Doc Code: TRACK1.REQ
Document Description: TrackOne Request

PTO/AIA/424 (04-14)

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Francisco Martinez de Velasco Cortina	Nonprovisional Application Number (if known):	116546-660CT2
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i)(1) and the prioritized examination fee set forth in 37 CFR 1.17(c) have been filed with the request. The publication fee requirement is met because that fee, set forth in 37 CFR 1.18(d), is currently $0. The basic filing fee, search fee, and examination fee are filed with the request or have been already been paid. I understand that any required excess claims fees or application size fee must be paid for the application.

2. I understand that the application may not contain, or be amended to contain, more than four independent claims, more than thirty total claims, or any multiple dependent claims, and that any request for an extension of time will cause an outstanding Track I request to be dismissed.

3. The applicable box is checked below:

I. ☑ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed inventor's oath or declaration under 37 CFR 1.63 or 37 CFR 1.64 for each inventor, **or** the application data sheet meeting the conditions specified in 37 CFR 1.53(f)(3)(i) is filed with the application.

II. ☐ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form.
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /li zhang/	Date 2015-03-04
Name (Print/Typed) Li Zhang	Practitioner Registration Number 70902

Note: *This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. Submit multiple forms if more than one signature is required.**

☑ *Total of 1 forms are submitted.

Privacy Act Statement

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

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

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

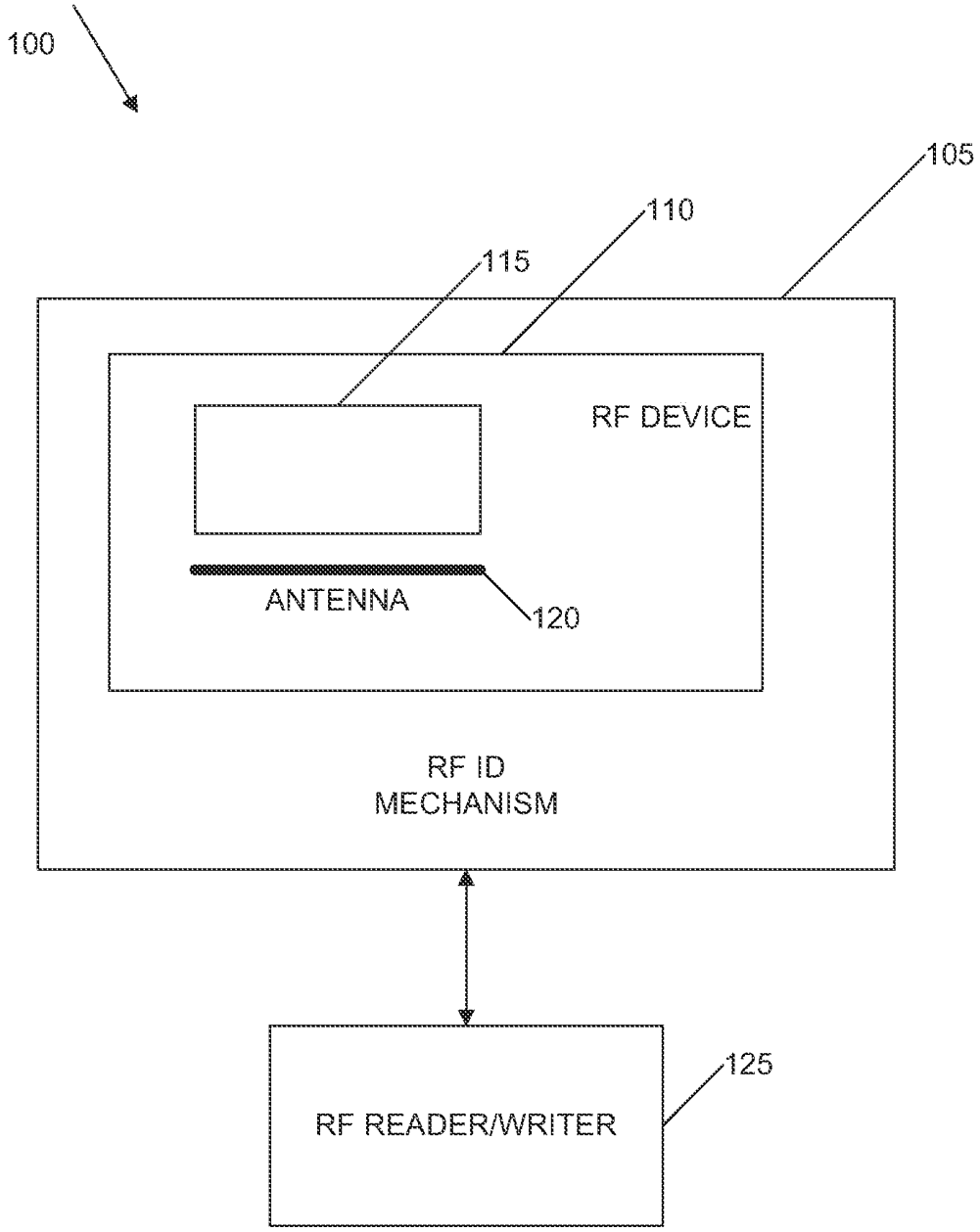

100
105
110
115
RF DEVICE
ANTENNA
120
RF ID
MECHANISM
125
RF READER/WRITER

FIG. 1

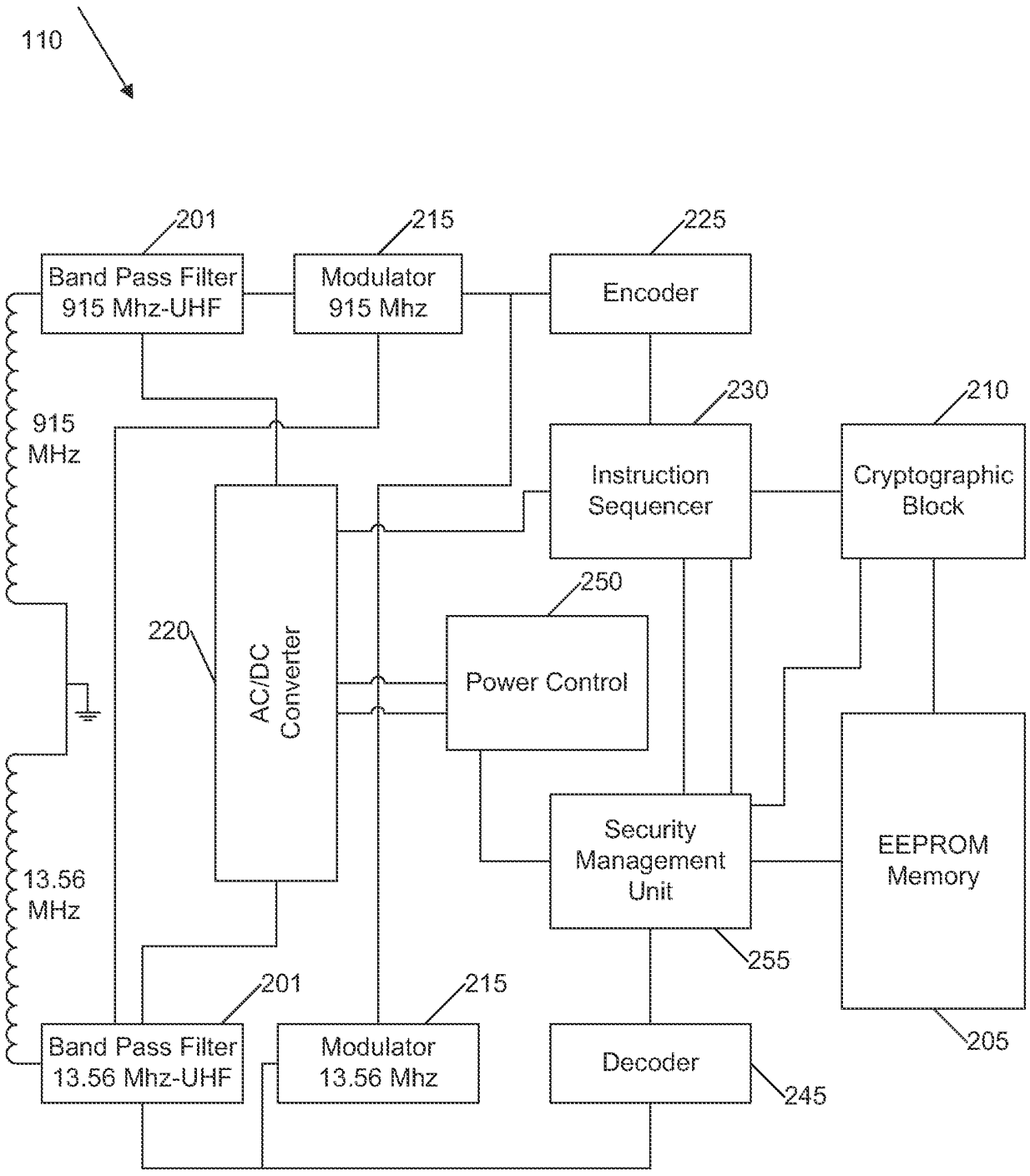

110
201
Band Pass Filter
915 Mhz-UHF
215
Modulator
915 Mhz
225
Encoder
915
MHz
230
Instruction
Sequencer
210
Cryptographic
Block
250
220
AC/DC
Converter
Power Control
13.56
MHz
Security
Management
Unit
EEPROM
Memory
255
201
215
Band Pass Filter
13.56 Mhz-UHF
Modulator
13.56 Mhz
Decoder
245
205

FIG. 2

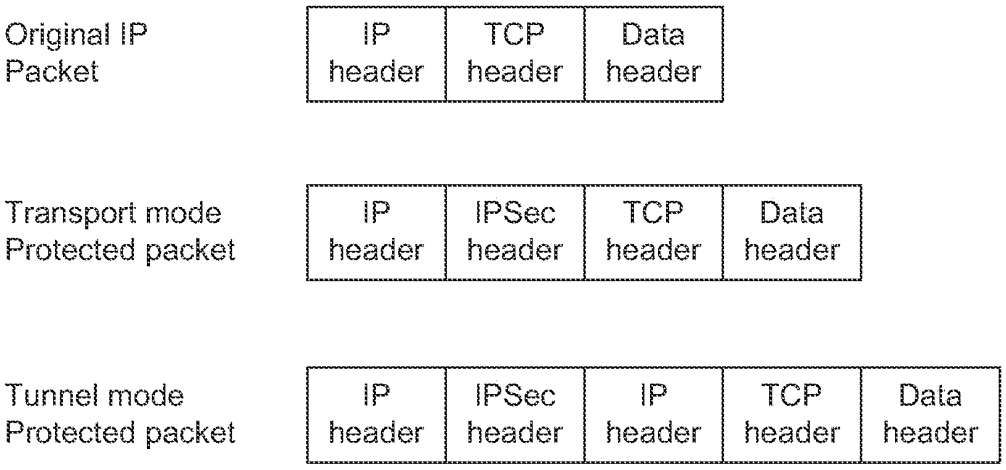

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIG. 3A

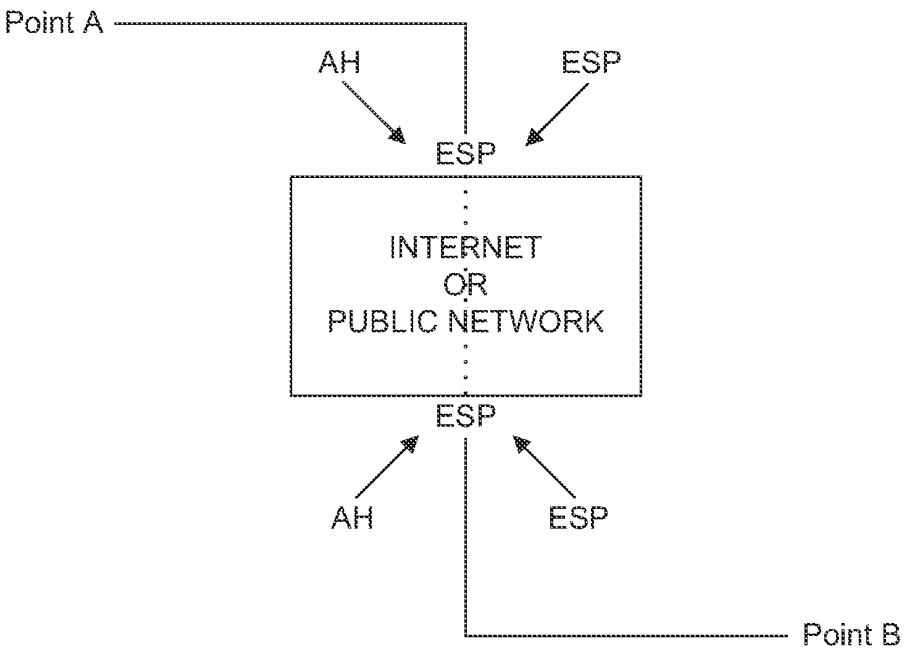

Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORK
ESP
AH
ESP
Point B

FIG. 3B

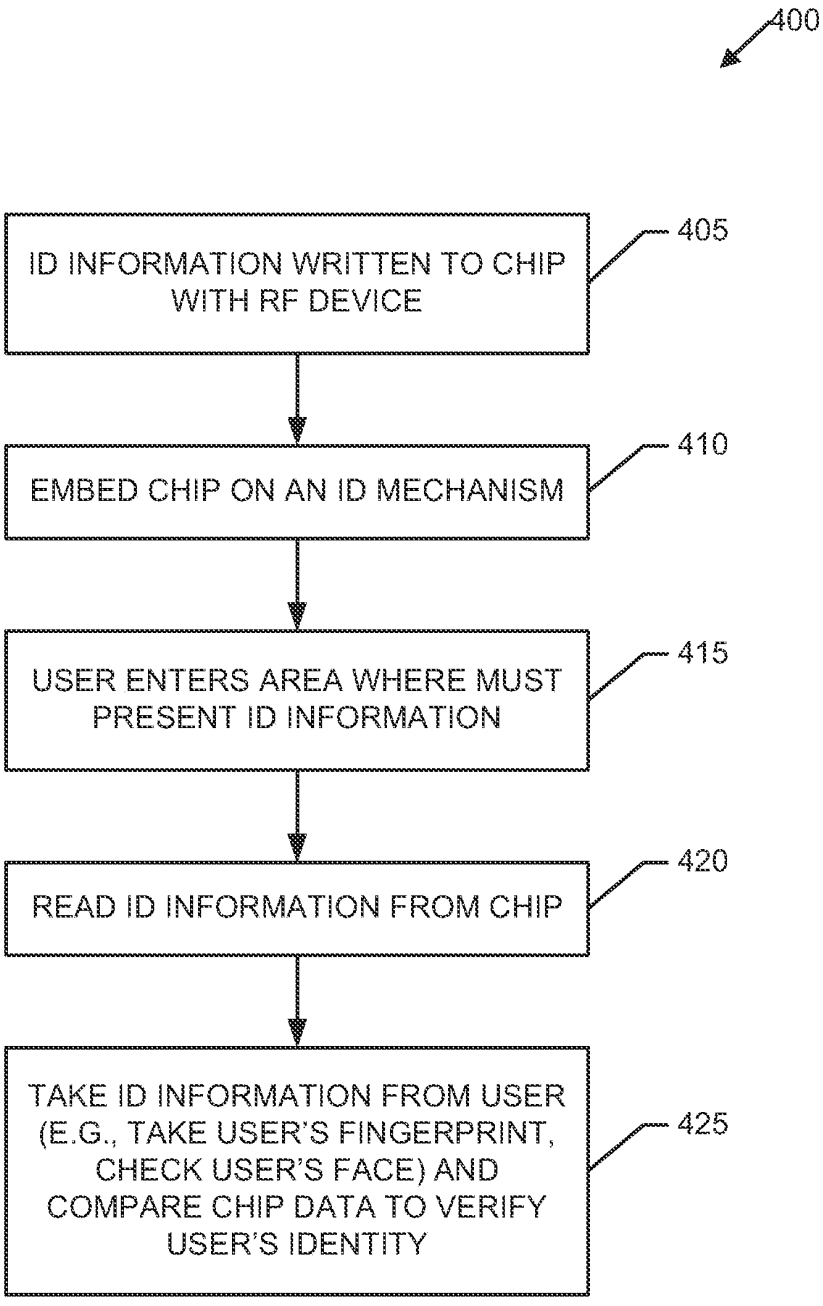

400
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
405
EMBED CHIP ON AN ID MECHANISM
410
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
415
READ ID INFORMATION FROM CHIP
420
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE CHIP DATA TO VERIFY USER'S IDENTITY
425

FIG. 4

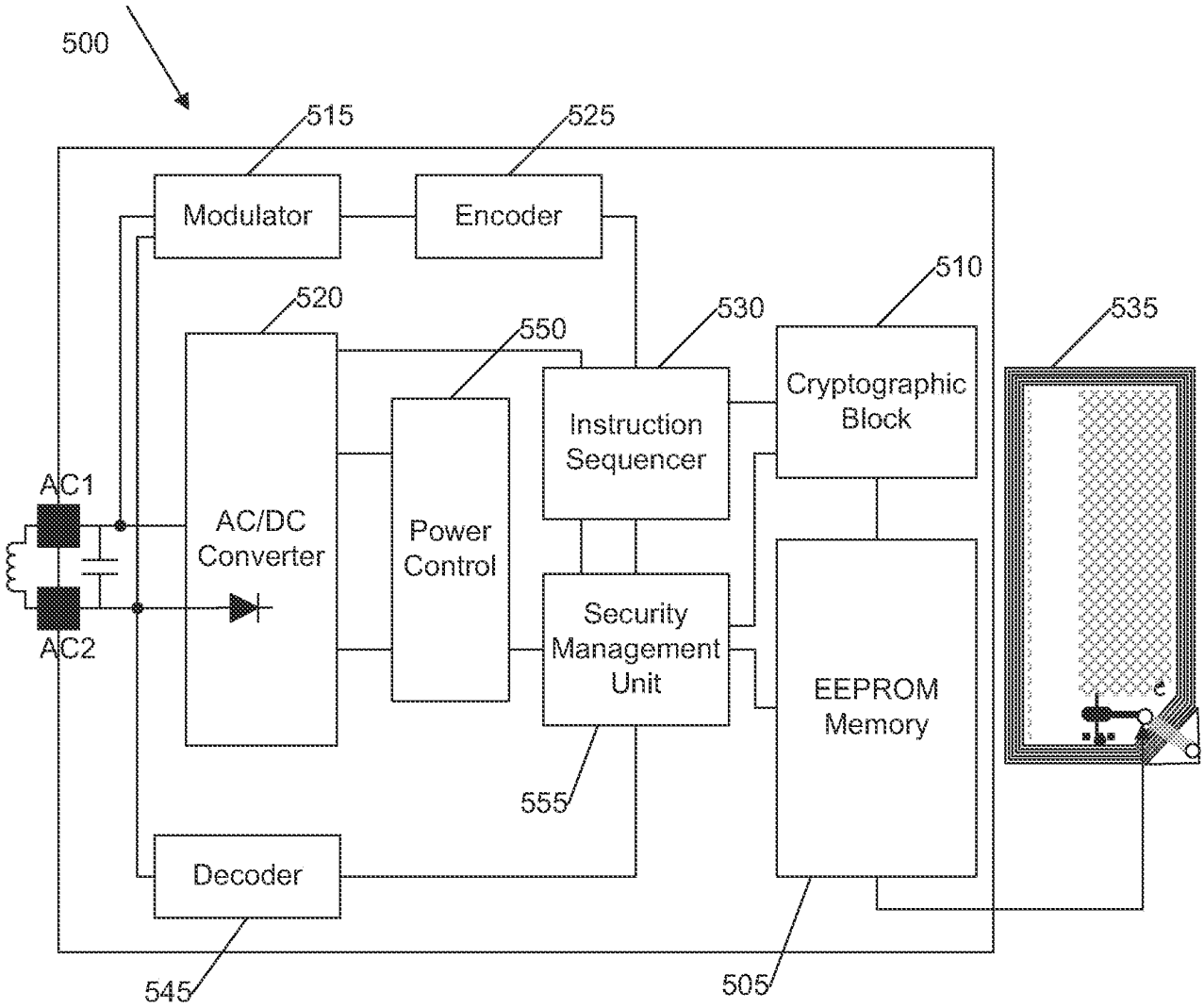

500
515
525
Modulator
Encoder
510
520
530
535
550
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
555
Decoder
545
505

FIG. 5

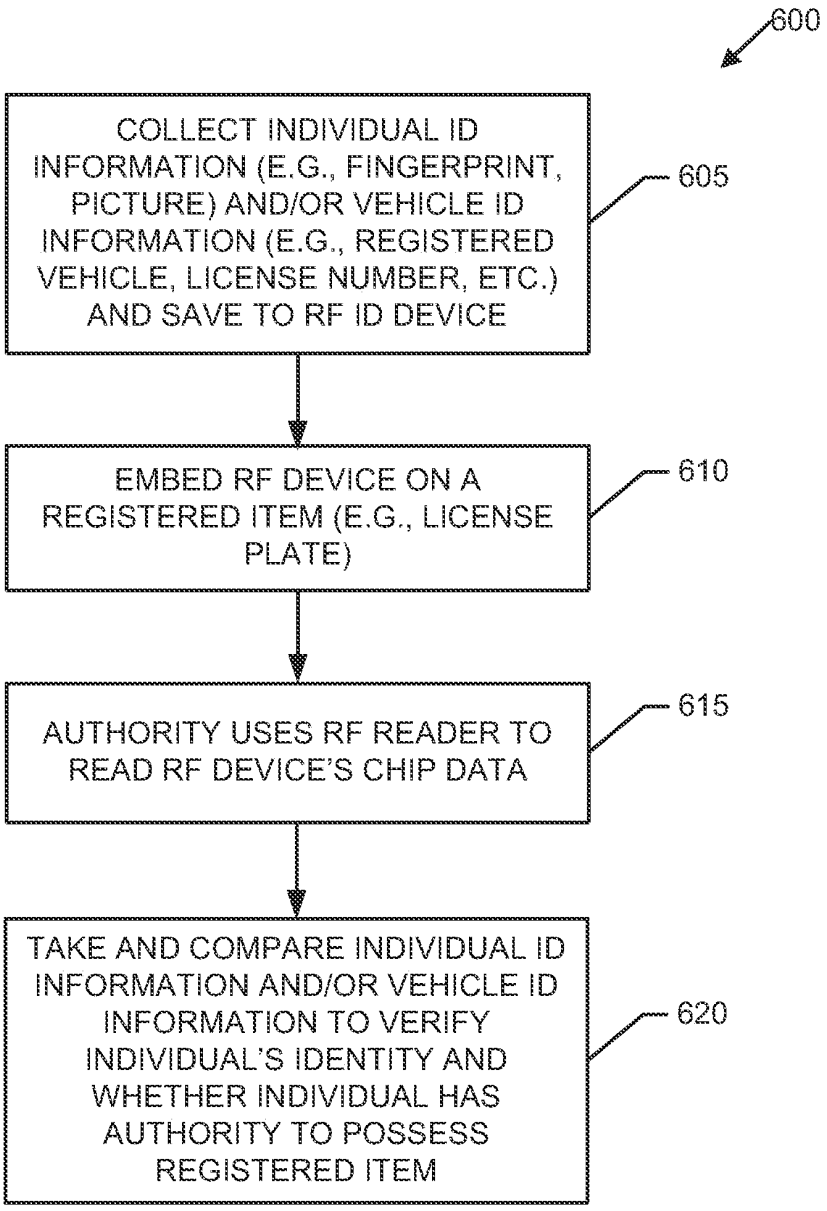

600
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
605
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
610
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
615
TAKE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

FIG. 6

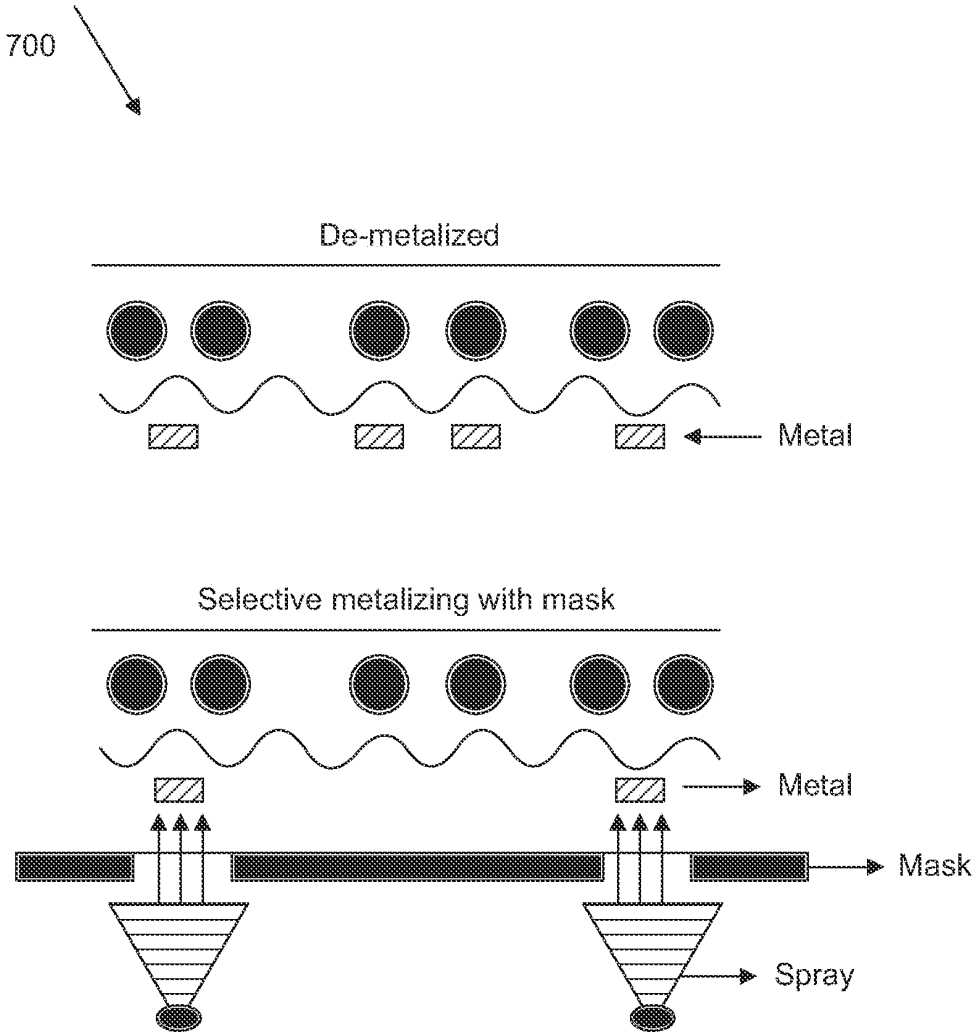

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIG. 7

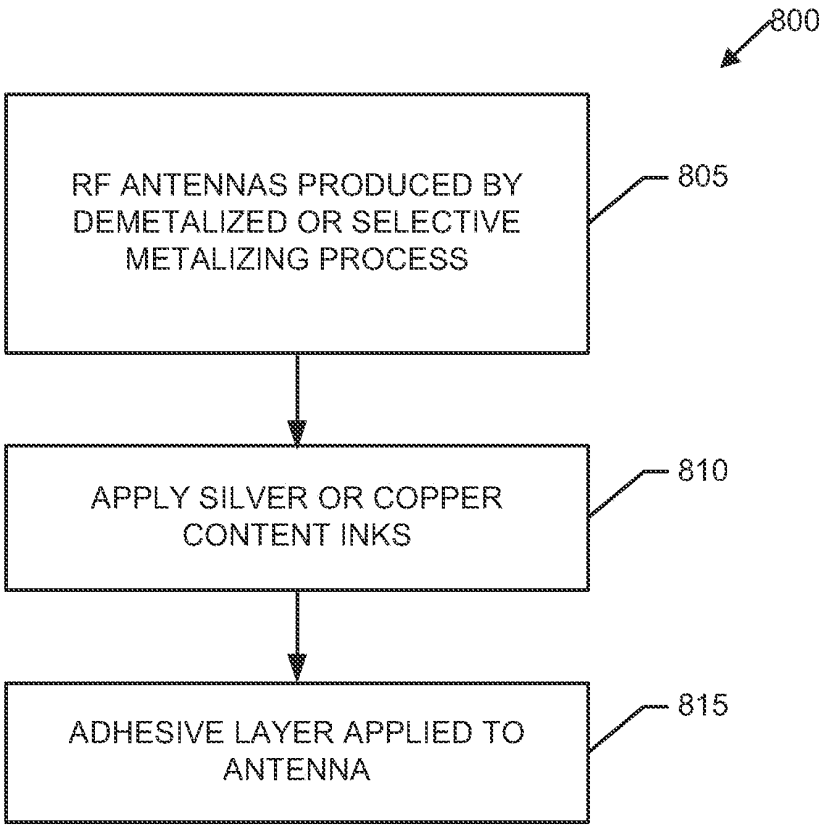

800
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
805
APPLY SILVER OR COPPER CONTENT INKS
810
ADHESIVE LAYER APPLIED TO ANTENNA
815

FIG. 8

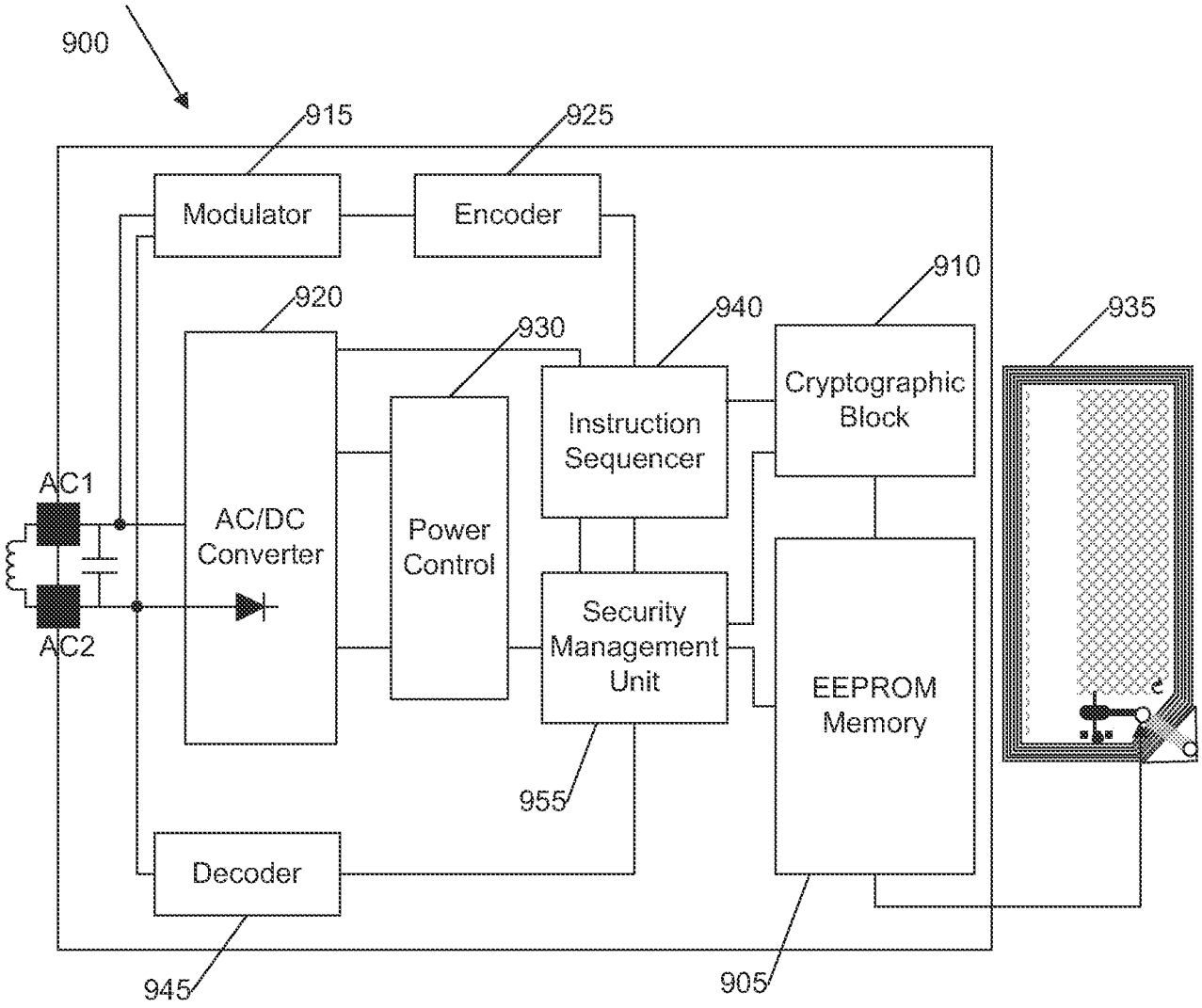

900
915
925
Modulator
Encoder
910
920
930
940
935
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
955
Decoder
945
905

FIG. 9

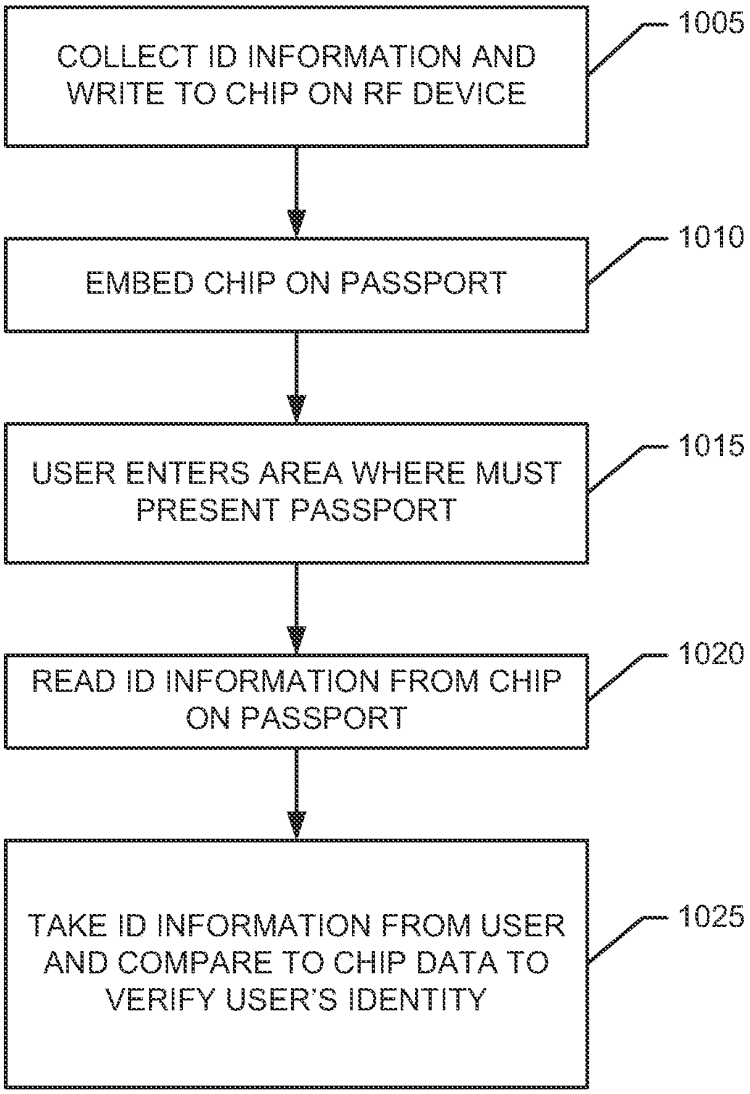

COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1005
EMBED CHIP ON PASSPORT
1010
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1015
READ ID INFORMATION FROM CHIP ON PASSPORT
1020
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY
1025

FIG. 10

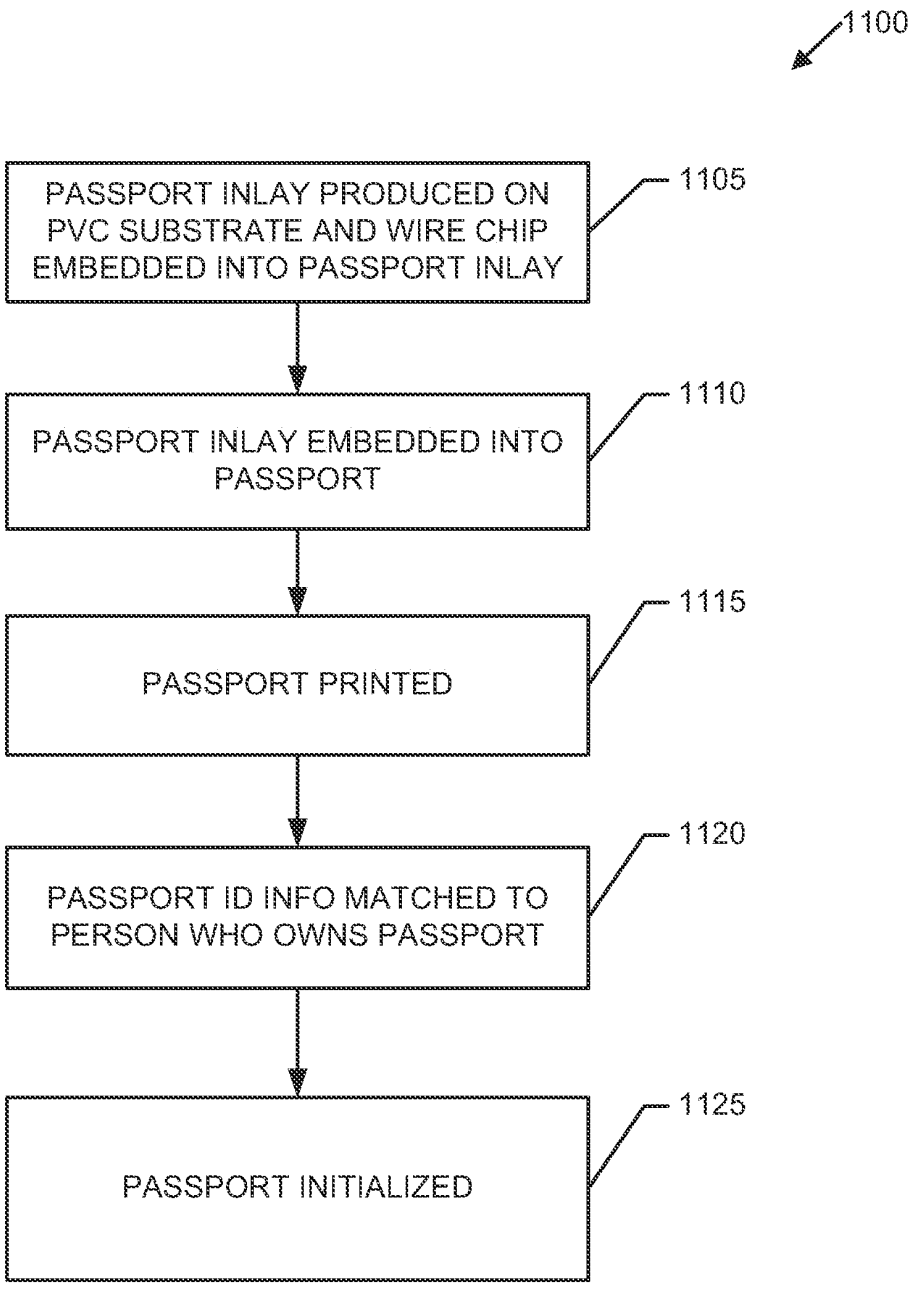

1100
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1105
PASSPORT INLAY EMBEDDED INTO PASSPORT
1110
PASSPORT PRINTED
1115
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1120
PASSPORT INITIALIZED
1125

FIG. 11

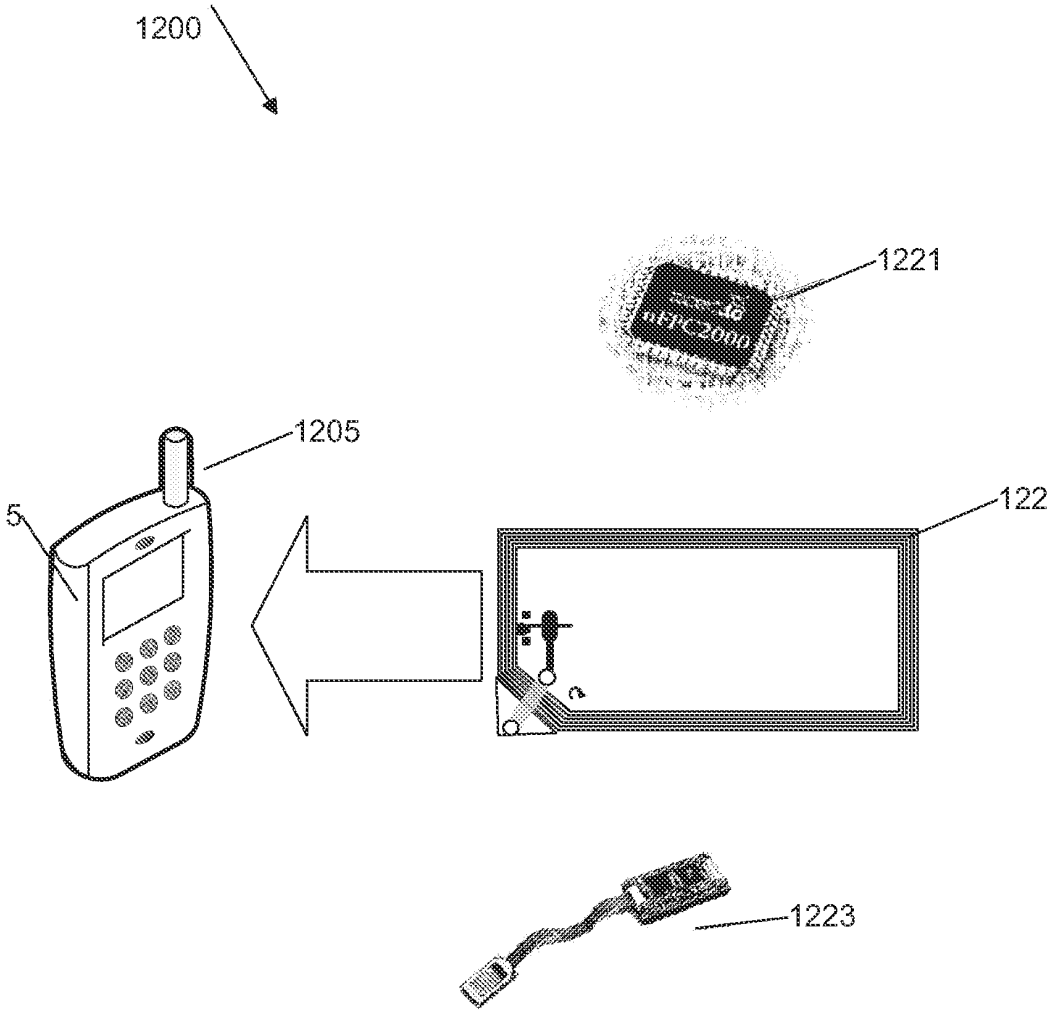


FIG. 12

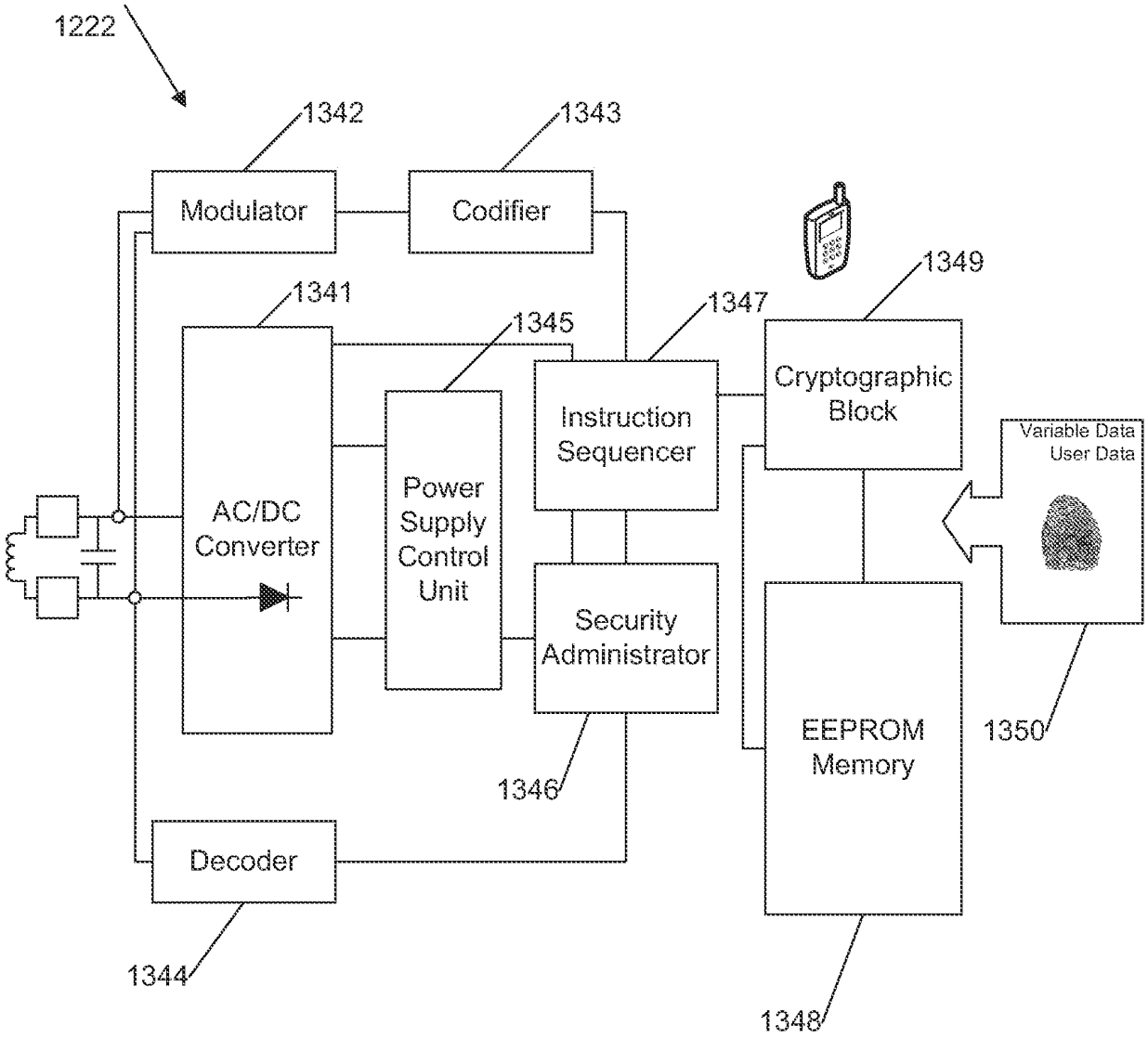

1222
1342
1343
Modulator
Codifier
1349
1341
1345
1347
Cryptographic Block
Instruction Sequencer
Variable Data
User Data
AC/DC Converter
Power Supply Control Unit
Security Administrator
EEPROM Memory
1350
1346
Decoder
1344
1348

FIG. 13

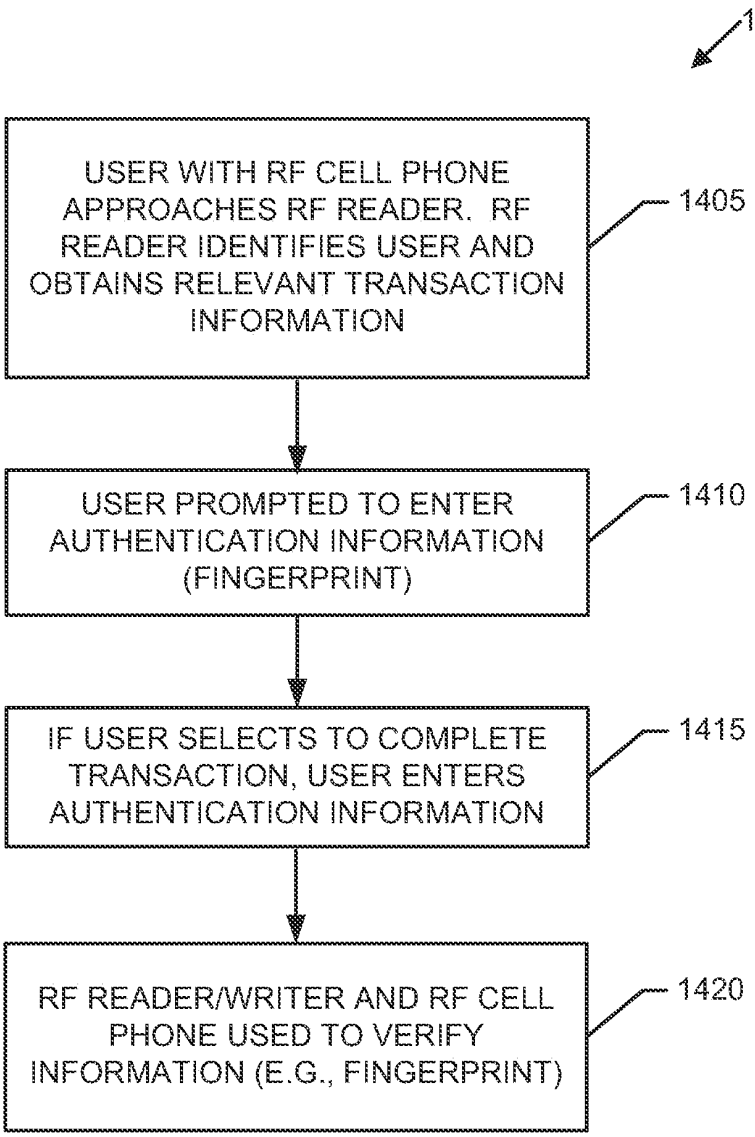

1400
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION
1405
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT)
1410
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION
1415
RF READER/WRITER AND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

FIG. 14

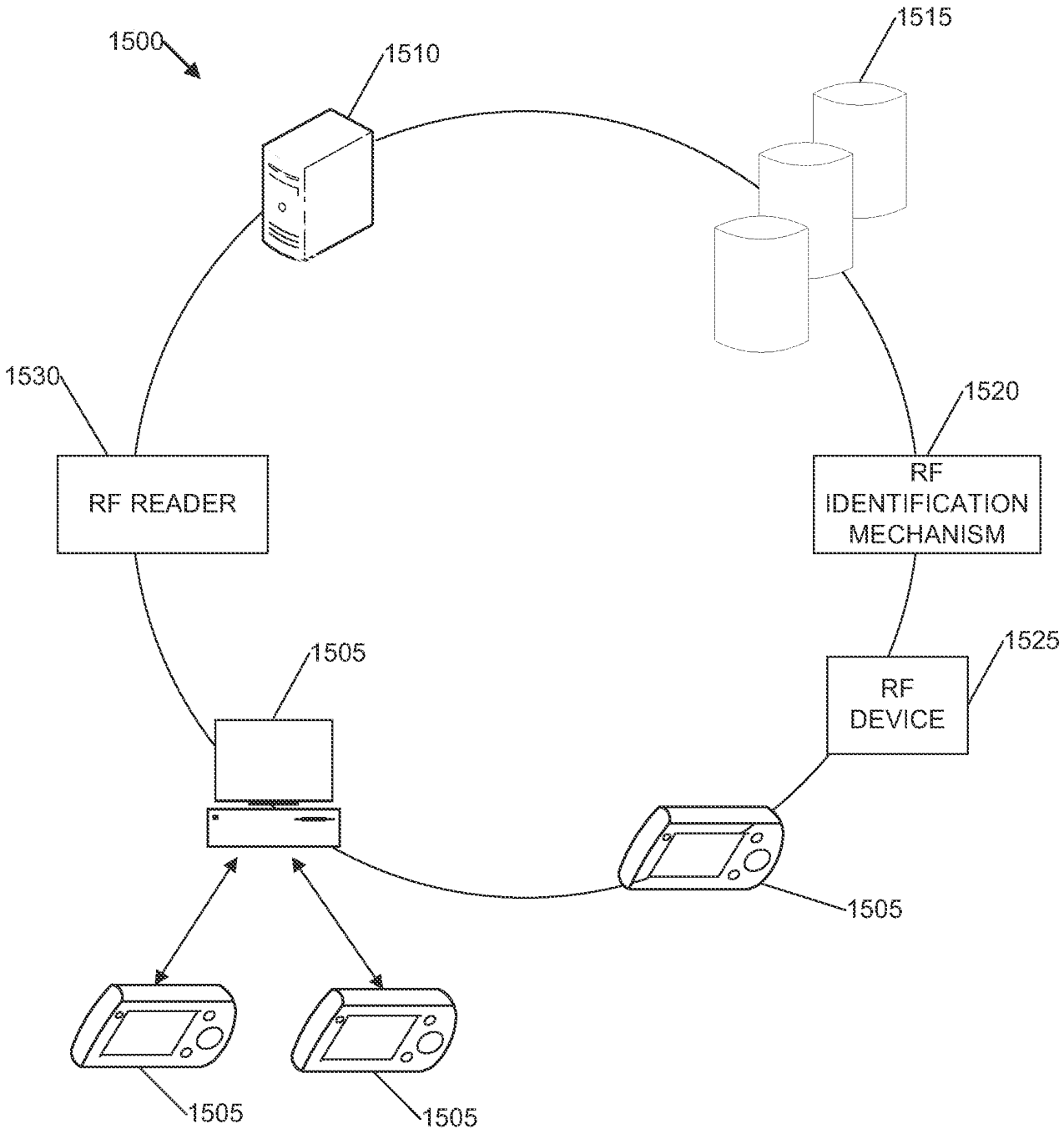

1500
1510
1515
1530
1520
RF READER
RF IDENTIFICATION MECHANISM
1505
1525
RF DEVICE
1505
1505
1505

FIG. 15

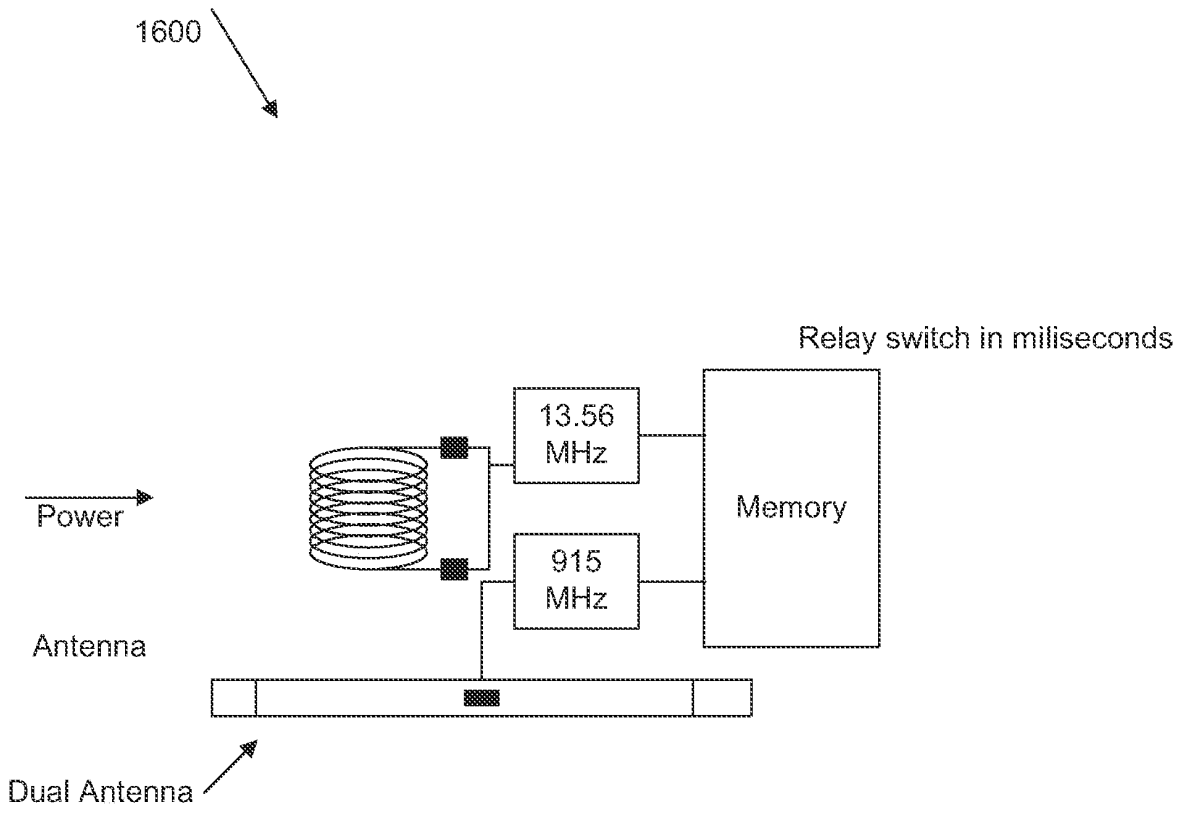

1600
Relay switch in miliseconds
13.56
MHz
915
MHz
Memory
Power
Antenna
Dual Antenna

FIG. 16

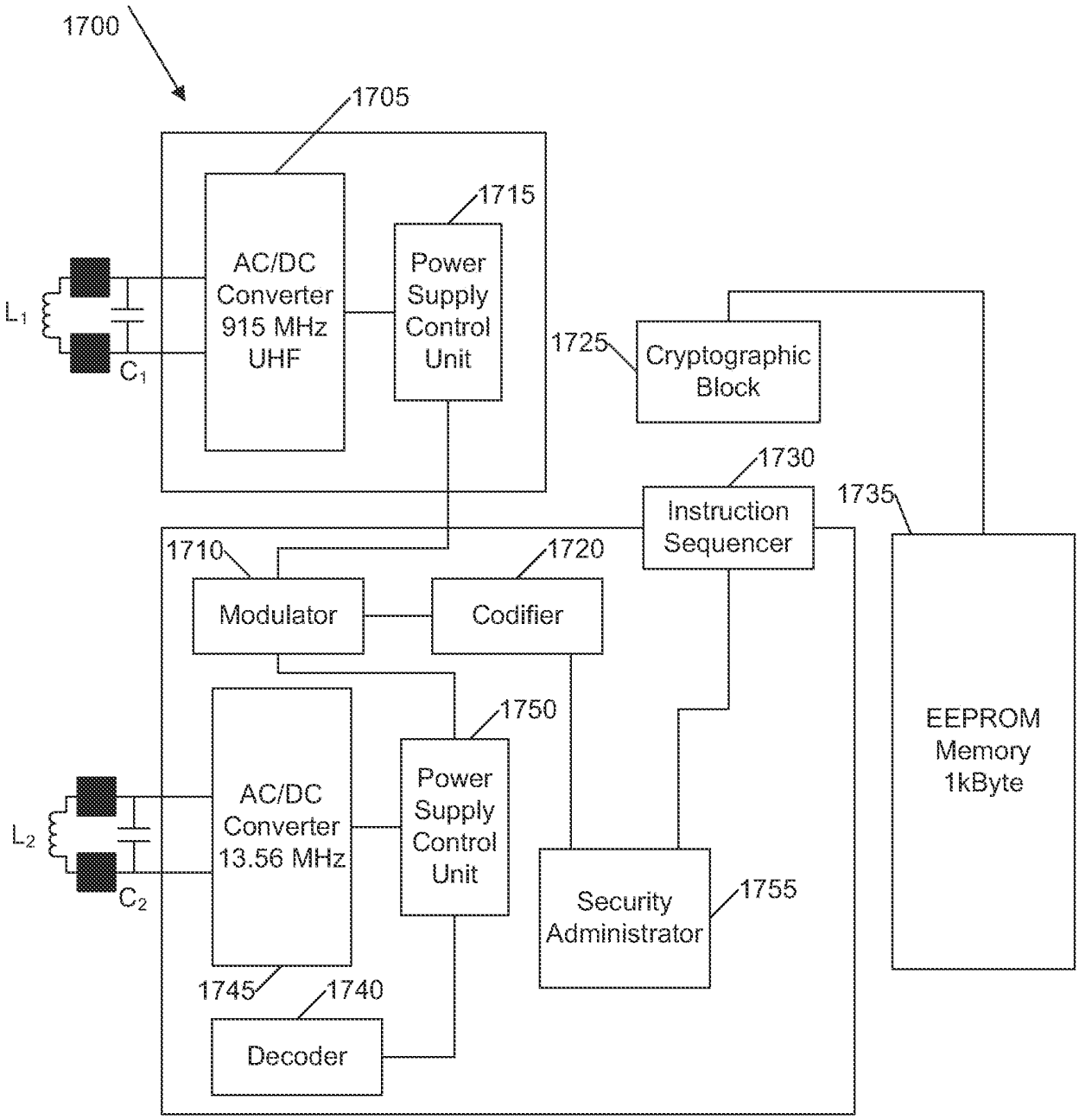

1700
1705
1715
AC/DC
Converter
915 MHz
UHF
Power
Supply
Control
Unit
L1
C1
1725
Cryptographic
Block
1730
1735
Instruction
Sequencer
1710
1720
Modulator
Codifier
1750
AC/DC
Converter
13.56 MHz
Power
Supply
Control
Unit
EEPROM
Memory
1kByte
L2
C2
Security
Administrator
1755
1745
1740
Decoder

