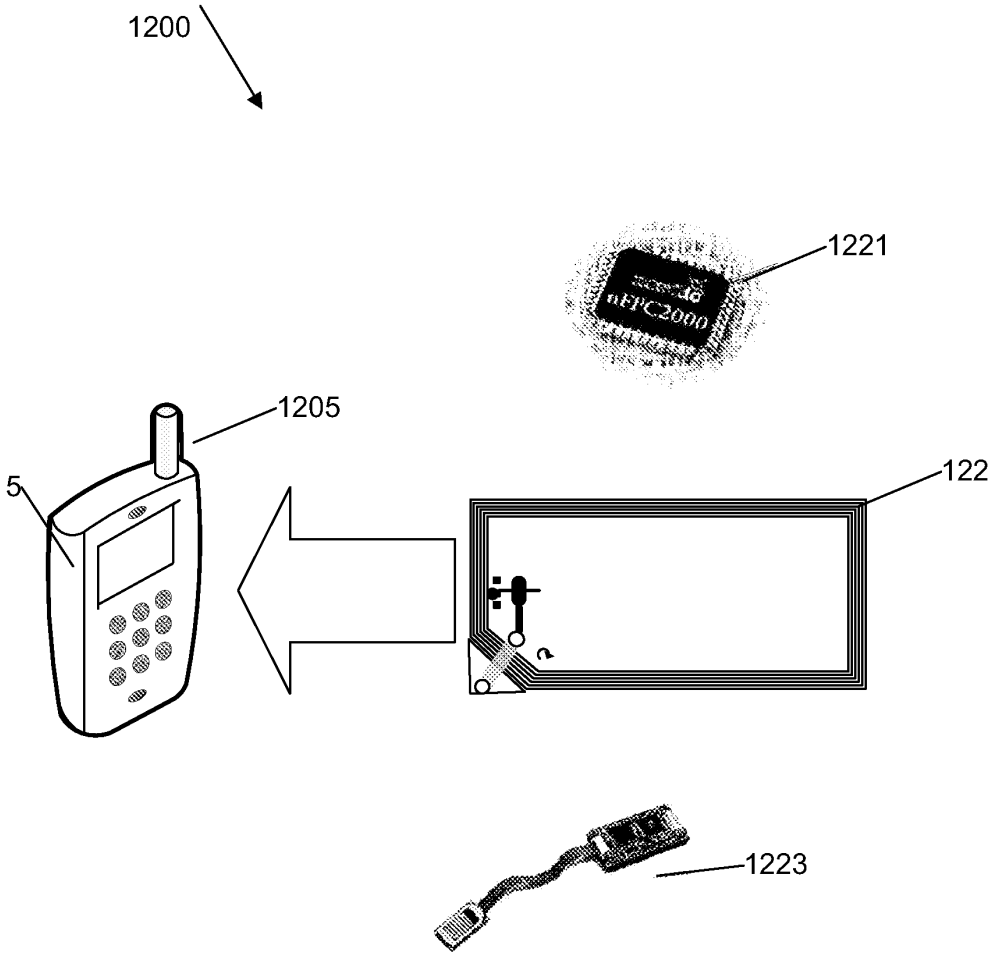


FIG. 12

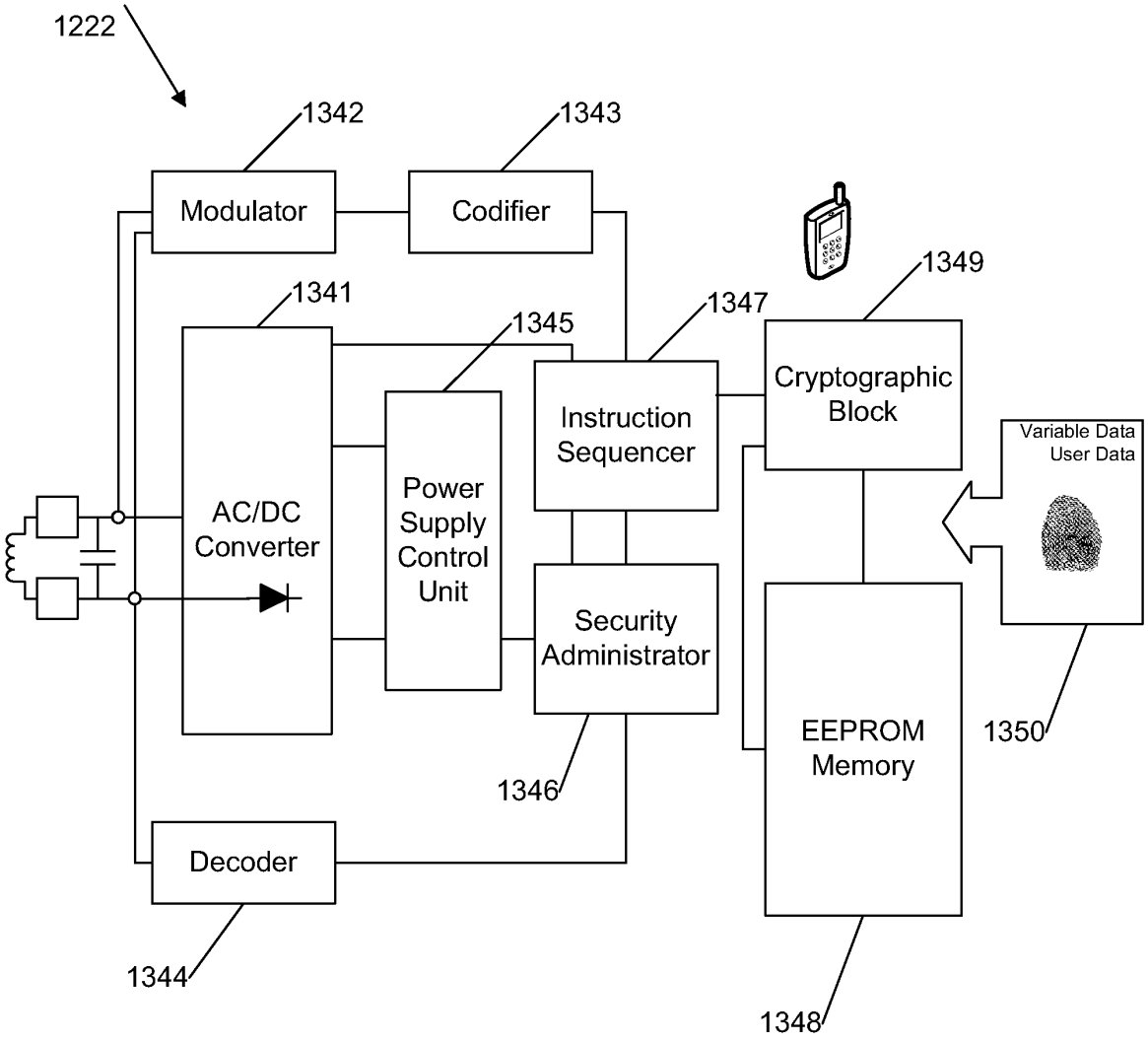

1222
1342
1343
Modulator
Codifier
1349
1341
1347
1345
Cryptographic Block
Instruction Sequencer
Variable Data
User Data
AC/DC Converter
Power Supply Control Unit
Security Administrator
EEPROM Memory
1350
1346
Decoder
1344
1348

FIG. 13

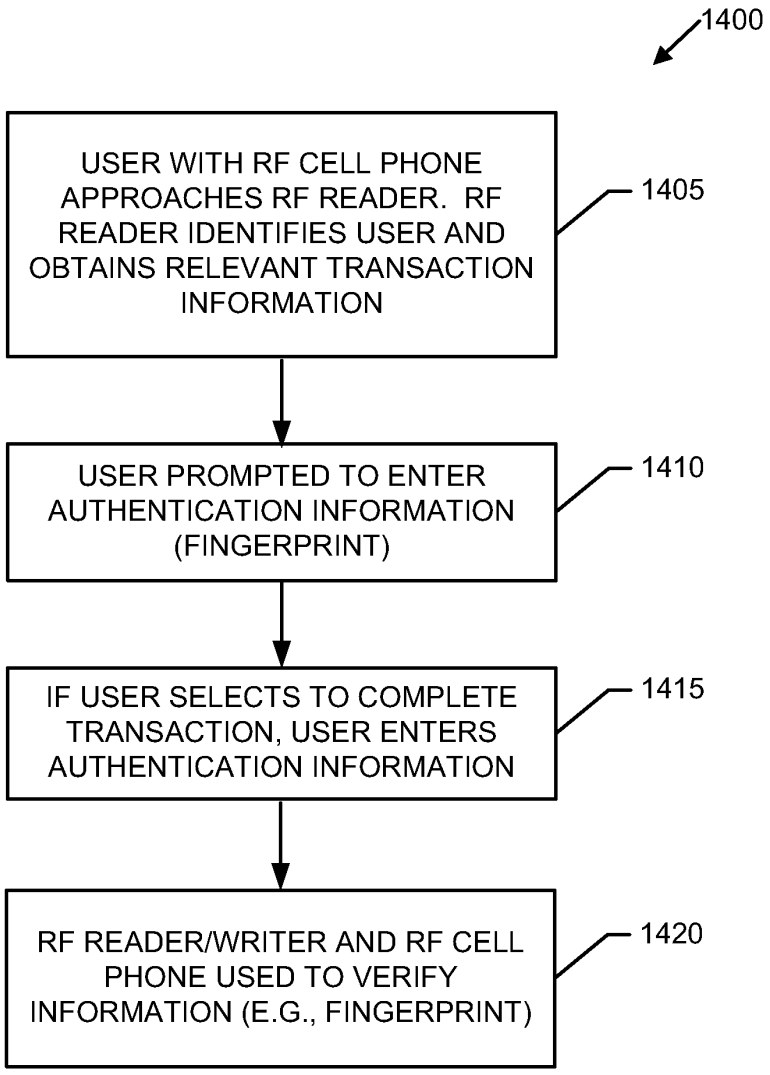

1400
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION
1405
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT)
1410
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION
1415
RF READER/WRITER AND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