FIG. 17

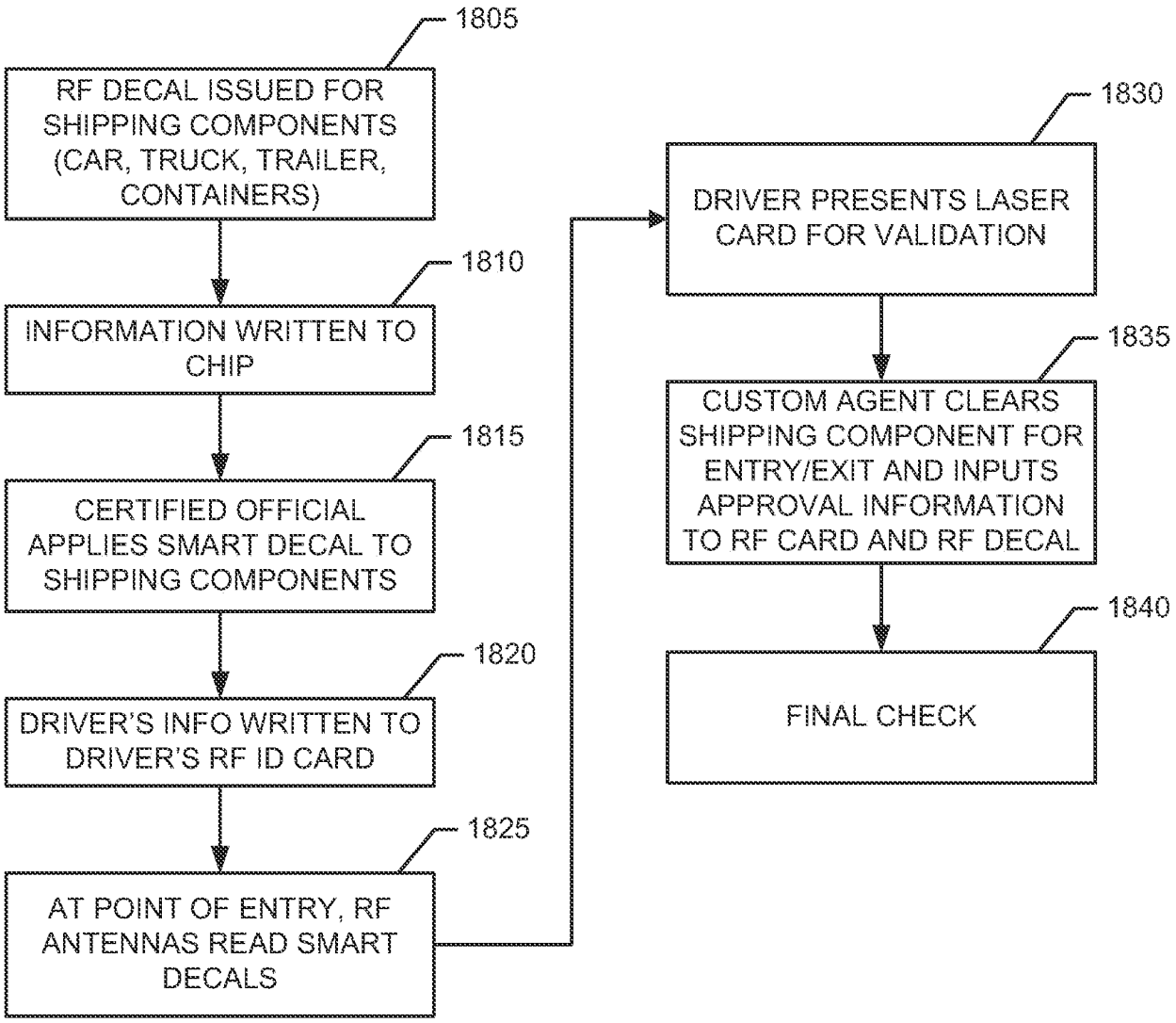

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS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

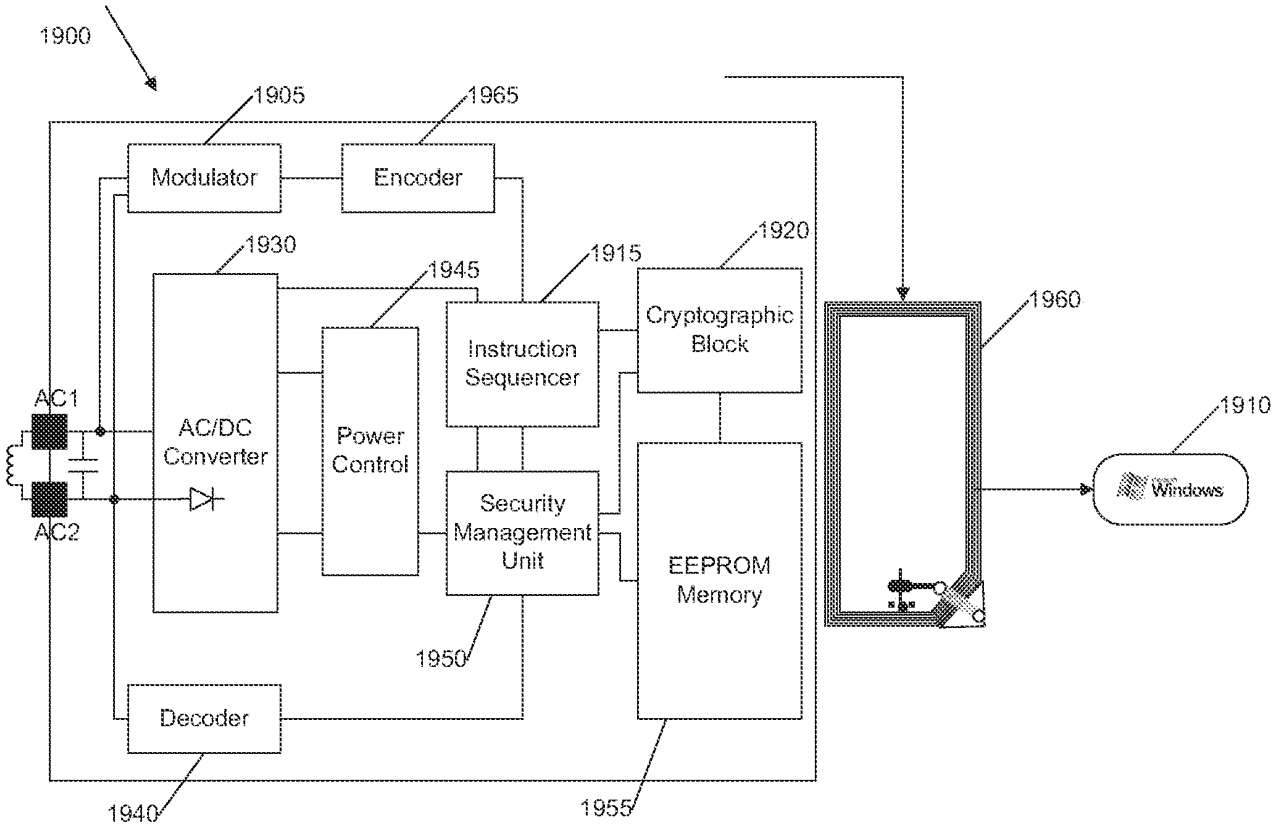

1900
1905
1965
Modulator
Encoder
1930
1945
1915
1920
Cryptographic Block
1960
Instruction Sequencer
AC1
AC/DC Converter
Power Control
1910
Windows
AC2
Security Management Unit
EEPROM Memory
1950
Decoder
1940
1955

FIG. 19

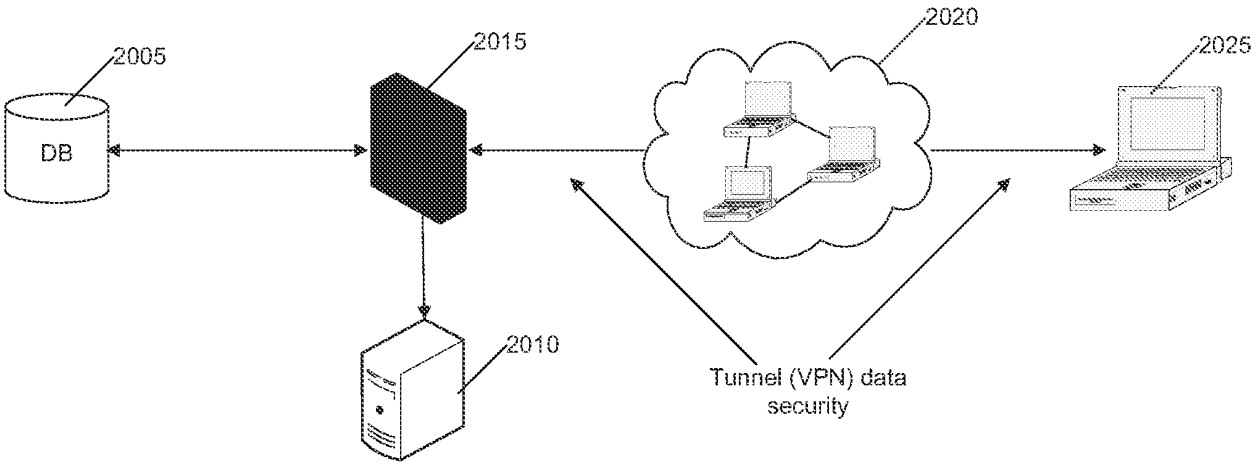


FIG. 20

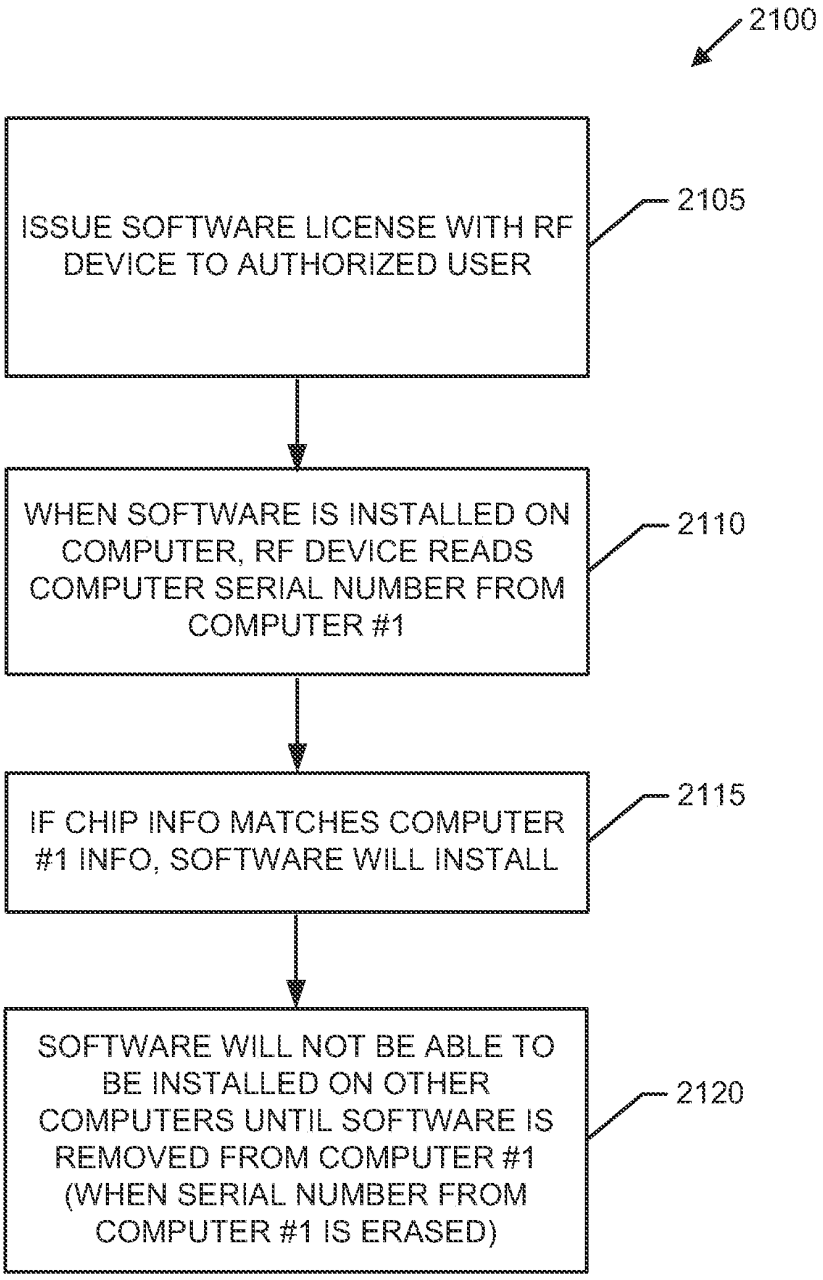

2100
ISSUE SOFTWARE LICENSE WITH RF DEVICE TO AUTHORIZED USER
2105
WHEN SOFTWARE IS INSTALLED ON COMPUTER, RF DEVICE READS COMPUTER SERIAL NUMBER FROM COMPUTER #1
2110
IF CHIP INFO MATCHES COMPUTER #1 INFO, SOFTWARE WILL INSTALL
2115
SOFTWARE WILL NOT BE ABLE TO BE INSTALLED ON OTHER COMPUTERS UNTIL SOFTWARE IS REMOVED FROM COMPUTER #1 (WHEN SERIAL NUMBER FROM COMPUTER #1 IS ERASED)
2120

FIG. 21

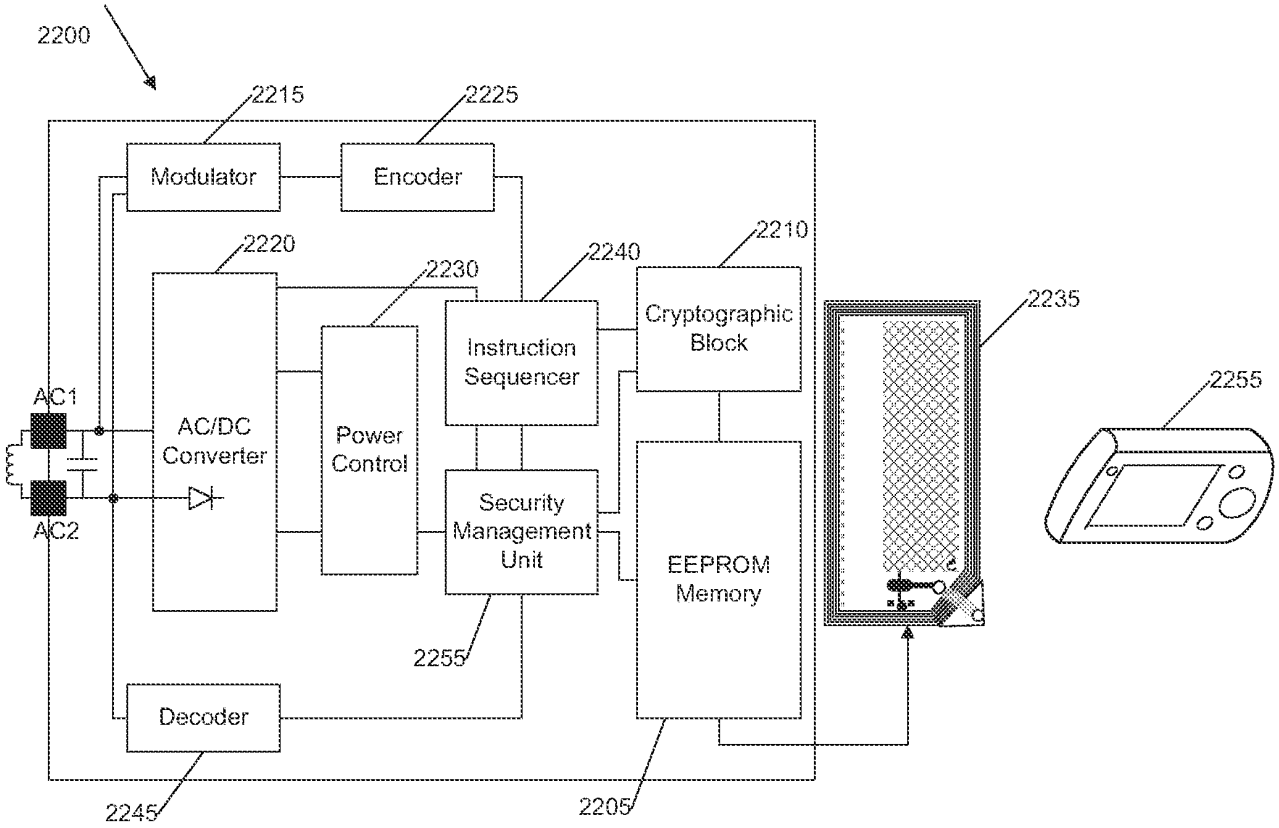

2200
2215
2225
Modulator
Encoder
2220
2230
2240
2210
2235
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
2255
AC2
Security Management Unit
EEPROM Memory
2255
Decoder
2245
2205

FIG. 22

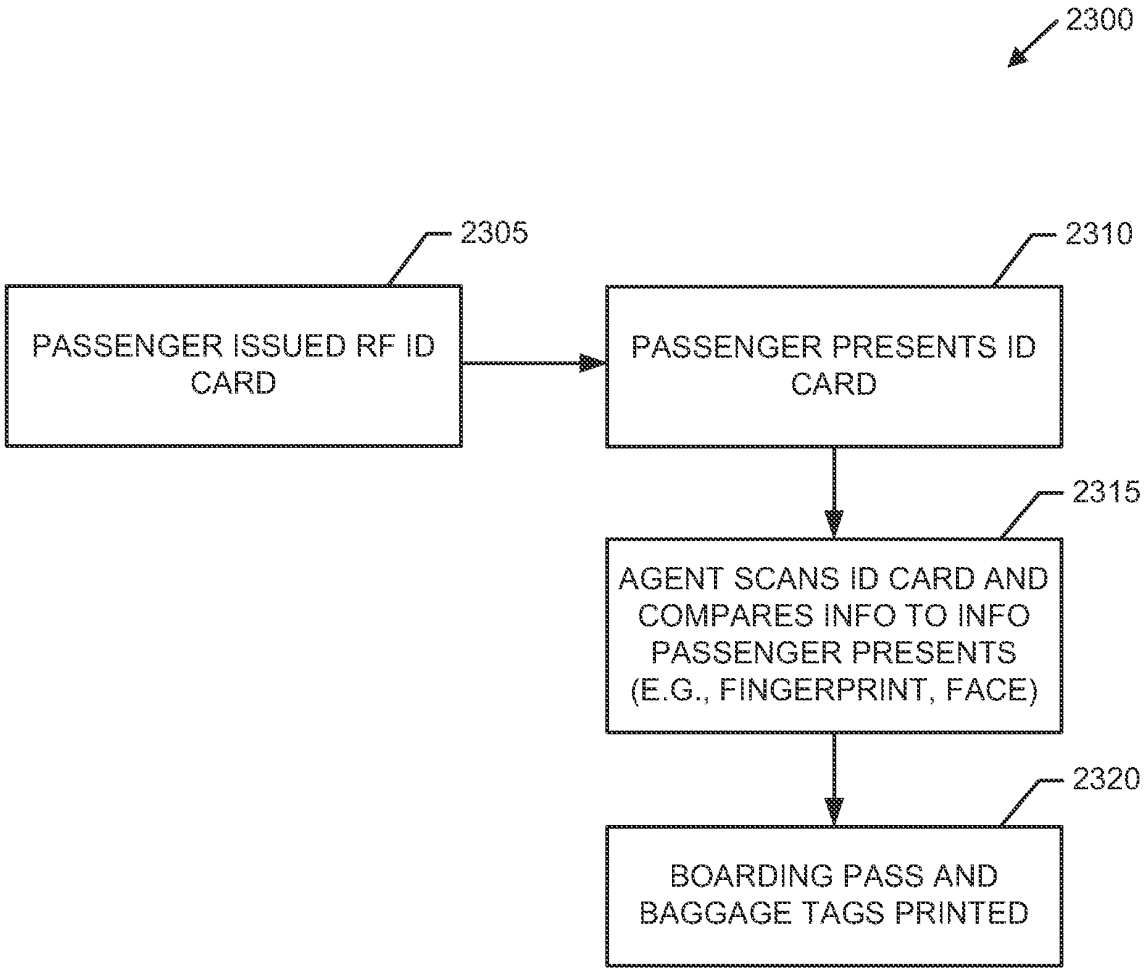

2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENT SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

FIG. 23

SPECIFICATION

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

BACKGROUND OF THE INVENTION

Field of the Invention

[0001] The present invention generally relates to a system and method for providing secure identification solutions, and specifically to a system and method for verifying and tracking identification information.

SUMMARY OF THE INVENTION

[0002] The present invention provides a method and system for verifying and tracking identification information. In an embodiment of the invention, a system for delivering security solutions is provided that includes at least one of the following: a radio frequency (RF) identification device, an identification mechanism (e.g., a card, sticker), and an RF reader/writer. The system and method can be used in numerous embodiments, including, but not limited to:

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

[0003] The embodiments of the present invention are discussed below. Those experienced in the art will see that multiple features of certain embodiments described below can be incorporated into other embodiments both described and not described below.

[0004] The present invention is not limited to the above embodiments. Additional advantages and novel features of the invention will be set forth in part in the Description that follows, and in part will become more apparent to those skilled in the art upon examination of the following or upon learning by practice of the invention.

BRIEF DESCRIPTION OF THE FIGURES

[0005] Figures 1, 2 and 4 illustrate the general invention, according to one embodiment of the present invention.

[0006] Figures 5-8 illustrate the RF registered item and method of use, in an embodiment of the present invention.

[0007] Figures 9-11 illustrate the RF passport and method of use, in an embodiment of the present invention.

[0008] Figures 12-14 illustrate the RF communications device and method of use, in an embodiment of the present invention.

[0009] Figures 15-18 illustrate a system and method for border crossing control, m an embodiment of the present invention.

[0010] Figures 3A-3B and 19-21 illustrate a system and method for limiting software downloads to authorized users, in an embodiment of the present invention.

[0011] Figures 22-23 illustrate a description of the system and method for airport security, in an embodiment of the present invention.

DESCRIPTION OF THE INVENTION

I. GENERAL RF IDENTIFICATION SYSTEM AND METHOD OF USE

[0012] Figure 1 illustrates an overview system diagram 100, according to one embodiment of the present invention. This embodiment comprises an RF device 110 connected to or embedded on an RF identification mechanism 105, and an RF reader/writer 125. The RF device 110 includes a chip 115 and an RF antenna 120.

A. RF Device

[0013] Figure 2 illustrates RF device 110, according to one embodiment of the present invention. The RF device includes a chip and an RF antenna. The RF device allows electronic identification via the reading of data stored in the chip in a contactless mode.

[0014] Figure 5 illustrates a dual frequency RF device 110, according to one embodiment of the present invention. Those experienced in the art will see that a one frequency or multiple (more than two) frequency RF device can also be used. The RF device includes the following components: A modulator 215 is a device that receives baseband signals from an antenna. An AC/DC converter 220 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 225 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 245 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 250 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 230 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 255 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 210 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 205 stores data. Information can be read and written from or to this device.

[0015] A more detailed description of an RF device can be found in U.S. Patent Application S.N. 10/118,092 filed 09 April 2002; PCT Patent Application PCT/IB02/01439, filed 30 April 2002, which are herein incorporated by reference. Additional information on the RF device can be found in the accompanying documents.

B. RF Identification Mechanism

[0016] Numerous features of RF identification mechanism are utilized in one embodiment of the present invention. In this embodiment, the RF device is embedded in the RF identification mechanism. One example of an RF identification mechanism is a card, and the description below refers to the identification mechanism as a card in several examples. However, those experienced in the art will recognize that multiple other embodiments of the identification mechanism are

possible, including, but not limited to: a card, a cellular phone, and a personal digital assistant (PDA).

[0017] There are a variety of ways to make identification cards that are resistant to fraud and counterfeiting. In one embodiment, the present invention incorporates numerous security features, as explained below.

C. Features of Secure Identification Mechanisms

[0018] The present invention offers a variety of solutions for making secure and durable identification mechanisms resistant to fraud and counterfeiting. The following features help make the identification card more secure. These features are only examples, and those experienced in the art will see that the present invention is not limited to these features and that many other features can be incorporated.

[0019] In one embodiment of the present invention, at least one of the following features is incorporated: visible features, machine readable features, and proprietary substrate based features. Visible features require only the human eye to detect the security features. Machine readable features require special hardware (e.g., an ultraviolet light source, magnetic reader) to detect the security features. Proprietary substrate based features are security features incorporated within a plastic substrate.

[0020] In one embodiment of the present invention, at least one of the following characteristics are present relative to the identification mechanism: it is extremely difficult to duplicate; it is tamper proof, it is recognizable either visually or utilizing a machine readable device; it is durable enough to withstand harsh environments; it is produced by specialized, difficult to obtain production equipment; it can be machine readable; and cost savings are realized by volume production of the identification mechanism.

[0021] Security features curb petty, semiprofessional and professional counterfeiters by creating features that are highly difficult to reproduce. For example, the ready accessibility of dye sublimation card printers, color scanners, color printers, heat sources (e.g., hair dryers), and color photo copiers make it relatively easy to reproduce ordinary photo identification cards. In one embodiment, the present invention, therefore, utilizes images and texts that cannot be scanned or

photocopied without noticeable distortion, or cannot be recreated without highly sophisticated and expensive equipment.

[0022] Security Features. In one embodiment, the present invention can incorporate at least one of the following security features:

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

- *Bidi-Tri-Dimensional at Three Levels*. This material must be created in an optical table by a qualified holographer and with a combination of design and dot-matrix effects created by precise digital means allow identification of the document's authenticity.

- *Hidden Images*. A hologram can contain a hidden image that cannot be detected with the naked eyes. The hidden image can be identified by shooting a laser at 45 degrees. The reflection shows a spectrum of a text shield or design. A special lens to protect the eye from laser damage can be used.

- *Dot-Matrix*. A dot-matrix 1,000 dots per inch (DPI) effect is created in a computer and comprises engraving dots with a laser in a specific angle which a minimum density of 1200 to 2000 DPI's. It allows printing of micro text contained within a hologram with great precision and creates very precise 2D and 3D effects.

- *Hot Stamping*. Hot stamping places a hologram on a document by thermal transfer. This hologram will interlace with a paper substrate and will not allow a hologram to be transferred from one document to another.

- *Moire Pattern*. The moire pattern is a design-based pattern which superimposes two patterns with non-identical spatial frequencies. The effect is visually detected after utilizing a normal photocopier to reproduce the original pattern. The reproduced pattern induces a "moire" or aliasing which immediately suggests the

reproduced image is counterfeit. The original is produced utilizing digital image technology which differs from normal photocopy technology. This effectively "tricks" the photocopier and reveals the moire in the reproduced pattern.

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

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

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

- *Ultraviolet Fluorescence: Offset Printed, Visual/Machine-Readable Art or Text which Produces Light When Activated by an Ultraviolet Light Source*. This

feature is normally undetectable to the naked eye and can be overlooked by the casual counterfeiter. This feature is difficult to produce with easily obtained equipment. Special fluorescent colors are available for added security.

- *Light Pipe*. This is a substrate based, machine readable feature requiring a light source to detect. This feature is produced using optical techniques which direct light to specific locations of the card (e.g., the edge). The effect is a brilliant light at a location different from where the light source is pointed, and usually in a specific color. Since this feature involves specific translucent materials and optical design of substrates, counterfeiters may never detect this feature. It is also almost impossible to recreate such a feature.

- *Laser Engraving*. This visual substrate-based feature can be either tactile or subsurface depending upon the types of plastics employed. The feature can be either graphic or alphanumeric. Using a laser, a pattern or alpha numeric text is ablated into the sub-layers of a plastic card. Depending on the parameters of the laser system and the materials of card substrate, a tactile or subsurface mark appears. This feature is particularly effective in the serialization of cards to reduce the risk of lost or stolen cards. The mark cannot be "scraped off without noticeable damage to the card surface. A tactile surface is helpful in quick recognition of authenticity. Laser systems of such complexity are expensive and difficult to obtain.

- *Metalized Stripe*. This stripe is a visual substrate-based feature which can also be machine readable. This feature uses a special metalized stripe (e.g., found commonly inside various currencies) or a holographic stripe (e.g., non-machine readable). These special stripes are placed within the card laminations and are visible to the naked eye. The special stripes can be proprietary in order to limit the availability to counterfeiters. The metalized stripes can be machine readable to verify authenticity. This level of security feature is high because counterfeiters need access to both card manufacturing equipment and the source of materials. These are both difficult to obtain.

- *Guilloche Pattern*. This feature is an intricate pattern of curvilinear fine lines which were originally created by "engine turning," commonly used in currency design. This visual feature is design-based and commonly produced using offset printing onto plastic. It is normally contained under a translucent lamination which acts as protection from abrasion. The fine lines are difficult to reproduce with full clarity and resolution on a copier, dye sublimation card printer, or scanner/personal computer/inkjet system because the dye sublimation printer can print only onto the surface of the card.

- *Rainbow Guilloche*. This feature is similar to the guilloche pattern above and is used in conjunction with a color spectrum which gradually changes from color to color achieving a continuous effect across the surface of the card. The level of security is slightly greater since use of a sophisticated color copier is required to duplicate the pattern effectively.

- *Cameo Effect*. This feature is the result of cropping the background of an image with software to print only a silhouette of the person which makes it more difficult to replace than a square image. This effect is combined and interlaced with other security features, such as hidden infrared on the background of the picture, or interlacing a photo with guilloche patterns on the back.

- *Ghost Image*. This feature provides the ability to print a second photo of a person, which is degraded by software, and it is printed on a faded gray or color scale over the personal data of the person to protect this information from tampering or altering. This effect is also achieved by software.

[0023] **Types of Holograms**. Many different types of holograms with unique visual effects are utilized for commercial and security applications, as well as promotional products. In one embodiment, the present invention includes at least one of the following holograms:

- *Two Dimensional (2D) Hologram*. This hologram lies on one single layer, which projects vivacity of color. With this technique, we convert standard color line artwork or photography into an array of holographic colors.

- *Three Dimensional (3D) Hologram*. This hologram is created from a solid model or sculpture. The product's third dimension is captured. The design becomes a 3D image after the depth of the image is captured through the use of a sculpture. A logo or product will be seen without the need of special glasses or lenses.

- *Two/Three Dimensional (2D/3D)*. This hologram combines a superficial layer with other dimensional layers, which can be a combination of both technologies, as mentioned previously. One image produces multi-color levels because of the positioning of the various layers. This system adds a third dimension to pictures.

- *Line Artwork & Photographs*. One embodiment of the present invention uses line artwork, photographs, or a combination of both, to create several layers of images separated by specific distances in order to give the illusion of depth. In general, two layers are enough, but if necessary, five different layers of images can be used.

- *Colorgrams*. Also known as true color holograms, colorgrams usually use someone's photo. It is made up of photographic quality art-work. These holograms are surprisingly capable of displaying true colors of the object, like true human skin tones or the original colors of a flag. If a counterfeiter cannot get the original photo, they cannot duplicate the label. It is a good way to prevent counterfeiting. The colorgram system is similar to the 2D/3D system. Full-color photographs are reproduced in their true, original colors at a specific angle, usually at a 45 degree viewing angle. The system can combine photographs with line artwork at different layer levels.

- *Stereograms*. Stereograms involve the latest in advanced technology. They are the result of a complex system that gathers full images, volume, movement, color and total animation. Total animation gives the sensation of the movement of a live recording.

- *HolomatrixTM from 50 DPI to 2000 DPI*. This feature comprises microtext, optical variable effects, and computer-generated optical devices. Graphic images

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

- *Diffractive Optical Variable Image Devices*. All the products classified as DOVIDs (Diffractive Optical Variable Image Devices) present an image which changes colors when tilted in various angles. This essential characteristic makes the Images impossible to copy or imitate by traditional printing and graphics software.

- *Optical Variable Devices*. An optical variable device (OVD) is a way of printing an image in such a way that certain characteristics vary when viewed or illuminated from different angles.

- *Combined Holograms*. These holograms combine two or more of the above mentioned types of holograms. Combining Holomatrix™ with any of the above types makes the hologram more complex and ideal for security applications.

[0024] Optional Tests. In one embodiment of the present invention, the identification mechanism is tested in multiple ways. Laboratory tests are used to demonstrate durability, tamper proof, temperature and humidity stability, abrasion resistance, adhesiveness and light stability to ensure durability of the identification mechanism and to ensure that the dyes will not fade or degrade before at least 5 years of extensive use. In addition, dual lamination can be performed.

[0025] One embodiment of the present invention can include at least one of the following tests.

- *Static Bending Test*. In this test, a composite card is tested to exceed 100,000 bending cycles without breaking or losing its integrity.

- *Heat Test*. In this test, a composite card is exposed for an extended period of time to intense sunlight, boiling water, and a temperature of up to 220 degrees Fahrenheit without twisting or bending.

- *Rigidity Test*. In this test, multiple layers are applied to a composite card to give it rigidity so that when it is laminated it will not lose its flat shape, guaranteeing that the bar code is readable.

- *Durability Test*. In this test, a card is placed in a steam pressure chamber at 160 degrees Fahrenheit for four days to test that the card will not warp or break, and that the over lamination will not come off.

- *Abrasion Test*. In this test, a card is placed in an agitator containing a water and sand solution and subjected to 30 minutes of agitation.

[0026] **Required Security Levels**. Multiple security levels exist and are explained below.

[0027] First Level Security Features. First-level security features are clearly visible so that any attempts to modify the text data, photo image, or other personalized information is evident at a simple glance.

[0028] In one embodiment, the first-level security features include a complex hologram with multiple security features, combining a complex hologram structure with micro printing. The printer and the hologram are transferred through a holographic registration and a fiber optic sensor to assure very high accuracy. The holographic pattern is always transferred in the same position.

[0029] In one embodiment of the present invention, the hologram includes at least one of the following general features:

- A highly integrated technology and expensive machinery is required for mass production. Only manufacturers with sophisticated know-how can maintain its quality.

- The hologram makes the object visibly distinguished from other printing materials or those color copied.

- Some types of hologram (e.g., Kaleidogram, Finegram) ensure more satisfying security features than of the flat types, since the most advanced equipment is necessary in the process of production.

[0030] In one embodiment of the present invention, reproduction features include:

- A Transparent Kaleidogram with protective OP layer that is heat transferred on to the card book. It covers the entire printed area.

- Attempts to remove the hologram layer will damage the composition of the hologram. Thus it cannot be reused, or tampered.

- Combined with micro-letter printing, the reproduction by color copy or photomechanical process is not feasible, as the 0.26 mm size characters is ruined when reproduced. Additional first-level security features can be integrated with the RF identification mechanism (e.g., card) in the future. An example of such security features would be icons, symbols, or guilloches that could be printed in special solvent sensitive inks. These features can be printed directly onto the intermediate transfer layer. These security features could be employed at some time in the future if a solvent tampering technique is identified.

[0031] Overall, the proposed first-level security features provide the document with excellent protection against altering and falsification, as well as acts of counterfeiting. The features are readily visible and any attempts to modify the underlying information is evident at a glance.

[0032] Second Level Security Features. Second-level security features can also be included. These second-level security features are invisible to the eye under normal viewing conditions, and are evident only when using a proper detection device. In one embodiment of the present invention, at least one of the following features is included:

- *Invisible Ultraviolet-Fluorescent Features*. The visible portion of the energy spectrum extends from deep blue at, for example, 400 nm to deep red at, for

example, 700 nm. Long wavelength ultraviolet energy in the region of the spectrum for example, between 350 nm and 400 run, such as 380 nm, is used to excite an embedded ultraviolet-fluorescent material. These high-energy ultraviolet photons are absorbed by the fluorescent material that happens to be invisible or transparent in the 400 rim. to 700 nm region of the spectrum. The ultraviolet photons pump the absorbing material to excited energy states. The material in the excited states quickly relaxes back and releases the absorbed energy again in the form of photons. Because some of the energy is lost in this transition, the emitted photons have less energy than the absorbed photons. The visible portion of the energy spectrum is positioned at the lower energy photon levels. Consequently, the process results in visible light being emitted from the material when it is illuminated by ultraviolet light. In a darkened room, the eye detects the glow being emitted by the ultraviolet-fluorescent material but not the ultraviolet light that is used to excite the material.

- *Two-Dimensional Bar Code*. The card solution can include a PDF-417 format barcode (two-dimensional barcode) that is printed onto the card. The PDF -41 7 barcode can hold several types of data (e.g., fingerprint minutiae, personal information).

[0033] *RF Device*. An RF device can complement all the previously mentioned security features, as it has a unique identifier (e.g., a unique 64 bit serial number), and the information contained on it is protected by sundry cryptographic methods. The capacity of the device will allow a great deal of information about the holder to be stored on the device (e.g., fingerprint minutiae or other biometric template, the holder's biographical information, statistical information). Those experienced in the art will see that an RF device allows data to be written to and read from the device via an antenna without the holder having to present the document for verification through traditional methods such as visual inspection, or other method of machine reading.

[0034] *Third Level Security Features*. Two optional security features can be changed every eighteen months: special IR-activated security taggant material and proprietary security taggant material.

[0035] *Special Infrared-Activated Security Taggant Material.* A special ceramic compound (e.g., such as a product named Taggant, provided by Secure Products) is mixed with a clear ink media in very small concentrations. (The ceramic compound is referred to as Taggant, but those experienced in the art will recognize that other ceramic compounds or equivalent product can be used.) This mixture is printed on the intermediate transfer material surface. After being ground to small particles that are approximately 2 - 3 pm in diameter, the special ceramic compound appears to be a very fine white-colored powder. The combination of the white color, the small particle sizes and the low concentration causes the material to be invisible to the eye.

[0036] A low-power, eye-safe near-infrared laser can be used to activate the special IRactivated taggant material. The input wavelength of the laser must be tuned within a 3-5 nm bandwidth in order to activate the material. The input energy is pumped into the material with the lower energy photons of the laser. The combination of the long lifetimes for the excited energy states and the high concentration of photons from the near infrared laser result in a second transition upward in energy level. In other words, two photons are absorbed by the material to increase the available excitation energy. These high excitation energy states relax releasing photons in the visible portion of the spectrum as well as the near-infrared portion.

[0037] This process of effectively adding two lower energy photons together to release a higher energy photon is called "up-conversion." The special IR-activated security taggant material has three separate emissions or security features. When an appropriate infrared laser, which is invisible to the eye, is focused on the special taggant material, three features are emitted simultaneously. These three features are a visible green spot at the point of focus, a visible blue spot at the point of focus, and an invisible infrared point at a higher energy level in the near infrared portion of the spectrum. When viewed by the eye, the green and blue spots blend together to create a vivid turquoise color. However, all three features can be detected automatically and separately with the proper equipment.

[0038] *Proprietary Security Taggant Material.* A proprietary security taggant material can also be included in the card design. A special ceramic taggant material (e.g., such as the one produced by Secure Products) exhibits multiple security features and is in part based on the "up conversion" concept. The white powder is ground into particles that are 2 - 3 nm in diameter and is mixed into a clear ink media in very small concentrations. Again, as before, the combination

of the white color, the small particle sizes and the low concentration causes the material to be invisible to the eye. However, this special material can be activated by several wavelengths and each activation wavelength results in a different response.

[0039] One characteristic and security feature is activated by a special low-power, eye-safe near-infrared laser. The activation bandwidth is approximately 3 nm and is located on the longer wavelength side of the activation energy required for the second-level feature. Laser devices are far less common in this area of the spectrum. When the special taggant is excited by a laser specially tuned to this excitation frequency and bandwidth, two separate emissions are observed. One emission is in the visible portion of the spectrum and can be observed as a green spot at the point of incidence. The second emission is in the near-infrared portion of the spectrum near the excitation wavelength of the first optional security feature.

[0040] A second characteristic and security feature is observed by using a second low power, eye-safe near-infrared laser at about the same excitation energy as the similar second-level feature. At this excitation wavelength, a green spot can be observed at the point of incidence due to the "up-conversion" process.

[0041] Finally, a third characteristic and security feature can be observed by applying energy in a wider bandwidth in the upper portions of the visible energy spectrum. This wavelength of energy is absorbed and re-emitted as longer wavelength infrared energy. In one embodiment, the initial implementation activities will focus on a verification process that utilizes a single excitation wavelength and a single observation wavelength. The implementation of the other embedded security characteristics can be phased into the program as new features are required to maintain the overall security of the card documents. Since these untapped security features and benefits will have existed in the documents from the initial issuance, the implementation of the new features will minimize the impact to the overall system.

[0042] In addition, new security features can be integrated into the present invention should the need arise.

D. Method of Using the General RF Identification System

[0043] Figure 4 illustrates the methods of using the RF identification system 400, according to one embodiment of the present invention.

[0044] In 405, the identification information (e.g., fingerprint, picture) is written to a chip with an RF device. In 410, the chip is then embedded on an identification mechanism (e.g., license plate, passport, card). In 415, a user enters an area where identification information must be presented. In 420, an RF reader/writer reads the identification information from the chip. In 425, the user allows identification information to be taken (e.g., a fingerprint scan, an authority checks a user's face) and this information is compared to the chip data to verify the user's identity.

II. RF REGISTERED ITEM AND METHOD OF USE

[0045] One embodiment of the present invention allows authorities to track information regarding a registered item (e.g., a vehicle), identify the item, and determine whether a driver of the item has the right to operate the vehicle. The present invention is described using the illustration of a license plate, but those experienced in the art will recognize that multiple other embodiments are possible, including, but not limited to: a sticker (e.g., a self-adhesive decal that can be placed on an automobile window, windshield or license plate), an RF embedded license plate (e.g., if the license plate is to be manufactured with some non-conductive material, the RF device can be embedded directly into the license plate), an encapsulated RF device (e.g., in the housing of a rear-view mirror, headlights or taillights, the vehicle's front or rear bumpers, or in any non conductive component of the vehicle; the device can be encapsulated in such a way that it will resist normal use and exposure to the elements, or embedded directly into the materials comprising the aforementioned placement media).

[0046] The present invention can be used, for example, for vehicle identification, border crossing solutions, traffic violations, insurance programs, pollution control, vehicle access control, traffic logistics planning and engineering, toll booths, and other vehicle control applications. The present invention takes centrally stored information and makes it accessible to the field (e.g., to police or other authorities). It also extends and expands the verification of individual and item (e.g., vehicle) information.

A. RF Registered Item

[0047] Figure 5 illustrates an RF registered item 500, according to one embodiment of the present invention. The registered item 500 includes the following components: A modulator 515 is a device that receives baseband signals from an antenna. An AC/DC converter 520 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 525

is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 545 is a device that decodes information from the encoder output so it may be used by another device or display. A power control 550 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 530 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 555 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 510 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 505 stores data. Information can be read and written from or to this device.

B. Method of Using RF Registered Item

[0048] Figure 6 illustrates the method of using RF registered item 600, according to one embodiment of the present invention. In 605, individual identification information (e.g., fingerprint, picture) and/or vehicle identification information (e.g., registered vehicle, license number) are collected and written to an RF device (i.e., a chip with an RF antenna). In 610, the RF device is embedded onto an identification mechanism, a license plate. In 615, an authority wishing to check a vehicle uses an RF reader/writer to read the chip data. In 620, the authority takes and compares the individual identification information (e.g., user's fingerprint, check user's face) and/or vehicle identification information (e.g., check make and model of vehicle, check vehicle license number) and to the chip data to verify an individual's identity and whether the individual has the authority to possess and operate the vehicle.

[0049] In one embodiment, a selective metalizing procedure is used to selectively metalize the areas which will not carry the RF device. This can be done by using a mask, as illustrated in Figure 7.

C. Method of Making RF Registered Item

[0050] In one embodiment, the identification mechanism (e.g., license plate) comprises a material that allows visual validation of the registration, even at night. The material can be a retro-reflective material, holographic foil, or another substrate with a high metal content.

[0051] Figure 8 illustrates method of making RF registered item 800, according to one embodiment of the present invention. In 805, antennas are produced on a demetalized or selective metalizing process. In 810, after demetalizing, resistance is decreased and conductivity

is increased by applying inks containing silver or copper (e.g., conductive inks). In 815, an adhesive layer is applied to the antenna in a Web environment or with automatic label capabilities.

[0052] In one embodiment of the present invention, at least one of the following is tracked:

- *Vehicle Identification Number (VIN)*. The VIN is the vehicle's international registration number and is the "fingerprint" of the car. Vehicle identification is performed by visually reading the car's VIN, and using the software to validate the VIN. This software allows a user to determine if the vehicle has been modified, altered, and/or stolen.

- *Owner Identification*. Owner identification is made using photographic information (e.g., a photograph) and/or biometric information (e.g., a fingerprint, iris pattern) stored in the RF device.

- *Tracking Information*. The RF device is used to read the VIN number and the owner's information. This can be used to identify a vehicle or individual reliably without having to connect to a central database.

- *Central Data Base*. The central data base validates the identity information for increased security (e.g., tracking who and where the device was produced and who it belongs to).

D. Optional Security Features

[0053] In one embodiment of the present invention, at least one of the following security features is included:

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

- *Secure Identification*. This feature requires information contained in the device to be unalterable without a determination of who wishes to alter the information and for what purpose. Highly secure chips with a hardware programmable cryptographic block with credit and debit exchange keys is used in one embodiment of the present invention. In addition, the individual information of the vehicle (e.g., the VIN) and the personal information (e.g., biometrics) contained in the device must be protected. • Secure Transaction. This feature protects the device from the equipment that reads and writes from the device. This equipment must be initialized using the same encryption keys as the RF device.

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

III. RF IDENTIFICATION MECHANISM AND METHOD OF USE

[0054] The present invention includes an RF identification mechanism, such as a passport, and a method of using the same. The present invention will be described in the context of a passport. However, those experienced in the art will recognize that the RF identification mechanism is not limited to a passport, and multiple other embodiments are available, including, but not limited to: a license, credit card, cell phone, etc.

A. RF Identification Mechanism

[0055] Figure 9 illustrates an RF registered item 900, according to one embodiment of the present invention. The registered item 900 includes the following components, as described earlier: a modulator 915, an AC/DC converter 920, an encoder 925, a power control 930, an instruction sequencer 940, a cryptographic block 910, a decoder 945, a security management unit 955, a memory 905, and an antenna 935.

B. Method of Using an RF Identification Mechanism

[0056] Figure 10 illustrates a method of using the RF passport, according to one embodiment of the present invention.

[0057] In 1005, identification information (e.g., a biometric template, photography, social security number, personal identification number) is collected and written to the chip on the RF device. In 1010, the RF device is embedded on a passport. In 1015, the user enters an area where a passport must be presented and an RF reader/writer reads the identification information from the RF device on the passport. In 1020, an authority collects second identification information from the user (e.g., takes the user's fingerprint, looks at the user's face) and the information is compared to the RF device data to verify the user's identity.

C. Method of Making an RF Identification Mechanism

[0058] Figure 11 illustrates how an RF passport is made, according to one embodiment of the present invention. In 1105, the passport inlay is produced on a PVC substrate. A copper wire and chip are embedded into the passport inlay. In Ill 0, the passport inlay is embedded into the passport document. In 1115, the passport is printed using a holographic retransfer film and dye sublimation inverse printing. In 1120, the RF passport identification information is matched to the person who owns the passport. In 1125, the passport is initialized, and personal information and/or biometrics are encoded on the passport to the RF device. This is done after the passport is personalized for security reasons. The RF passports are of no utility if they are stolen, as they need to be initialized with proper encryption keys and personalized.

IV. RF COMMUNICATION DEVICE AND METHOD OF USE

[0059] One embodiment of the RF communication device creates a communication through a network to a point of sale ("POS"). This is performed, for example, by a wireless RF device that stores a person's identification information, and can thus become a person's identification "document." This is discussed in the context of an RF cellular telephone, but those experienced in the art will recognize that any communication device, including but not limited to a personal digital assistant or a pager, can be used.

[0060] As a user with an RF cellular telephone approaches a POS with an RF reader/writer, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone. The user is then asked to enter authentication information (e.g., a fingerprint).

If the user wishes to complete a transaction, the user enters the authentication information. An exchange of information via the RF reader/writer and the RF cellular telephone results in verification that the authentication information matches the RF cellular telephone information.

[0061] The present invention, referred to in one embodiment as an RF cellular telephone, creates a communication through a network of cells to a point of sale (POS). This is performed by combining Global System for Mobile Communication (GSM) technology with a wireless RF device that can store a person's identification information, including an electronic or biometric "signature" (e.g., fingerprint, facial, iris, or other recognition feature). GSM technology includes a compact chip located on the back of the telephone. The compact chip has an operating system. The GSM telephones identify the telephones to a network carrier to avoid, for example, telephone cloning.

[0062] The RF cellular telephone can thus become a person's identification document (e.g., passport, boarding pass) and/or credit card or other card (e.g., mileage cards). Multiple types of information can be carried and stored on the RF cellular telephone. The following uses are examples of how the RF cellular telephone can be used: an RF cellular telephone can be used as a substitute for credit cards, transforming the cellular telephone into the media of commercial transactions and transform telephony into the identification media for commercial establishments or authorities; an RF cellular telephone can be a personal identification or a Portable Data File (PDF); an RF cellular telephone can be integrated with a Global Positioning System (GPS) receiver; an RF cellular telephone can be integrated with hand held devices to provide Internet access, and access to business and personal information (e.g., email); and an RF cellular telephone could be a boarding pass (e.g., e-ticket) and/or could track a user going through security with authentication by fingerprint at a gate or other local area. Those experienced in the art will recognize that there are multiple other examples and uses of the RF cellular telephone.

[0063] One embodiment of the present invention provides at least one of the following benefits: assists in avoiding current credit card fraud, through donation, substitution of identity, or counterfeit documents; reduces or eliminates the need to carry credit cards, documents (e.g., a boarding pass) or other information; reduces or eliminates the need for an entity to issue or update credit cards or identification documents (e.g., tickets), with associated fees (e.g., mailing costs); and reduces or eliminates the need to stand in line or wait for services.

[0064] The present invention is discussed in the context of using a fingerprint for identification, as this is a widely recognized identification tool. However, those skilled in the art will recognize that any type of identification information (e.g., Personal Identification Number (PIN)) or any other biometric identifier (e.g., a voice print, iris recognition, facial recognition) could be used.

A. RF Communications Device System

[0065] Figure 12 illustrates an RF communications device system, according to one embodiment of the present invention. The system includes an RF cellular telephone 1205 and a point of contact (POC) or point of sale (POS) 1210.

[0066] The POS 1210 can include an RF reader/writer 31 and a fingerprint digital scanning device 1232. One-to-one verification ensures that the information on the RF cellular telephone matches the holder of the RF cellular telephone.