FIG. 14

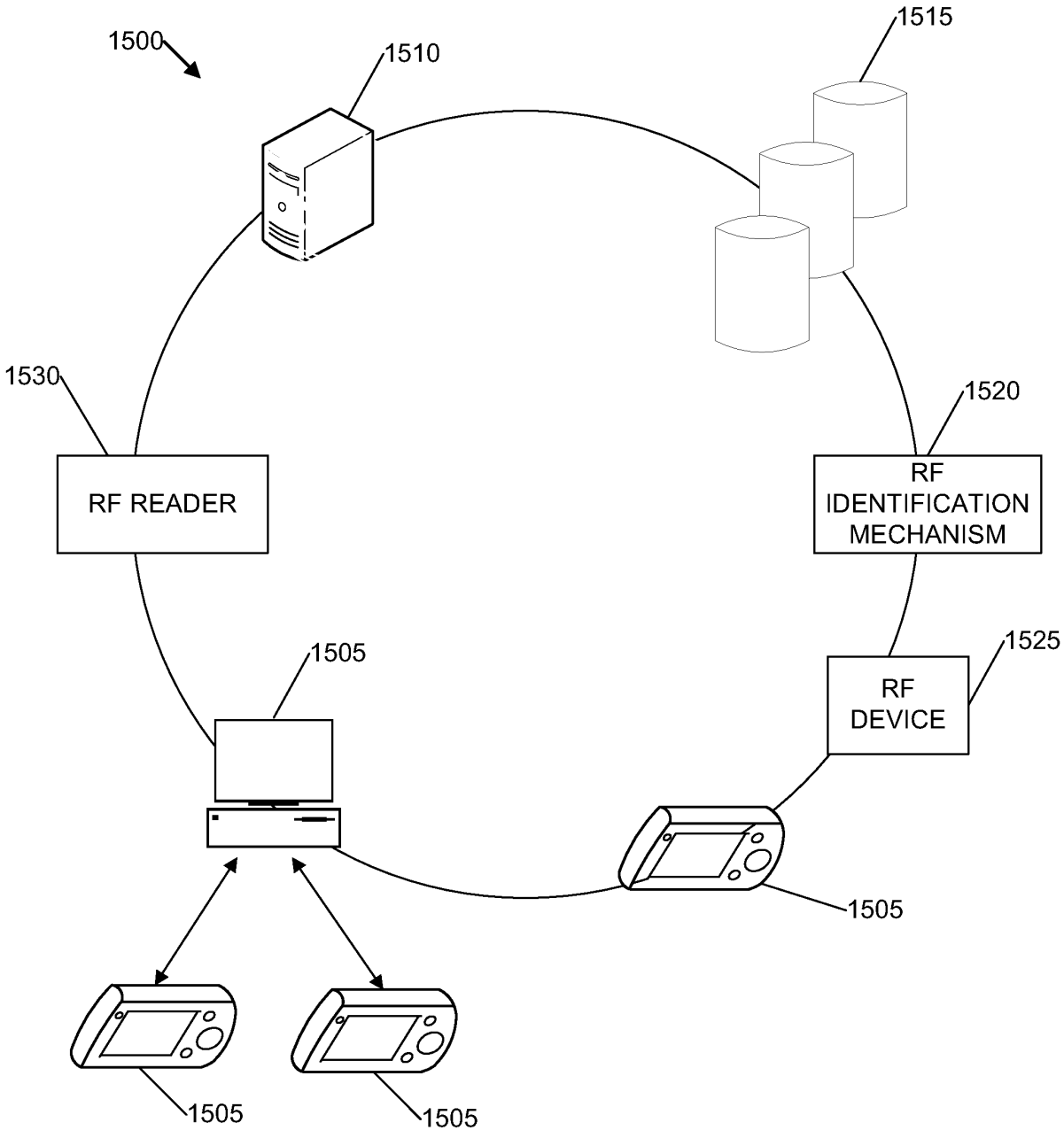

1500
1510
1515
1530
1520
RF READER
RF IDENTIFICATION MECHANISM
1505
1525
RF DEVICE
1505
1505
1505

FIG. 15

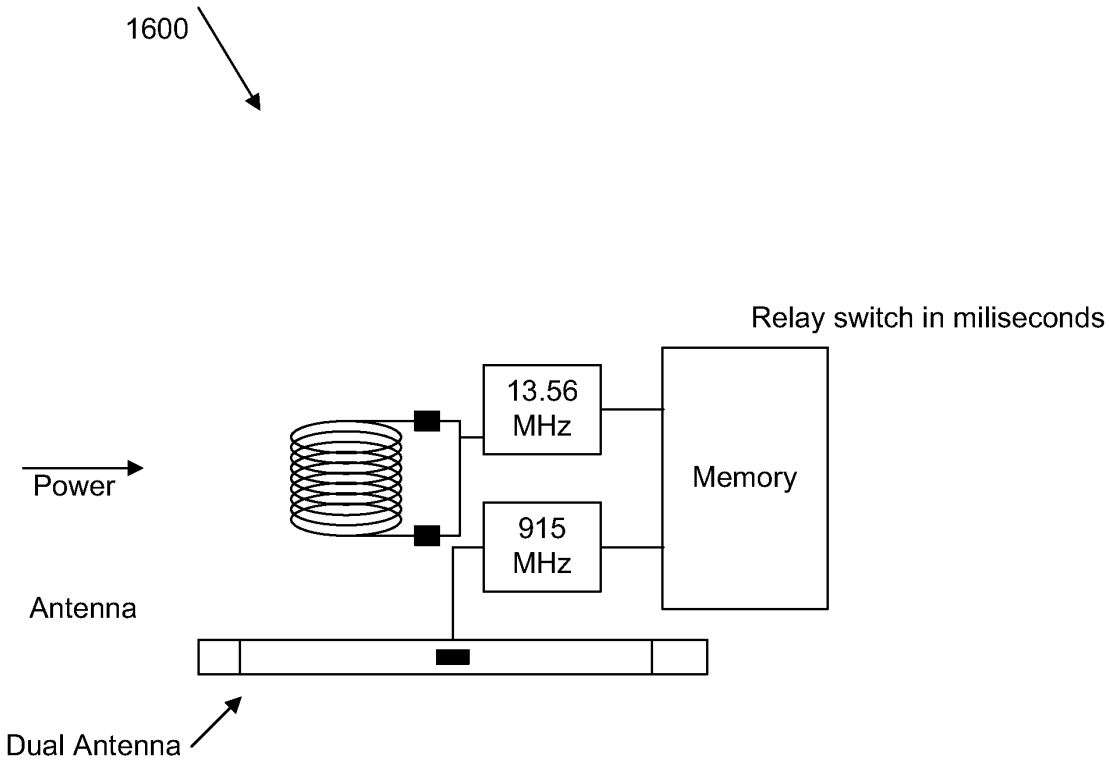

1600
Relay switch in miliseconds
13.56
MHz
915
MHz
Memory
Power
Antenna
Dual Antenna

FIG. 16