[0067] The RF cellular telephone 1205 can include the following: a fingerprint identifier 1221 (e.g., an Application Specific Integrated Circuit (ASIC) chip, which is a chip that is designed specifically to run fingerprint matching software on an operating system); and an RF device 1222 (with an antenna in the chip) to store identification information. In an alternative embodiment, the RF cellular telephone can include a fingerprint digital scanner 1223. As mentioned earlier, this could either be included on the RF cellular telephone, or on a fingerprint digital scanning device at the point of contact.

[0068] One embodiment of the RF device 1222 includes a chip and an RF antenna, as described herein. One embodiment of the chip is illustrated in Figure 13. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt 1348, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements are not met, a user cannot access the memory of the chip. The chip includes an ACDC converter 1341 and a connection to an RF antenna for power using a power supply control unit 1345. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator 1342 is a device that receives baseband signals from an antenna. An AC/DC converter 1341 is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder 1343 is a device for encoding information received so that it may be utilized by another device or protocol. A decoder 1344 is a device that decodes information from the encoder output so it may be used by another device or

display. A power control 1345 is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer 134 7 is a device that queues instructions to be sent to the chip's internal memory. A security management unit 1346 is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block 1349 is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory 1348 stores data. Information can be read and written from or to this device.

[0069] In an embodiment of the present invention, the chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel mileage card information). The RF cellular telephone also may include a cryptographic programmable block chip 1349 to enhance security.

B. Method of Using an RF Communications System

[0070] Figure 14 illustrates method of using an RF communications system 1400, according to one embodiment of the present invention. The present invention connects to a local POS, rather than a cellular carrier. Instead of a POS device obtaining credit card information via, for example, a magnetic stripe, the present invention, via an RF embedded on a cellular telephone, provides information to the POS, which has an RF reader/writer. In addition, the POS may include a device (e.g., a fingerprint reader) to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone. The fingerprint, or other identification feature, can be stored, for example, in the Chip, or at a remote location, for example, which is accessed by the POS device. Thus, for example, the store could run a one-to-one local verification of a user's identification by having the user imprint their fingerprint into a fingerprint reading device. The identification information, such as a fingerprint, is a string of information. That information is stored on the Chip. When the user puts a fingerprint on the POS fingerprint reader, the present invention will determine if the fingerprint matches the information stored on the RF cellular telephone. In an alternate embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone.

[0071] According to Figure 14, in 1405, a user carries an RF cellular telephone and approaches an RF reader/writer (e.g., in a hotel), which is continuously scanning. The RF reader/writer

connects to the network (e.g., the Internet), identifies the user, and obtains relevant transaction information (e.g., credit card information and hotel rewards card information).

[0072] In 141 0, the customer purchases a service or product and is prompted to enter authentication information (e.g., a fingerprint). In 1415, if the user wishes to complete the transaction, the user enters authentication information (e.g., imprints a fingerprint into a fingerprint scanner) and it is loaded to the RF device.

[0073] In 1420, the RF reader/writer and RF cellular telephone are used to verify the authentication information (e.g., the fingerprint scanner works with the RF reader/writer and the RF cellular telephone and/or other devices to ensure the customer's fingerprint matches the fingerprint stored on the RF cellular telephone) and this information is presented to a point of sale or access control device to retrieve purchase information.

[0074] Although the present invention has been described in the context of a POS, those skilled in the art will recognize that a user could use the RF cellular telephone without a POS. For example, a user could call a telephone number to buy a ticket to access a stadium, using identity verification and other transmitted information. As another example, a user could load a boarding pass or ticket to an event on an RF cellular telephone, and the boarding pass or ticket would be confirmed at an access control device around the perimeter of an airport lounge or stadium.

[0075] Additional information related to the present invention can be found in U.S. Patent Application 10/118,092, filed April 2, 2002, and PCT Patent Application IB0201439, filed April30, 2002, which are herein incorporated by reference.

V. SYSTEM AND METHOD FOR BORDER CROSSING CONTROL

[0076] One embodiment of the present invention provides a border crossing control mechanism using RF technology. This technology helps provide a flexible, efficient, and effective border crossing security system to meet the needs of rapidly changing security conditions. The present invention provides heightened security while at the same time efficiently and quickly moving vehicles and people across borders and through customs. In this embodiment, an identification mechanism (e.g., a laser card) is integrated with a vehicle decal that registers and matches any shipping components (e.g., drivers, vehicles, containers). The shipping components will be pre-registered in the decal at a point of origin. A fingerprint biometric of the driver is written into the

identification card and the decal at the factory. An RF antenna embedded into the decals allows tracking of, for example, the driver, cab and trailer, and validation of these components at strategic checkpoints. It also provides for designated routing through the port for inspection and clearance prior to departing the port.

[0077] The present invention can be used in a closed system or open system. In a closed system, all information resides on the RF laser card and RF decals. In an open system, information is passed from the point of original to country A's custom's inspectors, and from country A's customs inspectors to Country B's customs inspectors using a network (e.g., the Internet). This makes integration and implementation easier.

A. Border Crossing Control System

[0078] Figure 15 illustrates border crossing control system 1500, according to one embodiment of the present invention.

[0079] The system 1500 includes at least one client 1505, application server 1510, database 1515, RF identification mechanism 1520, RF device 1525, RF reader/writer 1530, connected by a network 1520.

[0080] **Client**. According to one embodiment of the present invention, clients are any computers (e.g., PC, PDA, cellular phone) connected to a network (e.g., LAN [Local Area Network], WAN [Wide Area Network], VPN tunnel [Virtual Private Network Tunnel], Internet).

[0081] **Application Server**. According to one embodiment of the present invention, an application server is used (e.g., an Oracle9iAS integrated into a J2EE application server). The application server can support web application software, wireless, web page caching, business intelligence features, and offer complete integration in a single product. The application server can also offer scalability, reliability, and security features. It can also include advanced clustering features to keep critical applications up and running 24x7; offers zero downtime and planned downtime through a fast start fault recovery architecture; and recover from incidents quickly and gracefully.

[0082] In the example embodiment of an Oracle9i application server, the high availability infrastructure includes Oracle9iAS Web Cache clusters, Oracle HTTP Server (Apache), and Oracle9iAS Containers for J2EE. In addition, database applications hosted on Oracle9i

Application Server can take advantage of Oracle9i Real Application Clusters (RAC) to make them more available. Oracle9i Application Server is the middle-tier deployment platform for all applications developed using Oracle9i Developer Suite. All applications can be deployed on the same middle-tier. Oracle9i Developer Suite is a complete and standards-based set of development tools. The suite includes Oracle9iAS Developer, Oracle's flagship J2EE and XML development environment that supports the full development life cycle of J2EE applications and Web services. It also includes Oracle9i Forms Developer for easily and quickly construct sophisticated database forms and business logic delivered through any Internet browser as a high performance, rich Java client.

[0083] **Database**. In one embodiment, the present invention uses a database with real application clusters (RAC) that can transparently scale and protect packaged applications with no changes necessary for the application (e.g., Oracle9i). RAC can scale all applications and also provides superior data protection with hot failover in less than 30 seconds.

[0084] According to one embodiment, the database provides a unique combination of scalability and availability in the same clustered database solution. With RAC, efficient scaling can be accomplished by simply adding servers to the overall cluster as the demand grows. Since RAC databases can grow flexibly, applications are protected from having to purchase excess computing power at a premium price. A RAC database can have costs significantly lower than the same solution implemented on an SMP (Symmetric Multi Processing) machine.

[0085] The database may include security and manageability features. The security features include: a Virtual Private Database (VPD); fine-grained auditing; data encryption.

[0086] The VPD technology provides programmatic row-level security and is enabled by associating tables or views with centrally defined access control policies. VPD addresses the application bypass problem and ensures that the same access control policy is enforced whether a user gains access to data through an application, ad hoc tool or SQL *Plus. As a result, multiple communities of users can securely share data within the same database.

[0087] Fine-grained auditing allows businesses to audit database activity by statement, system privilege, object or user. Its enhanced fine-grained auditing functionality enables organizations to centrally define specific audit policies that alert administrators to data access misuse. Audit

records, stored within the database, capture the user statement's exact SQL text and can be easily viewed through ad hoc queries.

[0088] Data encryption is the ability to natively encrypt data in the database, enabling applications to guard sensitive data. Server-based encryption supports industry-standard Data Encryption Standard (DES) and Triple-DES (3DES), in both two and three key modes for any organizations who require the strongest level of encryption. Encryption can also support the MD5 secure cryptographic hash to ensure data integrity and a Federal Information Processing Standard (PIPS) 140-certified random number generator for generating secure encryption keys.

[0089] The manageability features include intelligent self-managing and tuning. The database can enhance database manageability by automating routine tasks, reducing complexity of administration and making the database more self-tuning and self-managing. Features can be added to streamline space, memory, and resource management as well as other day-to-day database administrative tasks.

[0090] **RF Identification Mechanism, RF Device, and RF Reader/Writer**. One embodiment of the present invention comprises: an RF identification mechanism (e.g., an RF laser card), RF decals containing a Chip (e.g., a 2K bit chip or data memory circuit) with contactless read/write capabilities and an integrated RF antenna (e.g., a 13.56 MHz RF antenna); and an RF reader/writer.

[0091] **Multiple Chip Background Information**. Often multiple frequencies are used. This takes advantage of the best electromagnetic and electrostatic characteristics of certain frequencies, one for long range reading and the second for field penetration (e.g., rain). Multiple frequencies can be created using a dual modulator that can switch in milliseconds from one frequency to another. (See Figure 16.)

[0092] In one embodiment of the present invention, instead of, or in addition to incorporating the chip on the RF identification mechanism (e.g., RF smart laser card or RF decal), a chip can be embedded on a car windshield for smart windshield applications for vehicle registration, manufacturing, distribution of traffic violations, or any operation that requires contact with certain authorities. In this embodiment, the RF antenna can be used as radio antennas embedded

on glass with copper wire during the manufacturing process, and connected to a module or embedded in the glass itself.

[0093] The resonant frequency of the antenna circuit in the RF device can be given by solving this equation:

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

f = frequency (Hz)
L = inductance (H)
C = capaticance (F)

[0094] The frequencies at the poles are parallel resonant frequencies, and depending on the technology can be:

$f_1 = 13.56\ MH_z$
$f_2 = 915\ MH_z$

$$L = \frac{N^2 \mu_\circ A}{1}$$

N = number of windings around inductor
$\mu_\circ$ = permeability of freespace (Hm^{-1})
A = cross-sectional area of inductor (m^2)
L = length of inductor (m)

[0095] The inductance " L " depends on the number of turns of the coil, of the area perpendicular to the coil and of the permeability of free spaces and length of the coil. Therefore:

$$l = \frac{N^2 \mu_o A}{l} \Rightarrow$$

$$\frac{N^2 \mu_o A}{l} \quad \frac{l}{f^2 4\pi^2 C} \Rightarrow$$

$$l = f^2 4\pi^2 N^2 \mu_o A$$

[0096] For substitution, the following values are used:

$L_1 = 2.931X\ 10^8\ H$

$L_2 = 6.437X\ 10^{10}\ H$

[0097] The data signal between the antenna and the tag is modulated by amplitude and coded by a Manchester encoding. Thus, manchester data= NRZ data 1\ (NRZ clock).

Multiple RF Chip Overview

[0098] Figure 17 illustrates an overview of the chip, according to one embodiment of the present invention. As described in detail above, the chip includes: an AC/DC converter (915 MHz) 1705 and accompanying power supply control unit 1715; a modular 1710; a codifier 1720; an AC/DC converter (13.56 MHz) 1745 and accompanying power supply control unit 1750; a decoder 1740; a security administrator 1755; an instruction sequencer 1730; a cryptographic block 1725, and memory 1735.

B. Method of Using a RF Border Crossing Control System

[0100] 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.

[0101] 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.

[0102] 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.

[0103] 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

[0104] 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

[0105] 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.

[0106] 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.

[0107] **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.

[0108] 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.

[0109] 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.

[0110] 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.

[0111] Figure 3A illustrates the differences between transport mode and tunnel mode. The use of AH and ESP are illustrated in Figure 38.

B. Method of Limiting Software Downloads

[0112] 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.

[0113] 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

[0114] 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.

[0115] 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

[0116] 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.

[0117] 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).

[0118] The RF device contains an integrated computer chip and RF antenna for contactless communication at an operating frequency of, for example, 13.56 MHz.

[0119] 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.

[0120] As described above, the chip has a memory 2205 (e.g., 2k), an option hardware wired cryptographic block 2210 (with 4 exchange encrypted keys with up to 256 bits), a modulator 2215, a converter 2220, an encoder 2225, a power control2230, an instruction sequencer 2260, a decoder 2245, a security management unit 2255, a memory 2205.

B. Method of Airport Security

[0121] 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.

[0122] 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

[0123] Additional advantages and novel features of the invention will be set forth in part in the Attachments that follow, and in part will become more apparent to those skilled in the art upon examination of the following or upon learning by practice of the invention.

What is claimed

1. A mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

a biometric module configured to read biometric information;

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

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is successfully authenticated;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

2. The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

3. The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device, and wherein the POS device is configured to receive the encrypted key and payment information from the secure module, and transmit the encrypted key and payment information to a central database.

5. The mobile device of claim 4, wherein the POS device includes an RF reader.

6. The mobile device of claim 4, wherein the central database is configured to validate the key and the payment information.

7. The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.

9. The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

a biometric module configured to read biometric information;

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

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is successfully authenticated

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

a point of sale (POS) device configured to:

receive, from the secure module, the encrypted key and payment information; and

transmit, to a central database, the encrypted key and payment information; and

a central database configured to validate the key and the payment information.

11. The system of claim 10, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

12. The system of claim 10, wherein the payment information is associated with a primary account number.

13. The system of claim 10, wherein the POS device includes an RF reader.

14. The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. The system of claim 10, wherein the payment information is stored in a memory accessible only by the secure module.

16. The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

ABSTRACT

The present invention provides a method and system for verifying and tracking 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.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660CT2
	Application Number	
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Francisco		Martinez de Velasco Cortina	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	La Jolla	State/Province	CA	Country of Residence i	US

Mailing Address of Inventor:

Address 1	12760 Danielson Ct.		
Address 2			
City	Poway	State/Province	CA
Postal Code	92064	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Manfred		Rietzler	

Residence Information (Select One) ○ US Residency ◉ Non US Residency ○ Active US Military Service

City	Marktoberdorf	Country of Residence i	DE

Mailing Address of Inventor:

Address 1	12760 Danielson Ct.		
Address 2			
City	Poway	State/Province	CA
Postal Code	92064	Country i	CA

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660CT2
	Application Number	
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	27189		
Email Address	docketing@procopio.com	Add Email	Remove Email

Application Information:

Title of the Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS		
Attorney Docket Number	116546-660CT2	**Small Entity Status Claimed**	☐
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)	24	**Suggested Figure for Publication (if any)**	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	27189		

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660CT2
	Application Number	
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	14321781	2014-07-01

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14321781	Continuation of	14022135	2013-09-09	8766772	2014-07-01

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
14022135	Continuation of	13350665	2012-01-13	8587436	2013-11-19

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13350665	Continuation of	13175768	2011-07-01	8237568	2012-08-07

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
13175768	Continuation of	12688666	2010-01-15	8004410	2011-08-23

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
12688666	Continuation of	11279912	2006-04-17	7671746	2010-03-02

Prior Application Status	Patented				Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
11279912	Continuation of	10615026	2003-07-09	7081819	2006-07-25

Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
10615026	Claims benefit of provisional	60394241	2002-07-09

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660CT2
	Application Number	
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i]the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☒ Authorization to Permit Access to the Instant Application by the Participating Offices

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660CT2
	Application Number	
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	NEOLOGY, INC.		
Mailing Address Information:			
Address 1	12760 Danielson Ct.		
Address 2			
City	Poway	**State/Province**	CA
Country [i]	US	Postal Code	92064
Phone Number		Fax Number	

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660CT2
	Application Number	
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

Email Address	

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

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

Signature	/li zhang/			Date (YYYY-MM-DD)	2015-03-04
First Name	Li	Last Name	Zhang	Registration Number	70902

Additional Signature may be generated within this form by selecting the Add button. Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	116546-660CT2
	Application Number	
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS	

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

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

FOREIGN PATENT DOCUMENTS Remove

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

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

NON-PATENT LITERATURE DOCUMENTS Remove

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

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

CERTIFICATION STATEMENT

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

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

OR

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

☐ See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/li zhang/	Date (YYYY-MM-DD)	2015-03-04
Name/Print	Li Zhang	Registration Number	70902

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

Espacenet

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

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

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

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

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

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

Application number: DE2000142805 20000830

Priority number(s): DE2000142805 20000830

Abstract of DE10042805 (A1)

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

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

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

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

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

DE 100 42 805 A 1

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

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

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

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

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

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

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

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

DE 100 42 805 A 1

Beschreibung

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

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

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

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

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

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

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

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

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

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

1) Transponder

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

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

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

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

[0014] Weitere Vorteile von Transpondern sind:

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

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

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

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

1a) Befestigungsort Transponder

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

Bootslänge:

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

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

1b) Datenspeicher des Transponders

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

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

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

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

1c) Sende-/Empfangseinrichtung des Transponders

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

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

2) Lesegerät

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

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

3) Transponderpass

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

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

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

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

4) Registrierung und Markierung von Booten

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

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

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

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

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

5) Diebstahlmeldung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Zeichnungslegende

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

Patentansprüche

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

18. Verfahren nach einem der Ansprüche 16 oder 17,

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

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

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

21. Verfahren nach einem der Ansprüche 16 bis 20, dadurch gekennzeichnet, dass die automatisch weitergeleiteten Informationen bei einem als gestohlen gemeldeten Objekt (8) mindestens an eine zentrale exekutive Stelle (8x), 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

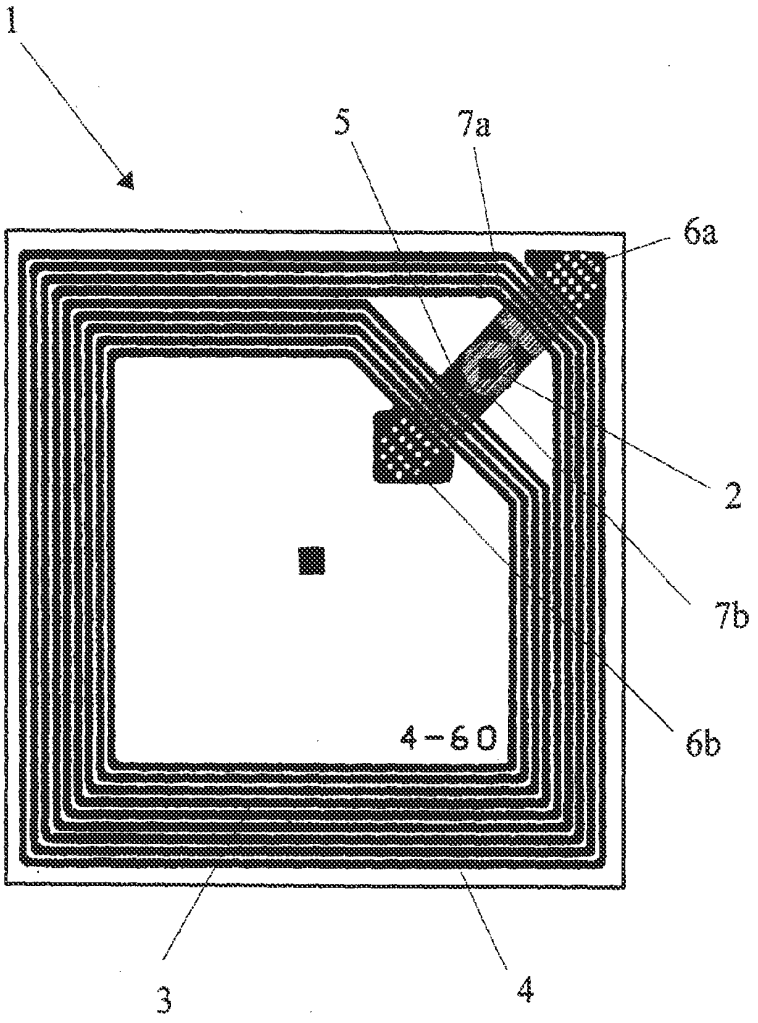


FIG. 1

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

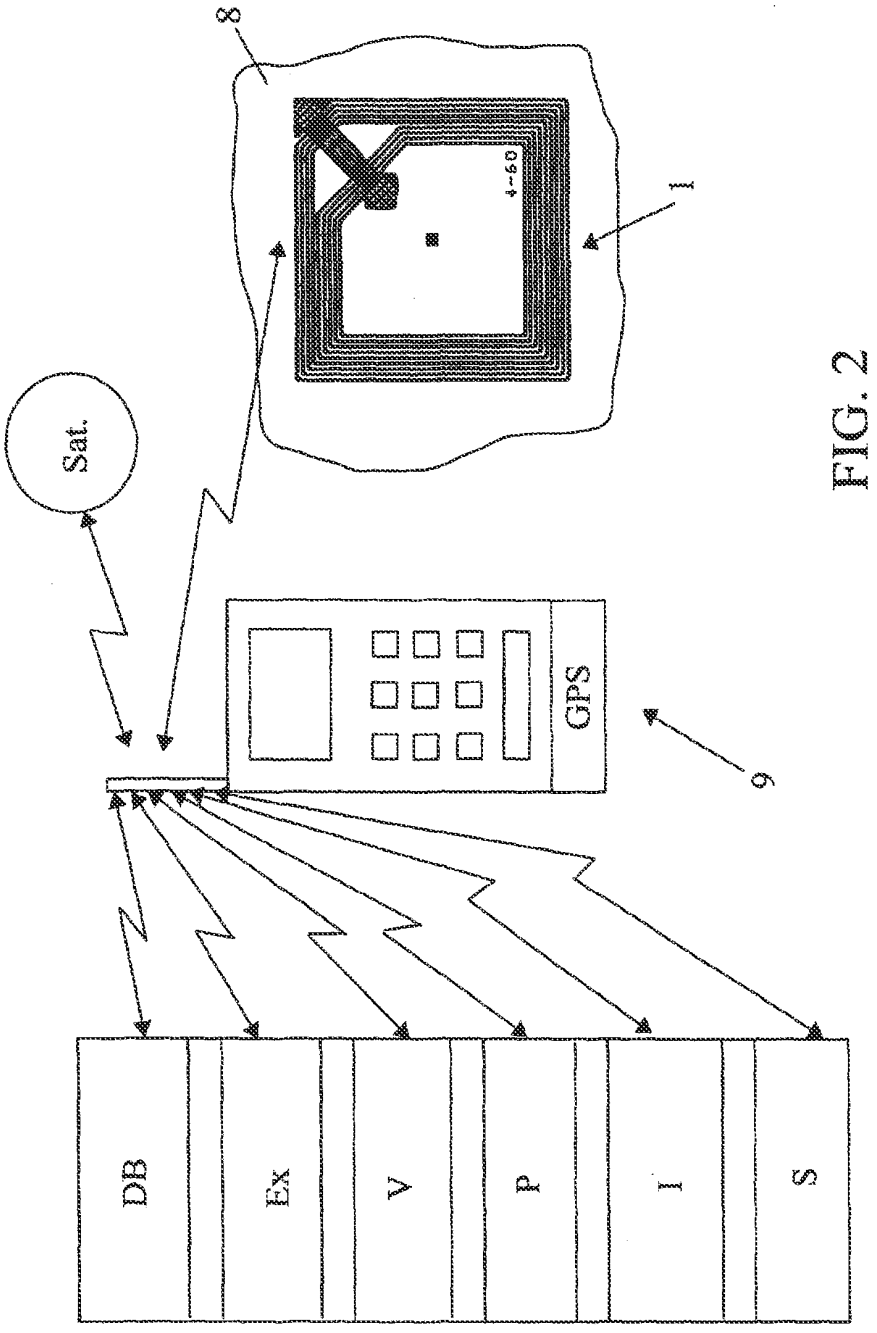


FIG. 2

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

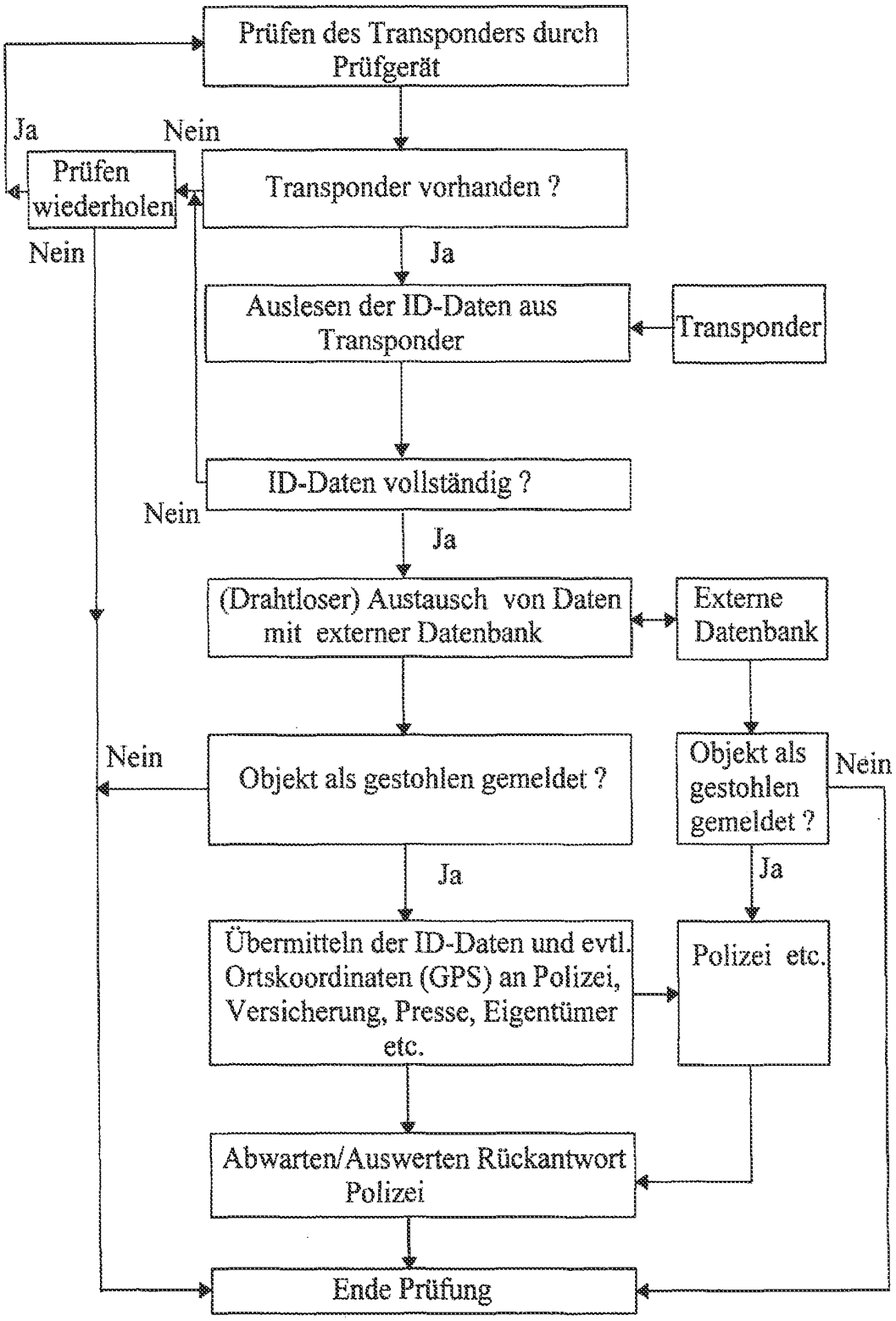


FIG. 3

Espacenet

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

Verfahren und Vorrichtung zur Echtheitskontrolle von Dokumenten in Form von Chipkarten

Inventor(s):

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

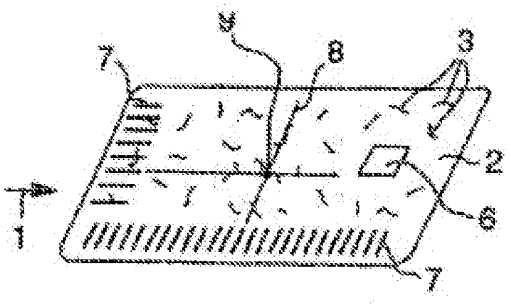
Classification: **- international:** ***G06K19/10;*** (IPC1-7): G07D7/00; G07F7/12
- cooperative: **G06K19/086**; **G06K19/10**

Application number: DE1996108757 19960306

Priority number(s): DE1996108757 19960306 ; DE1996108233 19960304

Abstract of DE19608757 (A1)

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



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

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

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

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

DE 196 08 757 A 1

(66) Innere Priorität:
196 08 233.1 04.03.96

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

(74) Vertreter:
LEINWEBER & ZIMMERMANN, 80331 München

(72) Erfinder:
Antrag auf Nichtnennung

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

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

DE 196 08 757 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 07. 97 702 037/274 5/23

Beschreibung

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

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

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

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

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

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

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

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

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

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

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

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

Patentansprüche

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

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

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

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

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

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

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

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

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

Hierzu 1 Seite(n) Zeichnungen

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

Fig. 1

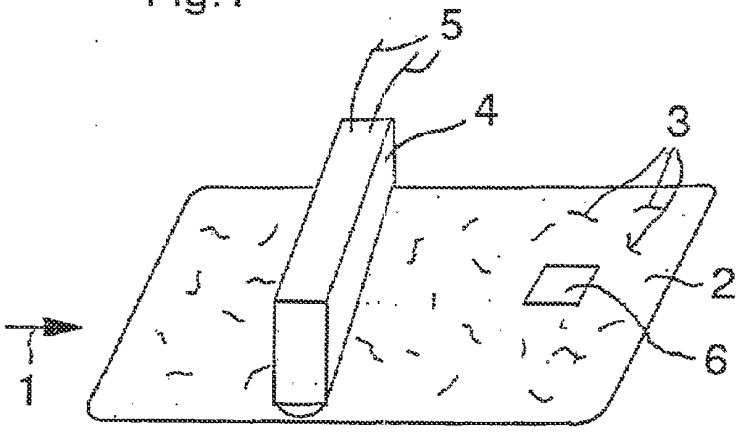
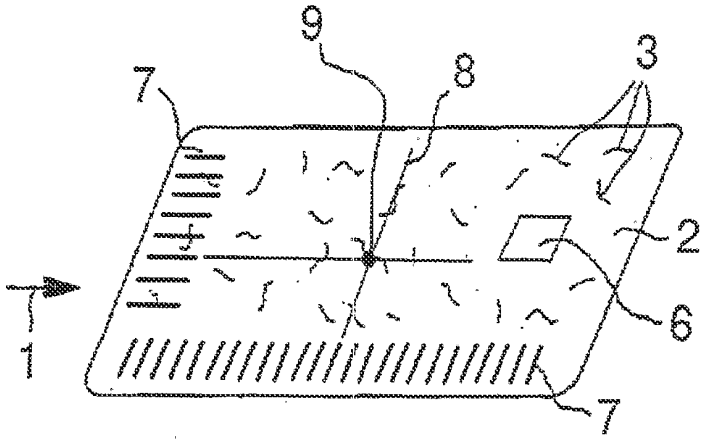


Fig. 2



702 037/274

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

(11) EP 0 977 145 A2

(12) EUROPEAN PATENT APPLICATION

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

(51) Int.Cl.⁷: G06K 19/077

(21) Application number: 99114603.3

(22) Date of filing: 26.07.1999

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

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

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

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

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

(54) Radio IC card

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

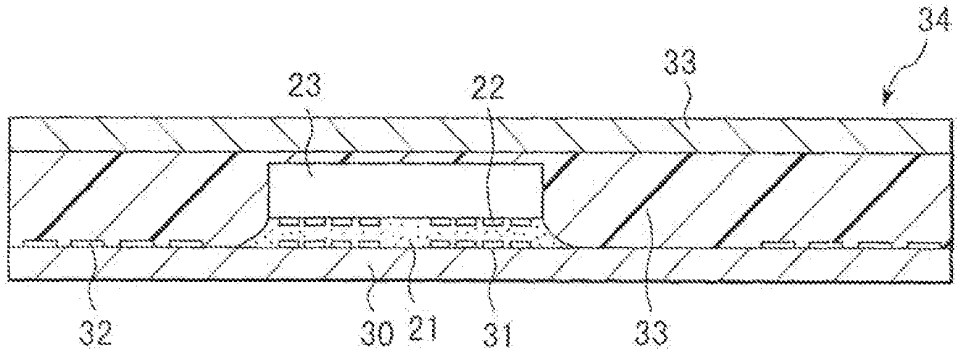


FIG. 14

EP 0 977 145 A2

Description

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

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

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

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

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

[0006] FIG. 1 shows a perspective view of a conventional radio IC card, and FIG. 2 is a cross-sectional view of the same.

[0007] A rectangular-spiral coil pattern 2 is formed on a wiring board 1. An IC chip 3 used as a semiconductor device is mounted on the wiring board 1. An electrode 4 of the IC chip 3 is electrically connected to an electrode 5 on the wiring board 1 by means of a gold ball bump 6.

[0008] A method of manufacturing the radio IC card will now be described.

[0009] The IC chip 3 is first mounted on the wiring board 1 by means of bonding.

[0010] Then a thermoplastic sheet 7 is provided on both sides of the wiring board 1 by thermal fusion.

[0011] The sheet 7 is formed of, e.g. vinyl chloride or PET (polyethylene terephthalate). The entirety of the wiring board 1 is resin-molded by the thermal fusion of sheet 7.

[0012] The thus formed radio IC card is, for example, about 0.2 to 0.7 mm thick.

[0013] FIG. 3 is an electric circuit diagram of this radio IC card. The IC chip 3 is connected to the coil pattern 2. The IC chip 3 has functions of data control, data storage, etc. The IC chip 3 performs data transmission between itself and the outside and receives power through the coil pattern 2.

[0014] However, in the above method, when the IC chip 3 and coil pattern 2 are physically and electrically connected, the IC chip 3 is mounted on the wiring board 1. This method requires expensive equipment such as a flip-chip bonder or a wire-bonder.

[0015] In the order of the manufacturing steps, the step of mounting the IC chip 3 must precede the others. Thus there are many restrictions on the manufacturing steps, and the manufacturing steps are complicated.

[0016] In addition, in the case of the resin-molding, a process management, for example, for considering heat-resistance, is needed and the reliability lowers.

[0017] FIG. 4 is a structure of another radio IC card.

[0018] An IC chip 2 and a communication antenna 9 connected to the IC chip 2 are mounted on a card body 8, and a button cell 10 is built in.

[0019] FIG. 5 is a structure of another radio IC card and FIG. 6 is a cross-sectional view of the IC card.

[0020] An IC chip 2, a communication antenna 9 connected to the IC chip 2, and a power supply coil 10 are mounted on the card body 8.

[0021] In order to ensure security and reliability, the radio IC card is formed in a shape which does not permit easy dissembling, for example, by mold-sealing or thermal-pressing.

[0022] In the case of the radio IC card including the cell, however, the life of the radio IC card is limited by the life of the cell and this is very economically disadvantageous.

[0023] There is also known an electromagnetic-induction-type radio IC card to which power is supplied from a radio IC card reader in the form of electromagnetic waves. In the case of this IC card, the reader needs to constantly send signals. This is not preferable from the standpoint of energy saving.

[0024] For example, in a gate entrance/exit system, incoming/outgoing persons with radio IC cards pass through the gate. The time of entrance/exit of persons is irregular.

[0025] Consequently, the frequency of communication of data read from the radio IC card by the card reader becomes irregular, and the time of wait until the beginning of data communication increases.

[0026] Even if the frequency of data communication is irregular, the card reader is required to constantly send signals

and to always wait for data from the radio IC card.

[0027] An object of the present invention is to provide a radio IC card and a method of manufacturing the same, wherein a semiconductor element is electrically connected to an antenna coil and the radio IC card can be obtained at low cost without the need to use an expensive mounting apparatus.

[0028] Another object of the invention is to provide a radio IC card and a method of manufacturing the same, as well as a data read/write apparatus, wherein energy saving can be achieved irrespective of the life of a cell.

[0029] Still another object of the invention is to provide a radio tag and a method of manufacturing the same, wherein a semiconductor element is electrically connected to an antenna coil and the radio tag can be obtained at low cost without the need to use an expensive mounting apparatus.

[0030] Still another object of the invention is to provide a radio tag and a method of manufacturing the same, wherein energy saving can be achieved irrespective of the life of a cell.

[0031] According to an aspect of the present invention, there is provided a radio IC card comprising: a board having at least two rectangular-spiral antennas formed thereon; and a semiconductor element having a rectangular-spiral antenna formed on a surface thereof, the semiconductor element being mounted on the board such that the antenna on the semiconductor element is situated opposed to one of the at least two antennas on the board.

[0032] In this radio IC card, the antenna on the semiconductor element is formed by bonding a piece of bonding wire among a plurality of electrode pads formed on the surface of the semiconductor element.

[0033] The antenna on the semiconductor element is formed of a metallic film.

[0034] A layer of the antenna formed of the metallic film and a layer of an insulating film are laminated on the surface of the semiconductor element.

[0035] The antenna is provided on each of upper and lower surfaces of the semiconductor element.

[0036] The semiconductor element is provided with a layer for formation of an electric element.

[0037] One of the antennas formed on the board has substantially the same shape as the antenna formed on the semiconductor element, and the other of the antennas on the board is greater in size than the one of the antennas on the board.

[0038] One of the antennas on the board and the other of the antennas on the board are electrically connected.

[0039] One of the antennas on the board and the antenna on the semiconductor device are electromagnetically connected.

[0040] The antenna is formed over the semiconductor element, with an insulating film interposed.

[0041] The antenna is formed over the semiconductor element, with a magnetic film interposed.

[0042] An insulating film is formed on each of the antennas on the board.

[0043] An insulating film, in which magnetic particles are dispersed, is formed on each of the antennas on the board.

[0044] The semiconductor element and the substrate are integrally sealed with resin.

[0045] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: forming a rectangular-spiral antenna on a surface of a semiconductor element; forming at least two rectangular-spiral antennas on a board; and disposing the antenna formed on the semiconductor element such that the antenna formed on the semiconductor element is opposed to one of the antennas formed on the board.

[0046] In this method, the antenna on the surface of the semiconductor element is formed by a thin-film patterning process.

[0047] The antenna on the surface of the semiconductor element is formed by a printing process.

[0048] The antenna on the surface of the semiconductor element is formed such that a plurality of electrode pads are provided on the surface of the semiconductor element and the electrode pads are connected by means of wire bonding.

[0049] The at least two antennas on the board are integrally formed.

[0050] The method includes a step of integrally sealing the semiconductor element and the board with resin.

[0051] According to another aspect of the invention, there is provided a radio IC card having at least one rectangular-spiral antenna and one semiconductor element mounted thereon, wherein a cavity portion is provided near the antenna and a permanent magnet is movably provided within the cavity portion.

[0052] The permanent magnet is movable in a direction of a central axis of the antenna.

[0053] The permanent magnet is rotatably provided within the cavity portion.

[0054] The antenna serves both for power supply to the semiconductor element and for data communication.

[0055] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: mounting at least one semiconductor element and one rectangular-spiral antenna on a first casing body in which a recess portion is formed in advance; inserting a permanent magnet movably in the recess portion; and attaching a second casing body to the first casing body provided with the at least one semiconductor element and one antenna and the permanent magnet.

[0056] According to another aspect of the invention, there is provided a data reader/writer apparatus comprising: a

radio IC card on which at least one rectangular-spiral antenna and a semiconductor element are mounted; and read/write means for performing data communication with the semiconductor element mounted on the radio IC card, the read/write means having a permanent magnet for inducing an electromotive force in the antenna mounted on the radio IC card by crossing a magnetic field over the antenna.

[0057] According to another aspect of the invention, there is provided a radio IC card having at least one data communication antenna and one semiconductor element mounted thereon, the radio IC card comprising a piezoelectric element connected to the semiconductor element.

[0058] The piezoelectric element is used as a board, and the at least one antenna and one semiconductor element are mounted on the piezoelectric element.

[0059] Electrodes are provided on both sides of the piezoelectric element, and these electrodes are electrically connected to at least the semiconductor element.

[0060] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: attaching at least one data communication antenna and one semiconductor element to a first casing body; attaching a piezoelectric element to the first casing body; and adhering a second casing body to the first casing body.

[0061] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: attaching at least one data communication antenna and one semiconductor element on a board formed of a piezoelectric element; and applying an outer coating to the board on which the antenna and the semiconductor element are attached.

[0062] According to another aspect of the invention, there is provided a data read/write apparatus comprising: a radio IC card having at least one data communication antenna and one semiconductor element mounted thereon and including a piezoelectric element connected to the semiconductor element; and read/write means for performing data communication with the semiconductor element by means of the antenna, the read/write means including a pressing mechanism for pressing the piezoelectric element of the radio IC card, thereby producing an electric charge in the piezoelectric element.

[0063] According to another aspect of the invention, there is provided a radio IC card comprising: a semiconductor element having a rectangular-spiral antenna formed on a surface thereof; a board having at least three rectangular-spiral antennas formed thereon such that one of the at least three antennas is situated, opposed to the antenna of the semiconductor element; a cavity portion provided near one of the other antennas on the board; and a permanent magnet provided movably in the cavity portion.

[0064] In this radio IC card, on the board there are provided: an antenna situated to be opposed to the antenna on the semiconductor element; a communication antenna electrically connected to the antenna; and a power supply antenna electrically connected to the communication antenna, a magnetic flux of the permanent magnet being crossed over the power supply antenna.

[0065] The antennas are sealed with an insulating material in which magnetic particles are dispersed.

[0066] According to another aspect of the invention, there is provided a method of manufacturing a radio IC card, the method comprising the steps of: mounting at least one semiconductor element and at least three rectangular-spiral antennas on a first casing body in which a recess portion is formed in advance; inserting a permanent magnet movably in the recess portion; and attaching a second casing body to the first casing body.

[0067] In this method, the method includes the steps of: storing the permanent magnet movably in a case; and mounting the case in the recess portion.

[0068] The first and second casing bodies are formed of an insulating material in which magnetic particles are dispersed.

[0069] According to another aspect of the invention, there is provided a radio tag, wherein a rectangular-spiral antenna is formed on a surface of a semiconductor element.

[0070] In this radio tag, the antenna on the semiconductor element is formed by bonding a piece of bonding wire among a plurality of electrode pads formed on the surface of the semiconductor element.

[0071] The antenna on the semiconductor element is formed of a metallic film.

[0072] A layer of the antenna formed of the metallic film and a layer of an insulating film are laminated on the surface of the semiconductor element.

[0073] The antenna is provided on each of upper and lower surfaces of the semiconductor element.

[0074] The semiconductor element is provided with a layer for formation of an electric element.

[0075] The antenna is provided over the semiconductor element, with an insulating film interposed.

[0076] The antenna is formed over the semiconductor element, with a magnetic film interposed.

[0077] The antenna is formed on the semiconductor element, with an insulating film containing dispersed magnetic particles interposed.

[0078] The semiconductor element having the antenna formed on the surface thereof is sealed with resin.

[0079] According to another aspect of the invention, there is provided a method of manufacturing a radio tag, the

method comprising the steps of: forming an insulating film over a surface of a semiconductor wafer on which a plurality of semiconductor elements are formed; forming rectangular-spiral antennas on the insulating film at positions corresponding to the semiconductor elements; and dicing the semiconductor elements out of the semiconductor wafer.

[0080] In this method, the antenna formed on the surface of each of the semiconductor elements is formed by a thin-film patterning process.

[0081] The antenna formed on the surface of each of the semiconductor elements is formed by a printing process.

[0082] The antenna on each of the semiconductor elements is formed by bonding a piece of bonding wire among a plurality of electrode pads formed on the surface of the semiconductor element.

[0083] Each of the semiconductor elements, on the surface of which the antenna is formed, is sealed with resin.

[0084] According to the above radio IC card and the method of manufacturing the same, as well as the data read/write apparatus and the radio tag and the method of manufacturing the same, the semiconductor element and antenna coil are connected electrically, and not physically. Without using expensive mounting apparatuses, these can be manufactured cost-effectively. Furthermore, energy saving can be achieved irrespective of the life of the cell.

[0085] This summary of the invention does not necessarily describe all necessary features so that the invention may also be a sub-combination of these described features.

[0086] The invention can be more fully understood from the following detailed description when taken in conjunction with the accompanying drawings, in which:

FIG. 1 is a perspective view of a conventional radio IC card;
FIG. 2 is a cross-sectional view of the conventional radio IC card;
FIG. 3 is an electric circuit diagram of the conventional IC card;
FIG. 4 schematically shows the structure of another conventional IC card;
FIG. 5 schematically shows the structure of another conventional IC card;
FIG. 6 is a cross-sectional view of the radio IC card shown in FIG. 5;
FIG. 7A shows a step of manufacturing a radio tag according to a first embodiment of the present invention;
FIG. 7B shows a step of manufacturing the radio tag according to the first embodiment;
FIG. 7C shows a step of manufacturing the radio tag according to the first embodiment;
FIG. 7D shows a step of manufacturing the radio tag according to the first embodiment;
FIG. 8A illustrates a process of manufacturing another example of the radio tag according to the first embodiment;
FIG. 8B is a cross-sectional view of the radio tag in FIG. 8A;
FIG. 8C is a partial cross-sectional view of the radio tag in FIG. 8B;
FIG. 8D is a cross-sectional view of the manufactured radio tag according to this process;
FIG. 9A shows a process of manufacturing the radio tag using a wire bonding method;
FIG. 9B is a side view of this radio tag;
FIG. 10 shows a modification of the radio tag according to the first embodiment;
FIG. 11 shows a modification of the radio tag according to the first embodiment;
FIG. 12 shows a modification of the radio tag according to the first embodiment;
FIG. 13A shows a step of manufacturing a radio IC card according to a second embodiment of the invention;
FIG. 13B shows a step of manufacturing the radio IC card according to the second embodiment;
FIG. 13C shows a step of manufacturing the radio IC card according to the second embodiment;
FIG. 13D shows a step of manufacturing the radio IC card according to the second embodiment;
FIG. 13E shows a step of manufacturing the radio IC card according to the second embodiment;
FIG. 14 is a cross-sectional view of the manufactured IC card;
FIG. 15 is an electric circuit diagram of the radio IC card;
FIG. 16 is a view for describing electromagnetic induction coupling between first and second antenna coils;
FIG. 17A shows a structure of a radio IC card according to a third embodiment of the invention;
FIG. 17B is a cross-sectional view of the radio IC card;
FIG. 18 is an exploded perspective view of the radio IC card;
FIG. 19 is a flow chart of manufacture of the radio IC card;
FIG. 20A is a diagram illustrating the generation of induction electromotive force due to a permanent magnet;
FIG. 20B is a diagram illustrating the generation of induction electromotive force due to the permanent magnet;
FIG. 21A shows a structure of a radio IC card on which a permanent magnet is rotatably mounted;
FIG. 21B is a partial cross-sectional view of the radio IC card shown in FIG. 21A;
FIG. 22A shows a structure of a radio IC card in a data read/write apparatus according to a fourth embodiment of the invention;
FIG. 22B is a cross-sectional view of the radio IC card;
FIG. 23 schematically shows a structure of a reader/writer in the data read/write apparatus;
FIG. 24 is an exploded perspective view of the radio IC card;

FIG. 25 is a view for explaining supply of power from the reader/writer to the radio IC card;
FIG. 26 is a view for explaining the supply of power from the reader/writer to the radio IC card;
FIG. 27 shows a structure of a radio IC card according to a fifth embodiment of the invention;
FIG. 28 shows a structure of a modification of the radio IC card as applied to an automatic wicket;
FIG. 29A shows a structure of a radio IC card according to a sixth embodiment of the invention;
FIG. 29B is a cross-sectional view of the radio IC card;
FIG. 30 is a view for explaining a piezoelectric effect of a piezoelectric element;
FIG. 31 is an electric circuit diagram of the radio IC card;
FIG. 32 is an exploded perspective diagram of the radio IC card;
FIG. 33 is a flow chart of manufacture of the radio IC card;
FIG. 34A shows a structure of a radio IC card according to a seventh embodiment of the invention;
FIG. 34B is a cross-sectional view of the radio IC card;
FIG. 35 is an exploded perspective view of the radio IC card;
FIG. 36 is a flow chart of manufacture of the radio IC card;
FIG. 37A shows an example of dimensions of the manufactured IC card;
FIG. 37B shows an example of dimensions of the radio IC card;
FIG. 38 shows a structure of a data reader/writer apparatus according to an eighth embodiment of the invention;
FIG. 39 is a view for describing power supply to the radio IC card in the apparatus;
FIG. 40A shows a structure of a radio IC card according to a ninth embodiment of the invention;
FIG. 40B is a cross-sectional view of the radio IC card;
FIG. 41A shows a manufacturing step of the radio IC card;
FIG. 41B shows a manufacturing step of the radio IC card;
FIG. 41C shows a manufacturing step of the radio IC card;
FIG. 41D shows a manufacturing step of the radio IC card;
FIG. 42 is a cross-sectional view of an IC chip portion in the radio IC card;
FIG. 43 is an exploded perspective view of the radio IC card; and
FIG. 44 is a flow chart of manufacture of the radio IC card.

(First Embodiment)

[0087] A first embodiment of the present invention will now be described with reference to the accompanying drawings.

[0088] FIGS. 7A to 7D illustrate steps of manufacturing a radio tag.

[0089] FIG. 7A shows a semiconductor wafer 20 on which a plurality of ICs are formed.

[0090] An insulating protection film 21 is formed on the surface of the semiconductor wafer 20, as shown in FIG. 7B. The insulating protection film 21 is formed of, e.g. P-SiN (PSG: Phosphosilicate Glass). The thickness of the insulating protection film 21 is in a range from 0.75 μm to 0.4 μm. The insulating protection film 21 may be formed of, for example, a metal oxide such as silicon dioxide, a resin such as polyimide, or air gap.

[0091] As is shown in FIG. 7C, a number of wound antennas (hereinafter referred to as "antenna coils") 22 are formed on the insulating protection film 21. The antenna coils 22 are formed of, e.g. gold-plated wire. Alternatively, the antenna coils 22 may be formed of thin-film patterns of Cu, Al, etc., or by printing conductive paste of Cu, etc.

[0092] Thereafter, the semiconductor wafer 20 is diced into IC chips 23, as shown in FIG. 7D.

[0093] Thus, radio tags provided with antenna coils are manufactured. The size of each radio tag is, for example, 4 mm (length) × 3 mm (width) × 0.3 mm (height).

[0094] The above-described radio tag has a data control function and a memory function which are achieved by the IC chip 23. Data transmission with the outside or power supply from the outside can be effected through the antenna coil 22.

[0095] According to the first embodiment, as described above, the insulating protection film 21 is formed on the surface of the semiconductor wafer 20, and the antenna coil 22 is formed on the insulating protection film 21. The semiconductor wafer 20 is then diced and the radio tags are formed. Thus, the IC chips 23 are electrically connected to the antenna coils 22 without physical connection. There is no need to use expensive apparatuses, such as flip-chip bonders or wire bonders, in order to mount the IC chips.

[0096] There is no need to conduct a process management, for example, for considering heat-resistance in resin-molding, and the reliability is enhanced.

[0097] The antenna coil 22 is formed on the IC chip 23, and the resultant structure is merely mounted. Therefore, the small-sized, inexpensive radio tag can be obtained.

[0098] A description will now be given of another example of the manufacture of the radio tag according to the first embodiment.

[0099] FIGS. 8A to 8D schematically illustrate manufacturing steps of the radio tag. FIG. 8A shows a plan view and a cross-sectional view. FIG. 8B is a cross-sectional view of the radio tag. FIG. 8C is an enlarged view of portion 8C in FIG. 8B, and FIG. 8D is a cross-sectional view of the manufactured radio tag.

[0100] An IC chip 23 applied to this example has a square shape with each side of, e.g. about 10 mm, and a thickness of about 20 μm at a minimum.

[0101] An insulating protection film 21 is formed on the surface of the IC chip 23. The insulating protection film 21 is formed of, e.g. silicon dioxide or a polyimide resin. The thickness of the insulating protection film 21 is about 10 to 100 μm. The insulating protection film 21 may be formed of a magnetic film such as ferrite, instead of silicon dioxide or a polyimide resin.

[0102] Magnetic particles may be dispersed in the insulating protection film 21. With the formation of the magnetic film, an inductance component of the antenna coil 22 which is to be formed subsequently can be increased. The insulating protection film 21 may be an air gap formed by etching silicon dioxide.

[0103] A conductive via-hole 24, which is a through-hole, is formed in the insulating protection film 21, as shown in FIG. 8B.

[0104] A rectangular spiral antenna coil (pattern coil) 22 is formed on the insulating protection film 21. The antenna coil 22 is formed of a conductive film of Al, Cu, Au, etc. The antenna coil 22 is thinly formed, with a pattern width and a pattern interval being in a range of several μm to several-ten μm. The antenna coil 22 may be formed by means of printing of a conductive paste of, e.g. Ag, Cu, etc.

[0105] Subsequently, the IC chip 23 is molded with a mold resin 25, as shown in FIG. 8D. For example, if the mold resin 25 is an epoxy resin, etc., transfer molding is adopted. If the mold resin 25 is PP (polypropylene), PPS (polyphenylsulfone), etc., injection molding is adopted. Thus, a radio tag with an outside shape of about 10 mm × 10 mm and a thickness of about 1 mm.

[0106] FIGS. 9A and 9B are schematic views showing another example of the radio tag which is manufactured by using wire bonding. FIG. 9A is a plan view and a FIG. 9B is a side view.

[0107] As is shown in FIG. 9A, electrodes 26 are formed at four corner portions on the surface of the IC chip 23. Each electrode 26 has a square shape with each side about 30 μm to 100 μm long.

[0108] The electrodes 26 are interconnected by a bonding wire element 27. The bonding of electrodes 26 is performed from the outer peripheral side toward the central side. As a result, a rectangular-helical antenna coil is formed. The bonding wire element 27 has a diameter of, e.g. about 10 μm to 100 μm and is formed of Au, Al or Cu.

[0109] The radio tag is thus manufactured.

[0110] In the process of manufacturing this radio tag, the formation of an insulating protection film is not needed, as shown in FIG. 9B, and the pattern resistance can be reduced sine the bulk-type coil material is used.

[0111] A modification of the manufacture of the radio tag according to the first embodiment will now be described.

[0112] FIG. 10 shows a multi-layer structure in which antenna coils 22 and insulating protection films 21 are formed in two tiers on the surface of the IC chip 23. By virtue of this structure, the number of turns of the antenna coils 22 is increased.

[0113] FIG. 11 shows a structure in which through-holes 28 are formed in the IC chip 23. Antenna coils 22 are formed on upper and lower surfaces of the IC chip 23. The antenna coils 22 are electrically connected through the through-holes 28.

[0114] FIG. 12 shows a radio tag with multi-functions, wherein various electric elements such as a capacitor 29, in addition to antenna coils 22, are provided on the IC chip 23. In the capacitor 29, an induction-type thick-film material of, e.g. titanium dioxide, lead perovskite, etc. is used.

[0115] Needless to say, with the above examples of the radio tag, too, the IC chip 23 and antenna coil 22 are connected electrically, and not physically. Without using expensive mounting apparatuses, the radio tags can be manufactured cost-effectively.

(2) A radio IC card (non-contact data carrier) according to a second embodiment of the invention will now be described with reference to FIGS. 13A to 13E.

[0116] A radio tag, like the first embodiment, is first manufactured.

[0117] An insulating protection film 21 is formed, as shown in FIG. 7B, on the surface of the semiconductor wafer 20 shown in FIG. 7A. The insulating protection film 21 is formed of, e.g. P-SiN (PSG: Phosphosilicate Glass). The thickness of the insulating protection film 21 is in a range from 0.75 μm to 0.4 μm. The insulating protection film 21 may be formed of, for example, a metal oxide such as silicon dioxide, a resin such as polyimide, or air gap.