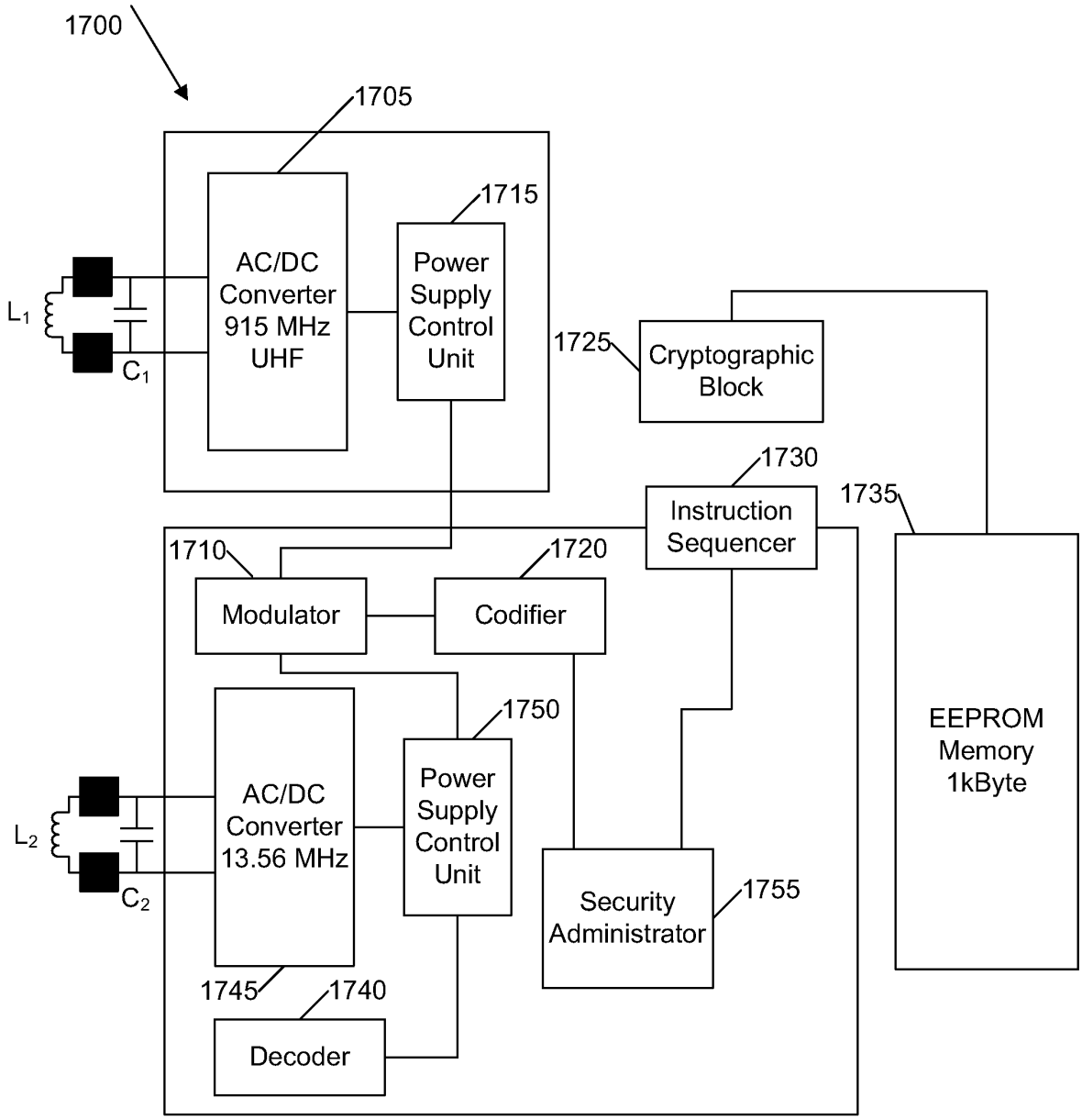

1700
1705
1715
AC/DC
Converter
915 MHz
UHF
Power
Supply
Control
Unit
L1
C1
1725
Cryptographic
Block
1730
1735
Instruction
Sequencer
1710
1720
Modulator
Codifier
1750
AC/DC
Converter
13.56 MHz
Power
Supply
Control
Unit
EEPROM
Memory
1kByte
L2
C2
Security
Administrator
1755
1745
1740
Decoder