[0118] As is shown in FIG. 7C, the antenna coil 22 (hereinafter referred to as "first antenna coil 22") is formed on the insulating protection film 21 by gold plating. The first antenna coils 22 may be formed of thin-film patterns of Cu, Al, etc , or by printing conductive paste of Cu, etc.

[0119] Thereafter, the semiconductor wafer 20 is diced into IC chips 23, as shown in FIG. 7D.

[0120] On the other hand, a second antenna coil 31 and a third antenna coil 32 are formed, as shown in FIG. 13B, on a surface of a module board 30 shown in FIG. 13A.

[0121] The second antenna coil 31 has substantially the same shape as the first antenna coil 32 formed on the radio tag.

[0122] Since the third antenna coil 32 is used for communication with the outside of the radio IC card or for power supply from the outside, it has a greater number of turns and a greater shape than the second antenna coil 31.

[0123] The second and third antenna coils 31 and 32 are electrically connected to constitute a closed loop circuit.

[0124] The second and third antenna coils 31 and 32 are simultaneously formed on the surface of the module board 30, for example, by a subtractive method, as in the formation of a regular printed circuit board.

[0125] The second and third antenna coils 31 and 32 may be formed by an additive method. The second and third antenna coils 31 and 32 may be formed by fixing coils of coated wire on the module board 30. Alternatively, the antenna coils may be formed of a combination of printed wire and wire coils.

[0126] Specifically, the second and third antenna coils 31 and 32 are both formed by etching Ag, Al, etc.

[0127] Alternatively, the second and third antenna coils 31 and 32 may both be formed by a printing method using Ag paste, or formed of coils of Cu. Furthermore, the second antenna coil 31 may be formed by printing or etching, while the third antenna coil 32 may be formed of coils.

[0128] In a subsequent step shown in FIG. 13C, an insulating film 33 is formed on the second antenna coil 31. The insulating film 33 is formed of a semi-hardened epoxy resin with a thickness of, e.g. 20 μm. For example, the insulating film 33 is formed by attaching an insulating adhesive film of a semi-hardened epoxy resin. The insulating film 33 may be formed of some other insulative resin such as polyimide or a metal oxide.

[0129] In the next step illustrated in FIG. 13D, the IC chip 23 (see FIG. 7D) is opposed to, and disposed on, the second antenna coil 31 on the module board 30.

[0130] In this case, the IC chip 23 is mounted in a face-down fashion. The mounting is performed under a suitable pressure such that the second antenna coil 31 is opposed to the first antenna coil 22 of the IC chi 23 with the insulating film 33 interposed.

[0131] In addition, the mounting is performed such that the gap between the first antenna coil 22 and second antenna coil 31 is mechanically controlled and the gap is set at about 20 μm or less.

[0132] In the mounting step, in order to completely harden the insulating adhesive film of, e.g. semi-hardened epoxy resin, which forms the insulating film 33, it is heated at about 200°C to 120°C for 10 to 120 seconds and fixed on the module board 30.

[0133] For example, the material of the insulating adhesive film may be applied in a viscous liquid phase. In this case, where the maintenance of the insulating film 33 is difficult under pressure, the height of the film may be controlled. For example, the insulating film 33 may be maintained by using a spacer of a polyester film with a thickness of, e.g. 10 μm, which serves also as the insulating film 33.

[0134] Subsequently, as shown in FIG. 13E, the entire module board 30 with the IC chip 23 is sealed with resin and coated with the polyester film 33. At last, the radio IC card 34 is obtained after printing and punching.

[0135] FIG. 14 is a cross-sectional view of the manufactured radio IC card 34. The method of forming the radio IC card is, for example, injection molding (e.g. insertion molding) using, e.g. a polyester resin, or pressing molding using, e.g. a vinyl chloride sheet.

[0136] FIG. 15 is an electric circuit diagram of the radio IC card 34.

[0137] Since the first antenna coil 22 of the IC chip 23 is disposed to be opposed to the second antenna coil 31 of the module board 30, electromagnetic induction coupling is effected between the first antenna coil 22 and second antenna coil 31.

[0138] Accordingly, if the third antenna coil 32 receives electric waves from the outside, an electromotive force occurs in the third antenna coil 32. The electromotive force is supplied to the second antenna coil 31 connected to the third antenna coil 32.

[0139] At the time current begins to flow in the second antenna coil 31, an electric field is generated at the second antenna coil 31.

[0140] This electric field acts on the first antenna coil 22 located near and opposed to the second antenna coil 31, and an electromotive force is induced in the first antenna coil 22.

[0141] This electromotive force is supplied to the IC circuit 35. In this manner, external electric waves are converted to power to be supplied to the IC circuit 35, through the third, second and first antenna coils 32, 31 and 22.

[0142] On the other hand, if current is output from the IC circuit 35, the current is supplied to the first antenna coil 22. At the time the current begins to flow through the first antenna coil 22, an electric field is generated at the first antenna coil 22.

[0143] This electric field acts on the second antenna coil 31 located near and opposed to the first antenna coil 22, and an electromotive force is induced in the second antenna coil 31.

[0144] The induced electromotive force is supplied to the third antenna coil 32. This causes electric waves to be radiated from the third antenna coil 32.

[0145] The electromagnetic induction coupling between the first antenna coil 32 and second antenna coil 31 will now

be described with reference to FIG. 16.

[0146] Assume that there are two single-turn coils having loop planes parallel to an xz-plane, i.e. those corresponding to the first antenna coil 22 and second antenna coil 31. A distance between the first and second antenna coils 22 and 31 is d.

[0147] An intensity H, at a location of the first antenna coil 22, of a magnetic field produced by a current Ia flowing in the second antenna coil 31 can be found by considering a y-axis component Hy alone and given by the Biot-Savart's law as follows:

$$Hy = \frac{Ia(2\pi ra)\left\{ra / \sqrt{(ra^2 + d^2)}\right\}}{4\pi(ra^2 + d^2)}$$

$$= \frac{ra^2 \cdot Ia}{2(ra^2 + d^2)^{3/2}} \qquad \ldots(1)$$

$$= \alpha Ia$$

$$\alpha = \frac{ra^2}{2(ra^2 + d^2)^{3/2}} \qquad (2)$$

[0148] It is understood from above that the magnetic field Hy is proportional to the current Ia. An electromotive force Vb produced by electromagnetic induction in the first antenna coil 22 is expressed by

$$Vb = - (d\Phi b/dt) \qquad (3)$$

where Φb is the magnetic flux density of the first antenna coil 22.

[0149] The relationship between the magnetic flux density Φb of the first antenna coil 22 and the magnetic field Hy is expressed by

$$\Phi b = \mu \, Hy \ (\mu: \text{magnetic permeability}) \qquad (4)$$

[0150] Accordingly, using equations (1), (3) and (4), the electromotive force Vb is given by

$$Vb = - (d\Phi b/dt)$$

$$= -\mu \ (dHy/dt)$$

$$= -\alpha \mu \ (dIa/dt) \qquad \ldots(5)$$

where μ is a constant determined by material.

[0151] The electromotive force Vb occurs in the first antenna coil 22 due to a temporal variation in the current Ia flowing through the second antenna coil 31.

[0152] It is understood from the above equation (2) that α increases as the distance d between the first and second antenna coils 22 and 31 decreases and the sensitivity for communication becomes higher as the distance d between the first and second antenna coils 22 and 31 decreases.

[0153] According to the second embodiment, the first antenna coil 22 is formed on the surface of the IC chip 23, and the second and third antenna coils 31 and 32 are formed on the module board 30. The IC chip 23 is disposed on the module board 30 such that the first antenna coil 22 of the IC chip 23 is opposed to the second antenna coil 31. Thus, unlike the prior art, the radio IC card wherein the IC circuit 35 and third antenna coil 32 are electrically connected, without physical connection, can be obtained.

[0154] Accordingly, such an expensive mounting apparatus as a flip-chip bonder or a wire bonder is not required to mount the IC chip 23.

[0155] In addition, in the case of the resin-molding, a process management, for example, for considering heat-resistance, is needed and the reliability lowers.

[0156] Moreover, the degree of freedom for the manufacturing process is high, and the manufacturing cost is reduced.

[0157] In the manufacturing of the radio tag according to the second embodiment, the antenna coils 22 are formed of gold-plated wiring elements, thin-film patterns, or by printing conductive paste.

[0158] As shown in FIGS. 9A and 9B, however, the first antenna coil 22 may be formed by means of wire bonding.

[0159] Alternatively, the first antenna coil 22 may be formed with a multi-layer structure, as shown in FIG. 10.

[0160] Alternatively, antenna coils 22 may be formed on the upper and lower surfaces of the IC chip 23, as shown in FIG. 11.

[0161] Alternatively, the IC chip 23 may be provided with various electric elements such as capacitor 29 so as to have multi-functions, as shown in FIG. 12.

(3) A third embodiment according to the present invention will now be described.

[0162] FIGS. 17A and 17B show the structure of the radio IC card according to the third embodiment. FIG. 17A is a plan view and FIG. 17B is a cross-sectional view.

[0163] A carrier body 40 is provided with an IC chip 23, a communication antenna 41 and a power supply coil 42. The communication antenna 41 and power supply coil 42 are formed in rectangular spiral shapes.

[0164] The communication antenna 41 and power supply coil 42 are connected to the IC chip 23.

[0165] The carrier body 40 is formed of, e.g. polystyrene (PS), polyethylene terephthalate (PET) or vinyl chloride. The size of the carrier body is, e.g. 86 mm × 54 mm × 3 mm.

[0166] The communication antenna 41 and power supply coil 42 are formed, for example, by winding fine conductors twice or more, or by winding electric lines twice or more by means of deposition, etc. For example, coated copper-wire coils, copper-wire coils or aluminum-wire coils are used for the communication antenna 41 and power supply coil 42.

[0167] A space (hereinafter referred to as "cavity") 43 is defined inside the power supply coil 42. A permanent magnet 44 is movably provided within the cavity 43.

[0168] The permanent magnet 44 has a plate shape. One surface side of the permanent magnet 44 is magnetized with an N-pole, and the other surface side is magnetized with an S-pole. As is shown in FIG. 17B, the permanent magnet 44 is disposed to be movable in the direction of the central axis (S1) of the power supply coil 42. The permanent magnet 44 is formed of, e.g. an Alnico molded magnet, a Ba ferrite magnet, a rare-earth cobalt magnet, carbon steel, tungsten steel, KS steel, or Comfe. The size of the permanent magnet 44 is, e.g. 20 mm × 40 mm × 1 mm.

[0169] A method of manufacturing the above radio IC card will now be described with reference to an exploded perspective view of FIG. 18 and a flow chart of FIG. 19. In the flow chart of FIG. 19, triangular symbol ▽ denotes the provision of structural elements, and circular symbol ○ denotes manufacturing steps.

[0170] As is shown in FIG. 18, the carrier body 40 is a combination of a first casing body (lower card casing body) 40a and a second casing body (upper card casing body) 40b.

[0171] The lower card casing body 40a is provided with recess portions 45 to 47 for receiving the IC chip 23, communication antenna 41 and power supply coil 42.

[0172] The upper card casing body 40b is provided with a cavity 43 for insertion of the permanent magnet 44.

[0173] To start with, as shown in FIG. 19, an IC chip 23 and a board 48 for the IC chip 23 are provided.

[0174] In step #1, the IC chip 23 is mounted on the board 48.

[0175] In step #2, the IC chip 23 mounted on the board 48 is set in the recess portion 45 in the lower card casing body 40a. In this step, the IC chip 23 is adhered to the recess portion 45.

[0176] The communication antenna 41 and power supply coil 42 are supplied to the manufacturing line.

[0177] Leads 41a and 42a for connection with the terminals of the board 48 extend from the communication antenna 41 and power supply coil 42.

[0178] In step #3, the communication antenna 41 and power supply coil 42 are set in the recess portions 46 and 47 in the lower card casing body 40a.

[0179] The leads 41a and 42a of the communication antenna 41 and power supply coil 42 are connected to the terminals of the board 48 by means of soldering.

[0180] The permanent magnet 44 is supplied to the manufacturing line. In step #4, the permanent magnet 44 is inserted in the cavity 43 in the upper card casing body 40b.

[0181] Subsequently, the lower card casing body 40a on which the IC chip 23, communication antenna 41 and power supply coil 42 are mounted is supplied to the manufacturing line, and the upper card casing body 40b in which the permanent magnet 44 is inserted are supplied to the manufacturing line.

[0182] In step #5, the lower card casing body 40a and upper card casing body 40b are combined and adhered to each other, whereby the carrier body 40 is formed.

[0183] In step #6, printing is effected on the surface of the carrier body 40.

[0184] At last, the manufactured radio IC card is examined.

[0185] The operation of the thus manufactured radio IC card will now be described.

[0186] If the radio IC card is carried by a person, etc., the entire body thereof moves. Thereby the permanent magnet 44 in the cavity 43 is moved.

[0187] The magnetic flux of the permanent magnet 44 crosses the power supply coil 42, and as a result an electromotive force is induced in the power supply coil 42. The induced electromagnetic force is supplied to the IC chip 23.

[0188] This operation will now be described more specifically with reference to FIGS. 20A and 20B which are enlarged partial views of the power supply coil 42.

[0189] If the radio IC card has moved, the permanent magnet 44 moves in the direction of the central axis si of the power supply coil 42 within the cavity 43.

[0190] Consider a case where the permanent magnet 44 is located at an end portion of the cavity 43, as shown in FIG. 20A, and a case where the permanent magnet 44 is located at a central portion of the cavity 43, as shown in FIG. 20B. Suppose that an upper surface of the permanent magnet 44 has an S-pole, and a lower surface thereof has an N-pole.

[0191] When the permanent magnet 44 is located at an end portion of the cavity 43, as shown in FIG. 20A, the flux density B within the power supply coil 42 takes a minimum value. When the permanent magnet 44 is located at a central portion of the cavity 43, as shown in FIG. 20B, the flux density takes a maximum value.

[0192] Accordingly, if the entire radio IC card is slightly moved, for example, by the hand of the user, the flux density B within the power supply coil 42 varies. The variation in the flux density B induces an electromotive force in the power supply coil 42. The electromotive force is supplied as power to the IC chip 23.

[0193] The permanent magnet 44 is movably provided within the cavity 43, but it may be provided, for example, in a rotatable manner.

[0194] FIGS. 21A and 21B show structures of the radio IC card. FIG. 21A is a partial plan view, and FIG. 21B is a partial cross-sectional view.

[0195] Both end portions of a plate-like permanent magnet 49 are rotatably supported by support members 50 and 51 within the cavity 43. The support member 51 is coupled to a dial 53. The dial 53 functions to rotate the permanent magnet 49 in the direction of arrow s2 from the outside, as shown in FIG. 21B.

[0196] In general, an induction electromotive force v occurs in a primary coil in such a direction as to cancel a temporal variation in magnetic flux within the coil. The electromotive force v is expressed by

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

where Φ is the flux, and t is time.

[0197] If the magnetic flux is B, the in-coil area is S, permeability is μ and magnetic field intensity is H,

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

[0198] The induction electromotive force v is expressed by

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

[0199] An example of calculation of induction electromotive force v is shown below. Since the cavity 43 is located within the power supply coil 42, the permeability of air is approximated on the basis of that of vacuum as follows:

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

[0200] The permanent magnet 44 is rotatable within the radio IC card. The permanent magnet 44 has a plate shape and a size of 2 mm × 20 mm, and is formed of, e.g. $SmCo_5$.

[0201] The coercive force of the permanent magnet 44 is expressed by

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

[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

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

[0203] In this example, an electromotive force of about 1 [V] is obtained.

[0204] According to the third embodiment, the cavity 43 is formed within the power supply coil 42 mounted on the radio IC card, and the permanent magnet 44 is movably provided within the cavity 43. Thus, electric energy due to induction electromotive force v can be supplied to the radio IC card by the permanent magnet 44 and, e.g. the manual operation, without using electric energy due to a cell or an electromagnetic coil.

[0205] Accordingly, exchange of a cell is not required, and power consumption in the standby state of the reader/writer can be reduced to achieve energy saving. Thus, the radio IC card with simple structure can be manufactured. For example, compared to the cell-built-in type radio IC card, the energy saving ratio of power supply is 100% and no waste cell is produced.

(4) A fourth embodiment of the present invention will now be described. The structural parts common to those shown in FIGS. 17A and 17B are denoted by like reference numerals, and a detailed description thereof is omitted.

[0206] The fourth embodiment relates to a data read/write apparatus using a radio IC card. FIGS. 22A and 22B show a structure of the radio IC card, and FIG. 23 schematically shows a structure of a radio IC card reader/writer 50.

[0207] In the radio IC card, the IC chip 23, communication antenna 41 and power supply coil 42 are mounted on the carrier body 40. The IC chip 23 is connected to the communication antenna 41 and power supply coil 42.

[0208] A method of manufacturing the radio IC card will now be described with reference to an exploded perspective view of FIG. 24.

[0209] The carrier body 40 is formed by combining a lower card casing body 40a and an upper card casing body 40b.

[0210] Like the radio IC card shown in FIG. 18, the lower card casing body 40a, the lower card casing body 40a is provided with recess portions 45 to 47 for receiving the IC chip 23, communication antenna 41 and power supply coil 42.

[0211] To start with, the IC chip 23 and board 48 are prepared. The IC chip 23 is mounted on the board 48. The IC chip 23 is set in the recess portion 45 in the lower card casing body 40a.

[0212] Then, the communication antenna 41 and power supply coil 42 are prepared. These antennas 41 and 42 have leads 41a and 42a for connection with terminals of the board 48.

[0213] The communication antenna 41 and power supply coil 42 are set in the recess portions 46 and 47 in the lower card casing body 40a.

[0214] The leads 41a and 42a are connected to the terminals of the board 48 by means of, e.g. soldering.

[0215] The lower card casing body 40a, on which the IC chip 23, communication antenna 41 and power supply coil 42 have been mounted, is combined with the upper card casing body 40b. The lower card casing body 40a and the upper card casing body 40b are adhered to each other to constitute the carrier body 40.

[0216] Following the above, printing is effected on the surface of the carrier body 40.

[0217] At last, the manufactured radio IC card is inspected.

[0218] On the other hand, the reader/writer 50 reads/writes data from/in the radio IC card which is situated as shown in FIG. 23.

[0219] The reader/writer 50 includes a read/write antenna 51 which corresponds in position to the communication antenna 41 of the radio IC card. The reader/writer 50 also includes a permanent magnet 52 which corresponds in position to the power supply coil 42 of the radio IC card.

[0220] The power supply operation of the data read/write apparatus with the above construction, by which power is supplied to the radio IC card, will now be described.

[0221] If the carrier body 40 is moved toward the reader/writer 50, the power supply coil 42 in the radio IC card approaches the permanent magnet 52 in the reader/writer 50, as shown in FIGS. 25 and 26. With the power supply coil 42 approaching the permanent magnet 52, the flux density B within the power supply coil 42 varies and an electromotive force is induced in the power supply coil 42. The induced electromotive force is supplied to the IC chip 23.

[0222] According to the fourth embodiment, the reader/writer 50 is provided with the permanent magnet 52. By approaching the carrier body 40 to the reader/writer 50, the electromotive force is induced in the power supply coil 42 and it is supplied to the IC chip 23 of the radio IC card. Like the first embodiment, electric energy can be supplied to the radio IC card when data read/write is effected by the reader/writer 50, without using electric energy due to a cell or an electromagnetic induction coil. Therefore, no exchange of a cell is required, and power consumption in the standby state of the reader/writer 50 can be reduced to achieve energy saving. Thus, the radio IC card with simple structure can be manufactured.

(5) A fifth embodiment of the present invention will now be described. The structural parts common to those shown in

FIGS. 17A and 17B are denoted by like reference numerals, and a detailed description thereof is omitted.

[0223] FIG. 27 is an exploded perspective view of a radio IC card.

[0224] A method of manufacturing the radio IC card will now be described.

[0225] The carrier body 40 is formed by combining a lower card casing body 40a and an upper card casing body 40b.

[0226] The lower card casing body 40a is provided with recess portions 61 and 62 for receiving the IC chip 23 and a communication/power-supply coil 60.

[0227] The upper card casing body 40b is provided with the cavity 43 for receiving the permanent magnet 44.

[0228] To begin with, the IC chip 23 and board 48 are prepared.

[0229] The IC chip 23 is mounted on the board 48.

[0230] The IC chip 23 mounted on the board 48 is set in the recess portion 61 in the lower card casing body 40a.

[0231] The communication/power-supply coil 60 is prepared. The coil 60 has leads 60a for connection with terminals of the board 48. The communication/power-supply coil 60 is set in the recess portion 62 in the lower card casing body 40a. The leads 60a are connected to the terminals of the board 48 by means of, e.g. soldering.

[0232] Then the permanent magnet 44 is prepared. The permanent magnet 44 is inserted in the cavity 43 in the upper card casing body 40b.

[0233] The lower card casing body 40a, on which the IC chip 23 and communication/power-supply coil 60 are mounted, and the upper card casing body 40b, in which the permanent magnet 44 is inserted, are combined and adhered to each other. Thus the carrier body 40 is constituted.

[0234] Following the above, printing is effected on the surface of the carrier body 40. Finally, the radio IC card is inspected.

[0235] The operation of the radio IC card thus manufactured will now be described.

[0236] If the radio IC card is carried by the user and moved, the permanent magnet 44 in the cavity 43 is moved.

[0237] With the movement of the permanent magnet 44, the magnetic flux of the permanent magnet 44 crosses the communication/power-supply coil 60. Consequently, an electromotive force is induced in the communication/power-supply coil 60. The induced electromotive force is supplied to the IC chip 23.

[0238] Needless to say, according to the fifth embodiment, the same advantages as with the first embodiment can be obtained with use of the communication/power-supply coil 60.

[0239] The third to fifth embodiments may be modified as follows.

[0240] For example, as shown in FIG. 28, a plurality of permanent magnets 71 may be arranged in an automatic wicket 70. The radio IC card shown in FIGS. 22A and 22B is made to pass by the permanent magnets 71. At this time, the flux density B within the power supply coil 42 varies, and an electromotive force induced in the power supply coil 42 is supplied to the IC chip 23.

(6) A sixth embodiment of the present invention will now be described with reference to the accompanying drawings.

[0241] FIG. 29A shows a structure of a radio IC card, and FIG. 29B is a cross-sectional view of the radio IC card.

[0242] An IC chip 23 and a communication antenna 41 are mounted on a carrier body 80. The communication antenna 41 is electrically connected to the IC chip 23.

[0243] The carrier body 80 is formed of, e.g. polystyrene (PS), polyethylene terephthalate (PET), vinyl chloride, etc.

[0244] The communication antenna 41 is formed of, e.g. a coated copper wire coil, a copper wire coil or an aluminum wire coil.

[0245] A piezoelectric element 81 electrically connected to the IC chip 23 is mounted on the carrier body 80. Electrodes 82a and 82b are provided at both ends of the piezoelectric element 81. The electrodes 82a and 82b are electrically connected to the IC chip 23.

[0246] The piezoelectric element 81 has such a piezoelectrical effect that when pressure is applied to the piezoelectric element 81, as shown in FIG. 30, it is polarized to have positive and negative charges (+,-). The piezoelectric element 81 is formed of, e.g. Rochelle salt, barium titanate, potassium dihydrogenphosphate, ammonium hydrogenphosphate, lithium sulfate, lithium niobate, zinc oxide, polyvinyl difluoride, antimony iodide-sulfide, or zinc zirconate-titanate.

[0247] FIG. 31 is an electric circuit diagram of the above radio IC card.

[0248] The communication antenna 41 and electrodes 82a and 82b are connected to the IC chip 23. The electrodes 82a and 82b are provided at both ends of the piezoelectric element 81. The piezoelectric element 81 serves as a power supply for the IC chip 23.

[0249] A method of manufacturing the radio IC card will now be described with reference to an exploded perspective view of FIG. 32 and a flow chart of FIG. 33.

[0250] The carrier body 80, as shown in FIG. 32, is formed by combining a first casing body (lower card casing body) 80a and a second casing body (upper card casing body) 80b.

[0251] A recess portion 83 for receiving the piezoelectric element 81 is formed in the lower card casing body 80a. Although not shown, the lower card casing body 80a is provided with recess portions for receiving the IC chip 23 and communication antenna 41.

[0252] To start with, as shown in FIG. 33, the IC chip 23 and board 84 are prepared. In step #10, the IC chip 23 is

mounted on the board 84. In the next step #11, the board 84 as a COB (chip-on-board) 85 is set in the recess portion 80 in the lower card casing body 80a.

[0253] The communication antenna 41 is supplied to the manufacturing line. The communication antenna 41 has leads 41a for connection with the terminals of the COB 85. In step #12, the communication antenna 41 is set in the recess portion in the lower card casing body 80a.

[0254] The leads 41a of the communication antenna 41 are connected to the terminals of the COB 85 by means of, e.g. soldering.

[0255] Subsequently, the piezoelectric element 81 and the terminals 82a and 82b to be provided at both ends of the piezoelectric element 81 are supplied. The electrodes 82a and 82b have leads 86 and 87 for connection with the terminals of the COB 85. The electrodes 82a and 82b are provided at both ends of the piezoelectric element 81.

[0256] In step #13, the piezoelectric element 81 with the electrodes is set in the recess portion in the lower card casing body 80a. The leads 86 and 87 of the electrodes 82a and 82b are connected to the terminals of the COB 85 by means of, e.g. soldering.

[0257] In step #14, the lower card casing body 80a on which the COB 85, communication antenna 41 and piezoelectric element 81 with electrodes are mounted, is combined with, and adhered to, the upper card casing body 80b. Thus, the carrier body 90 is constituted.

[0258] In step #15, printing is effected on the surface of the carrier body 90, and at last the manufactured radio IC card is inspected.

[0259] The size of the manufactured radio IC card is 86 mm × 54 mm, each side of the IC chip is 3 mm, each size of the communication antenna 41 is 45 mm, and the size of the piezoelectric element 81 is 30 mm × 45 mm × 2 mm.

[0260] The operation of the radio IC card will now be described.

[0261] If pressure is applied to the piezoelectric element 81 of the radio IC card, it is polarized to have positive and negative charges (+,-), as shown in FIG. 30. An electromotive force is produced at the electrodes 82a and 82b of the piezoelectric element 81, and it is supplied to the IC chip 23.

[0262] Accordingly, if pressure is applied to the piezoelectric element 81 of the radio IC card by a pressurizing mechanism or the hand of the user, the electromotive force produced by the piezoelectric element 81 is supplied to the IC chip 23.

[0263] As has been described above, according to the sixth embodiment, the electromotive force produced by the piezoelectric element 81 is supplied to the IC chip 23. Thus, like the third embodiment, no exchange of a cell is required, energy saving is realized, and the radio IC card with simple structure is obtained. For example, compared to the cell-built-in type non-contact data carrier, the energy saving ratio of power supply is 100% and no waste cell is produced. Therefore, the life of the apparatus can be increased while the apparatus can be operated with clean energy.

(7) A seventh embodiment of the present invention will now be described with reference to the accompanying drawings.

[0264] FIG. 34A shows the structure of a radio IC card and FIG. 34B is a cross-sectional view of the radio IC card.

[0265] An IC chip 23 and communication antenna 41 are mounted on the carrier body 90. The communication antenna 41 is electrically connected to the IC chip 23.

[0266] The carrier body 90 is formed of, e.g. polystyrene (PS), polyethylene terephthalate (PET) or vinyl chloride.

[0267] The communication antenna 41 is formed of, e.g. coated copper-wire coils, copper-wire coils or aluminum-wire coils.

[0268] The carrier body 90 incorporates a plate-like piezoelectric element (hereinafter referred to as "piezoelectric element board") 91. The piezoelectric element board 91 serves as a board of the radio IC card body.

[0269] The piezoelectric element board 91 has such a piezoelectrical effect that when pressure is applied to the piezoelectric element board 91, it is polarized to have positive and negative charges (+,-). Like the sixth embodiment, the piezoelectric element board 91 is formed of, e.g. Rochelle salt, barium titanate, potassium dihydrogenphosphate, ammonium hydrogenphosphate, lithium sulfate, lithium niobate, zinc oxide, polyvinyl difluoride, antimony iodide-sulfide, or zinc zirconate-titanate.

[0270] The IC chip 23 and communication antenna 41 are mounted on the piezoelectric element board 91.

[0271] The electrodes 92a and 92b are provided on both surfaces of the piezoelectric element board 91. The electrodes 92a and 92b are electrically connected to the IC chip 23. It is preferable to form the electrodes 92a and 92b as large as possible on both surfaces of the piezoelectric element board 91.

[0272] A method of manufacturing the radio IC card will now be described with reference to an exploded perspective view of FIG. 35 and a flow chart of FIG. 36.

[0273] As is shown in FIG. 35, the carrier body 90 is formed by providing the piezoelectric element board 91 with a lower outside sheet 90a and an upper outside sheet 90b.

[0274] The communication antenna 41 and electrodes 92a and 92b are formed on the piezoelectric element board 91.

[0275] To begin with, as shown in FIG. 35, the IC chip 23 and piezoelectric element board 91 are supplied to the manufacturing line. In step #20, the IC chip 23 is mounted on the piezoelectric element board 91.

[0276] In step #21, the lower outside sheet 70a and upper outside sheet 70b are attached, by means of pressing or

laminating, to both surfaces of the piezoelectric element board 91 on which the IC chip 23 is mounted. Thus, the carrier body 90 is formed.

[0277] In step #22, printing is effected on the surface of the carrier body 90.

[0278] At last, the manufactured radio IC card is inspected.

[0279] FIGS. 37A and 37B show an example of the size of the manufactured radio IC card. The size of the entire radio IC card is 86 mm × 54 mm × 3 mm.

[0280] The operation of the manufactured radio IC card will now be described.

[0281] If pressure is applied to the piezoelectric element board 91, it is polarized to have positive and negative charges (+,-), as shown in FIG. 30. An electromotive force is produced at the electrodes 92a and 92b of the piezoelectric element board 91, and it is supplied to the IC chip 23.

[0282] Accordingly, if pressure is applied to the piezoelectric element board 91 by a pressurizing mechanism or the hand of the user, the electromotive force produced by the piezoelectric element board 91 is supplied to the IC chip 23.

[0283] As has been described above, according to the seventh embodiment, the electromotive force produced by the piezoelectric element board 91 used as the board of the carrier body 90 is supplied to the IC chip 23. Thus, like the third embodiment, no exchange of a cell is required, energy saving is realized, and the radio IC card with simple structure is obtained.

[0284] For example, compared to the cell-built-in type radio IC card, the energy saving ratio of power supply is 100% and no waste cell is produced. Therefore, the life of the apparatus can be increased while the apparatus can be operated with clean energy.

(8) An eighth embodiment of the present invention will now be described with reference to the accompanying drawings.

[0285] FIG. 38 shows the structure of a data read/write apparatus.

[0286] The data read/write apparatus comprises, for example, the radio IC card 100 according to the seventh embodiment, as a radio IC card, and a reader/writer 101 for reading/writing data from/in the radio IC card 100.

[0287] Since the radio IC card 100 has the same structure as the radio IC card according to the seventh embodiment, a description thereof is omitted.

[0288] On the other hand, in the state in which the radio IC card 100 is set in position, the reader/writer 101 reads/writes data from/in the radio IC card 100.

[0289] The reader/writer 101 comprises a read/write antenna 102, which is so situated as to correspond in position to the communication antenna 41 of the radio IC card 100, and a data processing unit 103, connected to the read/write antenna 102, for controlling data read/write, processing data and storing data.

[0290] The reader/writer 101 has a carrier passage 105 communicating with a carrier insertion opening 104. A pair of rollers 106a and 106b are provided along the carrier passage 105.

[0291] When the radio IC card 100 is set in the reader/writer 101, the rollers 106a and 106b serve as a pressing mechanism for pressing the electrodes 92a and 92b provided on the piezoelectric element board 91 of radio IC card 100.

[0292] In addition to the rollers 106a and 106b, a plurality of rollers are provided along the carrier passage 105 in order to guide the radio IC card 100 through the carrier passage 105.

[0293] A power supply operation in the data read/write apparatus with the above structure, by which power is supplied to the radio IC card 100, will now be described.

[0294] If the radio IC card 100 is inserted into the carrier insertion opening 104 in the reader/writer 101, the radio IC card 100 is automatically guided into the carrier passage 105 and set in a data read/write position.

[0295] At this time, the rollers 106a and 106b press the electrodes 92a and 92b provided on the piezoelectric element board 91 of radio IC card 100, as shown in FIG. 39.

[0296] If pressure is applied to the piezoelectric element board 91, it is polarized to have positive and negative charges (+,-). An electromotive force is produced at the electrodes 92a and 92b of the piezoelectric element board 91, and it is supplied to the IC chip 23.

[0297] Thereby, data is transmitted between the radio IC card 100 and reader/writer 101 by means of their communication antennas 41 and 102.

[0298] In the eighth embodiment of the invention, the piezoelectric element board 91 of radio IC card 100 is pressed by the paired rollers 106a and 106b of reader/writer 101 to produce an electromotive force, and the electromotive force is supplied to the IC chip 23. Accordingly, like the fourth embodiment, electric energy can be supplied to the radio IC card 100 when data read/write is effected by the reader/writer 101, without using electric energy due to a cell or an electromagnetic induction coil.

[0299] Therefore, no exchange of a cell is required, and power consumption in the standby state of the reader/writer 101 can be reduced to achieve energy saving. Thus, the radio IC card 100 with simple structure can be manufactured.

(9) A ninth embodiment of the invention will now be described with reference to the accompanying drawings.

[0300] FIGS. 40A and 40B show the structure of a radio IC card. FIG. 40A is a plan view and FIG. 40B is a cross-sectional view.

[0301] An IC chip 23, a communication antenna 41 and a power supply coil 42 are mounted on a carrier body 110.

The communication antenna 41 and power supply coil 42 are formed in a rectangular spiral shape, respectively.

[0302] The communication antenna 41 is electrically connected to an antenna coil 31 situated opposed to an antenna coil 22 of the IC chip 23.

[0303] The power supply coil 42 is electrically connected to the communication antenna 41.

[0304] The power supply coil 110 is formed of, e.g. polystyrene (PS), polyethylene terephthalate (PET) or vinyl chloride.

[0305] The communication antenna 41 and power supply coil 42 are formed, for example, by winding fine conductors twice or more, or by winding electric lines twice or more by means of deposition, etc. For example, coated copper-wire coils, copper-wire coils or aluminum-wire coils are used for the communication antenna 41 and power supply coil 42.

[0306] A cavity 43 is defined inside the power supply coil 42. A permanent magnet 44 is movably provided within the cavity 43.

[0307] The permanent magnet 44 has a plate shape.

One surface side of the permanent magnet 44 is magnetized with an N-pole, and the other surface side is magnetized with an S-pole. As is shown in FIG. 40B, the permanent magnet 44 is disposed to be movable in the direction of the central axis (S1) of the power supply coil 42. The permanent magnet 44 is formed of, e.g. an Alnico molded magnet, a Ba ferrite magnet, a rare-earth cobalt magnet, carbon steel, tungsten steel, KS steel, or Cunife.

[0308] A method of manufacturing the radio IC card will now be described with reference to FIGS. 41A to 41D illustrating the respective manufacturing steps.

[0309] The IC chip 23 is formed, as in the first embodiment.

[0310] In brief, the insulating protection film 21 shown in FIG. 7B is formed on the surface of the semiconductor wafer 20 shown in FIG. 7A.

[0311] As is shown in FIG. 7C, the antenna coil 22 of, e.g. gold-plated wire, is formed on the insulating protection film 21.

[0312] Thereafter, the semiconductor wafer 20 is diced into IC chips 23, as shown in FIG. 7D.

[0313] On the other hand, as shown in FIG. 41B, the communication antenna coil 41 and antenna coil 31 are formed on a surface of a module board 111.

[0314] The shape of the antenna coil 31 is substantially the same as that of the antenna coil 22 formed on the IC chip 23.

[0315] Since the communication antenna coil 41 is used for communication with the outside, the number of turns of the coil 41 is made greater than that of the antenna coil 31 and the coil 41 is made larger than the coil 31. The communication antenna coil 41 and antenna coil 31 are electrically connected to each other.

[0316] The communication antenna coil 41 and antenna coil 31 are simultaneously formed on the surface of the module board 111, for example, by a subtractive method, as in the formation of a regular printed circuit board. These antenna coils 41 and 31 may be formed by an additive method.

[0317] These antenna coils 41 and 31 may be formed by fixing coils of coated wire on the module board 111. Alternatively, the antenna coils may be formed of a combination of printed wire and wire coils.

[0318] Specifically, the communication antenna coil 41 and antenna coil 31 are both formed by etching Ag, Al, etc. Alternatively, the antenna coils 41 and 31 may both be formed by a printing method using Ag paste, or formed of coils of Cu. Furthermore, the antenna coil 31 may be formed by printing or etching.

[0319] In a subsequent step, an insulating film 21 is formed on the antenna coil 31, as shown in FIG. 41C. The insulating film 21 is formed of a semi-hardened epoxy resin with a thickness of, e.g. 20 μm. For example, the insulating film 21 is formed by attaching an insulating adhesive film of a semi-hardened epoxy resin. The insulating film 21 may be formed of some other insulative resin such as polyimide or a metal oxide.

[0320] Thereafter, the IC chip 23 is opposed to, and disposed on, the antenna coil 31.

[0321] In this case, the IC chip 23 is mounted in a face-down fashion. The mounting is performed under a suitable pressure such that the antenna coil 31 is opposed to the antenna coil 22 of the IC chi 23 with the insulating film 21 interposed.

[0322] In addition, the mounting is performed such that the gap between the antenna coil 22 and antenna coil 31 is mechanically controlled and the gap is set at about 20 μm or less. In the mounting step, in order to completely harden the insulating adhesive film of, e.g. semi-hardened epoxy resin, which forms the insulating film 21, it is heated at about 200°C to 120°C for 10 to 120 seconds and fixed on the module board 111.

[0323] For example, the material of the insulating adhesive film may be applied in a viscous liquid phase. In this case, where the maintenance of the insulating film 21 is difficult under pressure, the height of the film may be controlled. For example, the insulating film 21 may be maintained by using a spacer of a polyester film with a thickness of, e.g. 10 μm, which serves also as the insulating film 21.

[0324] An insulating film 112 is then formed on the module board 111.

[0325] The power supply coil 42 is formed on the insulating film 112. The power supply coil 42 is formed, for example, by a subtractive method, as in the formation of a regular printed circuit board.

[0326] The power supply coil 42 may be formed by an additive method. The power supply coil 42 may be formed by fixing coils of coated wire on the module board 111. Alternatively, the coil 42 may be formed of a combination of printed wire and a wire coil.

[0327] A cavity portion 43 containing a permanent magnet 44 is provided. The permanent magnet 44 is movably provided within the cavity portion 43. The cavity portion 43 is mounted on the insulating film 112.

[0328] As is shown in FIG. 41D, the entire module board 111 with the IC chip 23 and cavity portion 43 is sealed with resin 113. Magnetic particles are dispersed in the resin 113.

[0329] The entire body of the module board 111 is coated with a polyester film 33. Finally, the radio IC card is obtained after printing and punching.

[0330] FIG. 42 is a cross-sectional view of the IC chip of the manufactured radio IC card. The method of forming the radio IC card is, for example, injection molding using, e.g. a polyester resin, or pressing molding using, e.g. a vinyl chloride sheet.

[0331] A method of manufacturing the radio IC card will now be described with reference to an exploded perspective view of FIG. 43 and a flow chart of FIG. 44.

[0332] As is shown in FIG. 43, the carrier body 110 is a combination of a first casing body (lower card casing body) 110a and a second casing body (upper card casing body) 110b.

[0333] The lower card casing body 110a is provided with recess portions 45 to 47 for receiving the IC chip 23, communication antenna 41 and power supply coil 42.

[0334] The lower card casing body 110a is provided with a recess portion 120 for electrical connection between the communication antenna 41 and power supply coil 42.

[0335] The cavity portion 43 for insertion of the permanent magnet 44 is provided on the upper card casing body 110b.

[0336] Magnetic particles are dispersed in both the lower card casing body 110a and upper card casing body 110b.

[0337] To start with, as shown in FIG. 44, the IC chip 23 and the board 48 for the IC chip 23 are prepared.

[0338] In step #30, the IC chip 23 is mounted on the board 48.

[0339] In step #31, the IC chip 23 mounted on the board 48 is set in the recess portion 45 in the lower card casing body 110a. In this case, the IC chip 23 is adhered to the recess portion 45.

[0340] Next, the communication antenna 41 and power supply coil 42 are supplied. The communication antenna 41 has leads 41a for connection with the terminals of the substrate 48. The communication antenna 41 also has leads 41b for electrical connection with the power supply coil 42.

[0341] The power supply coil 42 has leads 42a for electrical connection with the communication antenna 41.

[0342] In step #32, the communication antenna 41 and power supply coil 42 are set in the recess portions 46 and 47 in the lower card casing body 110a. The leads 41a of the communication antenna 41 are connected to the terminals of the board 48 by means of, e.g. soldering.

[0343] The leads 41a of the communication antenna 41 and the leads 42a of the power supply coil 42 are electrically connected by means of, e.g. soldering.

[0344] The permanent magnet 44 is then supplied. In step #33, the permanent magnet 44 is inserted in the cavity portion 43 on the upper card casing body 110b.

[0345] Subsequently, the lower card casing body 110a, on which the IC chip 23, communication antenna 41 and power supply coil 42 are mounted, is supplied. In addition, the upper card casing body 110b in which the permanent magnet 44 is inserted is supplied.

[0346] In step #34, the lower card casing body 110a and upper card casing body 110b are combined and adhered to each other. Thus, the carrier body 110 is constituted.

[0347] In step #35, printing is effected on the surface of the carrier body 110, and at last the manufactured radio IC card is inspected.

[0348] The operation of the radio IC card thus manufactured will now be described.

[0349] If the radio IC card is carried by a person, etc., the entire body thereof is moved. Thereby, the permanent magnet 44 in the cavity 43 moves.

[0350] The magnetic flux of the permanent magnet 44 crosses the power supply coil 42, thus inducing an electromotive force in the power supply coil 42. The electromotive force is supplied to the IC chip 23 through the communication antenna 41.

[0351] As has been described above, according to the ninth embodiment of the invention, electric energy can be supplied to the radio IC card due to the induced electromotive force v, which is produced by, e.g. a manual operation of the permanent magnet 44, without using electric energy due to a cell or an electromagnetic coil.

[0352] In this case, since magnetic particles are dispersed in the seal resin 113 or the lower and upper card casing bodies 110a and 110b, the sensitivity of transmission between the communication antenna 41 and IC chip 23 can be enhanced.

[0353] Furthermore, since the magnetic particles are dispersed, the electromotive force induced in the power supply coil 42 can be increased and also the power to be supplied to the IC chip 23 increased.

[0354] Accordingly, exchange of a cell is not required, and power consumption in the standby state of the reader/writer can be reduced to achieve energy saving. Thus, the radio IC card with simple structure can be manufactured. For example, compared to the cell-built-in type radio IC card, the energy saving ratio of power supply is 100% and no waste cell is produced.

Claims

1. A radio IC card for data communication with outside, characterized by comprising:

   a board (30) having at least two rectangular-spiral antennas (31, 32) formed thereon; and
   a semiconductor element (23) having a rectangular-spiral antenna (22) formed on a surface thereof, the semiconductor element being mounted on the board such that the antenna (22) on the semiconductor element is situated opposed to one (31) of said at least two antennas on the board (30).

2. A radio IC card according to claim 1, characterized in that said antenna (23) on the semiconductor element is formed by bonding a piece of bonding wire (27) among a plurality of electrode pads (26) formed on the surface of the semiconductor element.

3. A radio IC card according to claim 1, characterized in that the antenna (22) on the semiconductor element is formed of a metallic film.

4. A radio IC card according to claim 1, characterized in that a layer of the antenna (22) formed of a metallic film and a layer of an insulating film (21) are laminated on the surface of the semiconductor element.

5. A radio IC card according to claim 1, characterized in that said antenna (22) is provided on each of upper and lower surfaces of the semiconductor element (23).

6. A radio IC card according to claim 1, characterized in that said semiconductor element (23) is provided with a layer for formation of an electric element (29).

7. A radio IC card according to claim 1, characterized in that one (31) of the antennas formed on the board (30) has substantially the same shape as the antenna (22) formed on the semiconductor element, and the other (32) of the antennas on the board is greater in size than said one (31) of the antennas on the board.

8. A radio IC card according to claim 1, characterized in that one (31) of the antennas on the board and the other (32) of the antennas on the board are electrically connected.

9. A radio IC card according to claim 1, characterized in that one (31) of the antennas on the board and the antenna (22) on the semiconductor device are electromagnetically connected.

10. A radio IC card according to claim 1, characterized in that said antenna (22) is formed over the semiconductor element (23), with an insulating film (21) interposed.

11. A radio IC card according to claim 1, characterized in that said antenna (22) is formed over the semiconductor element (23), with a magnetic film interposed.

12. A radio IC card according to claim 1, characterized in that an insulating film (21) is formed on each of the antennas (31, 32) on the board.

13. A radio IC card according to claim 1, characterized in that an insulating film (21), in which magnetic particles are dispersed, is formed on each of the antennas (31, 32) on the board.

14. A radio IC card according to claim 1, characterized in that said semiconductor element (23) and said substrate (30) are integrally sealed with resin (25).

15. A method of manufacturing a radio IC card for data communication with outside, the method characterized by comprising the steps of:

forming a rectangular-spiral antenna (22) on a surface of a semiconductor element (23);
forming at least two rectangular-spiral antennas (31, 32) on a board (30); and
disposing the antenna (22) formed on the semiconductor element such that the antenna formed on the semiconductor element is opposed to one (31) of said antennas formed on the board.

16. A method of manufacturing a radio IC card, according to claim 15, characterized in that the antenna (22) on the surface of the semiconductor element is formed by a thin-film patterning process.

17. A method of manufacturing a radio IC card, according to claim 15, characterized in that the antenna (22) on the surface of the semiconductor element is formed by a printing process.

18. A method of manufacturing a radio IC card, according to claim 15, characterized in that the antenna (22) on the surface of the semiconductor element is formed such that a plurality of electrode pads (26) are provided on the surface of the semiconductor element and the electrode pads are connected by means of wire bonding.

19. A method of manufacturing a radio IC card, according to claim 15, characterized in that said at least two antennas (31, 32) on the board are integrally formed.

20. A method of manufacturing a radio IC card, according to claim 15, characterized in that the method includes a step of integrally sealing the semiconductor element (23) and the board (30) with resin (25).

21. A radio IC card having at least one rectangular-spiral antenna (42) and one semiconductor element (23) mounted thereon, characterized in that a cavity portion (43) is provided near the antenna and a permanent magnet (44) is movably provided within the cavity portion.

22. A radio IC card according to claim 21, characterized in that the permanent magnet (44) is movable in a direction of a central axis of the antenna (42).

23. A radio IC card according to claim 21, characterized in that the permanent magnet (44) is rotatably provided within the cavity portion (43).

24. A radio IC card according to claim 21, characterized in that the antenna (42) serves both for power supply to the semiconductor element (23) and for data communication.

25. A method of manufacturing a radio IC card for data communication with outside, the method characterized by comprising the steps of:

mounting at least one semiconductor element (23) and one rectangular-spiral antenna (41, 42) on a first casing body (40a) in which a recess portion is formed in advance;
inserting a permanent magnet (44) movably in the recess portion; and
attaching a second casing body (40b) to the first casing body provided with said at least one semiconductor element and one antenna and said permanent magnet.

26. A data reader/writer apparatus for reading/writing data from/in a radio IC card, the apparatus characterized by comprising:

a radio IC card on which at least one rectangular-spiral antenna (41, 42) and a semiconductor element (23) are mounted; and
read/write means for performing data communication with the semiconductor element mounted on the radio IC card, the read/write means having a permanent magnet (52) for inducing an electromotive force in the antenna mounted on the radio IC card by crossing a magnetic field over the antenna.

27. A radio IC card having at least one data communication antenna (41) and one semiconductor element (23) mounted thereon, characterized in that the radio IC card comprises a piezoelectric element (81) connected to the semiconductor element.

28. A radio IC card according to claim 27, characterized in that said piezoelectric element (81) is used as a board, and said at least one antenna (41) and one semiconductor element (23) are mounted on the piezoelectric element.

29. A radio IC card according to claim 27, characterized in that electrodes (92a, 92b) are provided on both sides of the piezoelectric element (91), and these electrodes are electrically connected to at least said semiconductor element (23).

30. A method of manufacturing a radio IC card for data communication with outside, the method characterized by comprising the steps of:

attaching at least one data communication antenna (41) and one semiconductor element (23) to a first casing body (80a);
attaching a piezoelectric element (81) to the first casing body (80a); and
adhering a second casing body (80b) to the first casing body (80a).

31. A method of manufacturing a radio IC card, the method characterized by comprising the steps of:

attaching at least one data communication antenna (41) and one semiconductor element (23) on a board (91) formed of a piezoelectric element; and
applying an outer coating to the board (91) on which the antenna and the semiconductor element are attached.

32. A data read/write apparatus characterized by comprising:

a radio IC card having at least one data communication antenna (41) and one semiconductor element (23) mounted thereon and including a piezoelectric element (81) connected to the semiconductor element (23); and
read/write means for performing data communication with the semiconductor element (23) by means of the antenna (41), the read/write means including a pressing mechanism (106a, 106b) for pressing the piezoelectric element (81) of the radio IC card, thereby producing an electric charge in the piezoelectric element.

33. A radio IC card for data communication with outside, characterized by comprising:

a semiconductor element (23) having a rectangular-spiral antenna (22) formed on a surface thereof;
a board (111) having at least three rectangular-spiral antennas (31, 41, 42) formed thereon such that one (31) of said at least three antennas is situated, opposed to the antenna (22) of the semiconductor element;
a cavity portion (43) provided near one (42) of the other antennas on the board; and
a permanent magnet (44) provided movably in the cavity portion.

34. A radio IC card according to claim 33, characterized in that on said board (111) there are provided:

an antenna (31) situated to be opposed to the antenna (22) on the semiconductor element (23);
a communication antenna (41) electrically connected to said antenna; and
a power supply antenna (42) electrically connected to the communication antenna (41), a magnetic flux of the permanent magnet (44) being crossed over the power supply antenna.

35. An IC card according to claim 33, characterized in that said antennas are sealed with an insulating material (113) in which magnetic particles are dispersed.

36. A method of manufacturing a radio IC card, the method characterized by comprising the steps of:

mounting at least one semiconductor element (23) and at least three rectangular-spiral antennas (31, 41, 42) on a first casing body (100a) in which a recess portion is formed in advance;
inserting a permanent magnet (44) movably in the recess portion; and
attaching a second casing body (110b) to the first casing body (110a).

37. A method of manufacturing a radio IC card according to claim 36, characterized in that the method includes the steps of:

storing the permanent magnet (44) movably in a case; and
mounting the case in the recess portion.

38. A method of manufacturing a radio IC card according to claim 36, characterized in that the first and second casing

bodies (110a, 110b) are formed of an insulating material in which magnetic particles are dispersed.

39. A radio tag for data communication with inside, characterized in that a rectangular-spiral antenna (22) is formed on a surface of a semiconductor element (23).

40. A radio tag according to claim 39, characterized in that said antenna (22) on the semiconductor element is formed by bonding a piece of bonding wire (27) among a plurality of electrode pads (26) formed on the surface of the semiconductor element.

41. A radio tag according to claim 39, characterized in that the antenna (22) on the semiconductor element is formed of a metallic film.

42. A radio tag according to claim 39, characterized in that a layer of the antenna (22) formed of a metallic film (21) and a layer of an insulating film (21) are laminated on the surface of the semiconductor element (23).

43. A radio tag according to claim 39, characterized in that said antenna (22) is provided on each of upper and lower surfaces of the semiconductor element (23).

44. A radio tag according to claim 39, characterized in that said semiconductor element (23) is provided with a layer for formation of an electric element (24).

45. A radio tag according to claim 39, characterized in that the antenna (22) is provided over the semiconductor element (23), with an insulating film (21) interposed.

46. A radio tag according to claim 39, characterized in that said antenna (22) is formed over the semiconductor element (23), with a magnetic film interposed.

47. A radio tag according to claim 39, characterized in that the antenna (22) is formed on the semiconductor element (23), with an insulating film (21) containing dispersed magnetic particles interposed.

48. A radio tag according to claim 39, characterized in that the semiconductor element (23) having the antenna (22) formed on the surface thereof is sealed with resin (25).

49. A method of manufacturing a radio tag for data communication with outside, the method characterized by comprising the steps of:

forming an insulating film (21) over a surface of a semiconductor wafer (20) on which a plurality of semiconductor elements (23) are formed;
forming rectangular-spiral antennas (22) on the insulating film at positions corresponding to the semiconductor elements; and
dicing the semiconductor elements (23) out of the semiconductor wafer (20).

50. A method of manufacturing a radio tag according to claim 49, characterized in that the antenna (22) formed on the surface of each of the semiconductor elements is formed by a thin-film patterning process.

51. A method of manufacturing a radio tag according to claim 49, characterized in that the antenna (22) formed on the surface of each of the semiconductor elements is formed by a printing process.

52. A method of manufacturing a radio tag according to claim 49, characterized in that said antenna (22) on each of the semiconductor elements is formed by bonding a piece of bonding wire among a plurality of electrode pads (26) formed on the surface of the semiconductor element.

53. A method of manufacturing a radio tag according to claim 49, characterized in that each of the semiconductor elements (23) on the surface of which the antenna is formed is sealed with resin (25).

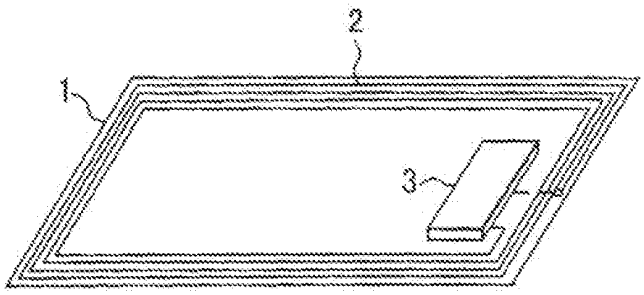


FIG. 1

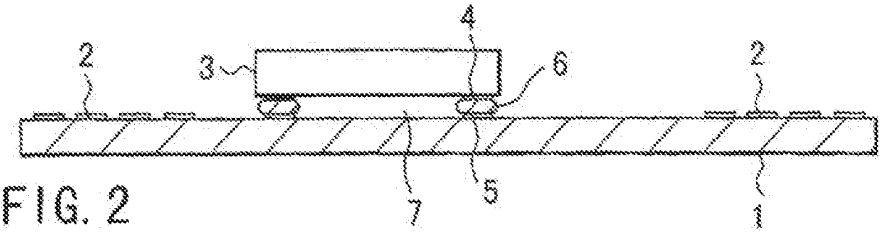


FIG. 2

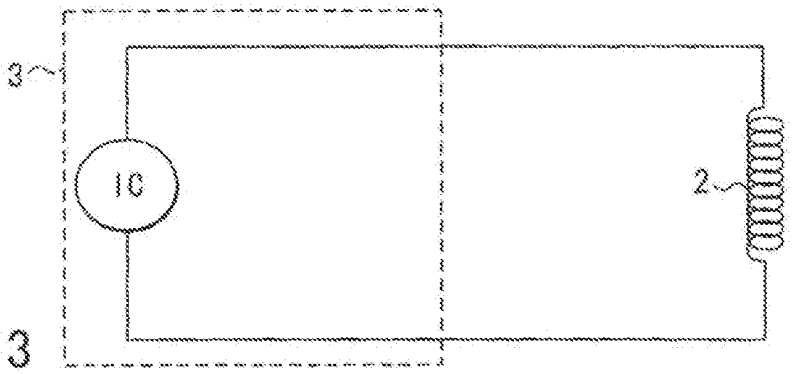


FIG. 3

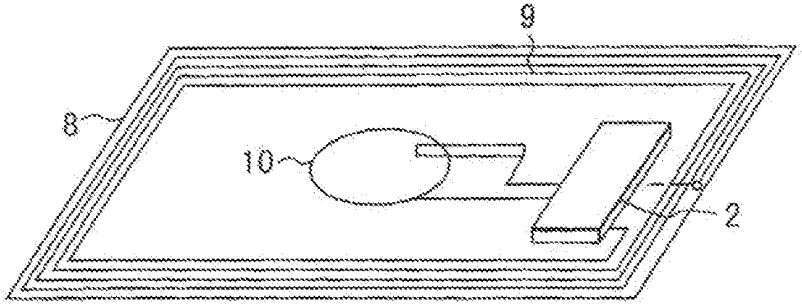


FIG. 4

FIG. 5

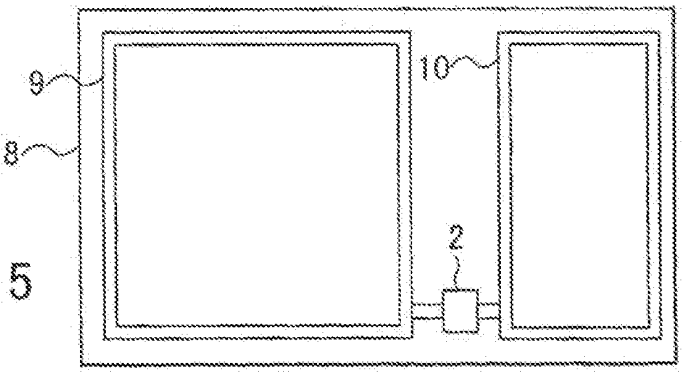


FIG. 6

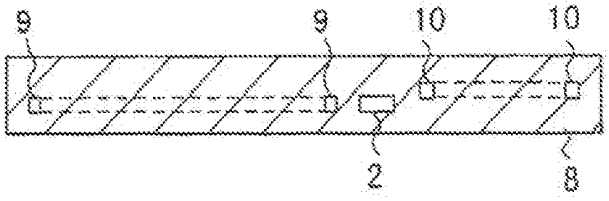


FIG. 7A

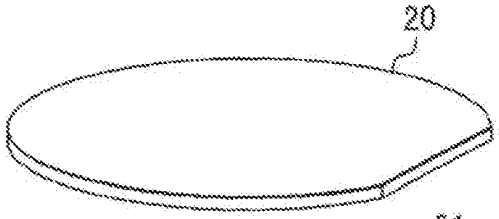


FIG. 7B

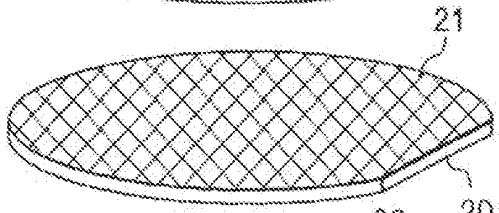


FIG. 7C

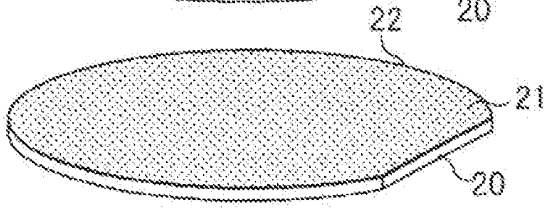
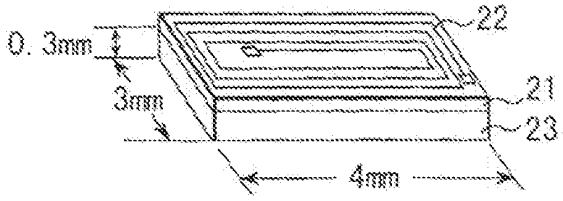


FIG. 7D



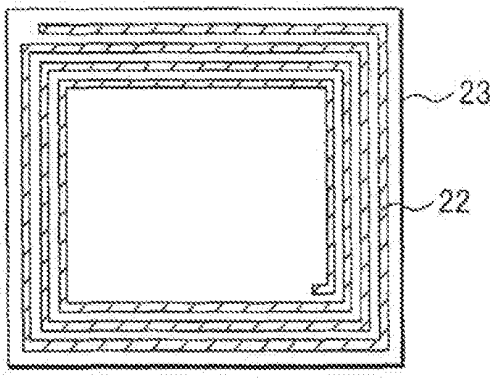


FIG. 8A

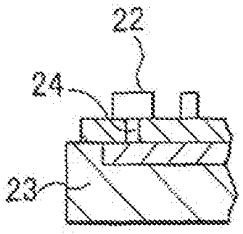


FIG. 8C



FIG. 8B

FIG. 8D

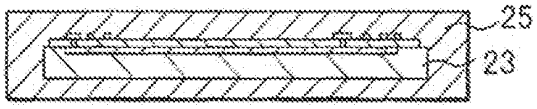


FIG. 9A

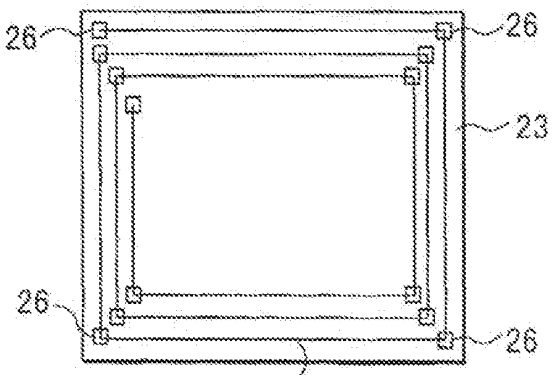


FIG. 9B



FIG. 10

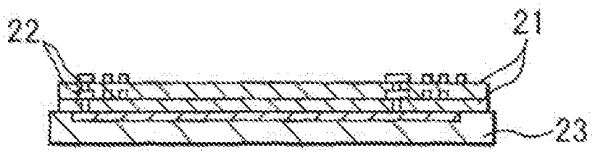


FIG. 11

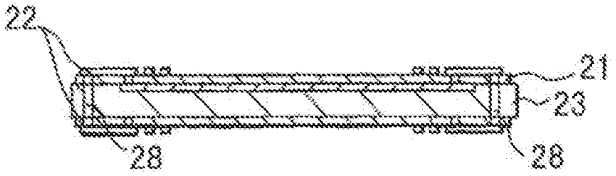


FIG. 12

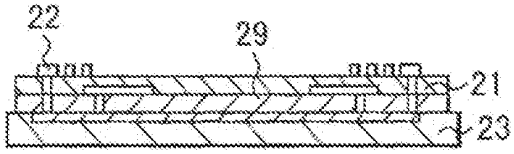


FIG. 13A

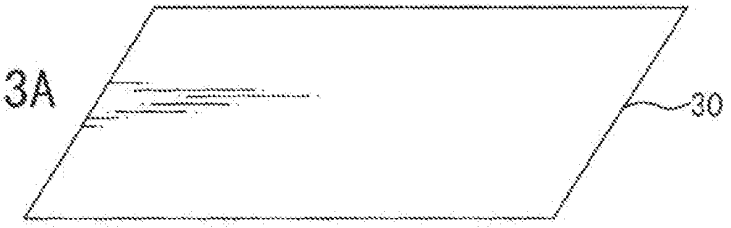


FIG. 13B

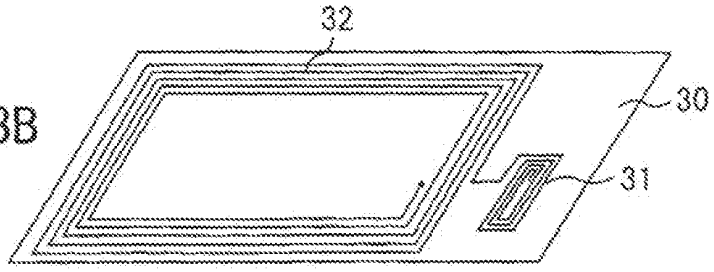
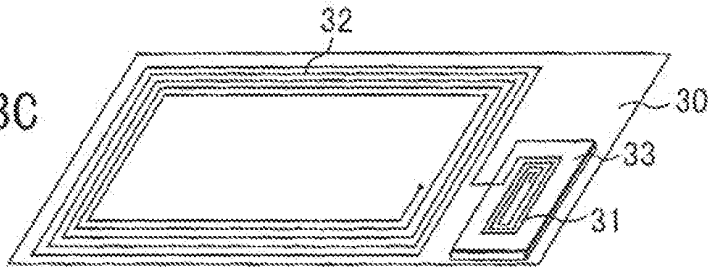


FIG. 13C



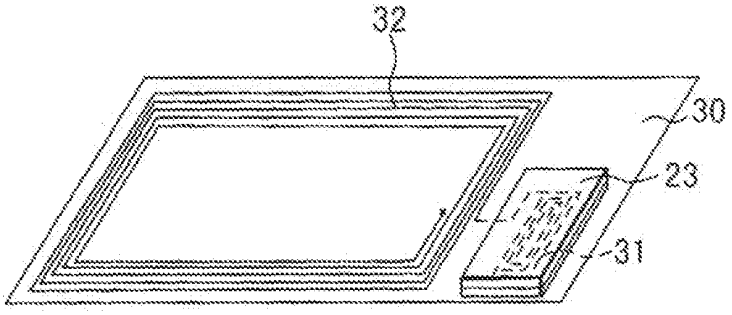


FIG. 13D

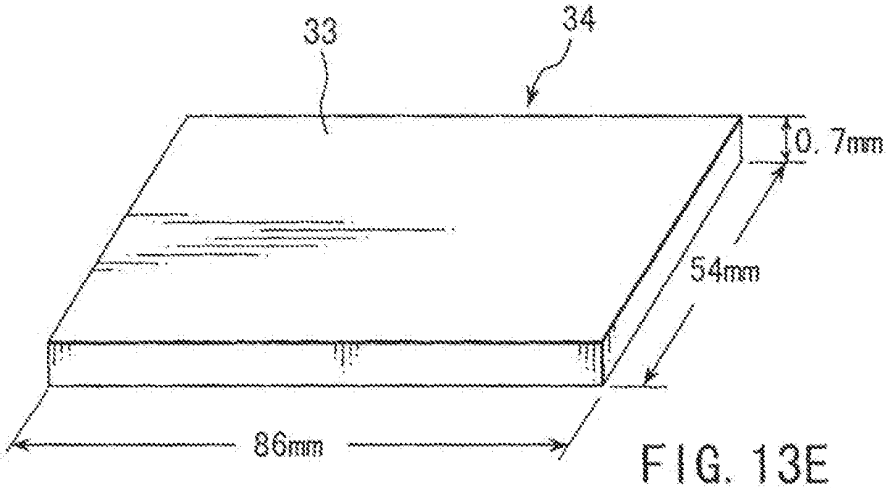


FIG. 13E

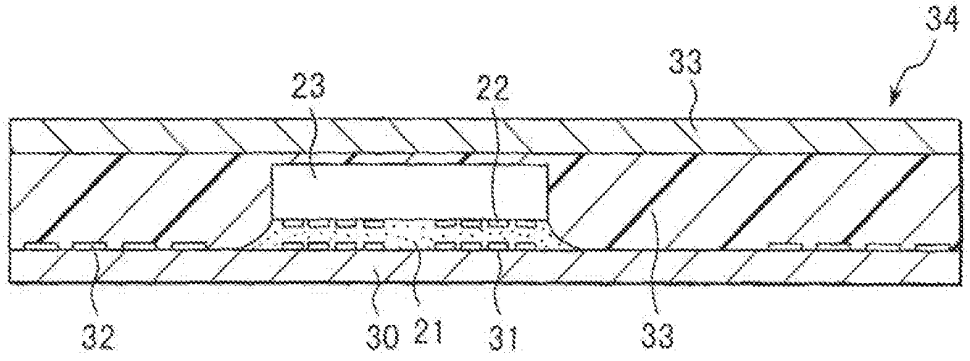


FIG. 14

FIG. 15

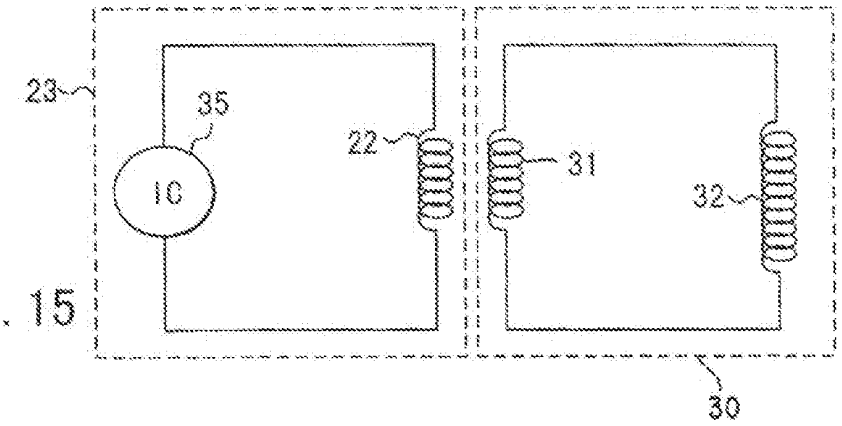


FIG. 16

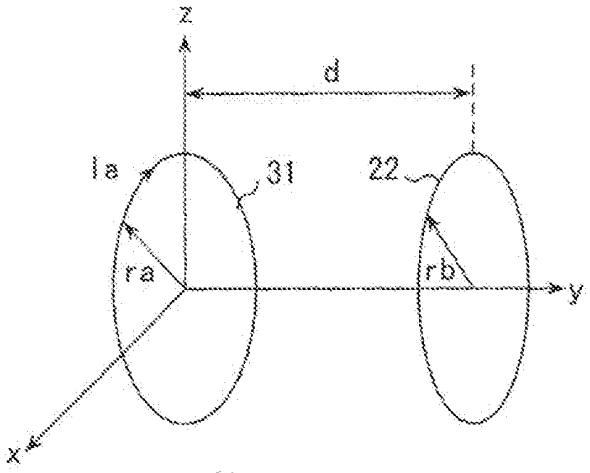


FIG. 17A

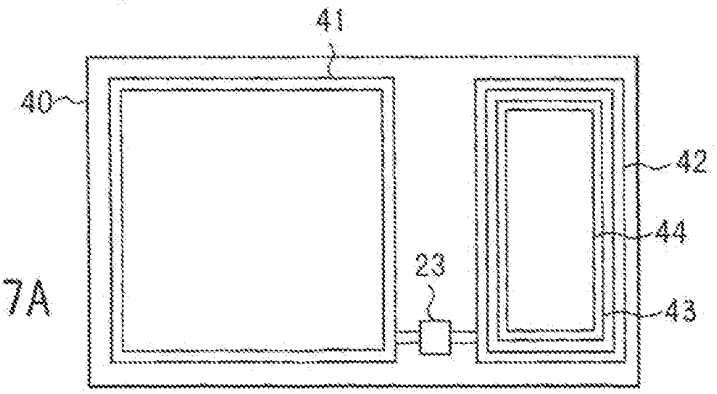
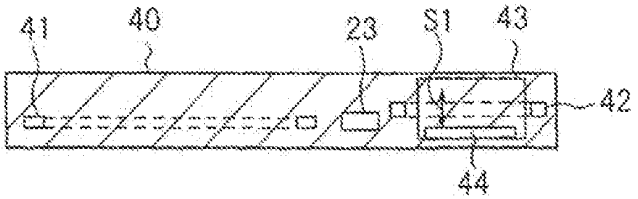


FIG. 17B



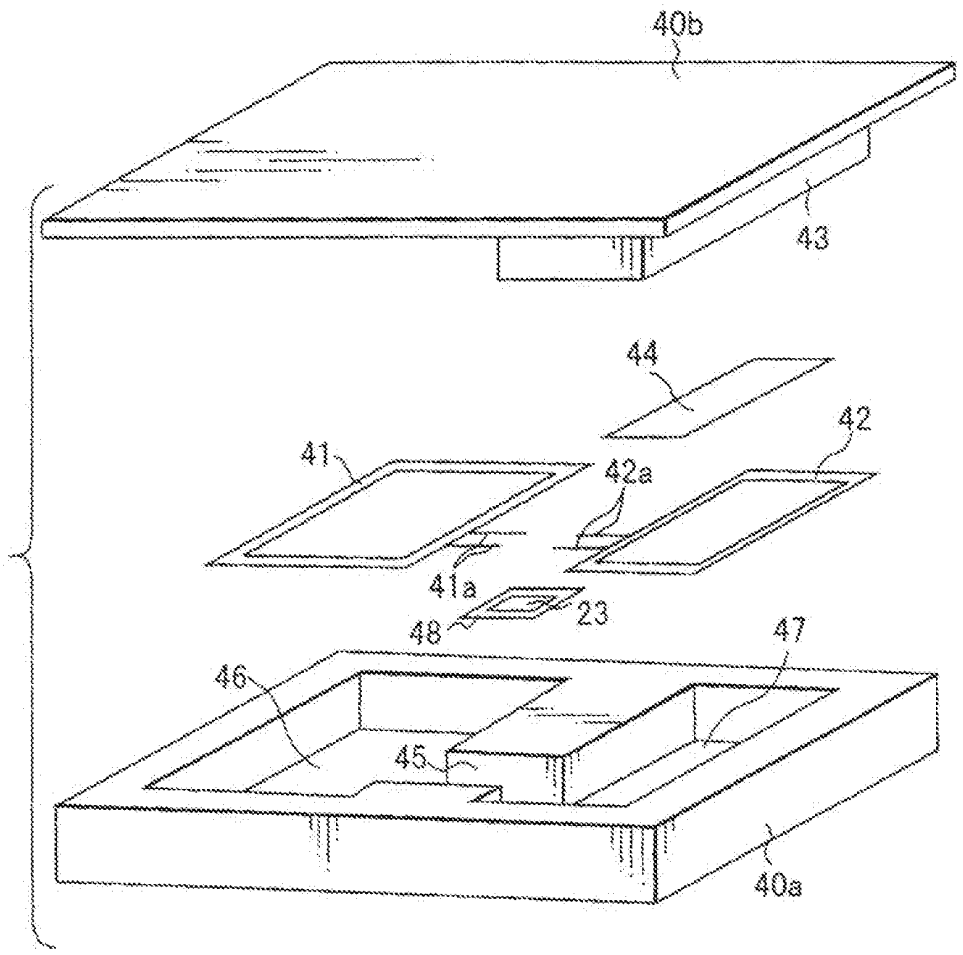


FIG. 18

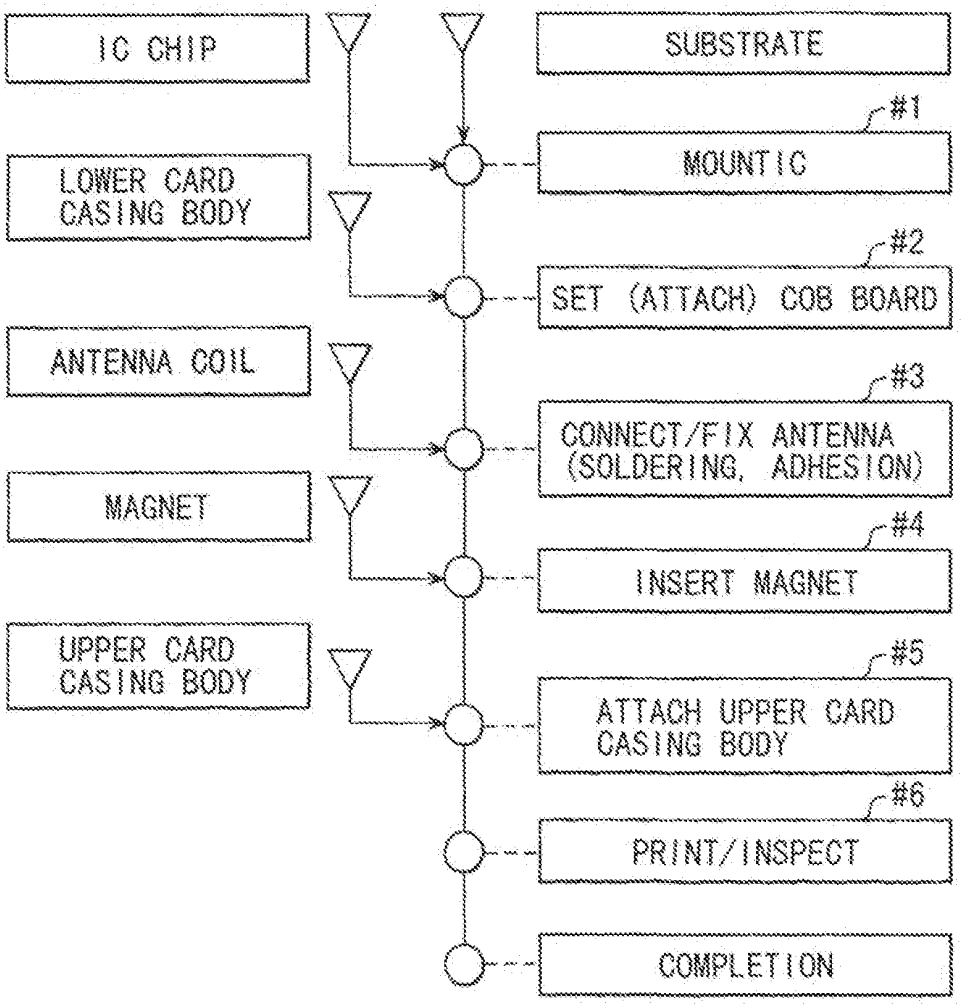

IC CHIP
LOWER CARD CASING BODY
ANTENNA COIL
MAGNET
UPPER CARD CASING BODY
SUBSTRATE
#1
MOUNT IC
#2
SET (ATTACH) COB BOARD
#3
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#4
INSERT MAGNET
#5
ATTACH UPPER CARD CASING BODY
#6
PRINT/INSPECT
COMPLETION

FIG. 19

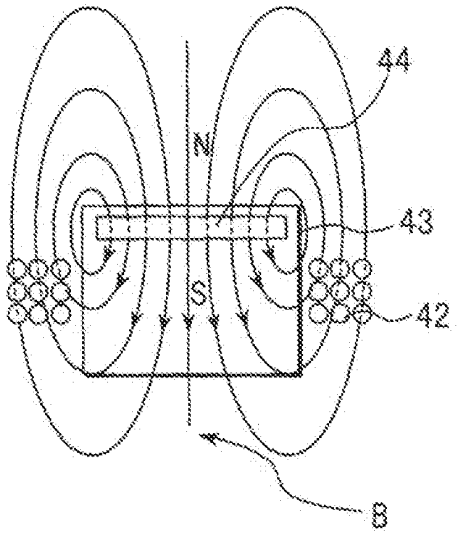


FIG. 20A

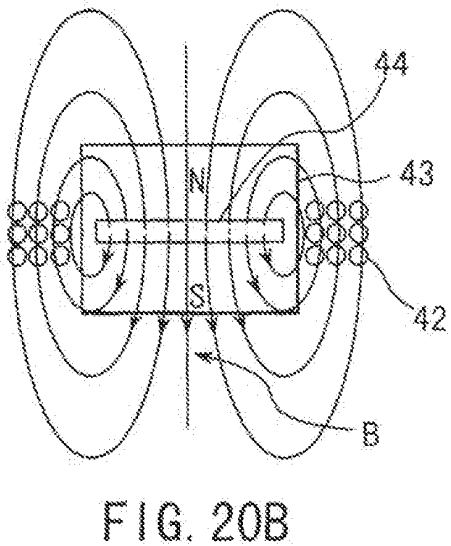


FIG. 20B

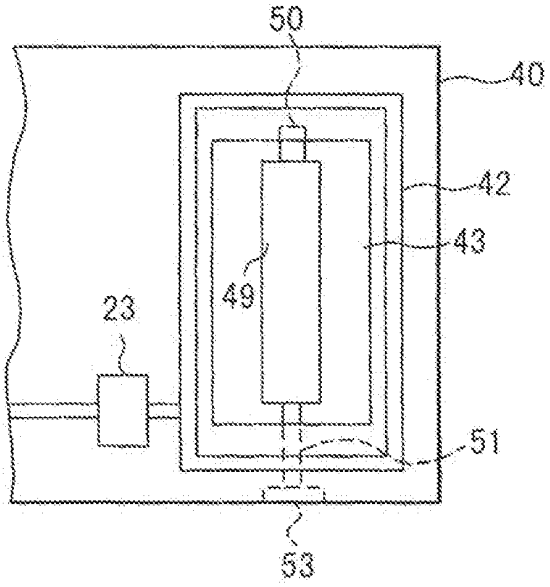


FIG. 21A

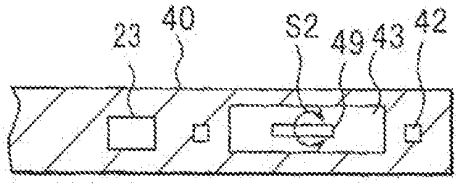


FIG. 21B

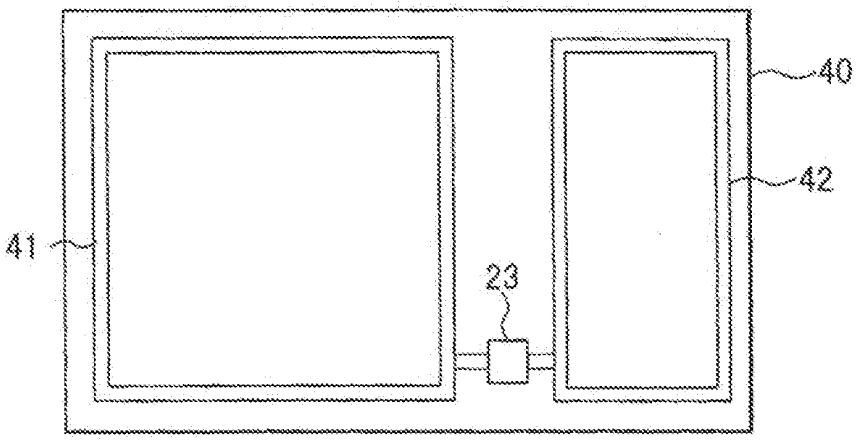


FIG. 22A

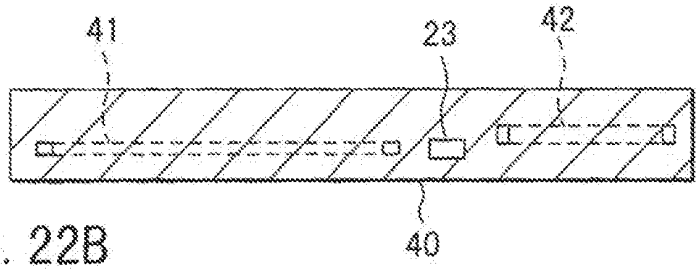


FIG. 22B

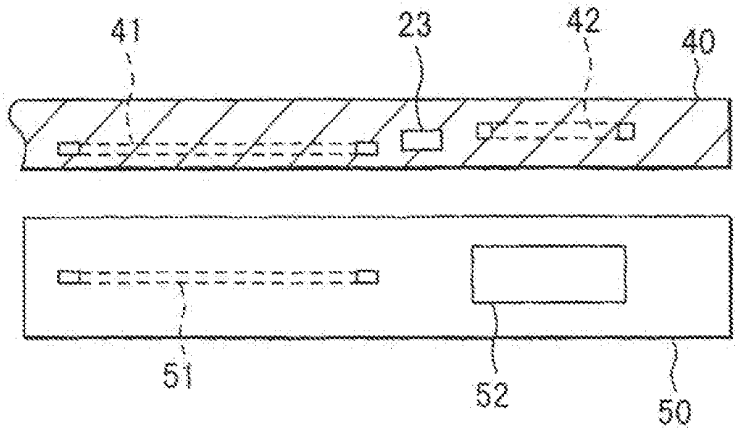


FIG. 23

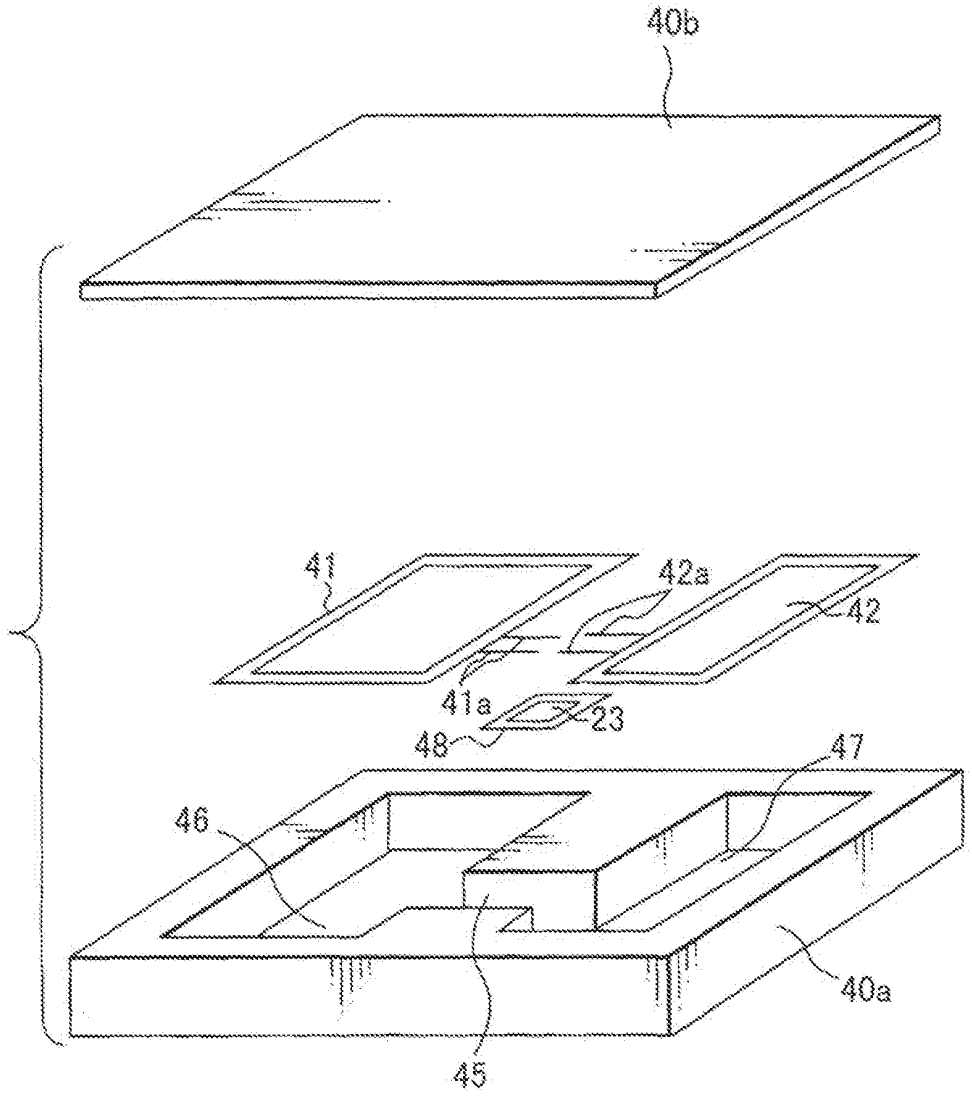


FIG. 24

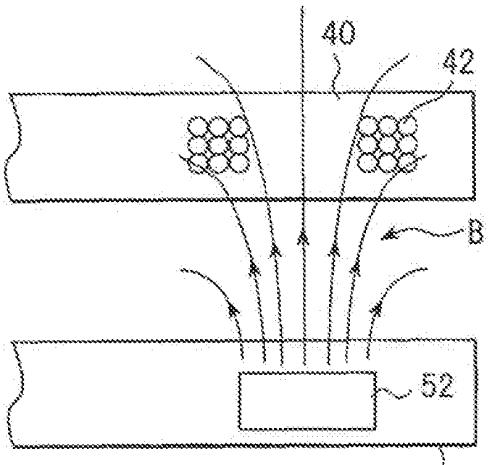


FIG. 25

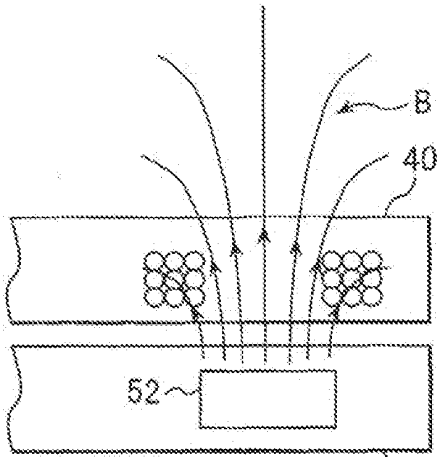


FIG. 26

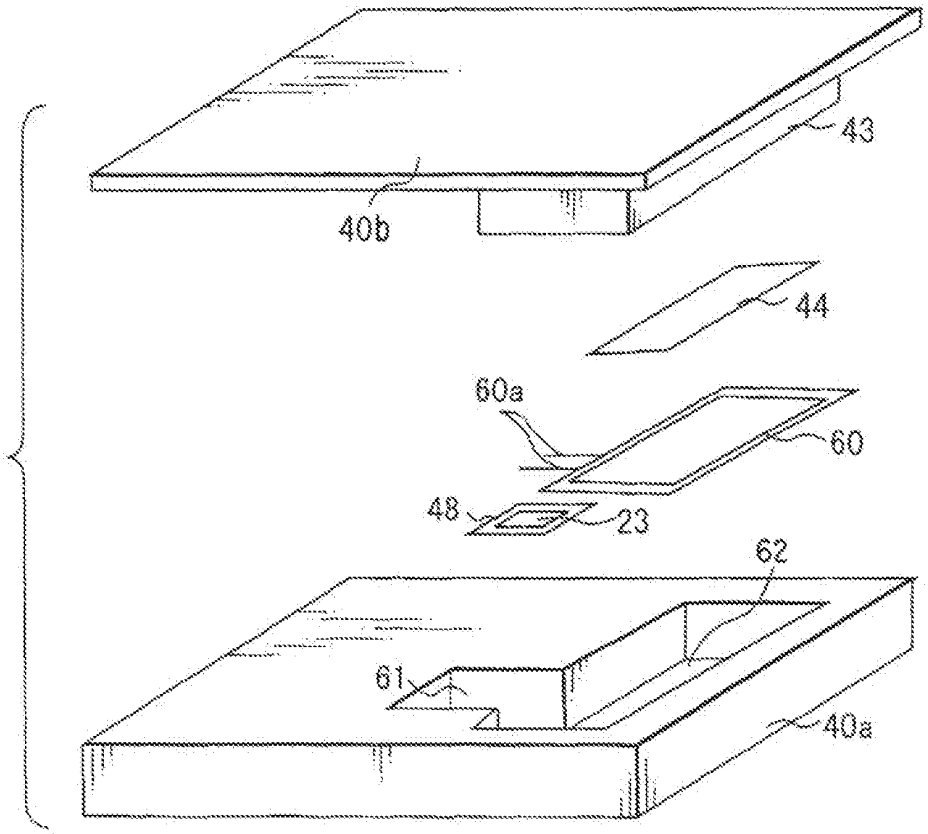


FIG. 27

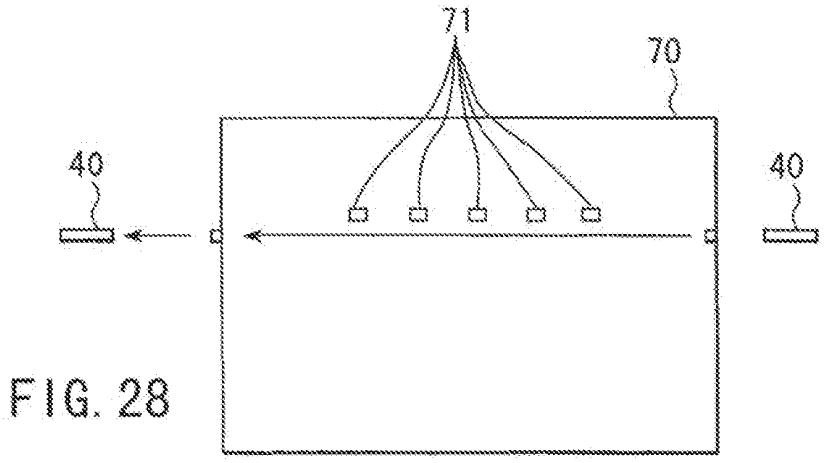


FIG. 28

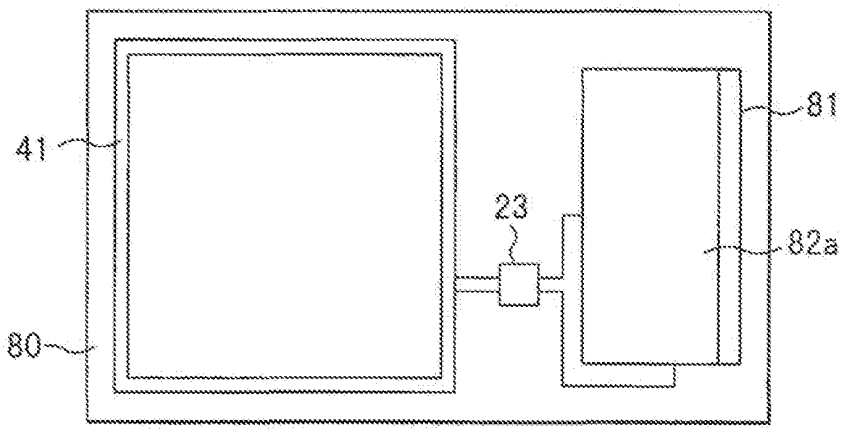


FIG. 29A

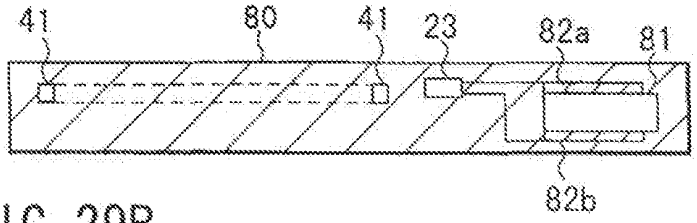


FIG. 29B

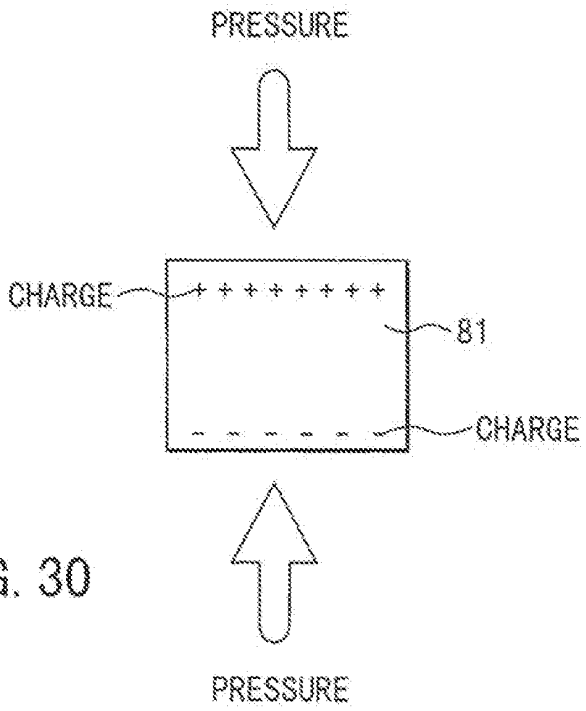


FIG. 30

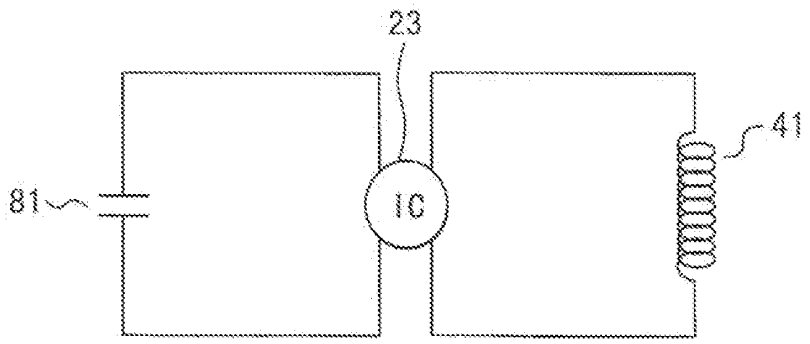


FIG. 31

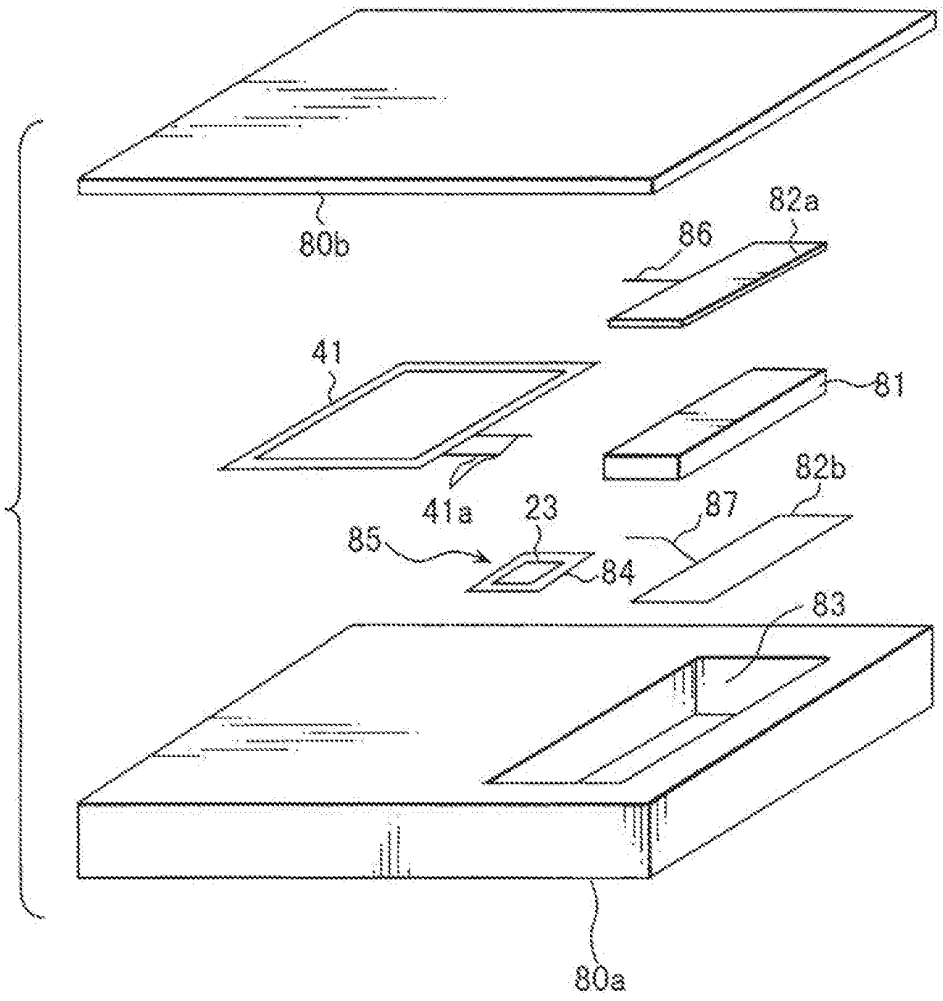


FIG. 32

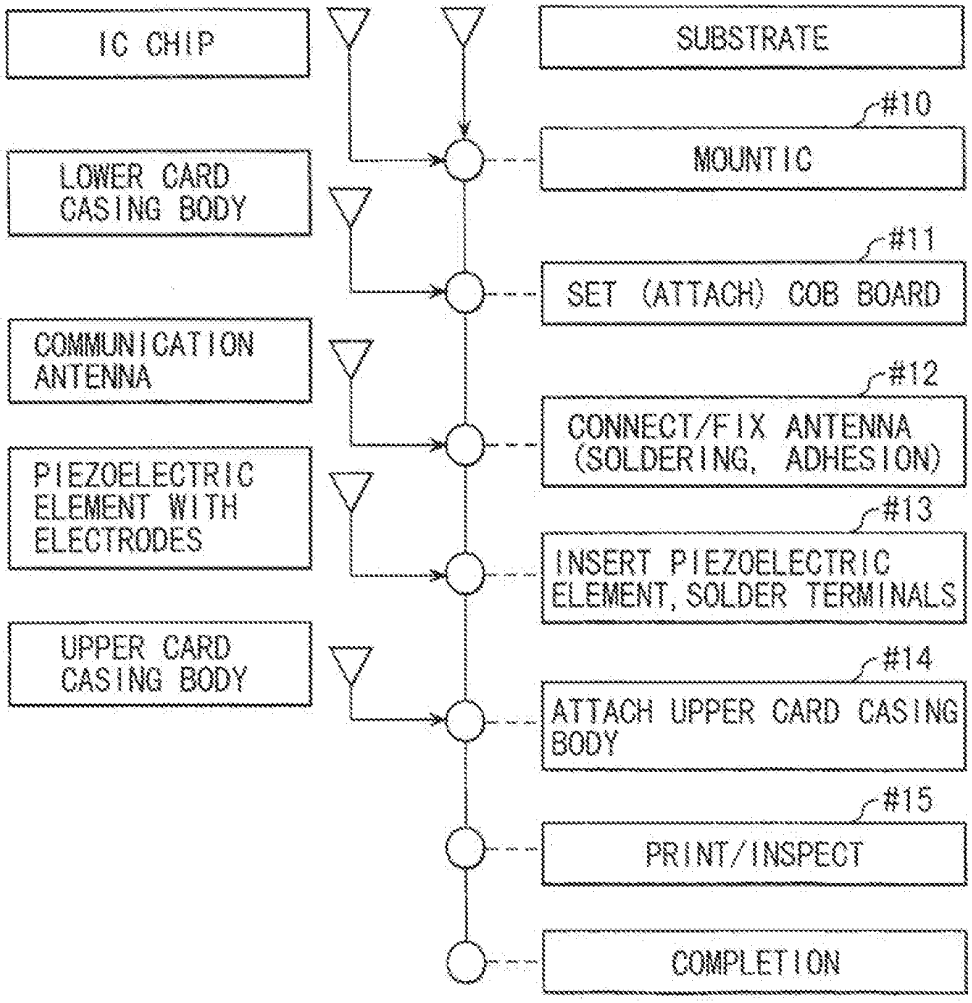

IC CHIP
LOWER CARD CASING BODY
COMMUNICATION ANTENNA
PIEZOELECTRIC ELEMENT WITH ELECTRODES
UPPER CARD CASING BODY
SUBSTRATE
#10
MOUNTIC
#11
SET (ATTACH) COB BOARD
#12
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#13
INSERT PIEZOELECTRIC ELEMENT, SOLDER TERMINALS
#14
ATTACH UPPER CARD CASING BODY
#15
PRINT/INSPECT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

FIG. 33

FIG. 34A

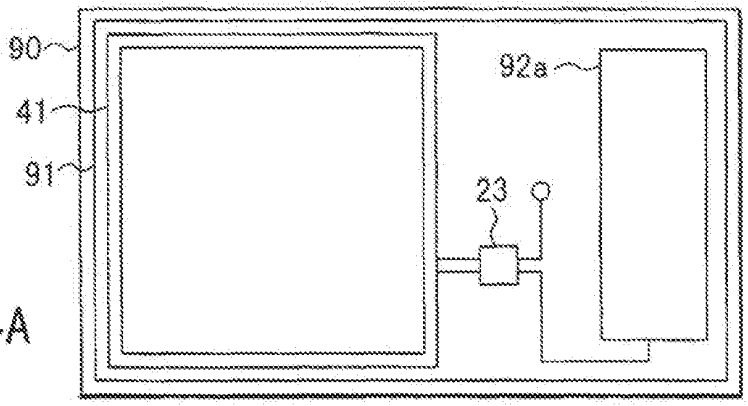


FIG. 34B

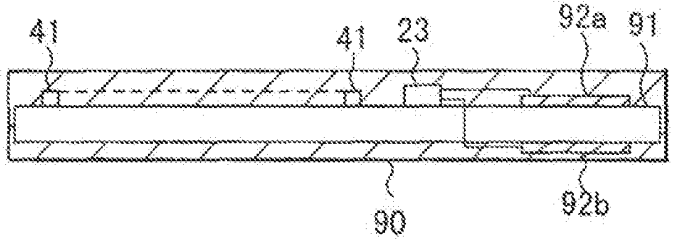
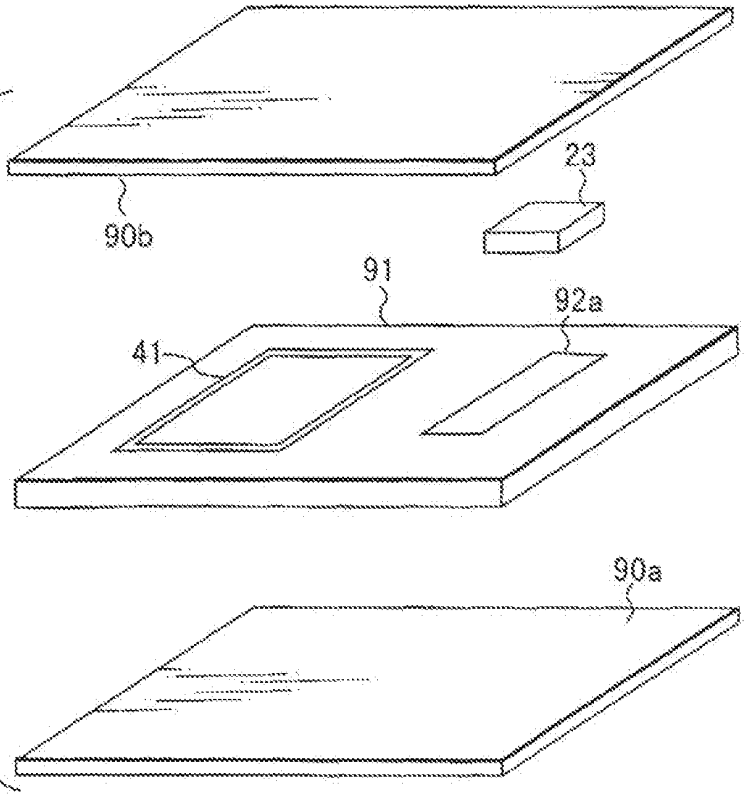


FIG. 35



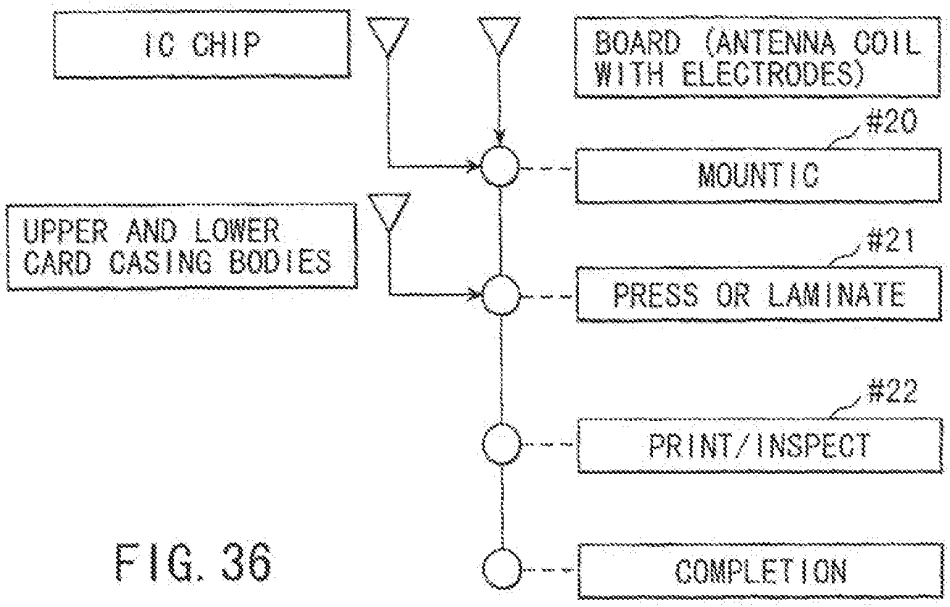


FIG. 36

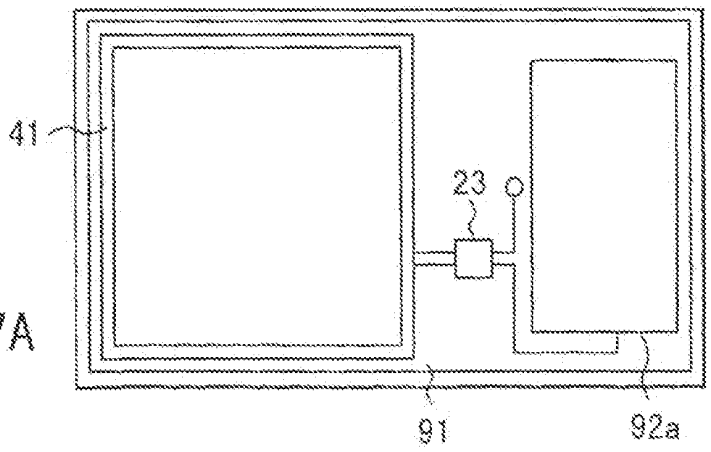


FIG. 37A

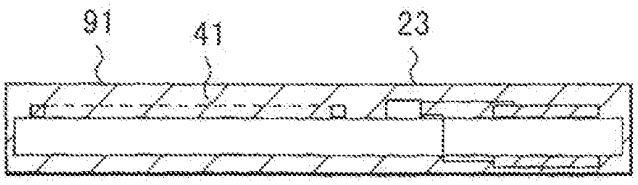


FIG. 37B

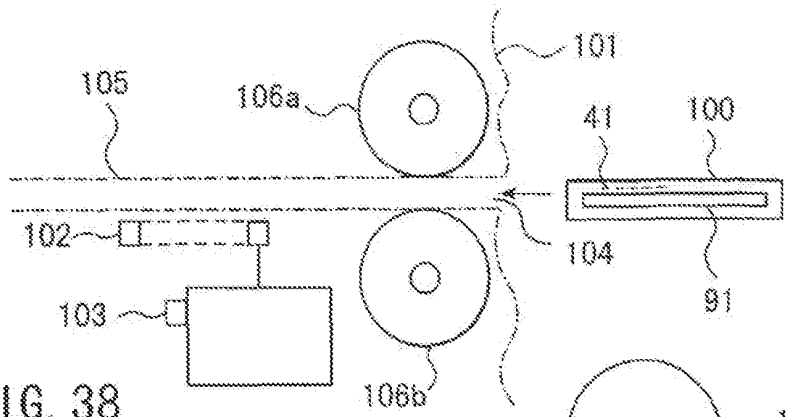


FIG. 38

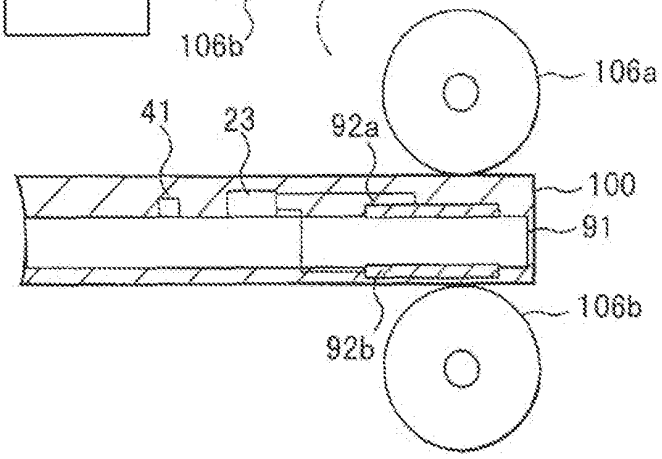


FIG. 39

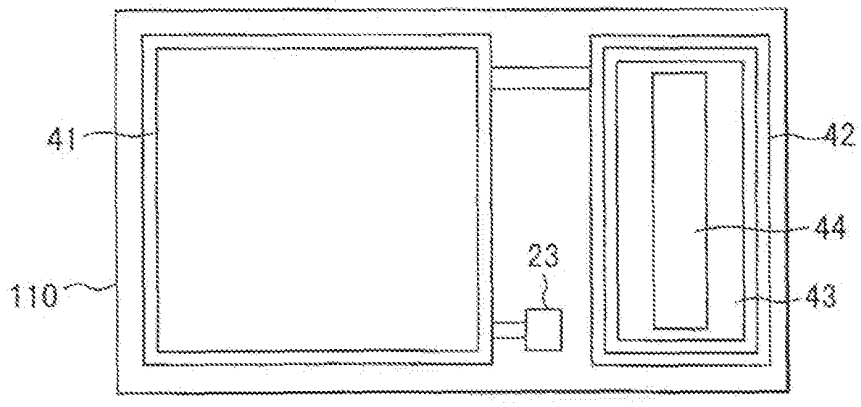


FIG. 40A

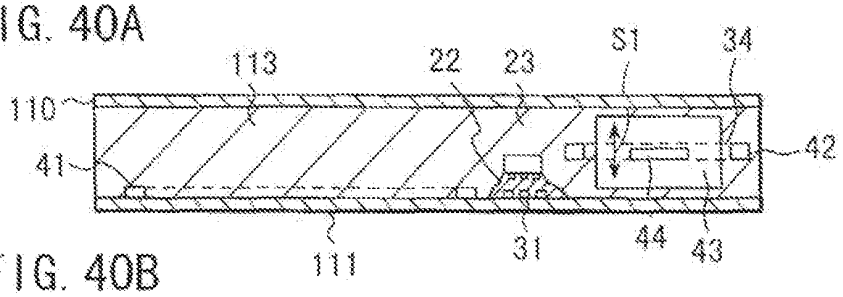


FIG. 40B

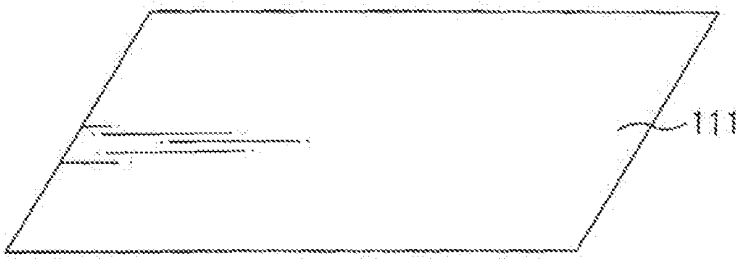


FIG. 41A

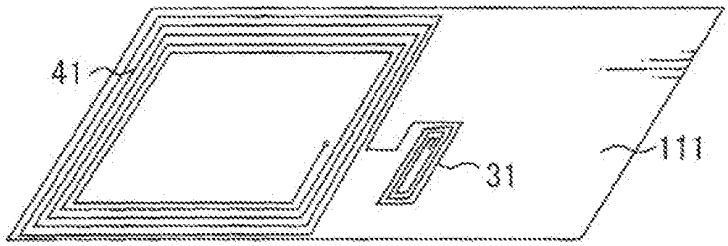


FIG. 41B

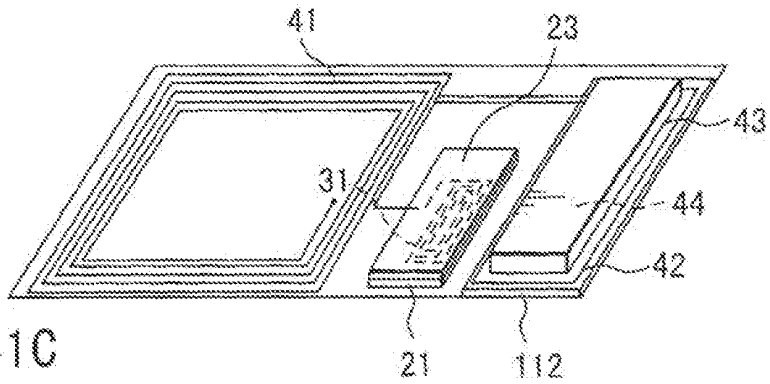


FIG. 41C

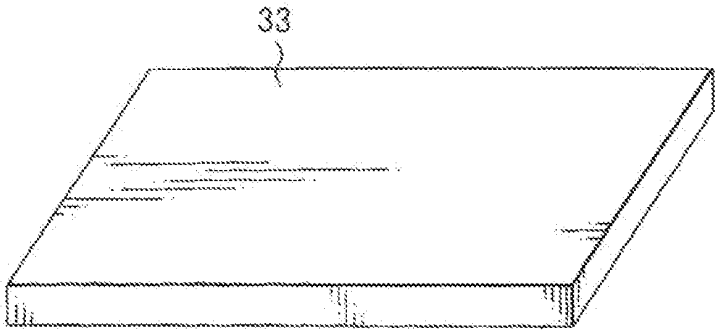
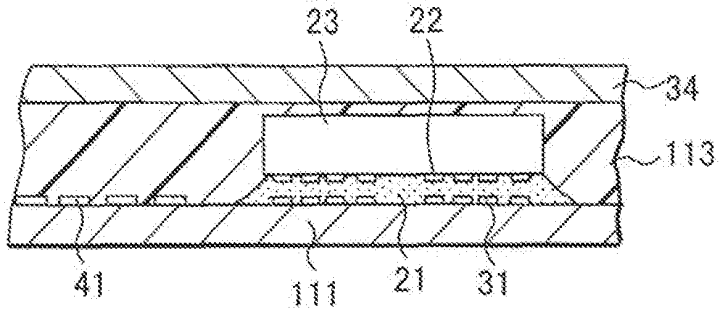