FIG. 17

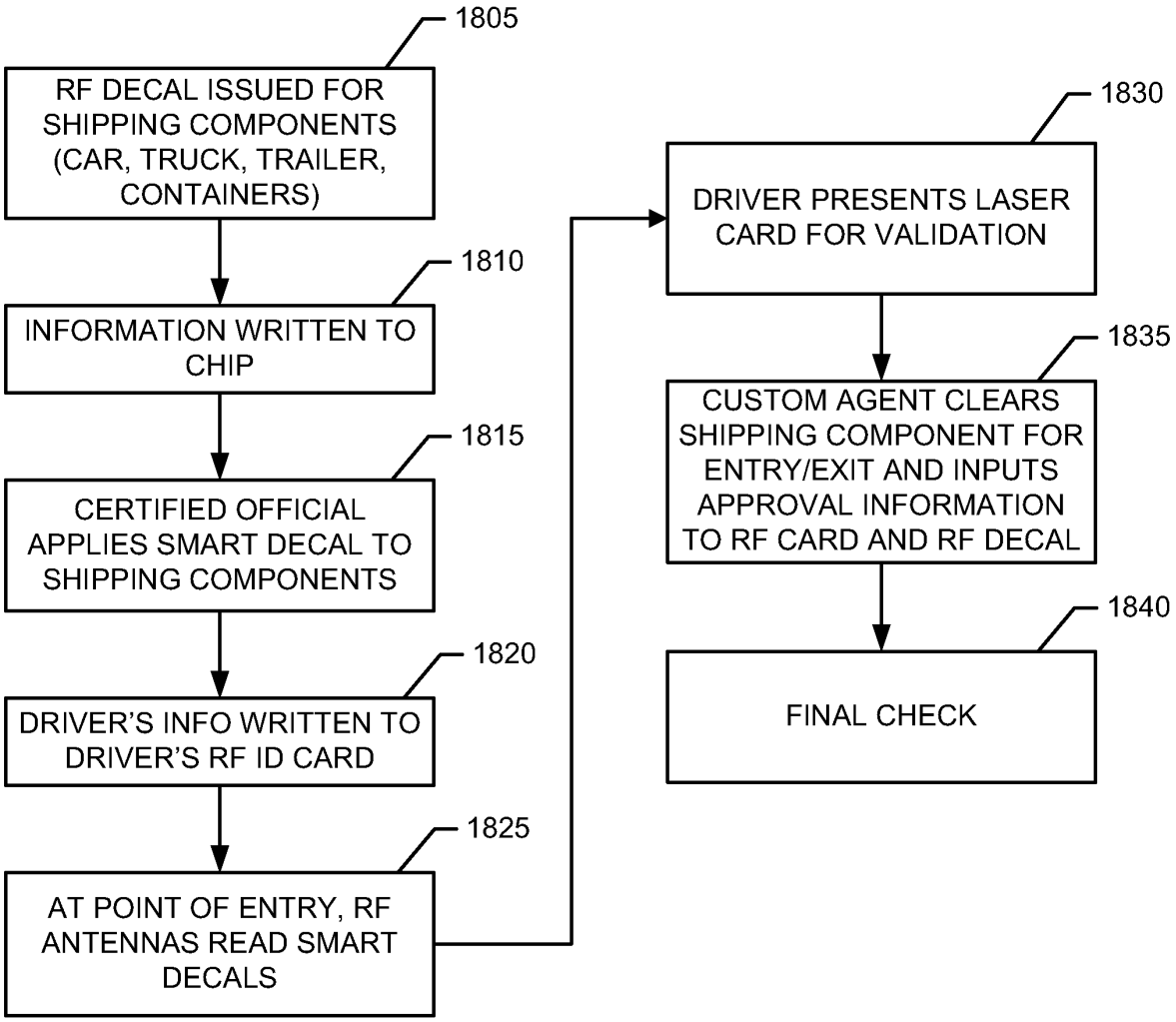

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS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

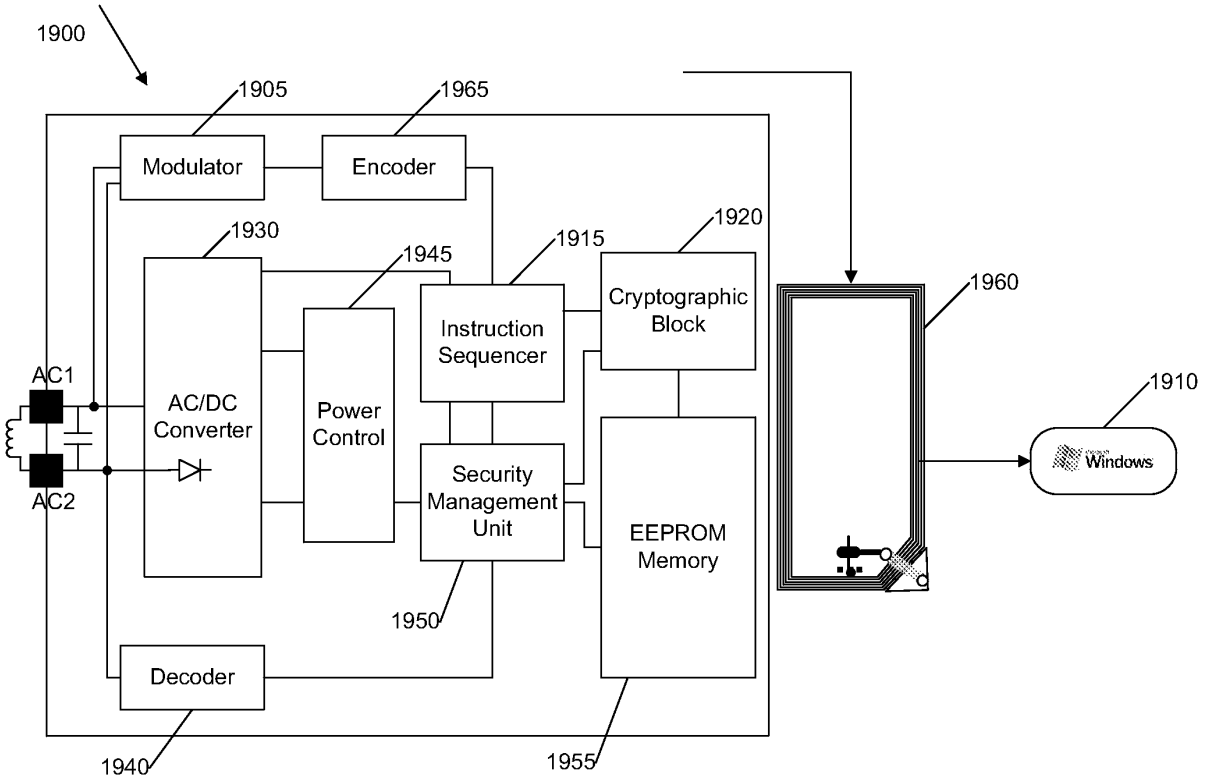

1900
1905
1965
Modulator
Encoder
1930
1945
1915
1920
Cryptographic Block
Instruction Sequencer
1960
AC1
AC/DC Converter
Power Control
1910
Windows
AC2
Security Management Unit
EEPROM Memory
1950
Decoder
1940
1955