FIG. 41D

FIG. 42


23
22
34
113
41
111
21
31

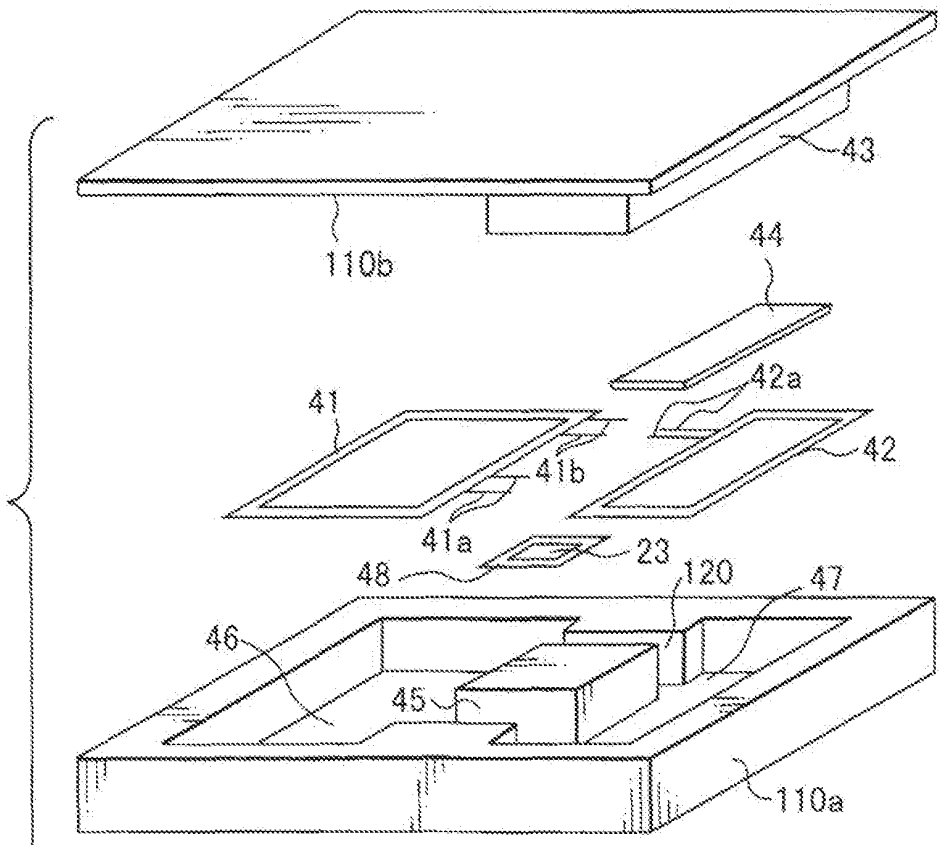

43
110b
44
42a
41
42
41b
41a
23
48
120
47
46
45
110a

FIG. 43

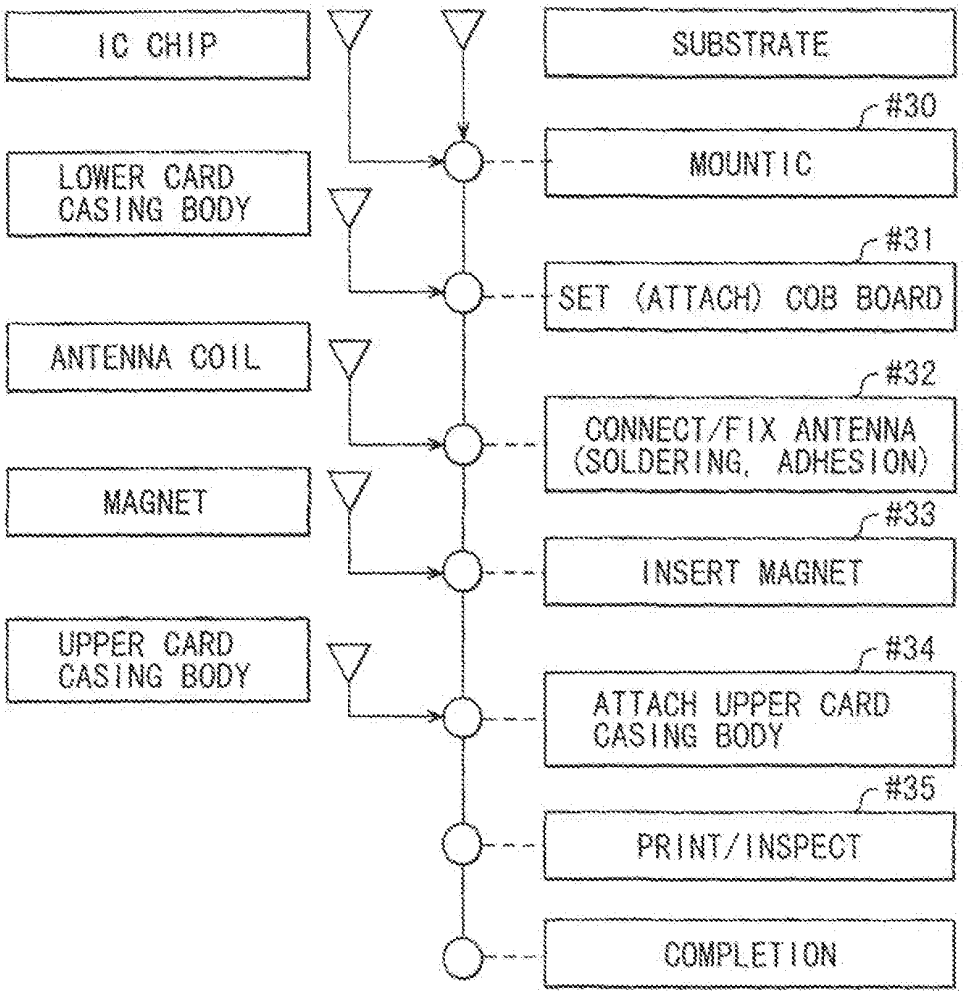

IC CHIP
LOWER CARD CASING BODY
ANTENNA COIL
MAGNET
UPPER CARD CASING BODY
SUBSTRATE
#30
MOUNTIC
#31
SET (ATTACH) COB BOARD
#32
CONNECT/FIX ANTENNA (SOLDERING, ADHESION)
#33
INSERT MAGNET
#34
ATTACH UPPER CARD CASING BODY
#35
PRINT/INSPECT
COMPLETION

FIG. 44

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

(11) EP 0 993 999 A2

(12) EUROPEAN PATENT APPLICATION

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

(51) Int Cl.⁷: **B60R 25/04**

(21) Application number: **99305339.6**

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

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

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

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

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

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

(54) Fuel pump immobilization

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

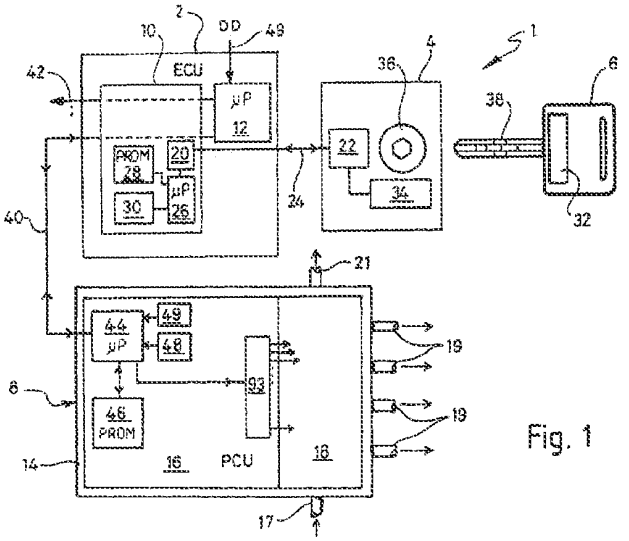


Fig. 1

EP 0 993 999 A2

Printed by Jouve, 75001 PARIS (FR)

Description

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

46.

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

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

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

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

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

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

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

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

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

Claims

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

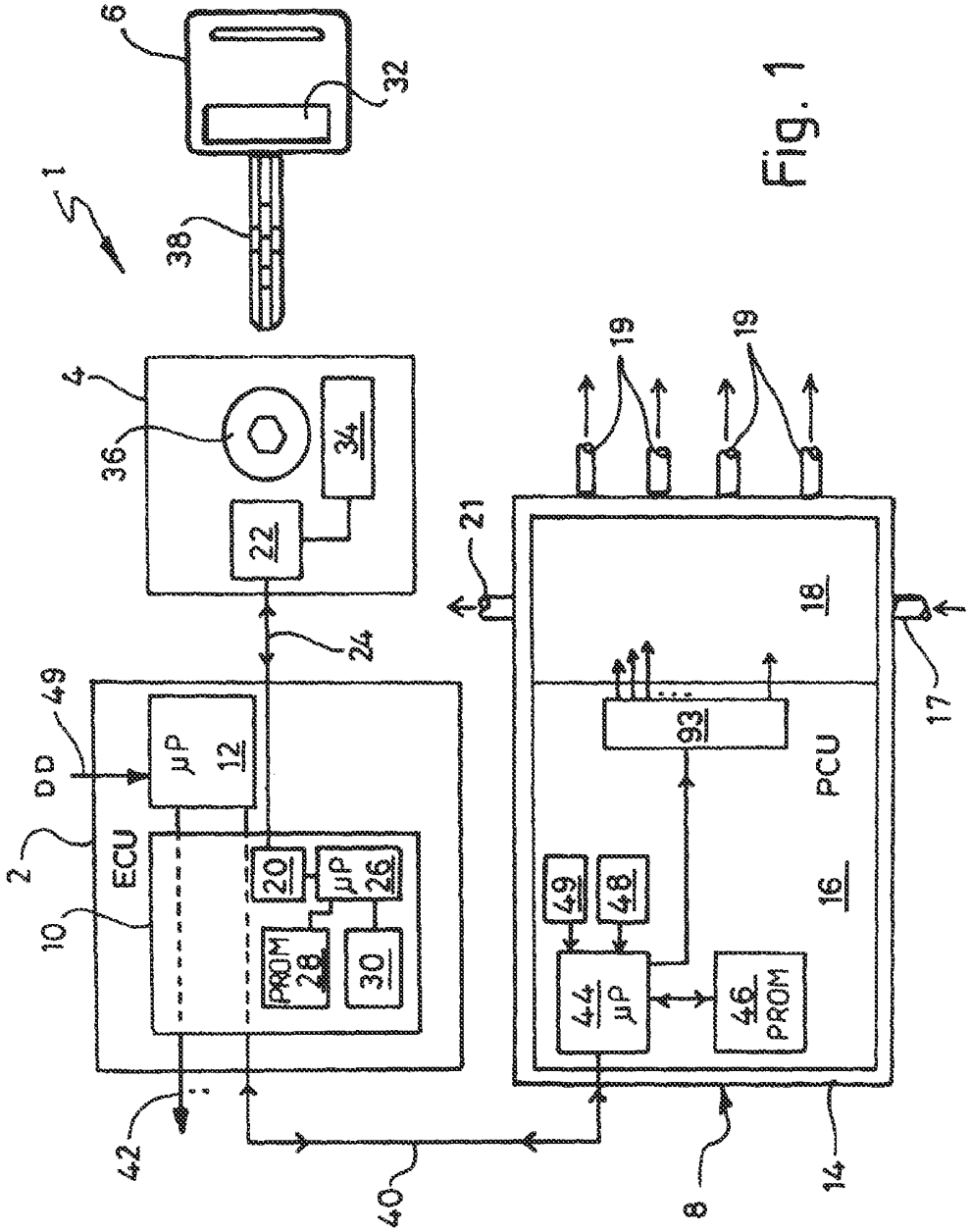

6
32
1
38
4
36
34
22
24
19
19
21
18
17
49
DD
µP
12
2
ECU
10
20
µP
26
PROM
28
30
93
PCU
16
49
48
44
µP
46
PROM
42
40
8
14

Fig. 1

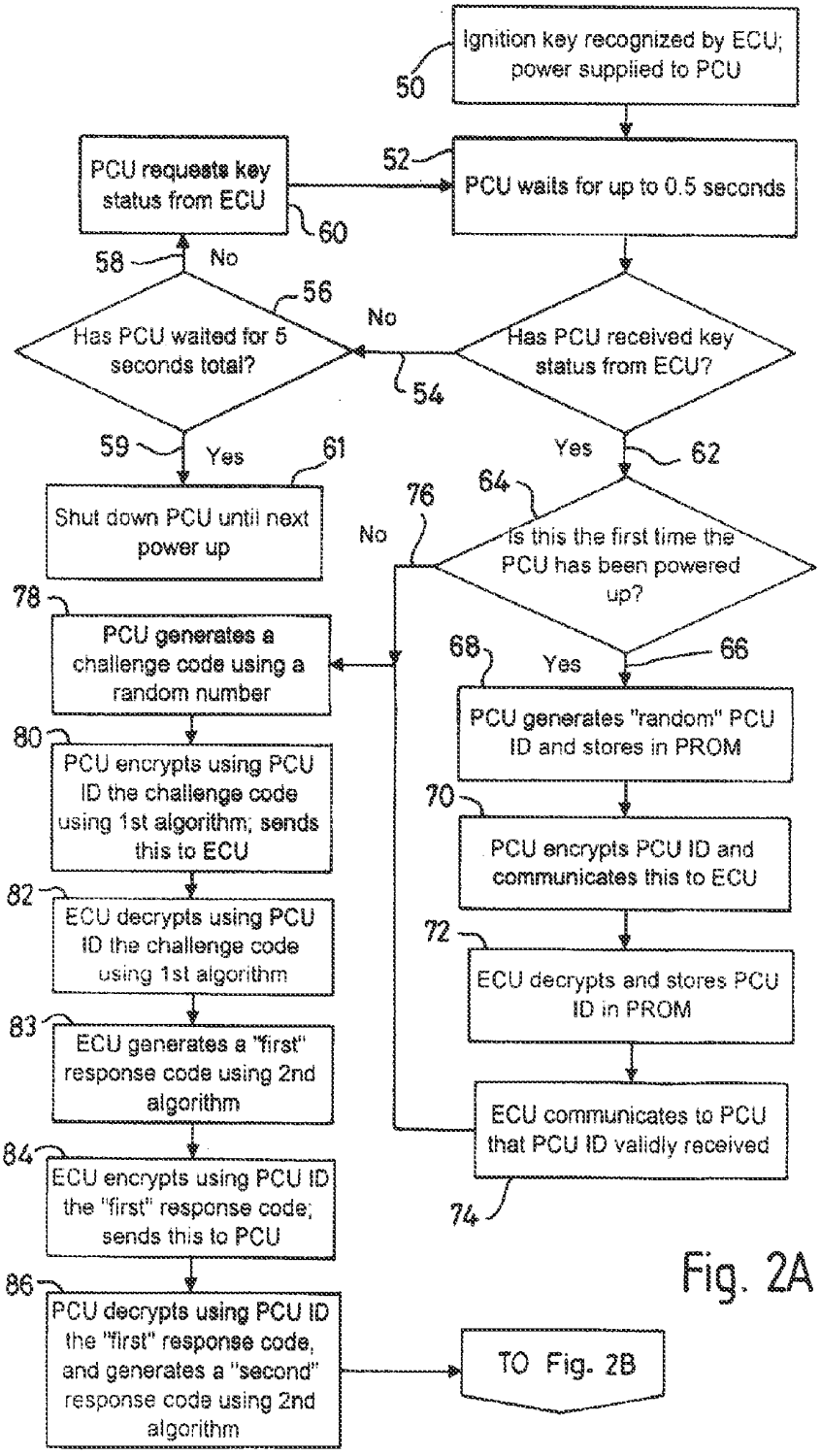

Ignition key recognized by ECU; power supplied to PCU
50
PCU waits for up to 0.5 seconds
52
PCU requests key status from ECU
60
No
58
Has PCU received key status from ECU?
No
54
Has PCU waited for 5 seconds total?
56
Yes
59
Yes
62
Shut down PCU until next power up
61
Is this the first time the PCU has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

Fig. 2A

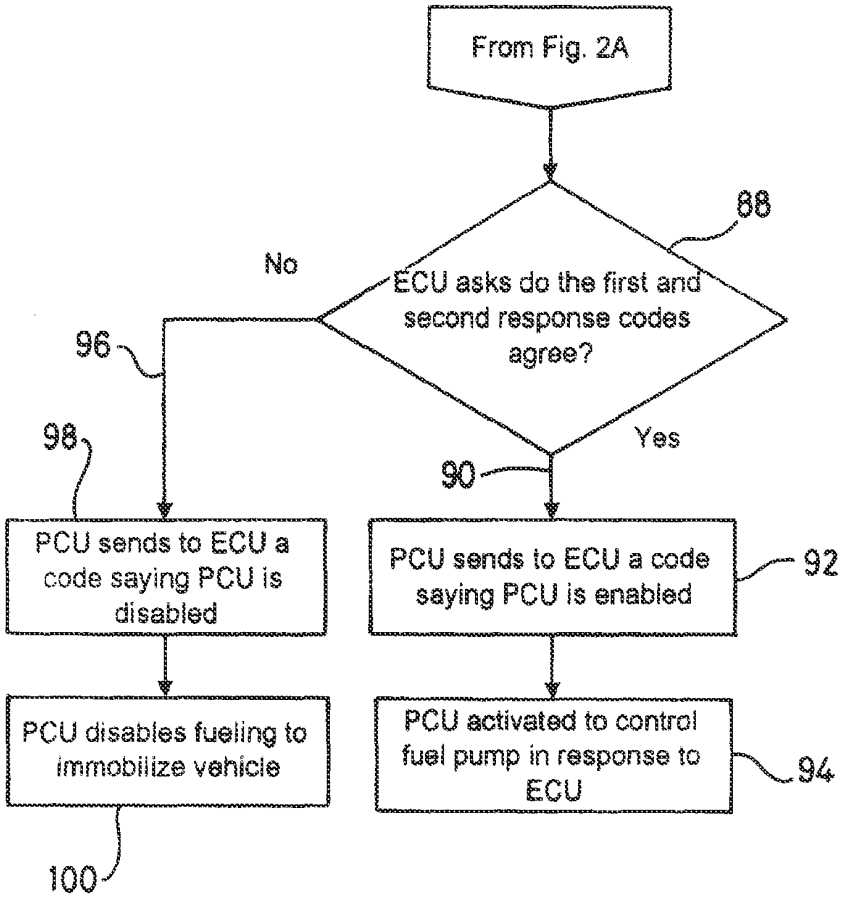

From Fig. 2A
88
ECU asks do the first and second response codes agree?
No
Yes
96
98
90
PCU sends to ECU a code saying PCU is disabled
PCU sends to ECU a code saying PCU is enabled
92
PCU disables fueling to immobilize vehicle
PCU activated to control fuel pump in response to ECU
94
100

Fig. 2B

Espacenet

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

NON-CONTACT DATA CARRIER AND BOOKLET THEREWITH

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

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

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

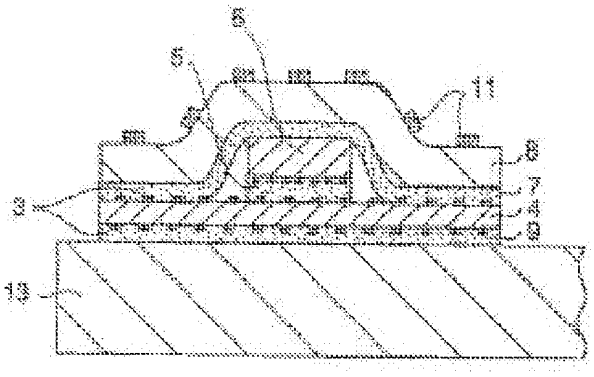
- cooperative:

Application number: JP20000220335 20000721

Priority number (s): JP20000220335 20000721

Abstract of JP2002042076 (A)

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



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

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

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

審査請求　未請求　請求項の数12　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願2000－220335(P2000－220335)

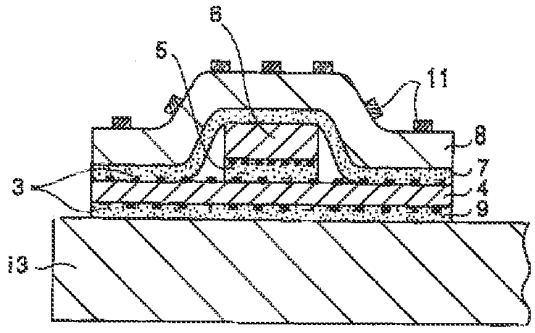
(22)出願日　平成12年７月21日(2000.7.21)

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

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

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

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



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

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

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

【０００７】

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

【０００８】

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

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

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

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

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

【００１３】

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

【００２８】

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

【図面の簡単な説明】

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

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

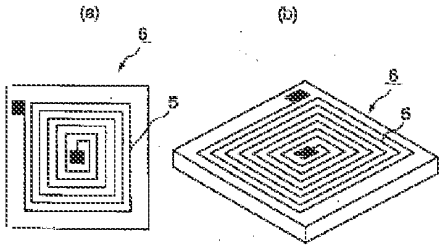
【図３】図２（ａ）のＡ－Ａ線断面図である。

【図４】本発明の非接触型データキャリアを有する冊子の一部断面図である。

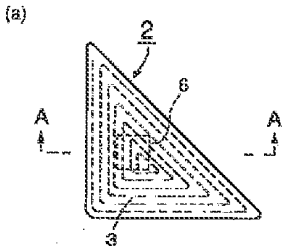
【図５】本発明の非接触型データキャリアを有する冊子の裏表紙を開いた状態を示す斜視図である。

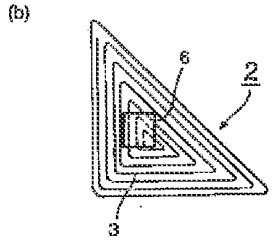
【図６】本発明の非接触型データキャリアを有する冊子の裏表紙を開いた後、本文用紙の一部をめくった状態を示す斜視図である。
【図７】本発明の非接触型データキャリアを有する冊子を閉じた状態を示す平面図である。
【図８】（ａ），（ｂ）は、それぞれ異なる形状の非接触型データキャリアを貼付する位置を示すマークが印刷されている冊子の一部切り欠き平面図である。
【符号の説明】
１　冊子
２　非接触型データキャリア
３　第１のコイルアンテナ
４　第１の基材シート
５　第２のコイルアンテナ
６　非接触型ＩＣチップ
７　接着層
８　第２の基材シート
９　接着剤層
１０　剥離紙
１１　地紋印刷
１２　表表紙
１３　裏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

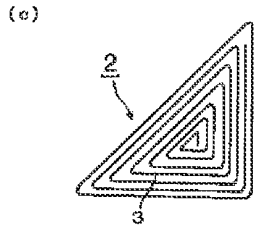
【図１】



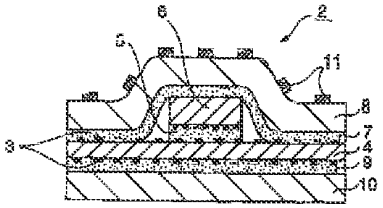
【図２】



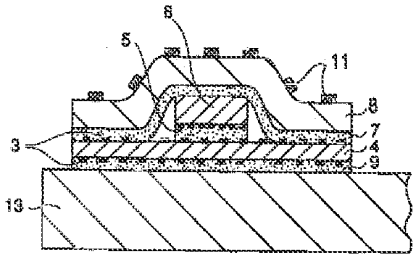




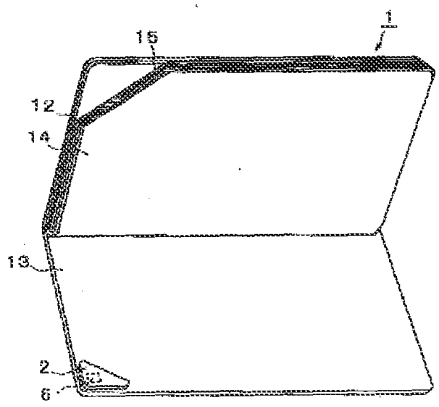
【図３】



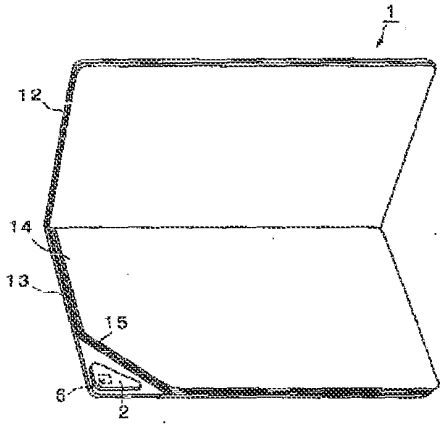
【図４】



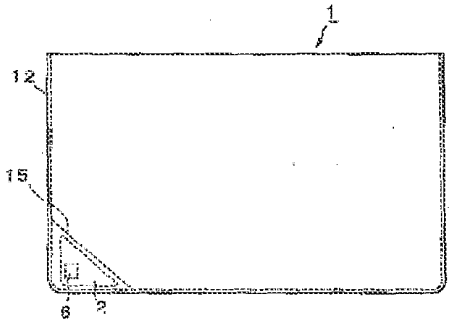
【図5】



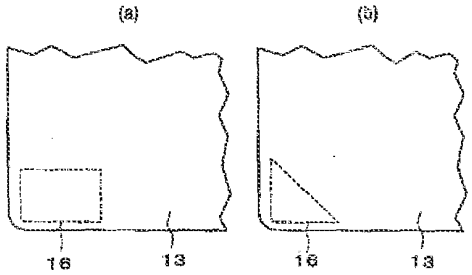
【図6】



【図7】



【図8】



フロントページの続き

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

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, L., R-W. [US/US]; 540 Buckingham #513, Richardson, TX 75081 (US).

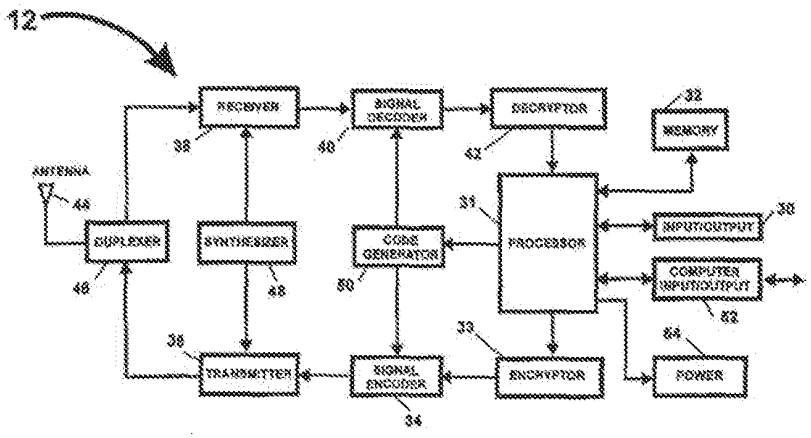
(72) Inventor: CLEVELAND, Joseph, Robert; 911 Grinnell Drive, Richardson, TX 75081 (US).

(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.

AE	Arab Emirates	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	ML	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	MK	Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon			PT	Portugal		
CN	China	KR	Republic of Korea	RO	Romania		
CU	Cuba	KZ	Kazakstan	RU	Russian Federation		
CZ	Czech Republic	LC	Saint Lucia	SD	Sudan		
DE	Germany	LI	Liechtenstein	SE	Sweden		
DK	Denmark	LK	Sri Lanka	SG	Singapore		
EE	Estonia	LR	Liberia				

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.

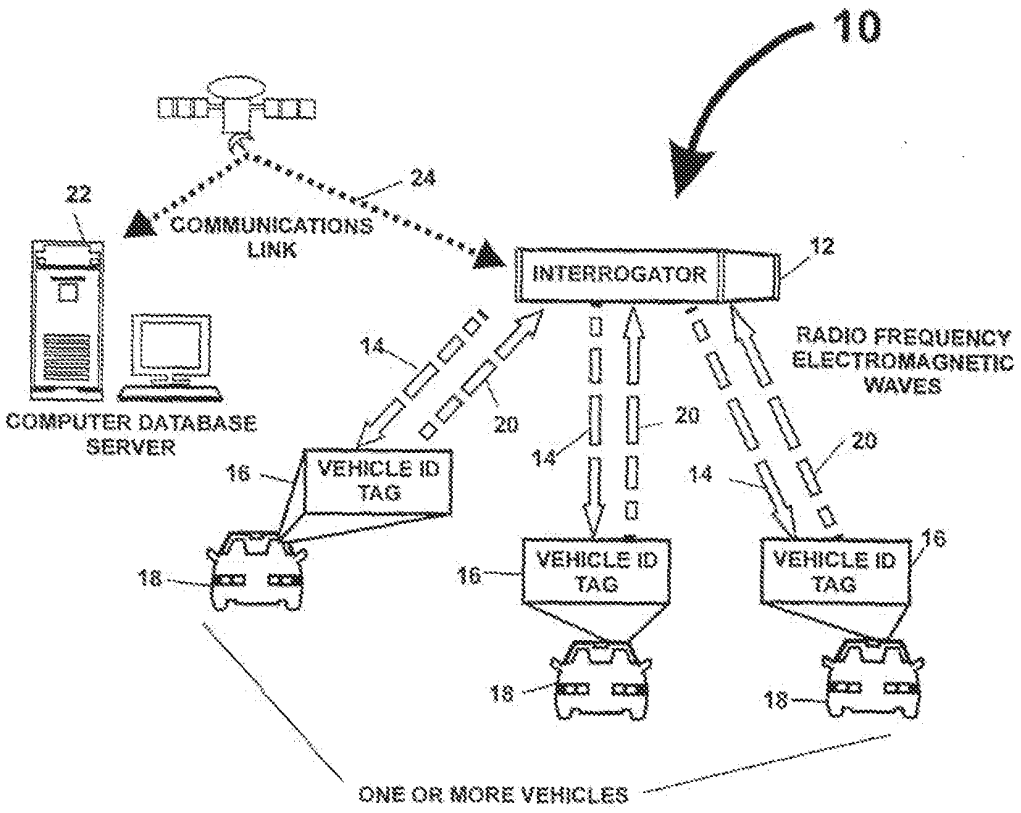

10
22
24
COMMUNICATIONS LINK
INTERROGATOR
12
COMPUTER DATABASE SERVER
14
20
RADIO FREQUENCY ELECTROMAGNETIC WAVES
16
VEHICLE ID TAG
18
ONE OR MORE VEHICLES

Figure 1

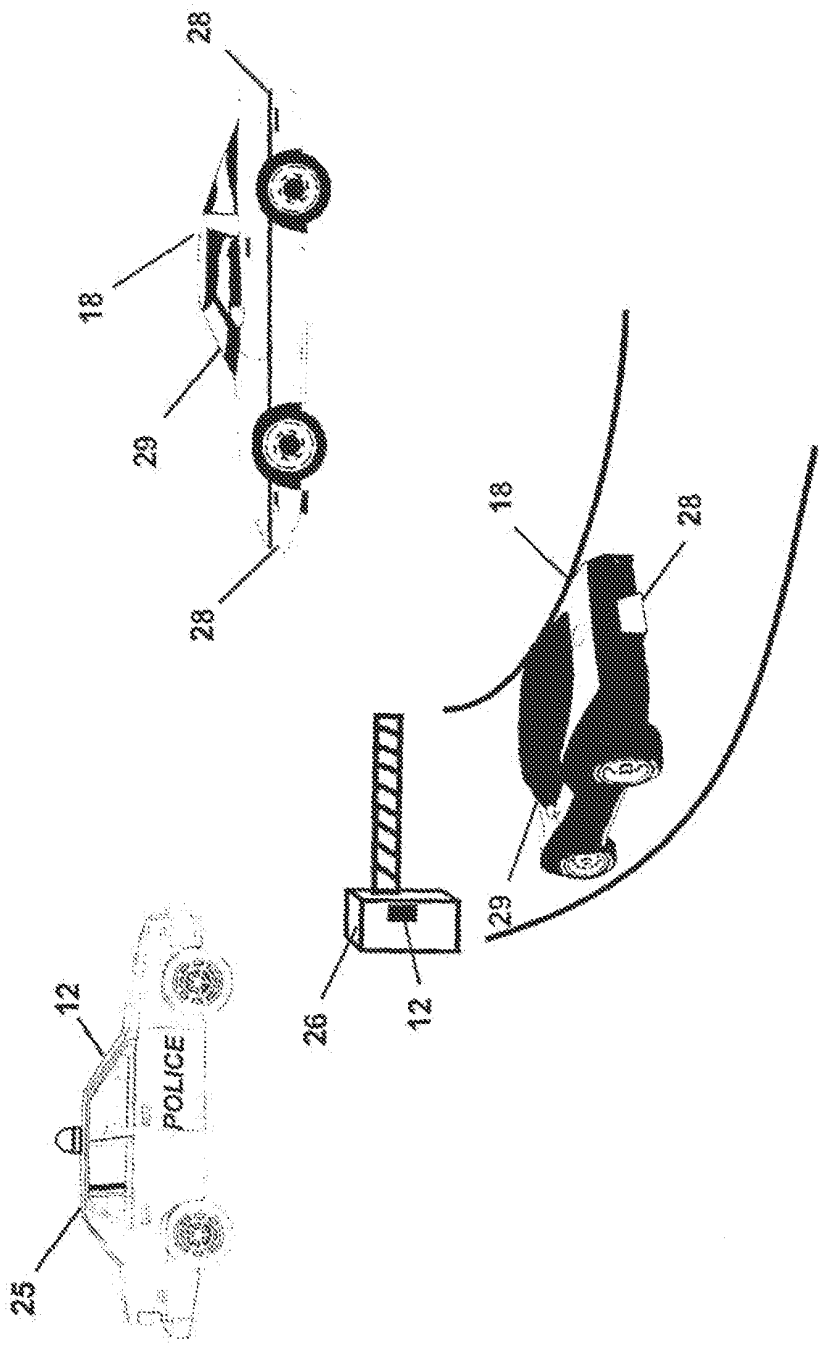


Figure 2

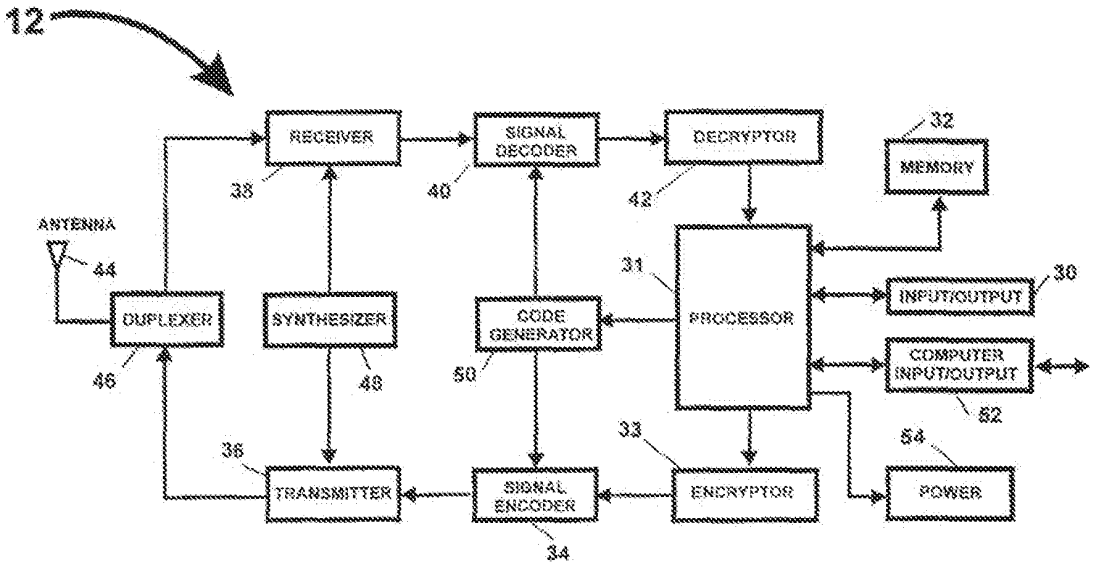

12
RECEIVER
SIGNAL DECODER
DECRYPTOR
32
MEMORY
38
40
42
ANTENNA
44
31
PROCESSOR
INPUT/OUTPUT
30
DUPLEXER
SYNTHESIZER
CODE GENERATOR
COMPUTER INPUT/OUTPUT
46
48
50
82
36
33
64
TRANSMITTER
SIGNAL ENCODER
ENCRYPTOR
POWER
34

Figure 3

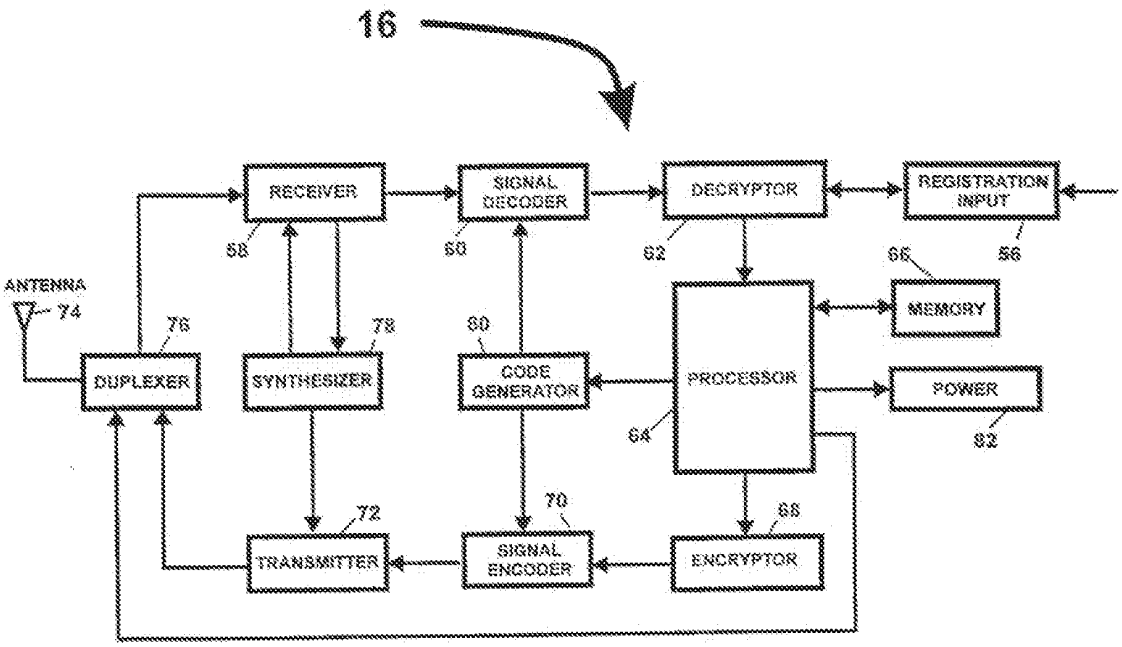

16
RECEIVER
SIGNAL DECODER
DECRYPTOR
REGISTRATION INPUT
58
60
62
56
66
ANTENNA
74
MEMORY
76
78
80
DUPLEXER
SYNTHESIZER
CODE GENERATOR
PROCESSOR
POWER
64
82
72
70
68
TRANSMITTER
SIGNAL ENCODER
ENCRYPTOR

Figure 4

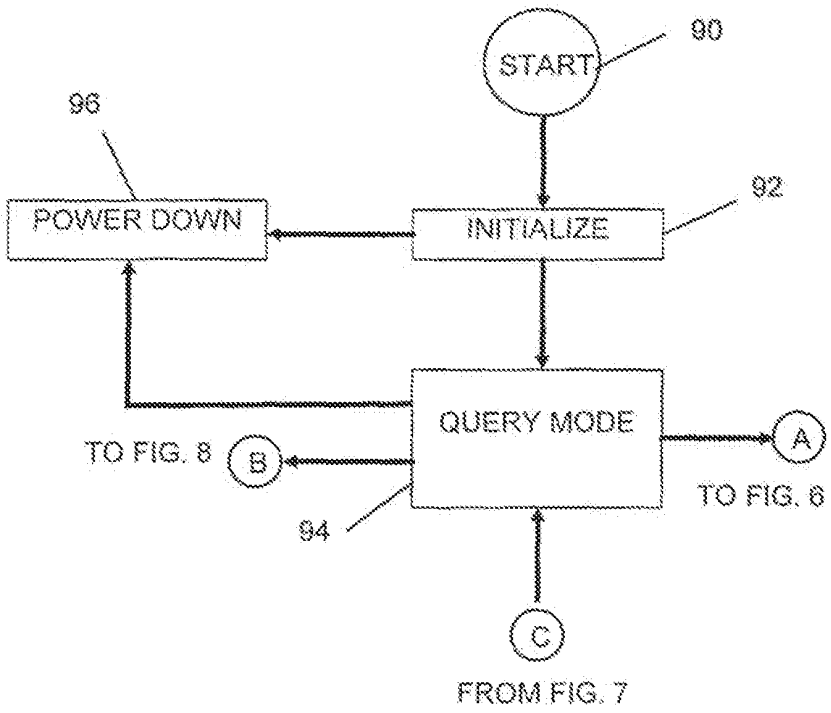

START
90
96
POWER DOWN
INITIALIZE
92
QUERY MODE
TO FIG. 8
B
A
TO FIG. 6
94
C
FROM FIG. 7

Figure 5

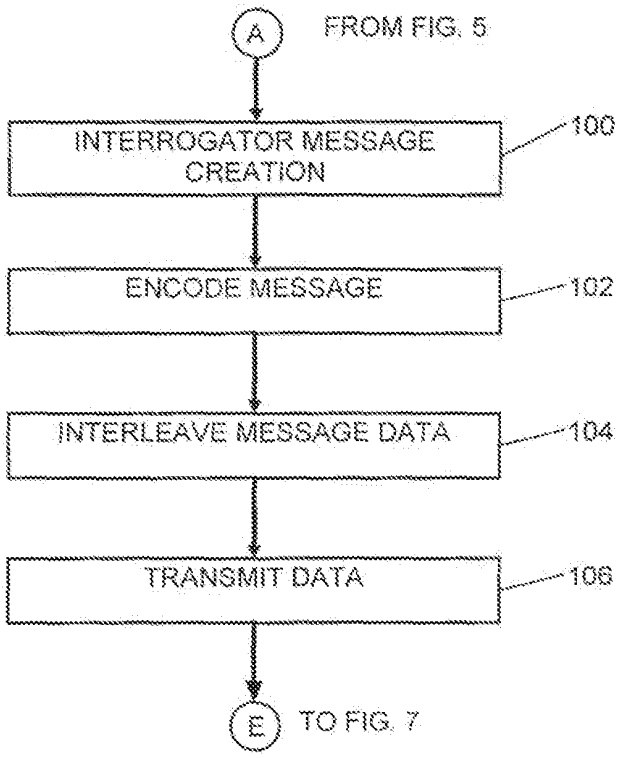

A
FROM FIG. 5
INTERROGATOR MESSAGE CREATION
100
ENCODE MESSAGE
102
INTERLEAVE MESSAGE DATA
104
TRANSMIT DATA
106
E
TO FIG. 7

Figure 6

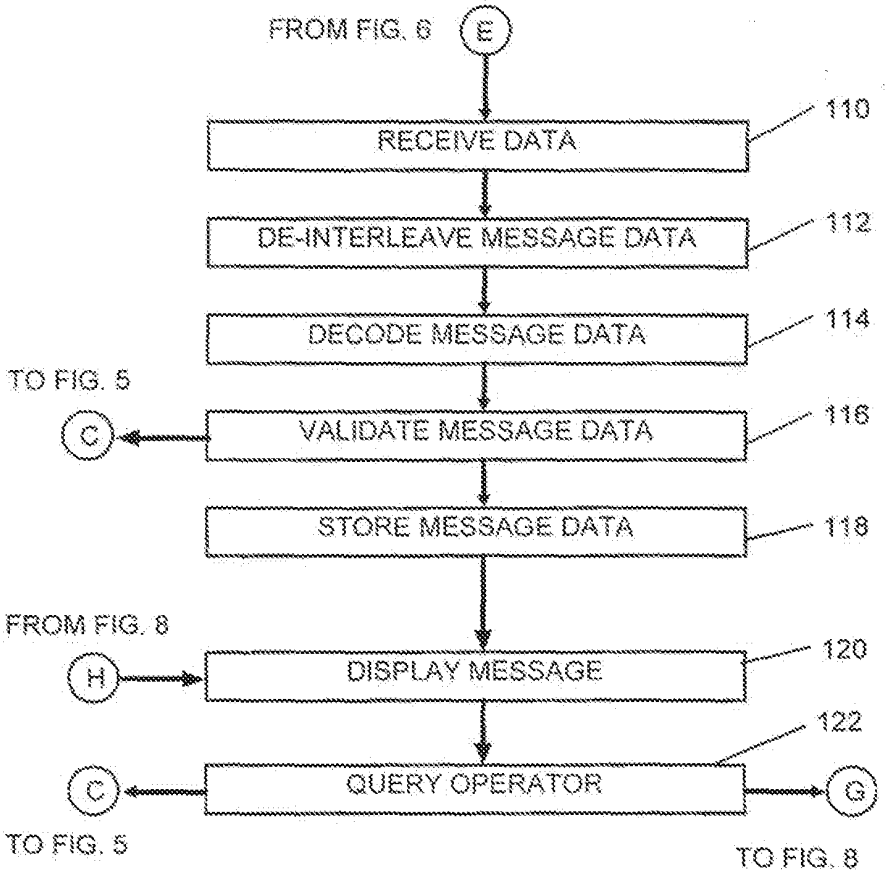

FROM FIG. 6
E
RECEIVE DATA
110
DE-INTERLEAVE MESSAGE DATA
112
DECODE MESSAGE DATA
114
TO FIG. 5
C
VALIDATE MESSAGE DATA
116
STORE MESSAGE DATA
118
FROM FIG. 8
H
DISPLAY MESSAGE
120
122
C
QUERY OPERATOR
G
TO FIG. 5
TO FIG. 8

Figure 7

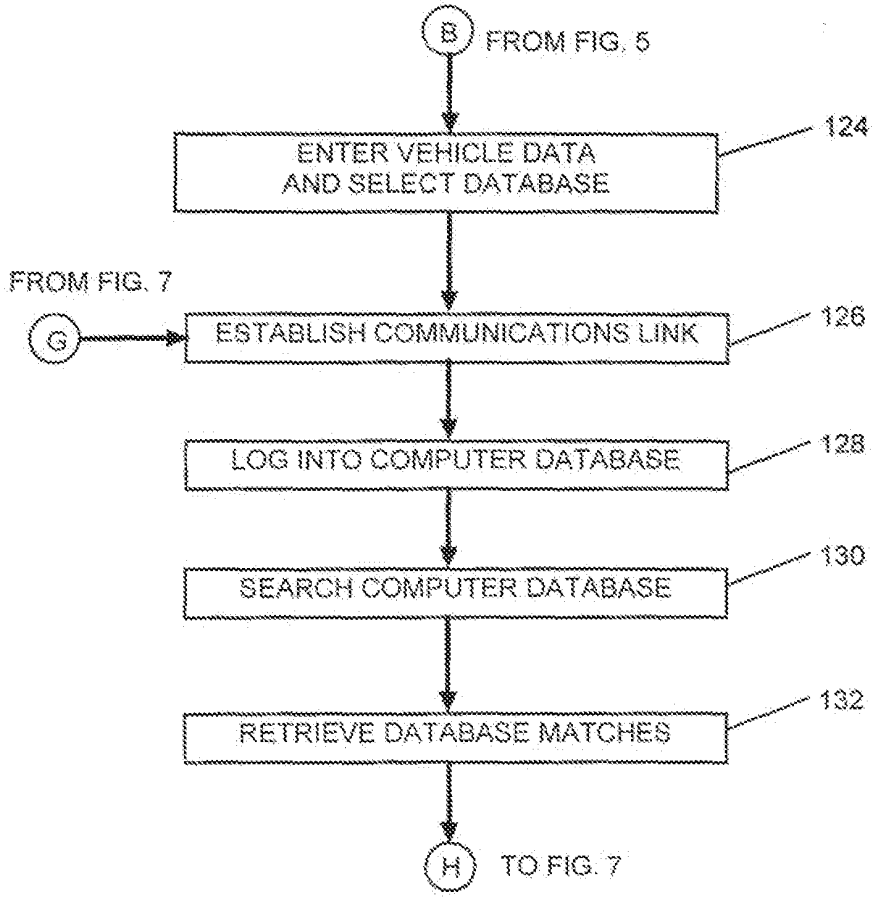

B
FROM FIG. 5
ENTER VEHICLE DATA AND SELECT DATABASE
124
FROM FIG. 7
G
ESTABLISH COMMUNICATIONS LINK
126
LOG INTO COMPUTER DATABASE
128
SEARCH COMPUTER DATABASE
130
RETRIEVE DATABASE MATCHES
132
H
TO FIG. 7

Figure 8

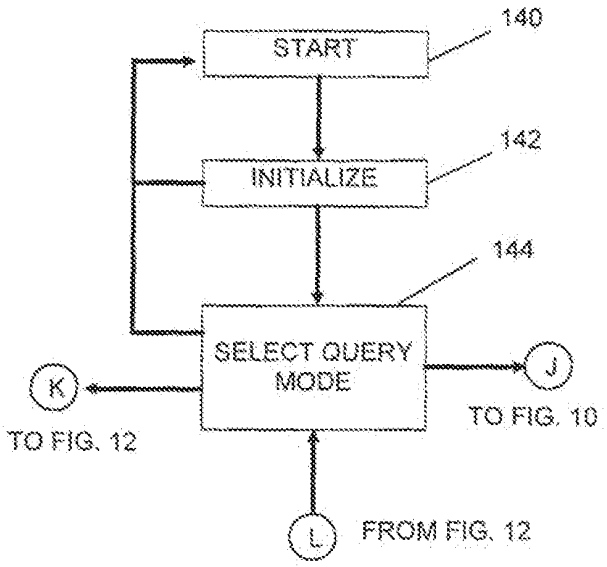

START
140
INITIALIZE
142
144
SELECT QUERY MODE
K
TO FIG. 12
J
TO FIG. 10
L
FROM FIG. 12

Figure 9

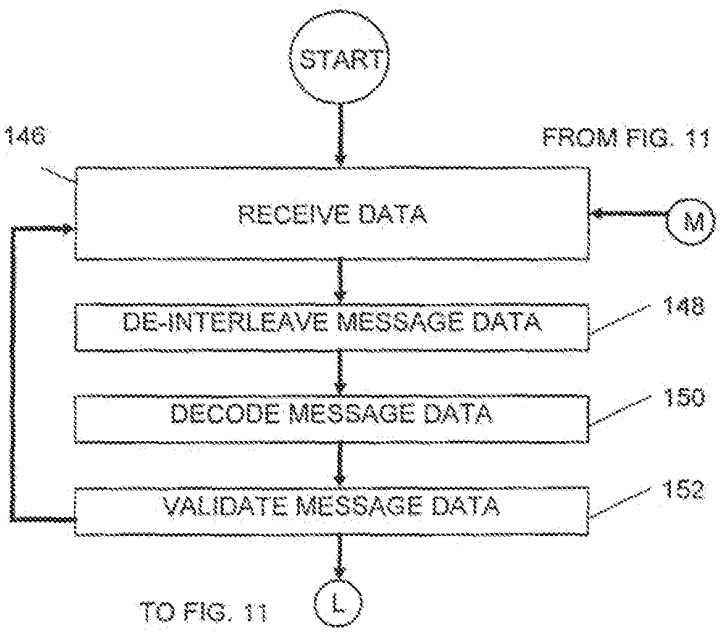

START
146
FROM FIG. 11
RECEIVE DATA
M
DE-INTERLEAVE MESSAGE DATA
148
DECODE MESSAGE DATA
150
VALIDATE MESSAGE DATA
152
TO FIG. 11
L

Figure 10

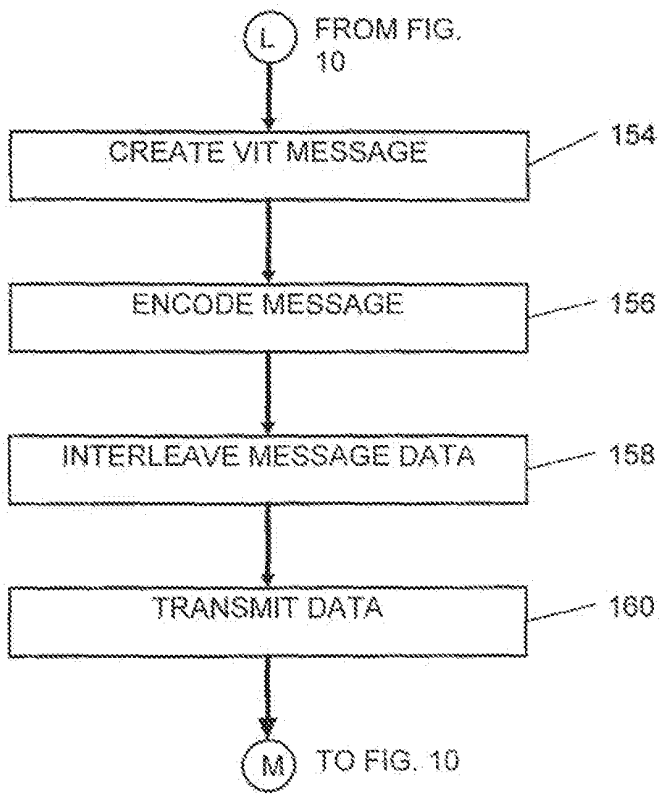

L
FROM FIG. 10
CREATE VIT MESSAGE
154
ENCODE MESSAGE
156
INTERLEAVE MESSAGE DATA
158
TRANSMIT DATA
160
M
TO FIG. 10

Figure 11

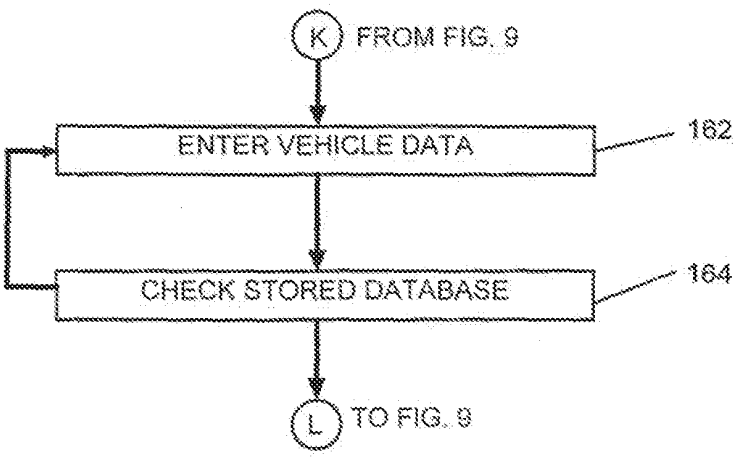

K
FROM FIG. 9
ENTER VEHICLE DATA
162
CHECK STORED DATABASE
164
L
TO FIG. 9

Figure 12

(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).