FIG. 19

116546.1108C4/14445676.01

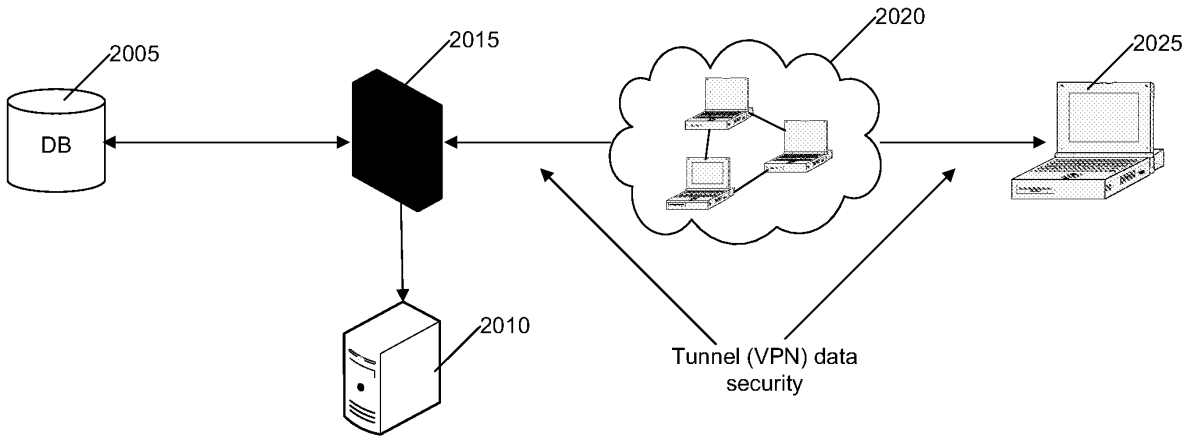


FIG. 20

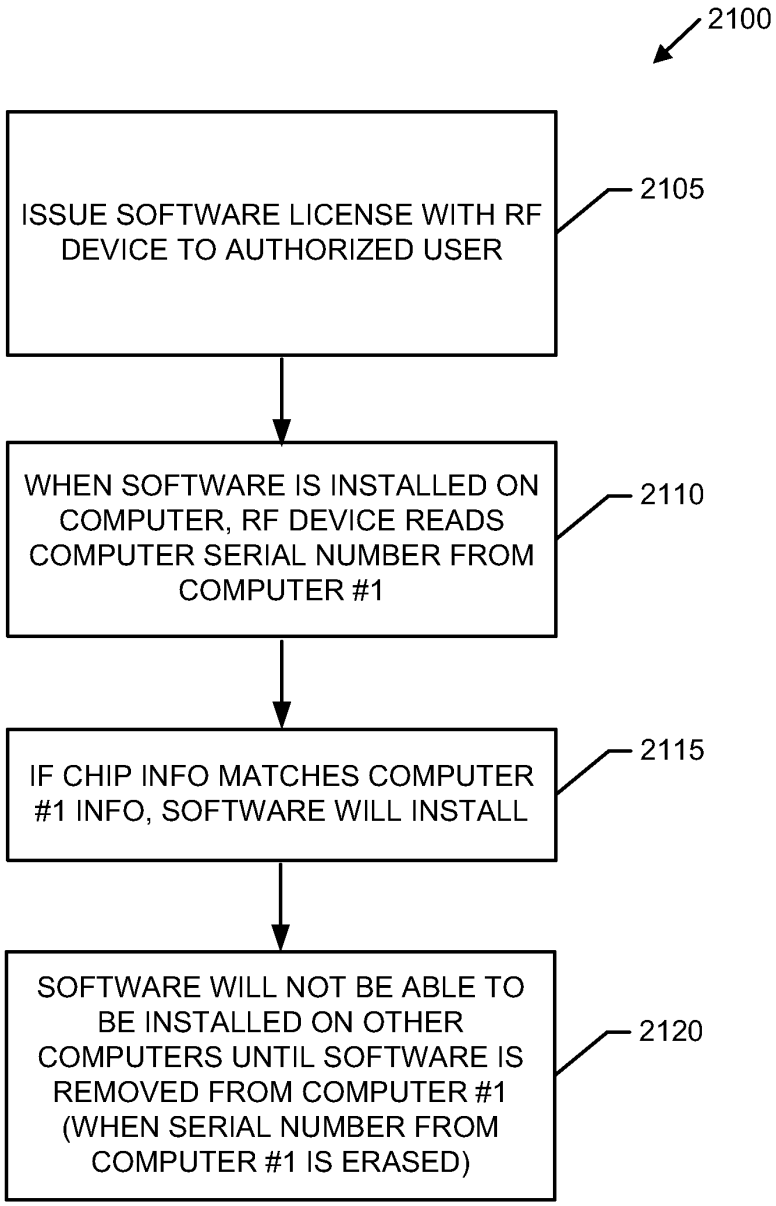

2100
ISSUE SOFTWARE LICENSE WITH RF DEVICE TO AUTHORIZED USER
2105
WHEN SOFTWARE IS INSTALLED ON COMPUTER, RF DEVICE READS COMPUTER SERIAL NUMBER FROM COMPUTER #1
2110
IF CHIP INFO MATCHES COMPUTER #1 INFO, SOFTWARE WILL INSTALL
2115
SOFTWARE WILL NOT BE ABLE TO BE INSTALLED ON OTHER COMPUTERS UNTIL SOFTWARE IS REMOVED FROM COMPUTER #1 (WHEN SERIAL NUMBER FROM COMPUTER #1 IS ERASED)
2120