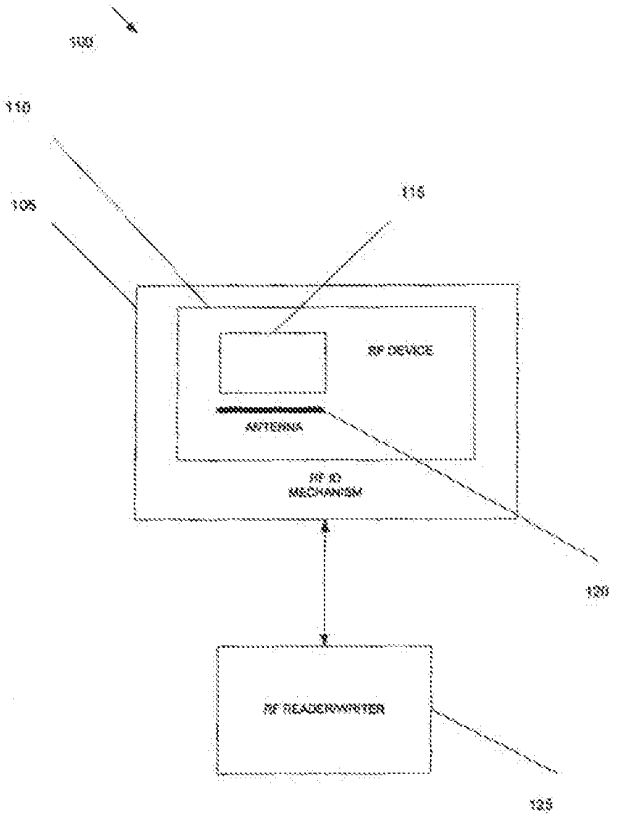
(74) Agent: MIDGLEY, Jonathan, Lee; Marks & Clerk, 57-60 Lincolns Inn Fields, London, WC2A 3LS (GB).

(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:

$$L_1 = 2.93 \text{K} 10^{8}\,H$$
$$L_2 = 6.43 \text{K} 10^{12}\,H$$

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

Multiple RF Chip Overview

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

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

B. Method of Using a RF Border Crossing Control System

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

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

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

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

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

VI. SYSTEM AND METHOD FOR LIMITING SOFTWARE DOWNLOADS

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

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

A. System for Limiting Software Downloads

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

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

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

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

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

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

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

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

B. Method of Limiting Software Downloads

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

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

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

VII. SYSTEM AND METHOD FOR AIRPORT SECURITY

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

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

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

A. Airport Security System

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

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

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

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

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

B. Method of Airport Security

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

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

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

CONCLUSION

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

WHAT IS CLAIMED IS:

1. A system of verifying information, comprising;

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

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

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

2. A method of verifying information, comprising:

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

incorporating the chip onto a radio frequency identification mechanism;

reading first identification information with a radio frequency reader; and

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

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

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

an item incorporating the radio frequency device; and

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

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

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

incorporating the chip onto the item;

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

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

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

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

a license plate incorporating the radio frequency device.

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

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

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

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

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

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

physical characteristics of a person authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of a person authorized to drive a vehicle.

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

physical characteristics of a person authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of a person authorized to drive a vehicle.

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

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

an identification mechanism incorporating the radio frequency device; and

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

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

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

incorporating the chip onto an identification mechanism;

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

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

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

physical characteristics of an individual authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of an individual authorized to drive a vehicle.

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

physical characteristics of an individual authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of an individual authorized to drive a vehicle.

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

a passport;

a driver's license; and

an identification card.

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

a passport;

a driver's license; and

an identification card.

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

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

a communication device incorporating the radio frequency device; and

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

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

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

incorporating the chip onto a communications device;

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

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

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

physical characteristics of the individual;

biometric information of the individual; and

personal knowledge of the individual.

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

physical characteristics of the individual;

biometric information of the individual; and

personal knowledge of the individual.

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

a cellular phone;

a personal digital assistant;

a pager;

a personal communications device

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

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

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

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

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

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

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

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

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

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

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

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

physical characteristics of the individual;

physical characteristics of a vehicle driven by the individual; and

biometric information of the individual;

physical characteristics of the at least one item; and

personal knowledge of the individual.

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

physical characteristics of the individual;

physical characteristics of a vehicle driven by the individual; and

biometric information of the individual;

physical characteristics of the at least one item; and

personal knowledge of the individual.

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

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

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

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

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

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

incorporating the chip onto at least one airport identification mechanism;

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

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

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

physical characteristics of the individual;

biometric information of the individual; and

personal knowledge of the individual.

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

physical characteristics of the individual;

biometric information of the individual; and

personal knowledge of the individual.

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

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

incorporating the chip into at least one identification device;

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

accepting second identification information from the user;

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

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

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

a identification mechanism incorporating the radio frequency device; and

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

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

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

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

information storage capabilities; and

transmission capabilities.

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

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

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

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

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

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

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

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

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

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

information storage capabilities; and

transmission capabilities.

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

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

physical characteristics of a person authorized to drive a vehicle;

physical characteristics of a vehicle; and

biometric information of a person authorized to drive a vehicle.

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

42. A system of verifying information, comprising;

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

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

43. A system of verifying information, comprising;

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

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

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

45. A method of verifying information, comprising:

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

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

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

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

physical characteristics of an individual;

biometric information of an individual;

personal knowledge of an individual; and

physical characteristics of an item.

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

48. A method of verifying information, comprising:

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

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

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

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

tamper-proof material;

a bidi-tri-dimensional feature;

a hidden image;

a dot-matrix;

hot stamping;

a moire pattern;

a hot stamped metalized hologram;

microprint;

ultraviolet fluorescence;

light piping;

laser engraving;

metalized striping;

a guilloche pattern;

a cameo effect;

ghost imaging;

a multidimensional hologram;

line artwork;

a photograph;

a colorgram;

a stereogram;

a holomatrix;

an optical variable device;

a combined hologram;

multi-dimensional bar codes; and

security taggant material.

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

a static bending test;

a heat test;

a rigidity test;

a durability test; and

an abrasion test.

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

tamper-proof material;

a bidi-tri-dimensional feature;

a hidden image;

a dot-matrix;

hot stamping;

a moire pattern;

a hot stamped metalized hologram;

microprint;

ultraviolet fluorescence;

light piping;

laser engraving;

metalized striping;

a guilloche pattern;

a cameo effect;

ghost imaging;

a multidimensional hologram;

line artwork;

a photograph;

a colorgram;

a stereogram;

a holomatrix;

an optical variable device;

a combined hologram;

multi-dimensional bar codes; and

security taggant material.

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

a static bending test;

a heat test;

a rigidity test;

a durability test; and

an abrasion test.

FIGURE 1

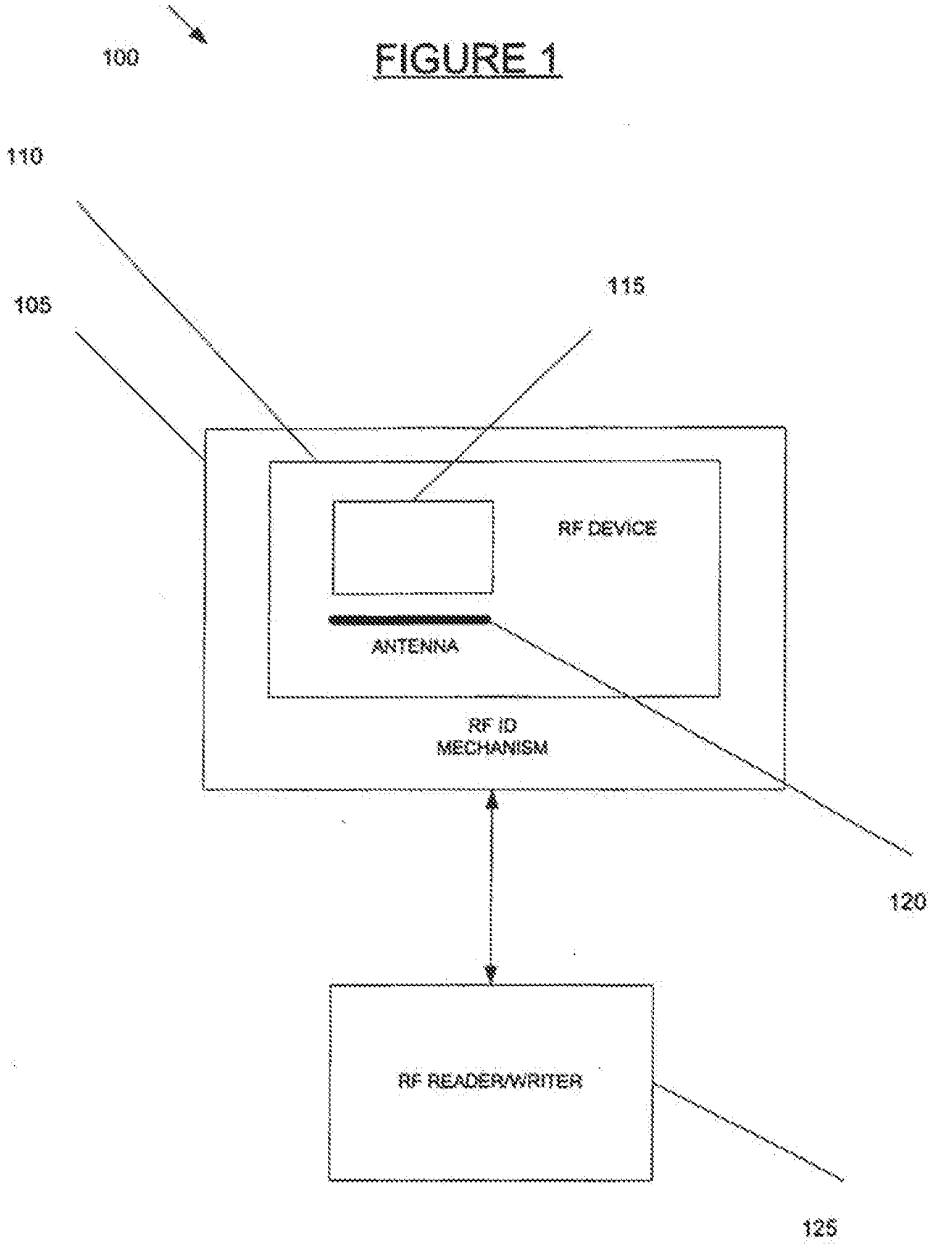

100
110
105
115
RF DEVICE
ANTENNA
RF ID
MECHANISM
120
RF READER/WRITER
125

FIGURE 2

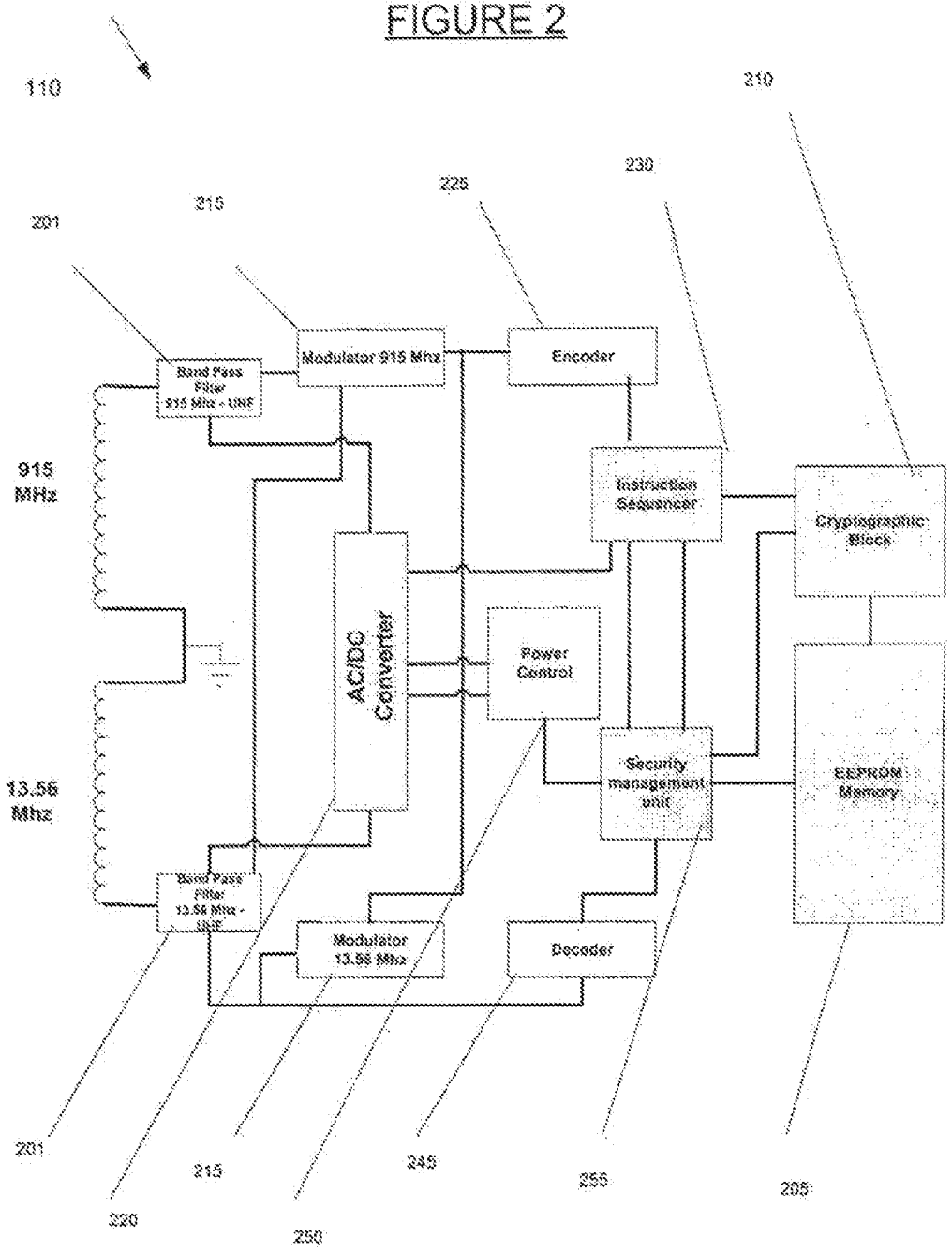

110
210
230
225
215
201
915 MHz
13.56 Mhz
Band Pass Filter 915 Mhz - UHF
Modulator 915 Mhz
Encoder
Instruction Sequencer
Cryptographic Block
AC/DC Converter
Power Control
Security management unit
EEPROM Memory
Band Pass Filter 13.56 Mhz - UHF
Modulator 13.56 Mhz
Decoder
201
215
245
255
205
220
250

FIGURE 3A

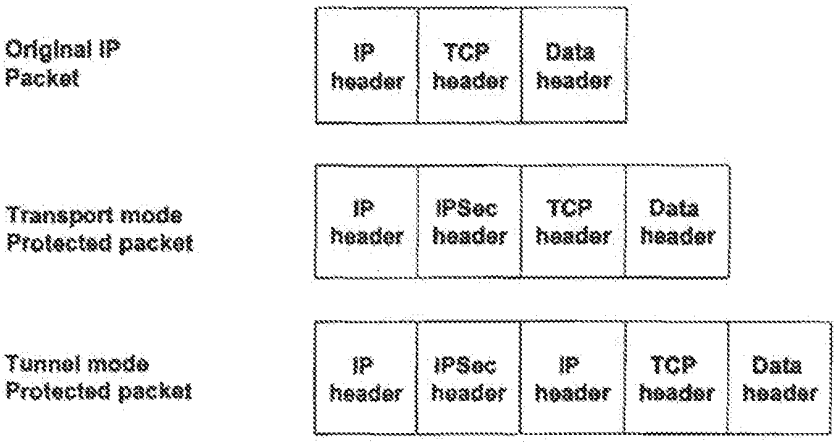
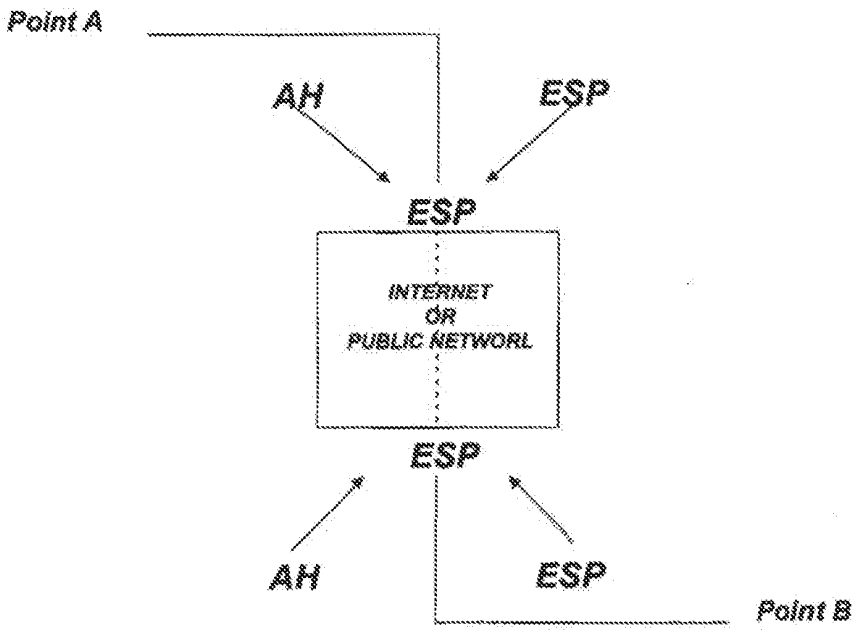

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIGURE 3B


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

400

FIGURE 4

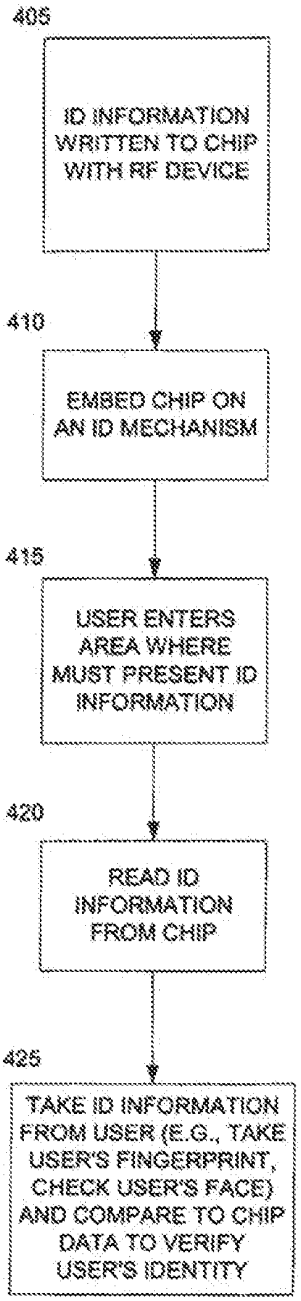

405
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
410
EMBED CHIP ON AN ID MECHANISM
415
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
420
READ ID INFORMATION FROM CHIP
425
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY

FIGURE 5

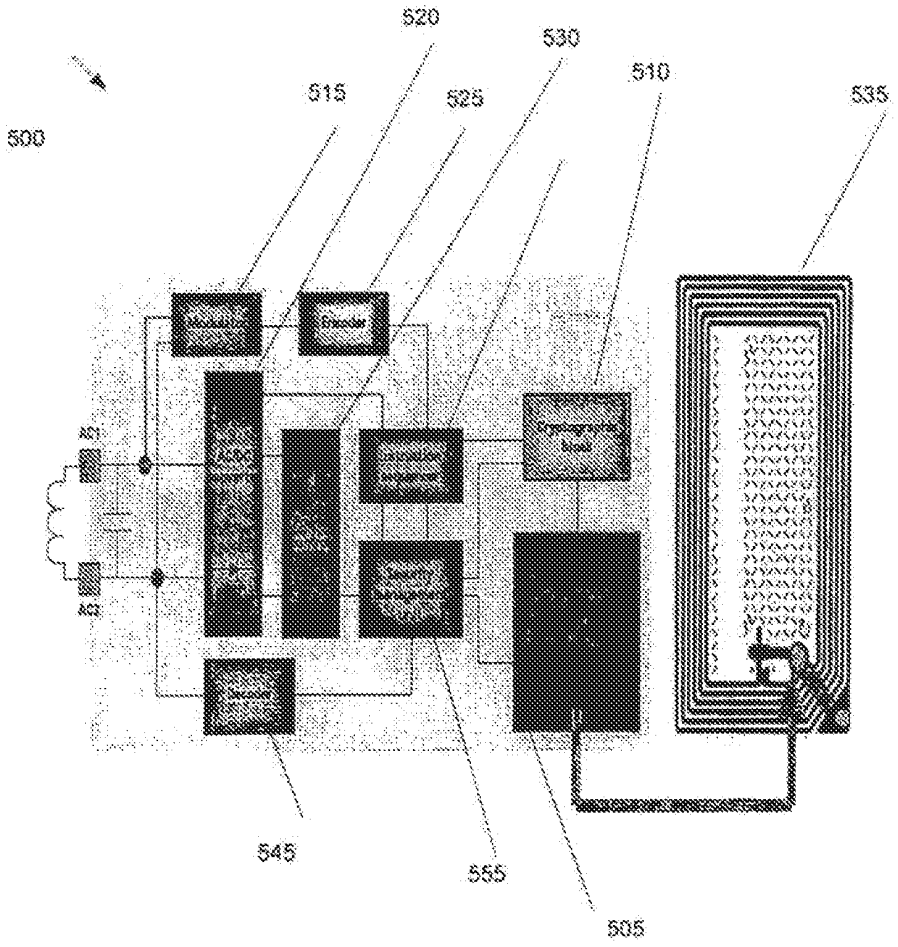


FIGURE 6

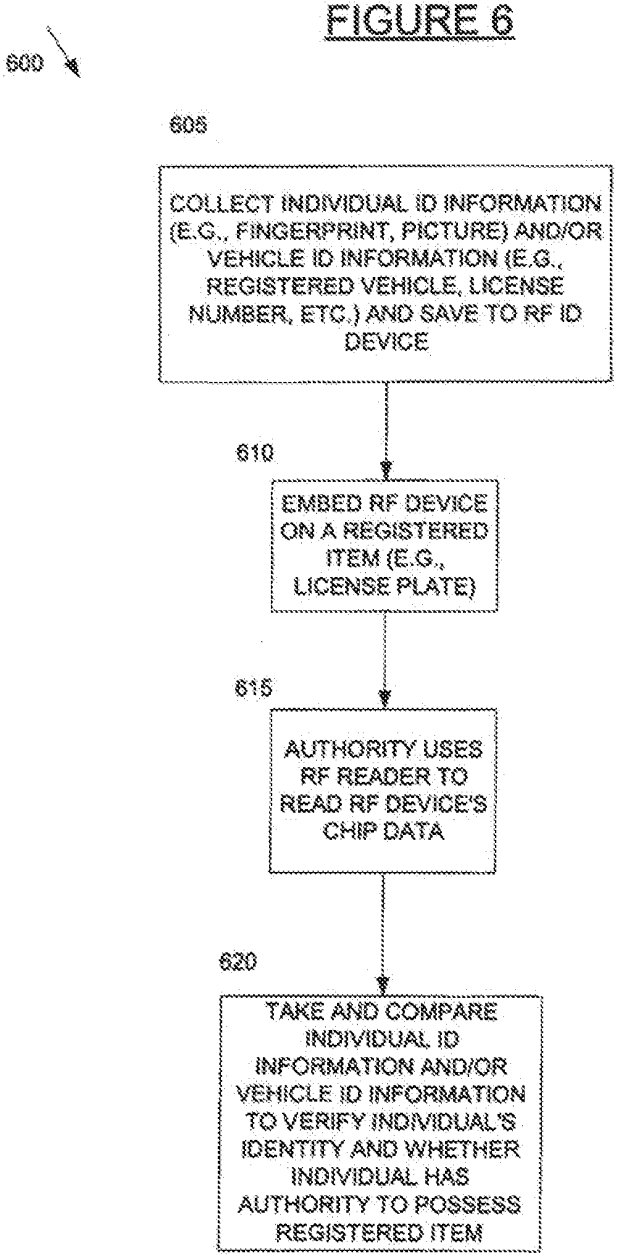

600
605
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
610
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
615
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
620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

FIGURE 7

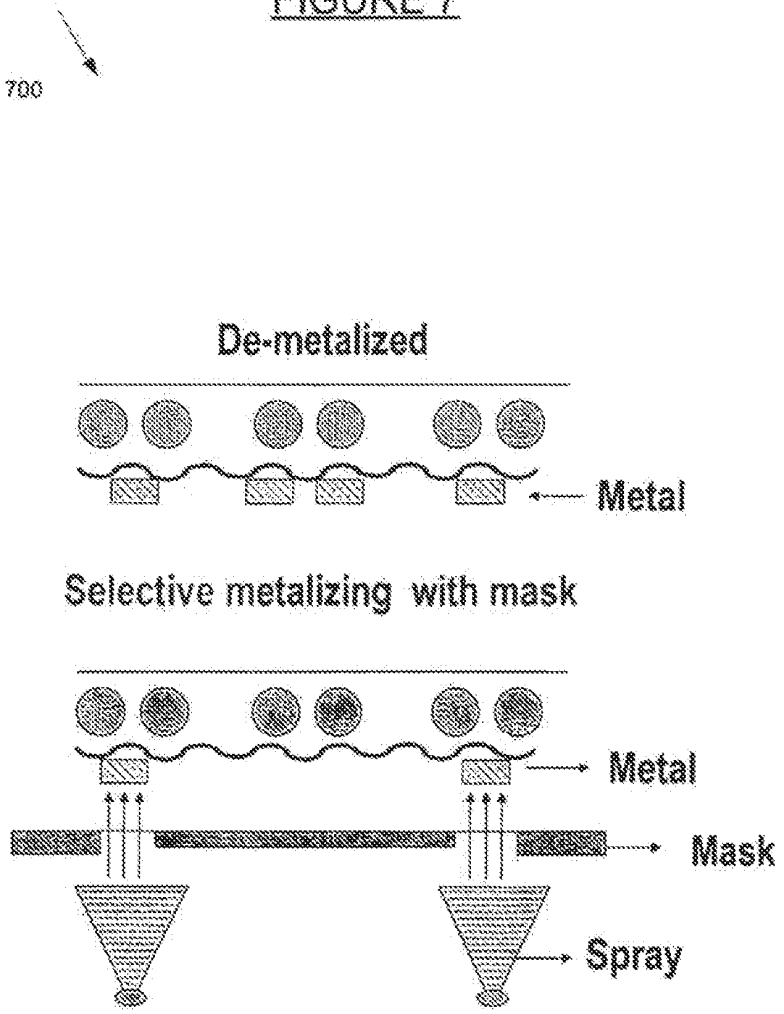

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIGURE 8

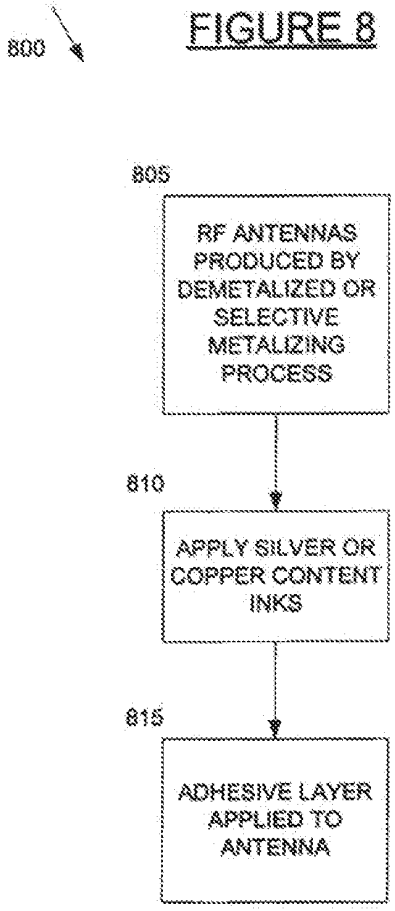

800
805
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
810
APPLY SILVER OR COPPER CONTENT INKS
815
ADHESIVE LAYER APPLIED TO ANTENNA

FIGURE 9

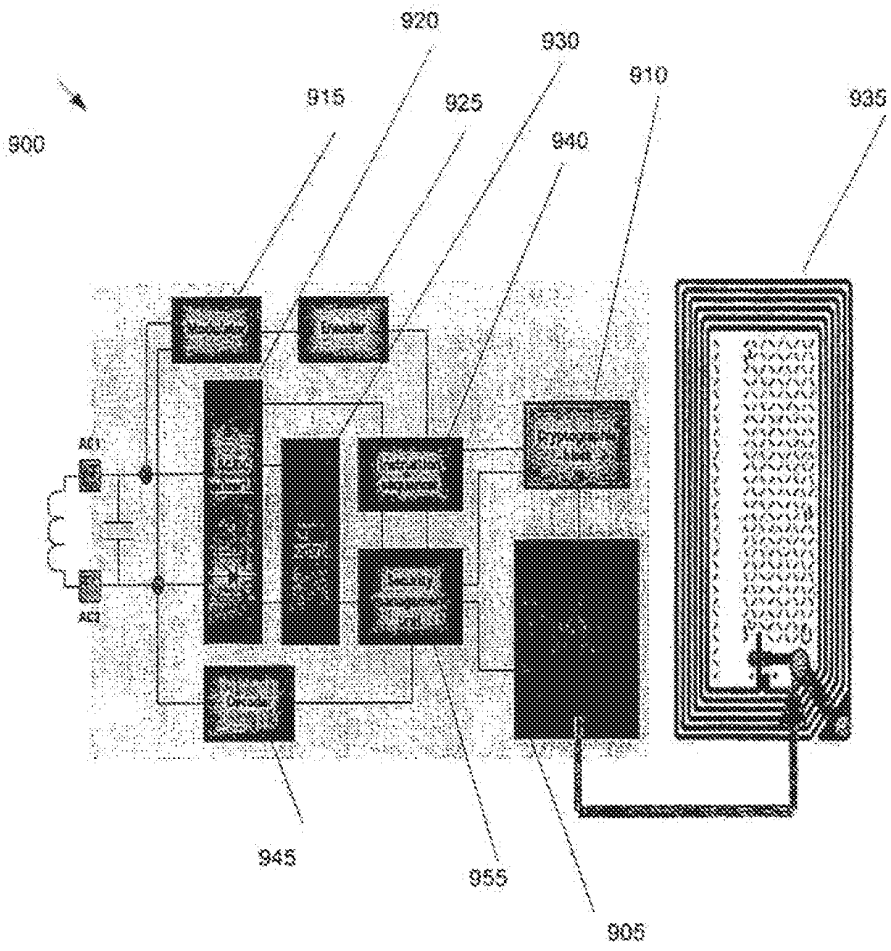


FIGURE 10

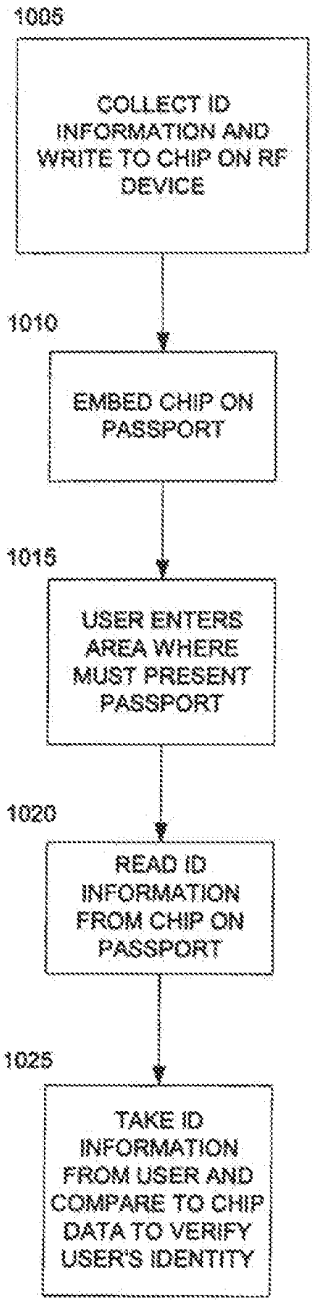

1005
COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1010
EMBED CHIP ON PASSPORT
1015
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1020
READ ID INFORMATION FROM CHIP ON PASSPORT
1025
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY

FIGURE 11

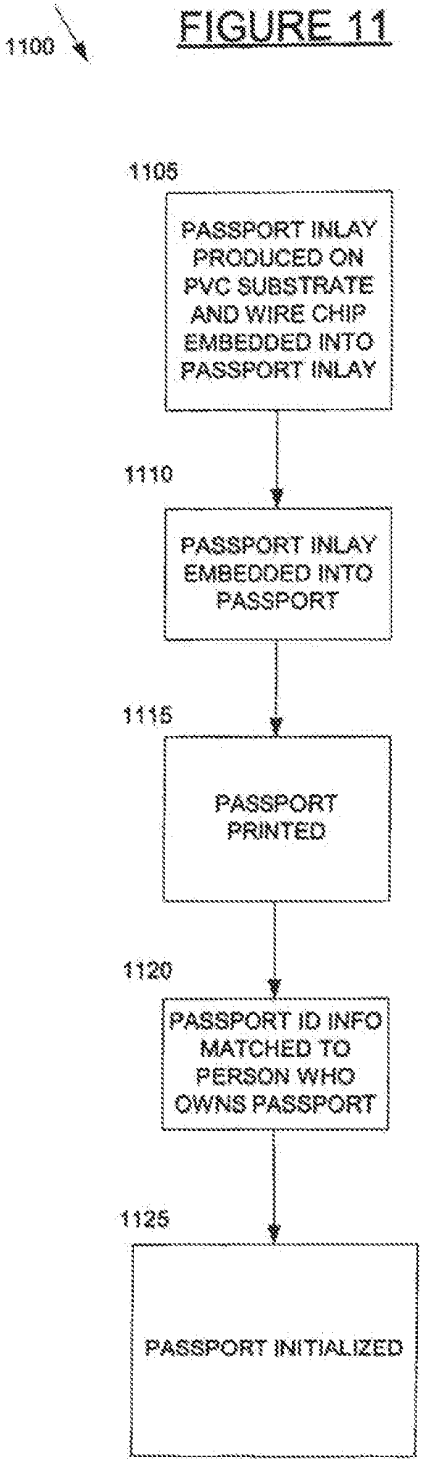

1100
1105
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1110
PASSPORT INLAY EMBEDDED INTO PASSPORT
1115
PASSPORT PRINTED
1120
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1125
PASSPORT INITIALIZED

FIGURE 12

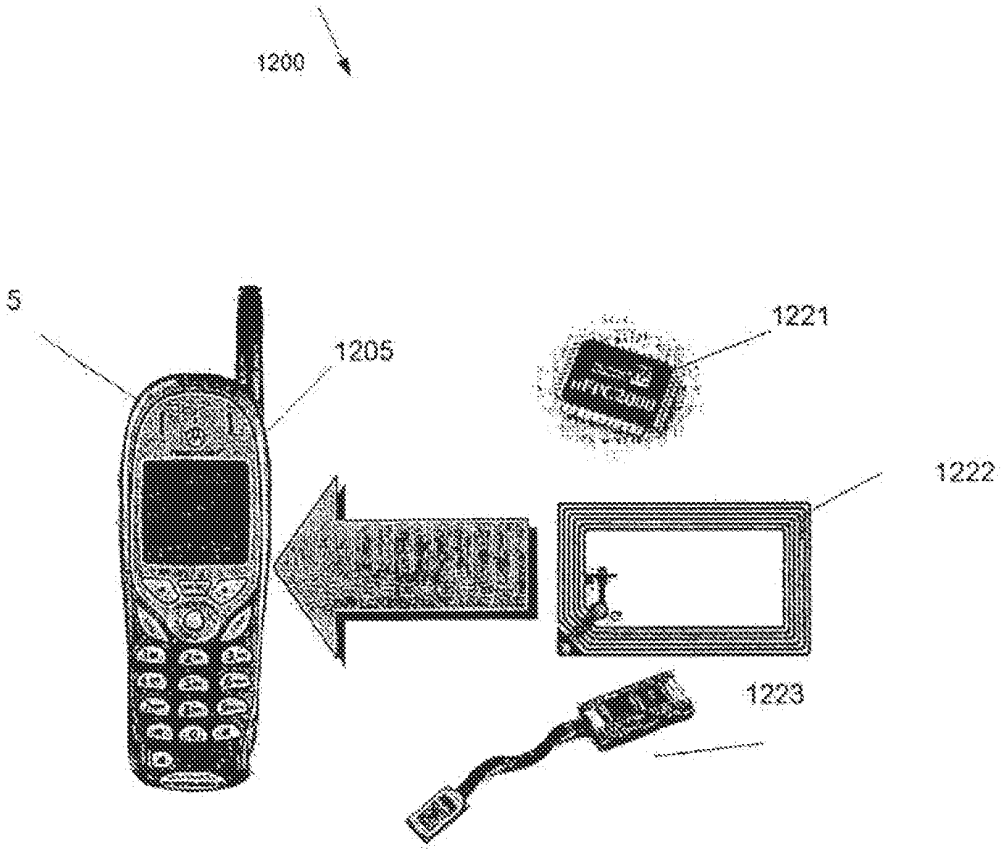


FIGURE 13

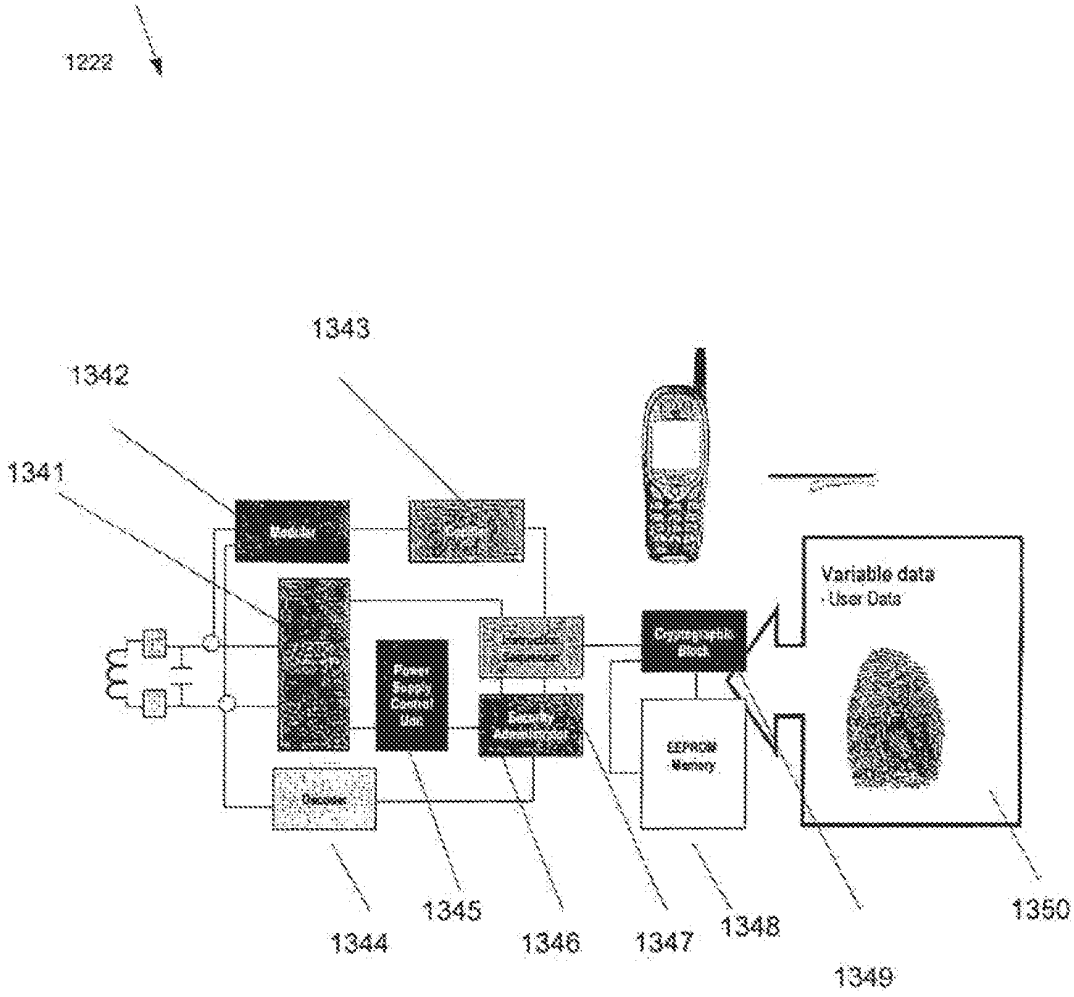

1222
1343
1342
1341
Variable data
· User Data
1344
1345
1346
1347
1348
1349
1350

FIGURE 14

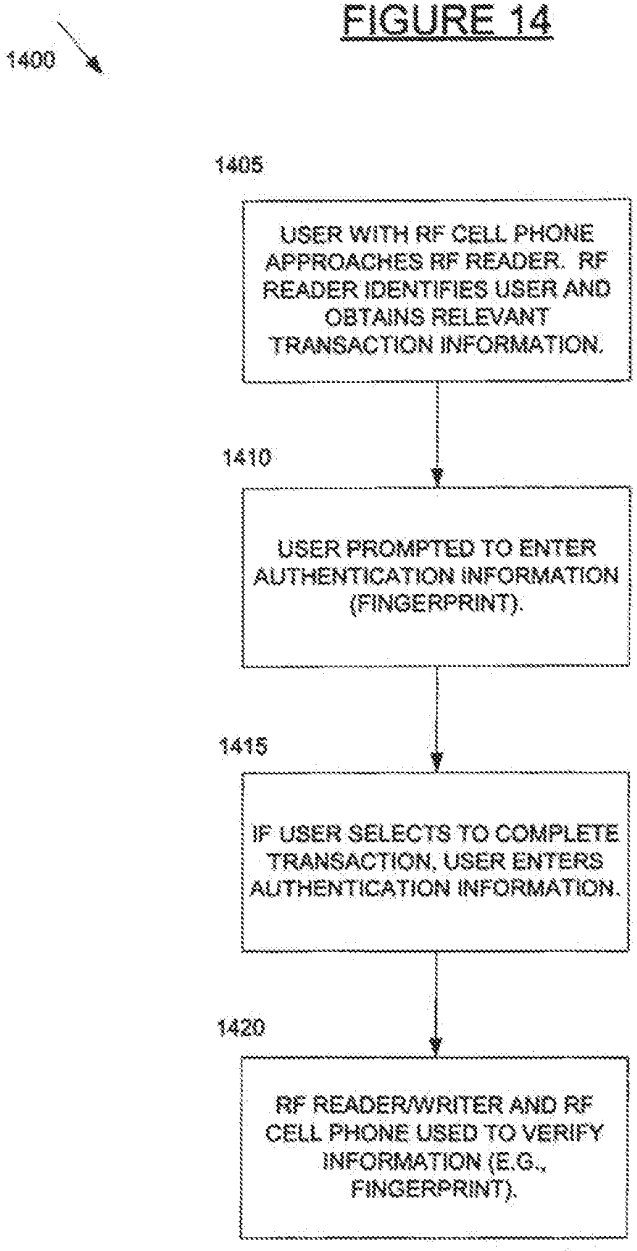

1400
1405
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION.
1410
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT).
1415
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION.
1420
RF READER/WRITER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

FIGURE 15

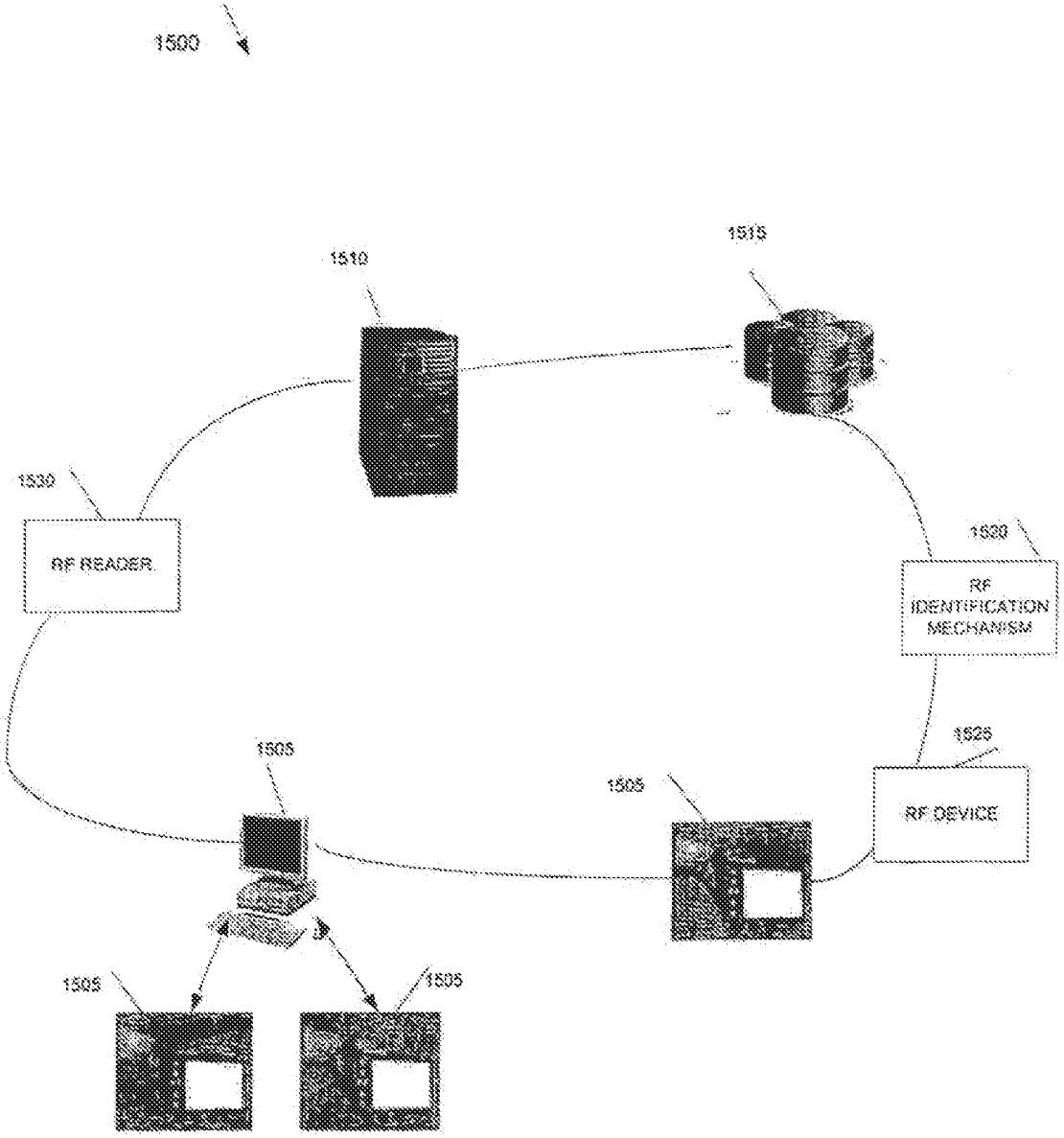

1500
1510
1515
1530
RF READER
1520
RF IDENTIFICATION MECHANISM
1525
RF DEVICE
1505
1505
1505
1505

FIGURE 16

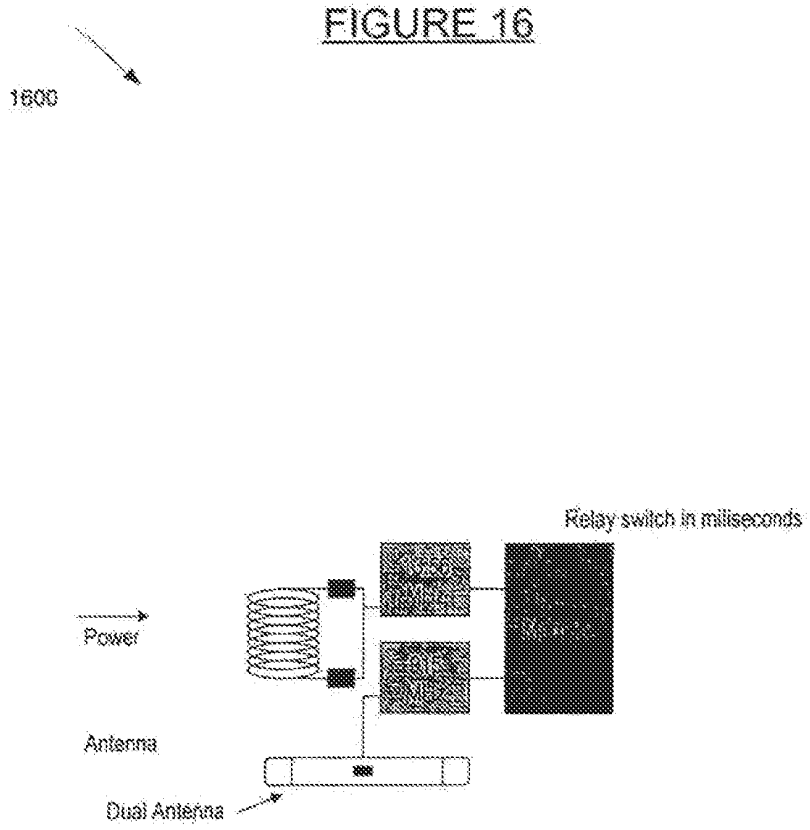

1600
Relay switch in miliseconds
Power
Antenna
Dual Antenna

FIGURE 17

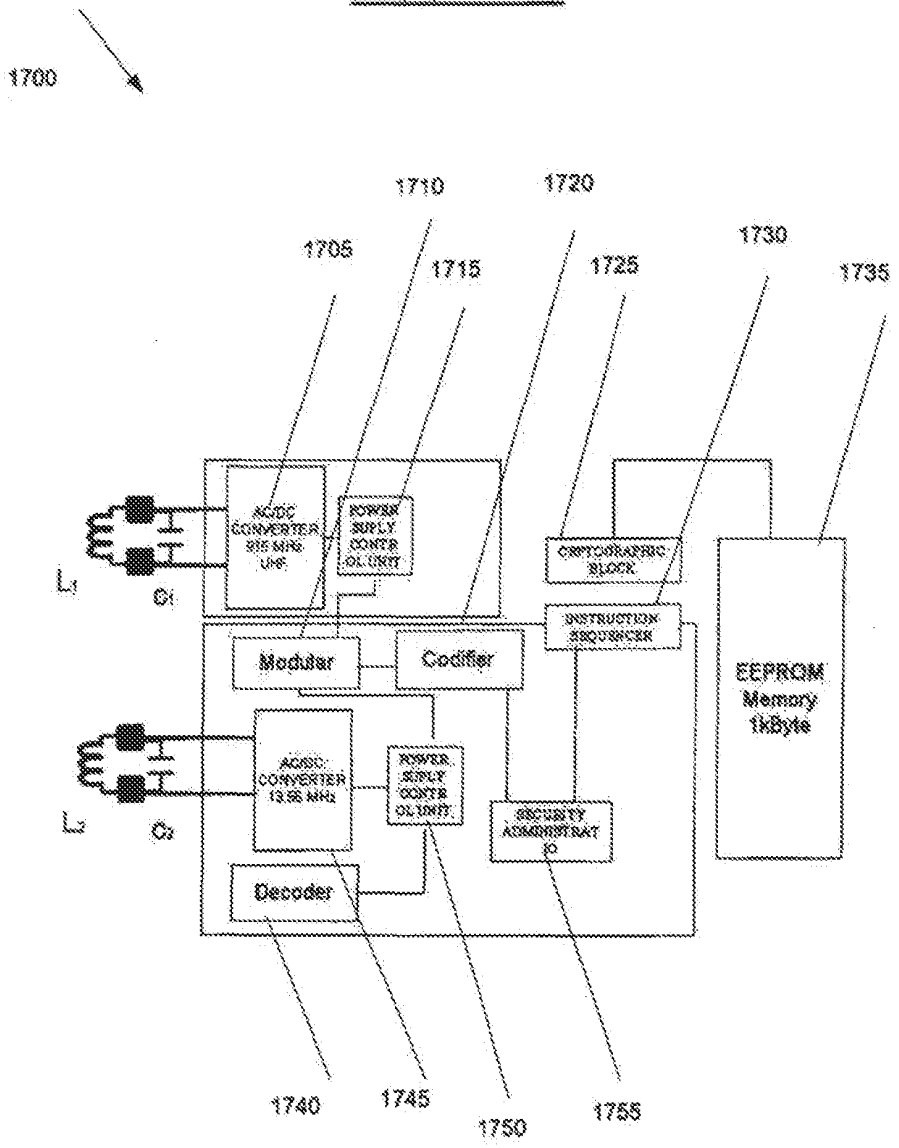

1700
1710
1720
1705
1715
1725
1730
1735
AC/DC CONVERTER 915 MHz Unit
POWER SUPPLY CONTROL UNIT
CRYPTOGRAPHIC BLOCK
INSTRUCTION SEQUENCER
Modulator
Codifier
EEPROM Memory 1kByte
L1
C1
AC/DC CONVERTER 13.56 MHz
POWER SUPPLY CONTROL UNIT
SECURITY ADMINISTRATOR
L2
C2
Decoder
1740
1745
1750
1755