FIG. 21

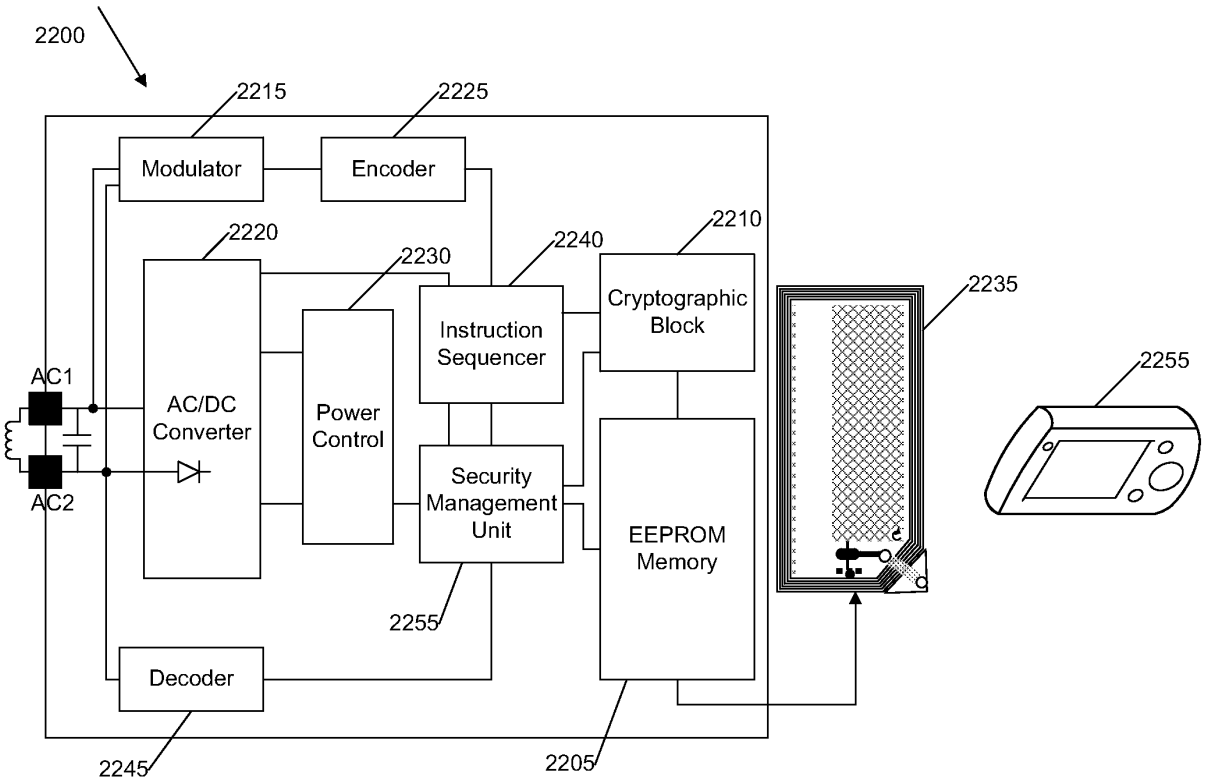

2200
2215
2225
Modulator
Encoder
2220
2230
2240
2210
2235
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
2255
AC2
Security Management Unit
EEPROM Memory
2255
Decoder
2245
2205

FIG. 22

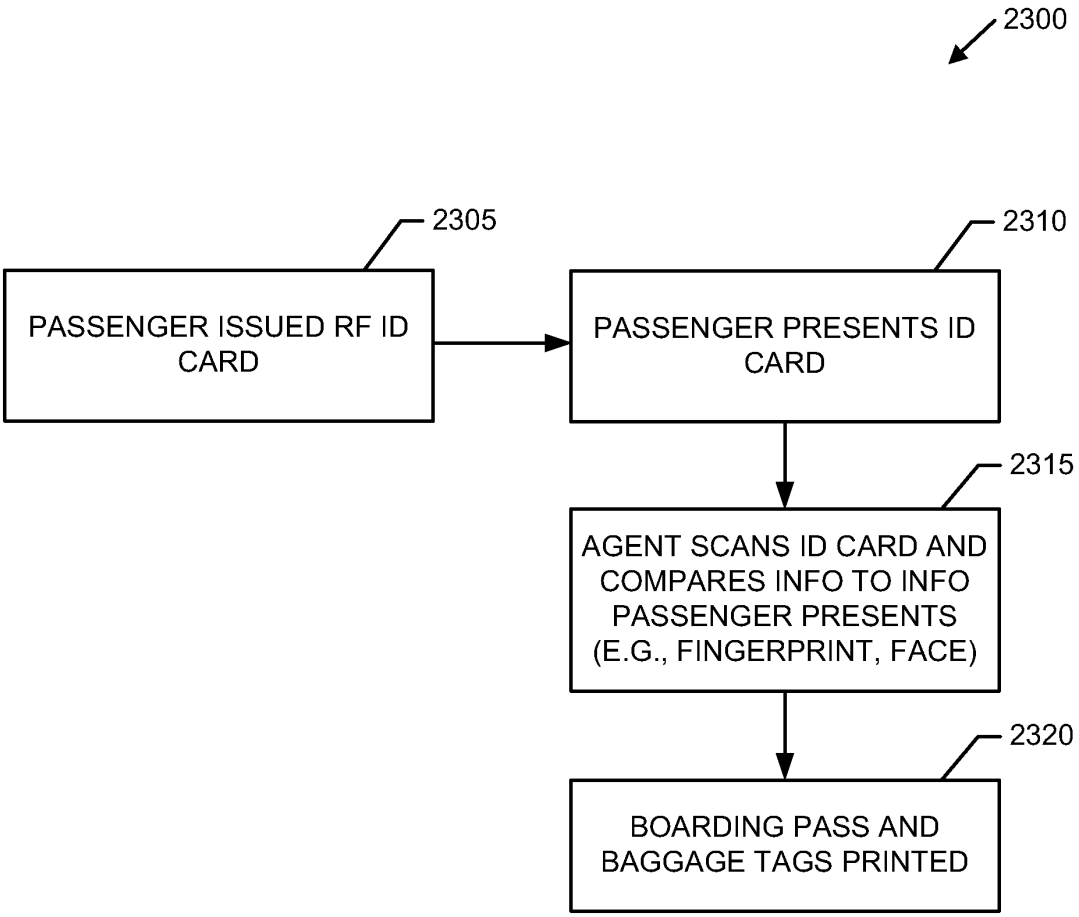

2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENT SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

FIG. 23

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 IDENTIFICATION SOLUTIONS

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/084,565 filed on November 19, 2013.

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): 3-11-2015

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 1 minute to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

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 IDENTIFICATION SOLUTIONS

As the below named inventor, I hereby declare that:

This declaration is directed to:

- ☐ The attached application, or
- ■ United States application or PCT international application number 14/084,565 filed on November 19, 2013.

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.

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.

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.

WHAT IS CLAIMED IS:

1. A mobile device, comprising:

a biometric input device configured to receive biometric data;

a short range radio frequency antenna;

memory configured to store biometric information for identifying an individual associated with transaction information, and

a processor coupled with the memory and the biometric input device, the processor configured to:

receive a signal via the short range radio frequency antenna, the signal comprising a request to access the memory and retrieve the transaction information,

receive biometric information from the biometric input device,

compare the received biometric information with the biometric information stored in the memory, and

provide the transaction information in response to the access request when the received biometric information matches the stored biometric information.

2. The mobile device of claim 1, wherein the mobile device is one of a cellphone, smartphone, or tablet.

3. The mobile device of claim 1, wherein the biometric input device is a fingerprint scanner.

4. The mobile device of claim 1, wherein the processor is further configured to provide the received biometric information or the stored biometric information with the transaction information.

5. The mobile device of claim 1, wherein the transaction information is account information.

6. The mobile device of claim 1, wherein the transaction information is credit card information.

7. The mobile device of claim 1, further comprising memory configured to store the transaction information.

8. The mobile device of claims 7, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

9. A cellular telephone, comprising:

a fingerprint scanner configured to receive fingerprint information;

a short range radio frequency antenna;

memory configured to store fingerprint information for identifying an individual associated with transaction information, and

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal via the short range radio frequency antenna, the signal comprising a request to access the memory and retrieve the transaction information,

receive fingerprint information from the fingerprint scanner,

compare the received fingerprint information with the fingerprint information stored in the memory, and

provide the transaction information in response to the access request when the received fingerprint information matches the stored fingerprint information.

10. The cellular telephone of claim 9, wherein the processor is further configured to provide the received fingerprint information or the stored fingerprint information with the transaction information.

11. The cellular telephone of claim 9, wherein the transaction information is account information.

12. The cellular telephone of claim 9, wherein the transaction information is credit card information.

13. The cellular telephone of claim 9, further comprising memory configured to store the transaction information.

14. The cellular telephone of claims 13, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

15. A cellular telephone, comprising:

cellular circuitry;

a fingerprint scanner configured to receive fingerprint information;

a short range radio frequency antenna and a chip, the chip comprising:

a memory, the memory configured to store fingerprint information for identifying an individual associated with transaction information, and

a processor coupled with the memory and the fingerprint scanner, the processor configured to:

receive a signal via the cellular circuitry, the signal comprising a request to access the memory and retrieve the transaction information,

receive fingerprint information from the fingerprint scanner,

compare the received fingerprint information with the fingerprint information stored in the memory, and

provide the transaction information in response to the access request when the received fingerprint information matches the stored fingerprint information.

16. The cellular telephone of claim 15, wherein the processor is further configured to provide the received fingerprint information or the stored fingerprint information with the transaction information.

17. The cellular telephone of claim 15, wherein the transaction information is account information.

18. The cellular telephone of claim 15, wherein the transaction information is credit card information.

19. The cellular telephone of claim 15, further comprising memory configured to store the transaction information.

20. The cellular telephone of claims 19, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

SPECIFICATION

SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

RELATED APPLICATIONS INFORMATION

This application is a continuation of Application Serial Number 14/084,565, filed on November 19, 2013, which is a continuation of 13/350,665, filed on January 13, 2012, now Patent Number 8,587,436, issued on November 19, 2013, which is a continuation of U.S. Patent Application Ser. No. 13/175,768, filed on July 1, 2011, now Patent Number 8,237,568, issued on August 7 2012, which is a continuation of U.S. 12/688,666, filed on January 15, 2010, now Patent Number 8,004,410, issued on August 23, 2011, which is a continuation of U.S. Application Number 11/279,912, filed on April 17, 2006, now Patent Number 7,671,746, issued on March 2, 2010, which is a continuation of U.S. Application Number 10/615,026, filed on July 9, 2003, now Patent Number 7,081,819, issued on July 25, 2006, which in turn claims the benefit under 35 U.S.C. 119(e) to U.S. Provisional Patent Application Ser. No. 60/394,241, filed July 9, 2002, all of which are incorporated herein by reference in their entirety as if set forth in full.

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, in 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 HolomatrixTM 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-417

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 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.

[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 "upconversion" 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) 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

[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 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

[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 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.

[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 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.

[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 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.

[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 April 30, 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 Oracle9i 1Developer, 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 (FIPS) 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 = capacitance (F)

[0094] 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*

$$L = \frac{N^2 \mu_o A}{l}$$

N = number of windings around inductor
μ_o *= permeability of freespace (H* m^{-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 ^ (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 3B.

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 control 2230, 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.