FIGURE 18

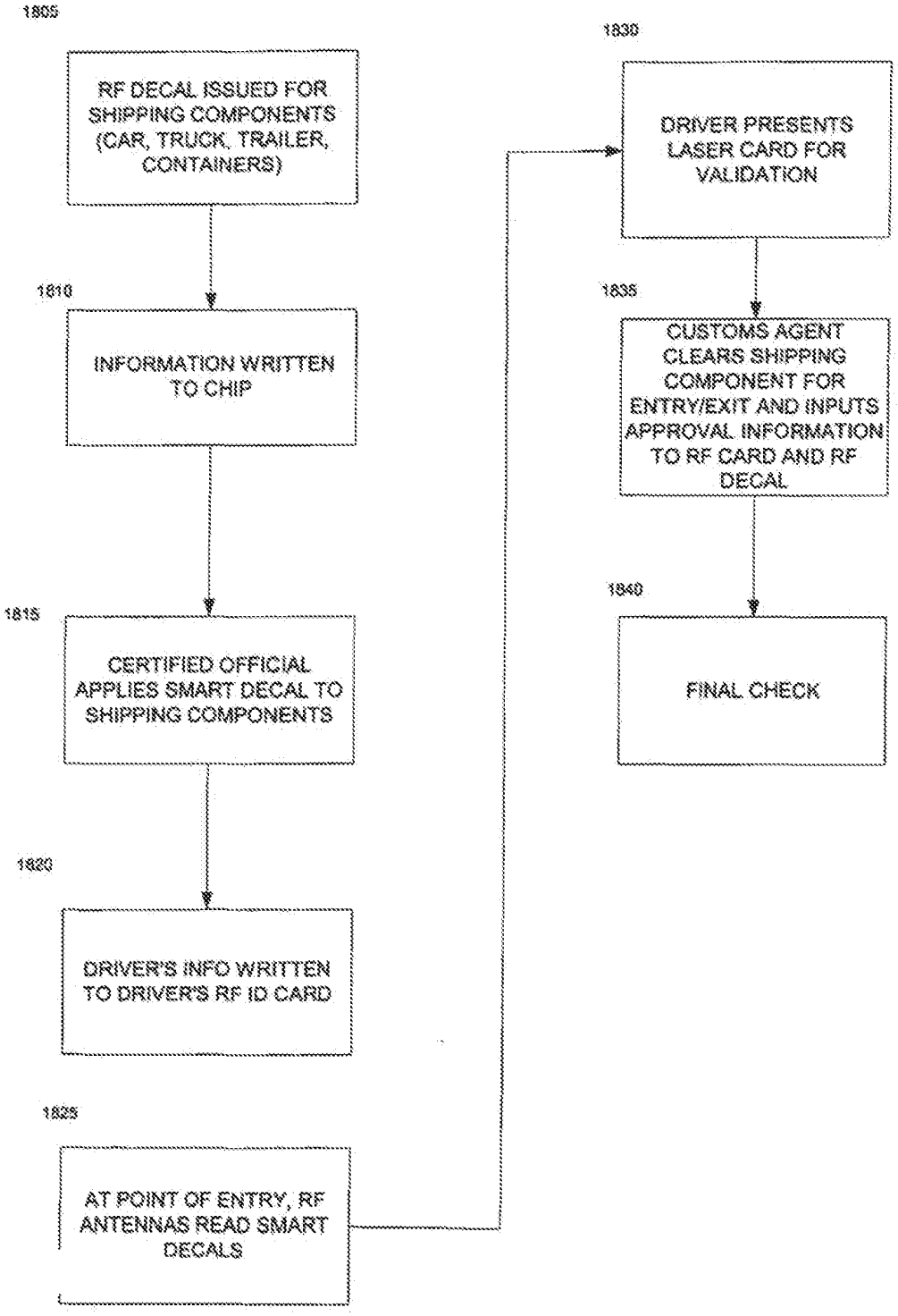

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS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

FIGURE 19

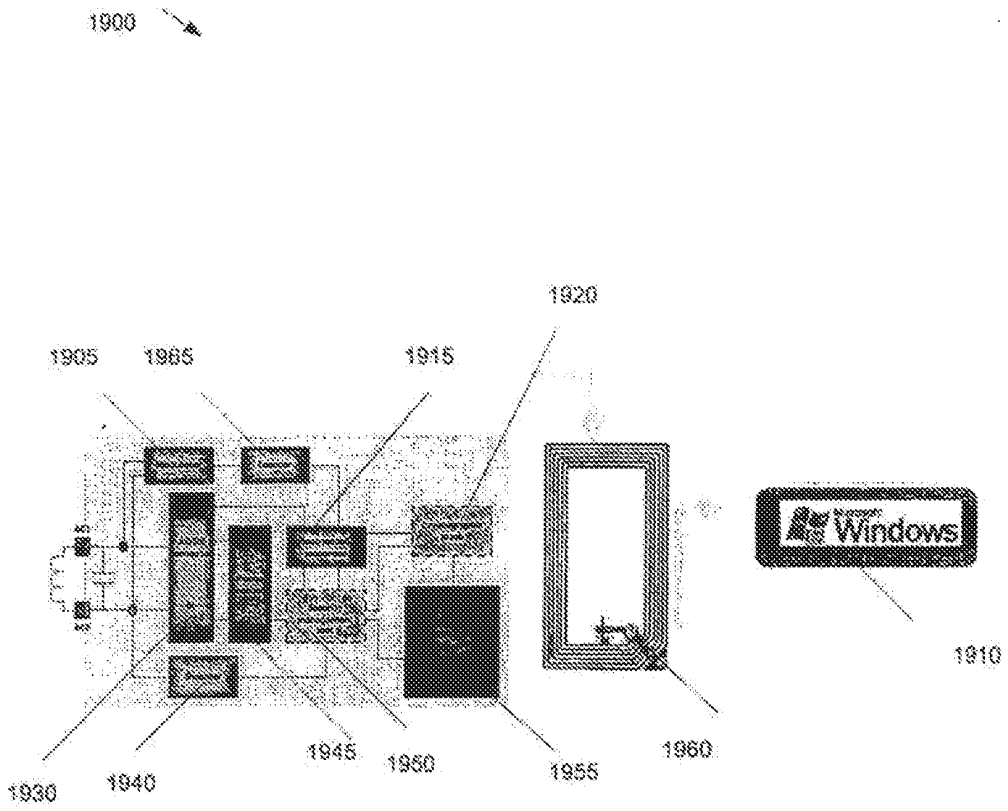
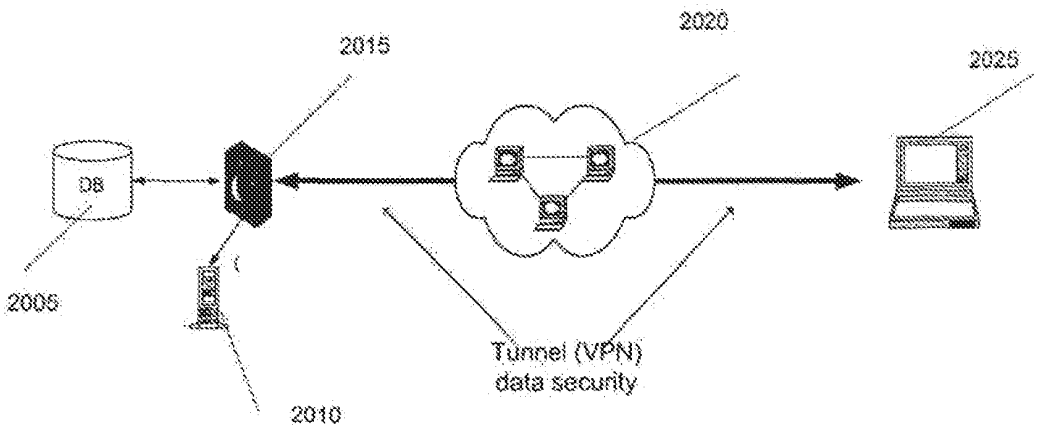

1900
1920
1905
1965
1915
Windows
1910
1930
1940
1945
1950
1955
1960

FIGURE 20



2100

FIGURE 21

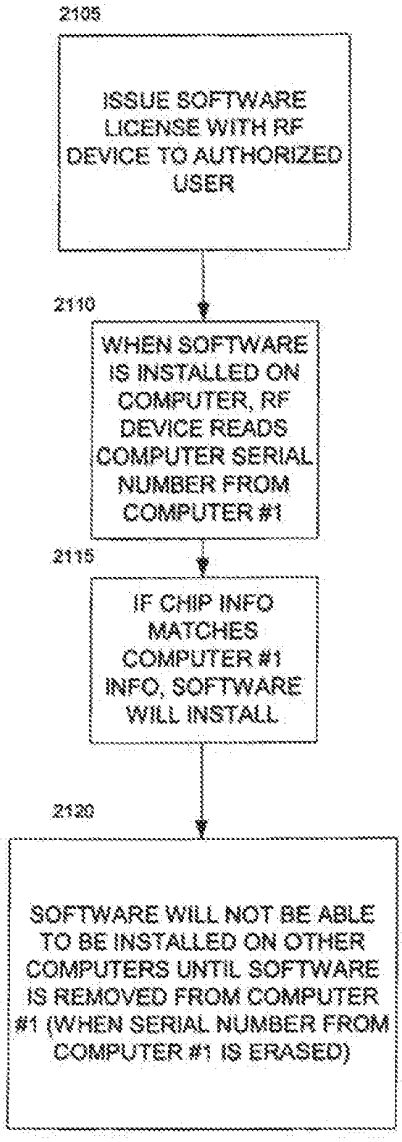


FIGURE 22

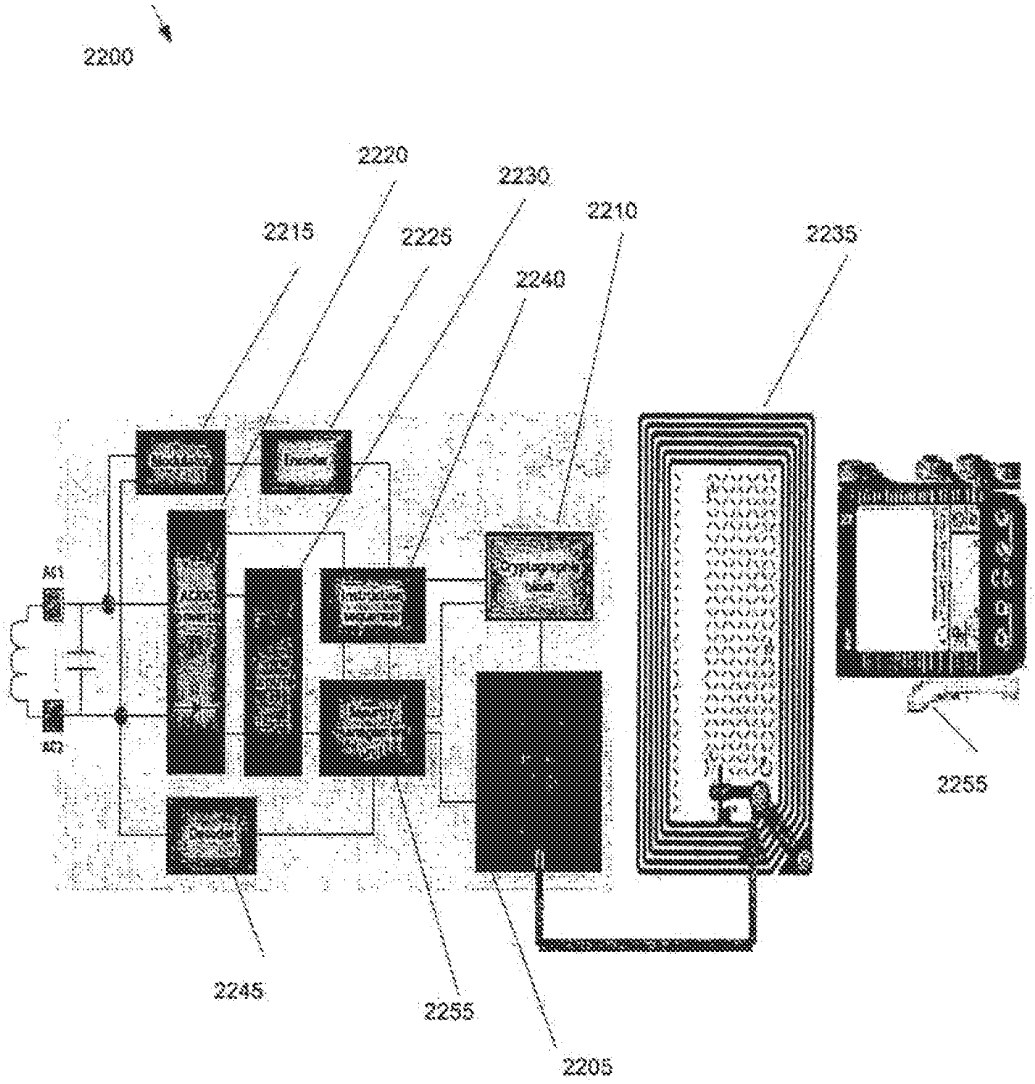
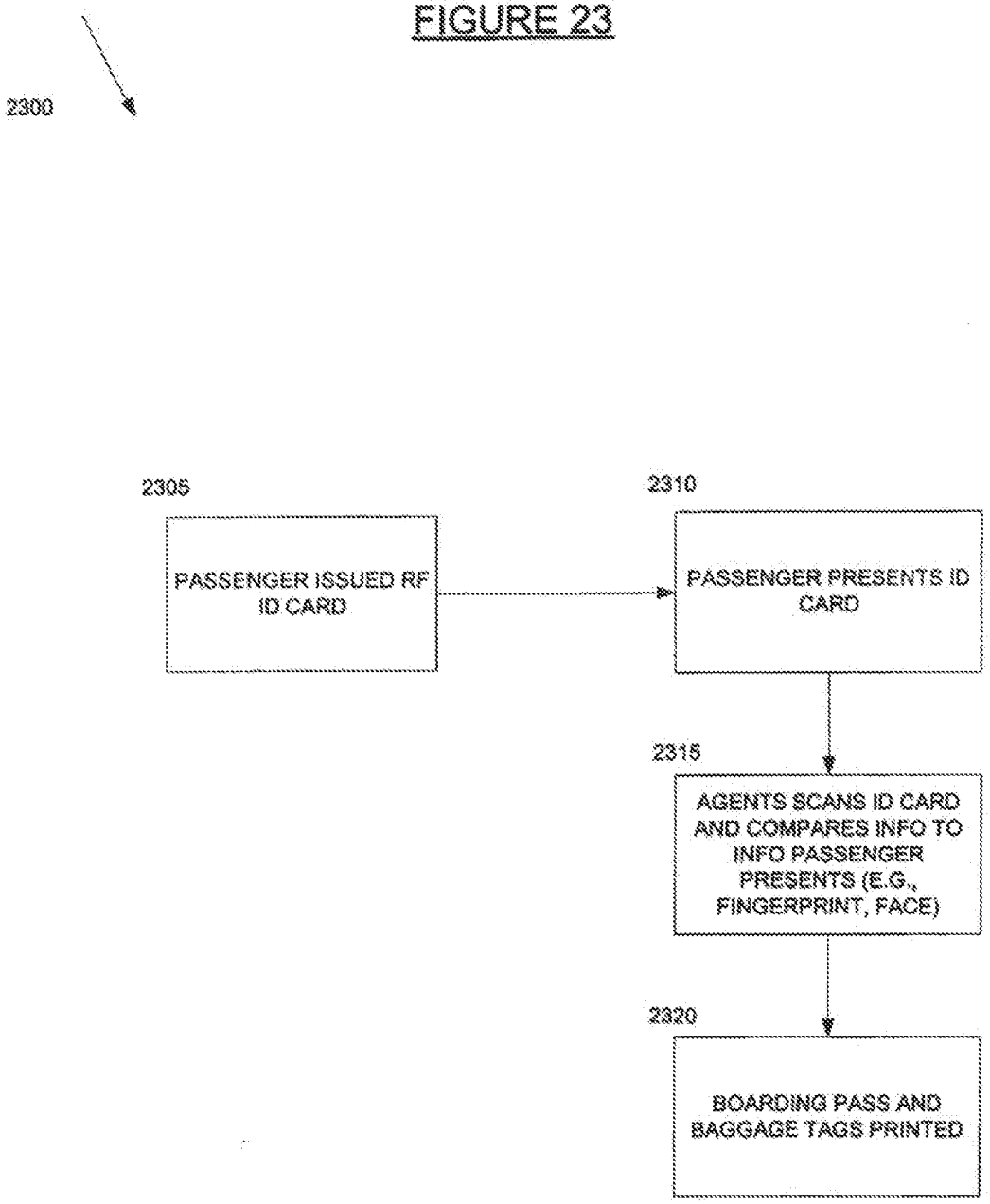


FIGURE 23


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

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

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

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

2. ☒ Claims Nos.: 3-48
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

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

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

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 3-48

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

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

INTERNATIONAL SEARCH REPORT

Interna plication No
PCT/IB 03/03702

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

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

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Li Zhang/cindy guido
Attorney Docket Number:	116546-660CT2

Filed as Large Entity

Filing Fees for Track I Prioritized Examination - Nonprovisional Application under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility application filing	1011	1	280	280
Utility Search Fee	1111	1	600	600
Utility Examination Fee	1311	1	720	720
Request for Prioritized Examination	1817	1	4000	4000
Pages:				
Claims:				
Miscellaneous-Filing:				
PROCESSING FEE, EXCEPT PROV. APPLS.	1830	1	140	140

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**5740**

Electronic Acknowledgement Receipt

EFS ID:	21680402
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Li Zhang/cindy guido
Filer Authorized By:	Li Zhang
Attorney Docket Number:	116546-660CT2
Receipt Date:	04-MAR-2015
Filing Date:	
Time Stamp:	20:46:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$5740
RAM confirmation Number	7034
Deposit Account	502075
Authorized User	ZHANG, LILY

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

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	TrackOne Request	116546_660CT2_Track_One_Form.PDF	119288 aab70e58a30266eaa9d38c351c26978a48c087a0	no	2
Warnings:					
Information:					
2	Drawings-only black and white line drawings	116546_660CT2_FIGURES.PDF	8267453 7897f89189d68f256b8e33066b002bf3281014b0	no	24
Warnings:					
Information:					
3		116546_6600C2_Specification_Track_One.PDF	261898 34398b88f42b9082d41136d687a057e2b1a73a32	yes	39

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	35
Claims	36	38
Abstract	39	39

Warnings:					
Information:					
4	Application Data Sheet	116546_660CT2_ADS.PDF	1561961 5d5671f56a77eca5587ad1a16b68178b1d2f11ce	no	8
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	116546_660CT2_IDS.PDF	614515 c5712ff3d8551e4ce3b78383b13c4c8038378e96	no	11
Warnings:					
Information:					

A U.S. Patent Number Citation is required in the Information Disclosure Statement (IDS) form. You may remove the form to add the required data in order to correct the Informational Message or if you chose not to, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.

6	Non Patent Literature	Anonymous_Security.pdf	173413 d75cb61523a2b6c9a1bb2509a01e0f46e5e7d20d	no	1
Warnings:					
Information:					
7	Non Patent Literature	Atmel.pdf	3746076 bfe124125d345ba7ab49937ff63aa0c06442ea80	no	12
Warnings:					
Information:					
8	Non Patent Literature	CCR.pdf	912554 a2bd35c7524be6b5ffe131e6edef5f549d55a77a	no	5
Warnings:					
Information:					
9	Foreign Reference	DE10042805A1.pdf	12644805 15185b18f8ef4d7216e6a390bdac05b6f68049fa	no	12
Warnings:					
Information:					
10	Foreign Reference	DE19608757A1.pdf	6243657 3e48af78b06995e4c9478d53a48ebeda79b7d8b0	no	6
Warnings:					
Information:					
11	Foreign Reference	EP0977145A2.pdf	5553821 b603626f49c6b57760f8e642c9acc5ae2730aa71	no	43
Warnings:					
Information:					
12	Foreign Reference	EP0993999A2.pdf	12611327 2c543c3aef63239bacf9e9cbb1ad0f814ac84cbb	no	10
Warnings:					
Information:					
13	Foreign Reference	ESR_101820330.pdf	317655 4cf3a9bd1f8846735118ed0bb4249bee9724f240	no	7
Warnings:					
Information:					
14	Non Patent Literature	Fancher.pdf	1969166 f6b7bd9680c8440ca470d201b40603bf72ca4d5c	no	7
Warnings:					
Information:					

15	Foreign Reference	JP2002042076A.pdf	6062031 aef9cae27c68146ab1bd10929b9bb097cc6dd2bf	no	9
Warnings:					
Information:					
16	Foreign Reference	JPOA_2004519130.pdf	263172 b9a532720615c437f12b4d24befa6d6e59b37b93	no	3
Warnings:					
Information:					
17	Non Patent Literature	Rakers.pdf	654929 82eeacb26ccd13a1c3d9e4734085e71a50f25e32	no	7
Warnings:					
Information:					
18	Foreign Reference	WO9843104.pdf	4029432 14b5aae0082493ceeafdf3e529347bcd5208fb21	no	38
Warnings:					
Information:					
19	Foreign Reference	WO2004006165.pdf	8287414 ccf962b3576495 01ea161f180ab49d88d34d635d	no	94
Warnings:					
Information:					
20	Fee Worksheet (SB06)	fee-info.pdf	38552 4cea45e8bf711be5201dcf8d11421ba7e6fb6a69	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	74333119	

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.

Electronic Acknowledgement Receipt

EFS ID:	21680402
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Li Zhang/cindy guido
Filer Authorized By:	Li Zhang
Attorney Docket Number:	116546-660CT2
Receipt Date:	04-MAR-2015
Filing Date:	
Time Stamp:	20:46:07
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$5740
RAM confirmation Number	7034
Deposit Account	502075
Authorized User	ZHANG, LILY

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

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	TrackOne Request	116546_660CT2_Track_One_Form.PDF	119288 aab70e58a30266eaa9d38c351c26978a48c087a0	no	2
Warnings:					
Information:					
2	Drawings-only black and white line drawings	116546_660CT2_FIGURES.PDF	8267453 7897f89189d68f256b8e33066b002bf3281014b0	no	24
Warnings:					
Information:					
3		116546_6600C2_Specification_Track_One.PDF	261898 34398b88f42b9082d41136d687a057e2b1a73a32	yes	39

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	35
Claims	36	38
Abstract	39	39

Warnings:					
Information:					
4	Application Data Sheet	116546_660CT2_ADS.PDF	1561961 5d5671f56a77eca5587ad1a16b68178b1d2f11ce	no	8
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	116546_660CT2_IDS.PDF	614515 c5712ff3d8551e4ce3b78383b13c4c8038378e96	no	11
Warnings:					
Information:					

A U.S. Patent Number Citation is required in the Information Disclosure Statement (IDS) form. You may remove the form to add the required data in order to correct the Informational Message or if you chose not to, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.

6	Non Patent Literature	Anonymous_Security.pdf	173413 d75cb61523a2b6c9a1bb2509a01e0f46e5e7d20d	no	1
Warnings:					
Information:					
7	Non Patent Literature	Atmel.pdf	3746076 bfe124125d345ba7ab49937ff63aa0c06442ea80	no	12
Warnings:					
Information:					
8	Non Patent Literature	CCR.pdf	912554 a2bd35c7524be6b5ffe131e6edef5f549d55a77a	no	5
Warnings:					
Information:					
9	Foreign Reference	DE10042805A1.pdf	12644805 15185b18f8ef4d7216e6a390bdac05b6f68049fa	no	12
Warnings:					
Information:					
10	Foreign Reference	DE19608757A1.pdf	6243657 3e48af78b06995e4c9478d53a48ebeda79b7d8b0	no	6
Warnings:					
Information:					
11	Foreign Reference	EP0977145A2.pdf	5553821 b603626f49c6b57760ff8e642c9acc5ae2730aa71	no	43
Warnings:					
Information:					
12	Foreign Reference	EP0993999A2.pdf	12611327 2c543c3aef63239bacf9e9cbb1ad0f814ac84cbb	no	10
Warnings:					
Information:					
13	Foreign Reference	ESR_101820330.pdf	317655 4cf3a9bd1f8846735118ed0bb4249bee9724f240	no	7
Warnings:					
Information:					
14	Non Patent Literature	Fancher.pdf	1969166 f6b7bd9680c8440ca470d201b40603bf72ca4d5c	no	7
Warnings:					
Information:					

15	Foreign Reference	JP2002042076A.pdf	6062031 aef9cae27c68146ab1bd10929b9bb097cc6dd2bf	no	9
Warnings:					
Information:					
16	Foreign Reference	JPOA_2004519130.pdf	263172 b9a532720615c437f12b4d24befa6d6e59b37b93	no	3
Warnings:					
Information:					
17	Non Patent Literature	Rakers.pdf	654929 82eeacb26ccd13a1c3d9e4734085e71a50f25e32	no	7
Warnings:					
Information:					
18	Foreign Reference	WO9843104.pdf	4029432 14b5aae0082493ceeafdf3e529347bcd5208fb21	no	38
Warnings:					
Information:					
19	Foreign Reference	WO2004006165.pdf	8287414 ccf962b3576495 01ea161f180ab49d88d34d635d	no	94
Warnings:					
Information:					
20	Fee Worksheet (SB06)	fee-info.pdf	38552 4cea45e8bf711be5201dcf8d11421ba7e6fb6a69	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	74333119	

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.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 03/24/2015

MNGUYEN SALE #00000003 Mailroom Dt: 03/04/2015 502075 14639034
01 FC : 1051 140.00 DA

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/639,034	03/04/2015	2683	1740	116546-660CT2	16	2

CONFIRMATION NO. 5934

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

FILING RECEIPT

OC000000074193719

Date Mailed: 03/26/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

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

Applicant(s)

NEOLOGY, INC., Poway, CA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 14/321,781 07/01/2014
which is a CON of 14/022,135 09/09/2013 PAT 8766772
which is a CON of 13/350,665 01/13/2012 PAT 8587436
which is a CON of 13/175,768 07/01/2011 PAT 8237568
which is a CON of 12/688,666 01/15/2010 PAT 8004410
which is a CON of 11/279,912 04/17/2006 PAT 7671746
which is a CON of 10/615,026 07/09/2003 PAT 7081819
which claims benefit of 60/394,241 07/09/2002

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 03/24/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/639,034**

Projected Publication Date: 07/02/2015

Non-Publication Request: No

Early Publication Request: No

Title

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Preliminary Class

340

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/639,034

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	280
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	600
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	16 minus 20 =	*			OR	x 80 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 420 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	1600

APPLICATION AS AMENDED - PART II

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

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

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-660CT2

CONFIRMATION NO. 5934

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

NOTICE

OC000000074193720

Date Mailed: 03/26/2015

INFORMATIONAL NOTICE TO APPLICANT

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

The item(s) indicated below are also required and should be submitted with any reply to this notice to avoid further processing delays.

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):
  Francisco Martinez de Velasco Cortina
  Manfred Rietzler

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED
MAR 30 2015
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.: 14/639,034

1. THE REQUEST FILED March 4, 2015 IS **GRANTED.**

The above-identified application has met the requirements for prioritized examination

A. ☒ for an original nonprovisional application (Track I).
B. ☐ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;
B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;
C. filing a **request for continued examination**;
D. filing a notice of appeal;
E. filing a request for suspension of action;
F. mailing of a notice of allowance;
G. mailing of a final Office action;
H. completion of examination as defined in 37 CFR 41.102; or
I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Brian W. Brown at 571-272-5338.

/Brian W. Brown/
[*Signature*]

Petitions Examiner, Office of Petitions
(Title)

U.S. Patent and Trademark Office
PTO-2298 (Rev. 02-2012)

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-660CT2	5934

27189 7590 05/29/2015

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
05/29/2015	ELECTRONIC

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

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

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

docketing@procopio.com
PTONotifications@procopio.com

Office Action Summary	Application No. 14/639,034	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/04/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-16* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-16* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *03/04/2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date *03/04/2015*.

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

4) ☒ Other: *Smart Card Technology Past Present and Future, Understanding the requirements of ISO IEC 14443, RFID Handbook Active Load Moduulations*.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Claims 1-16 have been examined in this application. This communication is the first action on the merits (FOAM). An Information Disclosure Statement (IDS), submitted 03/04/2015, has been considered.

Claim Rejections - 35 USC § 112

3. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 4-6, 10, and 13 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

5. Per claims 4-6, 10, and 13, the claims are directed to a point of sale (POS) terminal. Claims 1 and 10 are directed to a "A mobile device," see lines 2 on page 36 and line 10 on page 37. The claim limitations directed to other matters than a “mobile device” render the claims indefinite.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

8. JUDICIAL EXCEPTIONS TO SECTION 101

9. The Supreme Court held that the patent claims in Alice Corporation Pry. Ltd. v. CLS Bank International, el al. ("Alice Corp. ") are not patent-eligible under 35 U.S.C. § 101. 10. The Supreme Court made clear in Alice Corp. that it applies the framework set forth in Mayo Collaborative Services v. Prometheus Laboratories, Inc., 566 U.S. _ (2012) (Mayo), to analyze all claims directed to laws of nature, natural phenomena, and abstract ideas for subject matter eligibility under 35 U.S.C. § 101. This framework is currently being used by the USPTO to examine claims involving laws of nature, but had not been used for claims involving abstract ideas. Therefore, the following instructions differ from prior USPTO guidance in two ways:

10. 1) Alice Corp. establishes that the same analysis should be used for all types of judicial exceptions, whereas prior USPTO guidance applied a different analysis to claims with abstract ideas (Bilski guidance in MPEP 2106(11) (B)) than to claims with laws of nature (Mayo guidance in MPEP 2106.01).

11. 2) Alice Corp. also establishes that the same analysis should be used for all categories of claims (e.g., product and process claims), whereas prior guidance applied a different analysis to product claims involving abstract ideas (relying on tangibility in MPEP 2106(II) (A)) than to process claims (Bilski guidance).

12. ALICE V. CLS BANK: TWO-PART ANALYSIS

13. Following Alice Corp, all claims (product and process) having an abstract idea must be analyzed using the following two-part analysis set forth in Mayo. For additional guidance, see "2014 Interim Guidance on Patent Subject Matter Eligibility" December 16, 2014. This memorandum is located at:

14. http://www.gpo.gov/fdsys/pkg/FR-2014-12-16/pdf/2014-29414.pdf

15. and is publicly available at:

16. http://www.uspto.gov/patents/law/exam/interim .guidance subject matter eligibility.jsp

17. First, a determination whether the claim is directed to a judicial exception (i. e., abstract idea).

18. Examples of abstract ideas referenced in Alice Corp. include:

19. Fundamental economic practices;

20. Certain methods of organizing human activities;

21. [A]n idea of itself; and,

22. Mathematical relationships/formulas.

23. Second, a determination whether any element, or combination of elements, in the claim are sufficient to ensure that the claim amounts to significantly more than the judicial exception (i.e., the abstract idea) itself.

24. Limitations referenced in Alice Corp. that may be enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

25. Improvements to another technology or technical fields;

26. Improvements to the functioning of the computer itself;

27. Meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment.

28. Limitations referenced in Alice Corp. that are not enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

29. Adding the words "apply it" (or an equivalent) with an abstract idea, or mere instructions to implement an abstract idea on a computer;

30. Requiting no more than a genetic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry. See also, MPEP 2106(1).

31. Claims 1-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

32. Claim(s) 1-16 are directed to an abstract idea of payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency, which is a fundamental economic practice. The additional element(s) or combination of elements in the claim(s) other than the abstract idea(s) per se amount(s) to no more than significantly more than the abstract idea itself. The method steps amount to mere instructions to implement the idea on a generic computer structure that serves to perform generic computer functions that are well-understood, routine, and conventional activities previously known to the pertinent industry, do not add meaningful limitations to the method as they would be routinely used by those of

ordinary skill in the art in order to apply the correlation and yield predictable results. The functions performed by the "module(s)" appear to be conventional and routine carried out by a general purpose computer. Moreover, the claims do not appear to improve the functioning of the "module(s)" or effect an improvement in another technology or field; i.e. besides business method or solutions. The claims do not recite limitations beyond to provide grounds for an eligible application. One of ordinary skill in the art is able to readily understand the invention and carry out the recited limitations in order to apply the correlation using a generic computer or computers with instructions.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

34. Claims 1-6, 8-13, 15-16 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,163,771 to Walker et al. (herein after referred to as simply Walker), in view of U.S. Patent 6,848,048 to Holmes (herein after referred to as simply Holmes).

35. Per claim 1, Walker teaches all of the following limitations:

a. A mobile device, comprising [Abstract]:

b. Walker does not teach short range radio frequency (RF) circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to modify the teachings of Walker to include the teaching of Holmes to include a short range radio

frequency in motivation of establishing a communication protocol to transfer data (see ISO/IEC 14443).

c. Memory (memory) configured to store biometric authentication information (biometric information) and payment information (account number), wherein the biometric authentication information is associated with the payment information [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

d. a biometric module configured to read biometric information [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

e. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory (processor); and [Walker Col. 6, Ln. 14-35 and Figures 1-3 and 6].

f. a secure module configured to (processor) [Walker, Abstract]:

g. generate a key (generates a single use credit card number) when the biometric information read by the biometric reading device is successfully authenticated [Col. 6, Ln. 14-38 and Figures 1-3];

h. Walker does not explicitly teach encrypt the key and the payment information stored in memory [Col. 4, Ln. 5-21, Col. 6, Ln. 61-67, Col. 8, Ln. 9-36 and Figures 1-8]; however, Holmes teaches encrypt the key [...] [Abstract, Col. 1, Ln. 60-63, Col. 2, 34-38, Col. 4-5, Ln. 62-, 1-21]

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walked, to include the teachings of Holmes to encrypt the generated key in

motivation of increasing security measures during transfer of the key or single use credit card or information required to process a transaction. Furthermore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the payment information stored in the memory (specified amount of the transaction for example) along with the key before encrypting both in motivation of increasing security measures [Walker, Col. 8, Lines 8-36].

i. Walker teaches provide […] the encrypted key and payment information (single – use credit card number, which the payment information (account number) is embedded in) for use in a transaction (ability to send information between two parties, considered a transaction) [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Walker does not explicitly teach provide, via the short range RF circuitry (medium over which information may be transferred ... radio frequency "RF") […]; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to allow the transfer of the encrypted key via short range RF circuitry as defined by known standards (ISO/IEC 14443) in motivation of increasing security measures.

36. Per claims 2 and 11, Walker teaches wherein the biometric module is configured to read biometric information provided by a user to complete the transaction [Walker, Col. 5, Ln. 59-61 and Figures 1-3].

37. Per claims 3 and 12, Walker teaches wherein the payment information is associated with a primary account number (account number) [Col. 6, Ln. 14-35, 54-59, Col. 7, Ln. 27-36 and Figures 1-3 and 6].

38. Per claim 4, Walker teaches (merchant) [...] transmit the encrypted key and payment information to a central database [Col. 8, Ln. 33-60]

Walker does not explicitly teach wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device, and wherein the POS device is configured to receive the encrypted key and payment information from the secure module [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Holmes teaches wherein the secure module is configured to provide the encrypted key [...]to a point of sale (POS) device (cash register), and wherein the POS device is configured to receive the encrypted key [...] [Col. 2, Ln. 38-53, Figures 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to transmit the encrypted key to a point of sale terminal or cash register in motivation of completing the transaction.

Furthermore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the transfer of both the encrypted key and the payment information via RF to a point of sale terminal in motivation of increasing security measures in processing the transaction.

39. Per claims 5 and 13, Walker does not explicitly teaches wherein the POS device includes an RF reader; however, Holmes does [Col. 2, Ln. 38-53, Figures 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to insure that the POS includes an RF reader, in motivation of allowing the device to communicate with the POS.

40. Per claim 6, Walker teaches wherein the central database is configured to validate the key and the payment information [Abstract, Col. 8, Ln. 33-67 and Figures 1-9].

41. Per claims 8 and 15, Walker teaches wherein the payment information (account number) is stored in a memory accessible only by the secure module (central processor 101) [Col. 6-7, Ln. 61-, 1-3 and Figures 1-3].

42. Per claims 9 and 16, Walker does not explicitly teach wherein the short range RF circuitry comprises a radio frequency identification (RFID) device; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes in order to utilize radio frequency identification as defined by known standards (ISO/IEC 14443) in motivation of increasing security measures.

43. Per claim 10, Walker teaches

a. A system, comprising [Abstract]:

b. a mobile device, comprising [Abstract]:

c. Walker does not teach short range radio frequency (RF) circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to modify the teachings of Walker to include the teaching of Holmes to include a short range radio

frequency in motivation of establishing a communication protocol to transfer data (see ISO/IEC 14443).

d. memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

e. a biometric module configured to read biometric information [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

f. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and [Walker Col. 6, Ln. 14-35 and Figures 1-3 and 6]

g. a secure module configured to (processor) [Walker, Abstract]:

h. generate a key when the biometric information read by the biometric reading device is successfully authenticated encrypt the key and the payment information stored in memory; and [Col. 6, Ln. 14-38 and Figures 1-3];

i. Walker does not explicitly teach encrypt the key and the payment information stored in memory; however, Holmes teaches encrypt the key [...] [Abstract, Col. 1, Ln. 60-63, Col. 2, 34-38, Col. 4-5, Ln. 62-, 1-21]

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walked, to include the teachings of Holmes to encrypt the generated key in motivation of increasing security measures during transfer of the key or single use credit

card or information required to process a transaction. Furthermore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the payment information stored in the memory (specified amount of the transaction for example) along with the key before encrypting both in motivation of increasing security measures [Walker, Col. 8, Lines 8-36].

j. Walker teaches provide […] the encrypted key and payment information (single – use credit card number, which the payment information (account number) is embedded in) for use in a transaction (ability to send information between two parties, considered a transaction) [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Walker does not explicitly teach provide, via the short range RF circuitry (medium over which information may be transferred ... radio frequency "RF") […]; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to allow the transfer of the encrypted key via short range RF circuitry as defined by known standards (ISO/IEC 14443) in motivation of increasing security measures.

j. Walker does not explicitly teach a point of sale (POS) (cash register) device configured to; however, Holmes does [Col. 2, Ln. 38-53, Figures 1-3]:

It would have been obvious to one of ordinary skill in the art to combine the teaching of Walker to include the teaching of Holmes to include a POS device at a merchant in motivation of conducting transactions.

k. Walker teaches [...] secure module (processor) [...] [Abstract, Col. 8, Ln. 19-35 and Figure 1-3]

Walker does not explicitly teach receive [...] the encrypted key [...]; however, Holmes does, [Abstract, Col. 1, Ln. 60-63, Col. 2, 34-53, Col. 4-5, Ln. 62-, 1-21 and figures 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teaching of Holmes to include the receiving of the encrypted key by the POS (cash register) in motivation of processing the transaction through the RF communication interface with the user device.

Furthermore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include allowing the POS or register to receive the payment information (account number) along with the encrypted key in motivation of increasing security measures.

l. Walker teaches transmit, to a central database, the encrypted key and payment information [Col. 8, Ln. 33-60]; and

m. a central database configured to validate the key and the payment information [Abstract, Col. 8, Ln. 33-67 and Figures 1-9].

44. Claims 7 and 14 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Walker, in view of Holmes, as applied to claims 1 and 10 above, in further view of U.S. Patent Application Publication 2002/0112177 to Voltmer et al. (herein after referred to as simply Voltmer).

45. Per claims 7 and 14, Walker in view of Holmes do not explicitly teaches wherein the biometric authentication information is stored separately from the payment information [Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3]

Voltmer teaches storing separately a plurality of information [Paragraphs 009-0091 and Figures 12A and 12B].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the teachings of Voltmer to store the data in partitions or separately in motivation of increasing security measures or facilitating the upload of information from the memory.

Double Patenting

46. Claims 1-16 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claim1-16 of Pending Application Number 14/659502. Although the claims at issue are not identical, they are not patentably distinct from each other because all of the limitations are the same except for the instant Application reciting "generate a key when the biometric information read by the biometric reading device is successfully authenticated" whereas the Pending Application (14/659502) recites "generate a key when the biometric information read by the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory." Generating the key after authentication is requires that the biometric information is matched otherwise authentication is not possible; therefore the claims are not patentably distinct from each other.

Conclusion

47. The prior art made of record and not relied upon, see PTO-892, is considered pertinent to applicant's disclosure.

48. Examiner notes:

49. Smart cards or any mobile device, which incorporates an antenna to allow RFID communication with a terminal or Point of sale or another device is well described in "the RFID Handbook" which was published in March 1998 (http://rfid-handbook.de/the-book.html).

50. It is well known and routine in the art to conform to established standards, such as ISO/IEC 14443, in order to conduct a transaction and process the transaction using a contactless device. See attached reference ISO/IEC 14443.

51. Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on MON - FRI: 7:30AM-5PM EST Every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Hayes can be reached on (571)272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/
Patent Examiner, Art Unit 4128
05/16/2015

/JOHN HAYES/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 14/639,034	Applicant(s)/Patent Under Reexamination MARTINEZ DE VELASCO CORTI	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,163,771 A	12-2000	Walker et al.	705/18
*	B	US-6,848,048 B1	01-2005	Holmes, William S.	713/162
*	C	US-2002/0112177	08-2002	Voltmer et al.	713/200
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	RFID Handbook - Active Load Modulation
	V	Smart Card Technology Past Present and Future Mohammmed 2004
	W	Understanding the Requirements of ISO IEC 14443
	X	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	
	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/04/2015	Application Number	14639034 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/04/2015	Application Number	14639034 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	
(Not for submission under 37 CFR 1.99)	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

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

Receipt date: 03/04/2015	Application Number	14639034 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/04/2015	Application Number	14639034 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/04/2015	Application Number	14639034 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	
(Not for submission under 37 CFR 1.99)	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/04/2015	Application Number	14639034 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	
(Not for submission under 37 CFR 1.99)	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

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

FOREIGN PATENT DOCUMENTS Remove

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O./

Receipt date: 03/04/2015	Application Number	14639034 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	
(Not for submission under 37 CFR 1.99)	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

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

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

NON-PATENT LITERATURE DOCUMENTS **Remove**

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

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

EXAMINER SIGNATURE

Examiner Signature	/El Mehdi Oussir/	Date Considered	05/18/2015

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

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

Receipt date: 03/04/2015	Application Number	14639034 - GAU: 3685
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	
	Examiner Name	
	Attorney Docket Number	116546-660CT2

[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. /E.O./

UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 5934

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/639,034	03/04/2015 RULE	705	3685	116546-660CT2

APPLICANTS

NEOLOGY, INC., Poway, CA;

INVENTORS

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

**** CONTINUING DATA ***************************

This application is a CON of 14/321,781 07/01/2014
which is a CON of 14/022,135 09/09/2013 PAT 8766772
which is a CON of 13/350,665 01/13/2012 PAT 8587436
which is a CON of 13/175,768 07/01/2011 PAT 8237568
which is a CON of 12/688,666 01/15/2010 PAT 8004410
which is a CON of 11/279,912 04/17/2006 PAT 7671746
which is a CON of 10/615,026 07/09/2003 PAT 7081819
which claims benefit of 60/394,241 07/09/2002

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

03/24/2015

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /EL MEHDI OUSSIR/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	24	16	2

ADDRESS

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

TITLE

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

FILING FEE RECEIVED		
1740	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14639034	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC- SEARCHED		
Symbol	Date	Examiner
G06Q	5/8/2015	EO
H04L	5/8/2015	EO

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
705		5/8/2015	EO

SEARCH NOTES		
Search Notes	Date	Examiner
consulted Calvin Hewitt	5/15/2015	EO

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

/E.O./ Examiner.Art Unit 3685	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14639034	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

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

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

CLAIM		DATE								
Final	Original	05/18/2015								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L4	16	(biometric near1 data) near2 stored near2 (separately or different)	US-PGPUB; USPAT	OR	ON	2015/05/18 15:53
L5	5	"7911643"	US-PGPUB; USPAT	OR	ON	2015/05/18 15:59
L7	0	(separatly near1 stor$3) with data	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
L8	12789	(stor$3 near1 data) with separately	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
L9	1434	8 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
L10	1011	9 and ((information or data) near4 (separately))	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
L14	919	10 and (memory)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:07
L18	0	14 and (stor$3 near4 saperately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:08
L19	498	(authentication near4 stor$3 near4 separately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:13
L20	34	19 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:16
L21	48796	(stor$4 near3 information separately) same (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
L23	29064	(stor$4 near3 information separately) with (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
L24	5880	23 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
L25	51	24 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:26
L26	1	"20020112177"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:32
L27	1	"20020077993"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:40
S1	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:26
S2	1	("6163771").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:27

5/18/2015 5:13:12 PM
C:\Users\eoussir\Documents\EAST\Workspaces\14639034_Mobile device RFID transaction biometric POS.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-660CT2

CONFIRMATION NO. 5934

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

PUBLICATION NOTICE

OC000000076075212

Title:SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Publication No.US-2015-0186884-A1
Publication Date:07/02/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

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	14/639,034
Filing Date	March 4, 2015
First Named Inventor	Francisco Martinez de Velasco Cortina
Title	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

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 0651-0051
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

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 Acknowledgement Receipt

EFS ID:	23069696
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Noel C. Gillespie/cindy guido
Filer Authorized By:	Noel C. Gillespie
Attorney Docket Number:	116546-660CT2
Receipt Date:	30-JUL-2015
Filing Date:	04-MAR-2015
Time Stamp:	13:43:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	Declarations_signed_116546_660CT2.PDF	387615 2a2c74f6aa3fe47a994546419a9f61901715b63e	no	2

Warnings:	
Information:	

2	Power of Attorney	POA_signed_116546_660CT2.PDF	960556 6788b0be1fd6ac007fe3f6127ce5500025fa6390	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	1348171

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

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

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

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

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/639,034

filed on March 4, 2015.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Francisco Martinez de Velasco Cortina Date (Optional): 7/7/2015

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 TRANSACTIONAL SOLUTIONS

As the below named inventor, I hereby declare that:

This declaration is directed to:

☐ The attached application, or

☒ United States application or PCT international application number 14/639,034

filed on March 4, 2015.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Manfred 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.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-660CT2

CONFIRMATION NO. 5934

POA ACCEPTANCE LETTER

27189
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

OC000000076748741

Date Mailed: 08/10/2015

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 07/30/2015.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/ltaba/

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	March 4, 2015	Francisco Martinez de Velasco Cortina	116546-660CT2	5934

EXAMINER	
OUSSIR, EL MEHDI	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
November 30, 2015	EFS WEB

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

RESPONSE TO NON-FINAL OFFICE ACTION

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

Commissioner:

In response to the Non- Final Office Action dated May 29, 2015, Applicant submits the present communication. Allowance of the above identified application is respectfully requested in view of the following submission, where:

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

REMARKS begin on page 4 of this paper.

LISTING OF CLAIMS

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

LISTING OF CLAIMS:

1. (Original) A mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

a biometric module configured to read biometric information;

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

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is successfully authenticated;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

2. (Original) The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

3. (Original) The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. (Currently Amended) The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device~~, and wherein the POS device is configured to receive the encrypted key and payment information from the secure module, and transmit the encrypted key and payment information to a central database~~.

5. (Canceled)

6. (Canceled)

7. (Original) The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. (Original) The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.

9. (Original) The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. (Original) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

a biometric module configured to read biometric information;

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

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is successfully authenticated

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

a point of sale (POS) device configured to:

receive, from the secure module, the encrypted key and payment information; and

transmit, to a central database, the encrypted key and payment information; and

a central database configured to validate the key and the payment information.

11. (Original) The system of claim 10, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

12. (Original) The system of claim 10, wherein the payment information is associated with a primary account number.

13. (Original) The system of claim 10, wherein the POS device includes an RF reader.

14. (Original) The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. (Original) The system of claim 10, wherein the payment information is stored in a memory accessible only by the secure module.

16. (Original) The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

REMARKS

The present communication is in response to the Non-Final Office Action dated May 29, 2015. Claims 5-6 have been canceled. Claim 4 has been amended to clarify the subject matter regarded as the invention. No new matter has been added. Reconsideration and allowance are respectfully requested for all pending Claims 1-4 and 7-16.

Double Patenting

Claims 1-16 have been provisionally rejected on the ground of non-statutory obviousness-type double patenting as being unpatentable over Claims 1-16 of co-pending Application No. 14/659,502. Upon the indication of allowable subject matter, and provided the double patenting rejection is still maintained and pertinent with respect to the otherwise allowable claims, Applicant will submit a terminal disclaimer to obviate that double patenting rejection. Accordingly, Applicant requests that the provisional double patenting rejection be held in abeyance pending the indication of allowable subject matter.

Claim Rejections – 35 U.S.C. § 112, Second Paragraph

Claims 4-6 and 10 have been amended in a manner that is believed to overcome the Examiner's rejection of the claims under 35 U.S.C. § 112, second paragraph.

The Examiner has rejected Claim 13 under 35 U.S.C. § 112, second paragraph. The rejection is respectfully traversed. Claim 10 is directed towards a system that includes a point of sale (POS) device. As such, Claim 13 is not rendered indefinite by reciting to matters directed towards the POS device. Accordingly, Applicant respectfully request withdrawal of the rejection with respect to Claim 13.

Claim Rejections- 35 U.S.C. § 101

The Examiner has rejected Claims 1-16 under 35 U.S.C. § 101 as being directed toward a judicial exception. Specifically, the Examiner purports that Claims 1-16 are directed towards the abstract idea of "using a mobile device to complete [a] transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency," which the Examiner categorizes as a fundamental economic practice. (Office Action,

at p. 5). The Examiner further states that "additional element(s) or combination of elements in the claim(s) other than the abstract idea(s) per se amount(s) to no more than significantly more than the abstract idea itself." (Office Action, at p. 5). Applicant respectfully disagrees with the Examiner's analysis and conclusion, particularly in light of *July 2015 Update: Subject Matter Eligibility* (July Update), which the Office has published to supplement the *2014 Interim Guidance on Subject Matter Eligibility* (2014 IEG).

The July Update clarified several key aspects of the two-part *Mayo* test that the Supreme Court adopted in *Alice Corp. v. CLS Bank.* First, with respect to the abstract idea inquiry (i.e. first step of the *Mayo* test), the July Update echoes the 2014 IED and urges comparison to concepts already found to be abstract in case law precedent. (July Update, at p. 3). In fact, the July Update insists that "a claimed concept is not identified as an abstract idea unless it is similar to at least one concept that the courts have identified as an abstract idea." (July Update, at p. 3, emphasis added). Even if the Examiner's description of the claimed concept is assumed to be correct, "using a mobile device to complete [a] transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency" is not similar to any of the concepts identified as abstract ideas in earlier cases.

The Examiner categorized the claimed concept as a fundamental economic practice. Yet the July Update defines fundamental economic practices to as foundational or basic practices that are analogous to abstract ideas that have been identified in previous court cases. Specifically, judicial precedents indicate that creating a contractual relationship, hedging, and mitigating settlement risks are abstract ideas that fall into the category of fundamental economic practices. By contrast, Claims 1-16 are set forth a mechanism for securitizing the electronic payment information provided to complete a sales transaction, which bears no similarity to creating a contractual relationship, hedging, or mitigating settlement risks. As such, contrary to the Examiner's assertion, Claims 1-16 are not directed toward an abstract idea.

However, even assuming *arguendo* that securitizing electronic payment information is an abstract idea, Claims 1-16 recite additional elements that amount to significantly more than the abstract idea. With respect to the significantly more inquiry (i.e., second step of the *Mayo* test),

the July Update instructs that "examiners should rely on what the courts have recognized, or those in the art would recognize, as elements that are well-understood, routine, and conventional." (July Update, at p. 7, emphasis added). Notably, independent Claims 1 and 10 recite specialized hardware that is not mere generic computer components or a general purpose computer. For example, independent Claims 1 and 10 each recite a biometric module configured to read biometric information and an authentication module configured to authenticate biometric information. Independent Claims 1 and 10 each further recite a secure module configured generate a key and encrypt the key and payment information in response to a successful authentication of the biometric information, and a short range radio frequency (RF) module configured to transmit the encrypted key and payment information.

But the July Update also stresses that a claim reciting a generic computer component performing a generic computer function is not *per se* patent ineligible. (July Update, at p. 7). To further clarify computer functions that are "well understood, routine, and conventional" when claimed in a merely generic manner, the July Update provides the following examples:

- Performing repetitive calculations,
- Receiving, processing, and storing data,
- Electronically scanning or extracting data from a physical document,
- Electronic recordkeeping,
- Automated mental tasks, and
- Receiving or transmitting data over a network, e.g., using the Internet to gather data.

Thus, even if assuming *arguendo* that Claims 1-16 set forth generic computer components, the claimed elements and functions are beyond those recognized by the courts as being well-understood, routine or conventional. Specifically, independent Claims 1 and 10 each recite reading and authenticating biometric information. Independent Claims 1 and 10 each further recite generating a key and encrypting the key and payment information in response to successfully authenticating the biometric information. In addition, the encrypted key and payment information are provided using short range RF circuitry. Accordingly, with reference to the foregoing list of judicially recognized "well understood, routine, and conventional" computer functions, Applicant respectfully submits that the claimed mechanism for securitizing electronic

payment information provided to complete a transaction is not what the courts would recognize as well understood, routine, or conventional.

Furthermore, Applicant respectfully submits that the claimed concept is also beyond what those in the art would consider to be well understood, routine, and conventional. Contrary to the Examiner's assertion, the claims do recite an improvement to another technology or technical field besides business method or solutions. Specifically, conventional means of transmitting payment information are unsecured and susceptible to malicious interlopers. By contrast, Claims 1-16 sets forth a mechanism that ensures the security of payment information when such information is provided to complete a sales transaction. For instance, biometric information is required to be successfully authenticated prior to encryption and provision of payment information along with a key. As such, even if assuming that the concept claimed in Claims 1-16 are directed toward an abstract idea, Claims 1-16 recite elements that amounts to significantly more than the abstract idea.

For at least the foregoing reasons, Applicant respectfully requests that the Examiner's rejections of Claims 1-16 under 35 U.S.C. § 101 be withdrawn.

Claim Rejections - 35 U.S.C. § 103

The Examiner has rejected Claim 1-6, 8-13, and 15-16 as being unpatentable over Walker et al. (U.S. Patent No. 6,163,771) in view of Holmes (U.S. Patent No. 6,848,048). The remaining claims stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Walker, Holmes, and Votmer et al. (U.S. Pub. No. 2002/0112177). The rejections are respectfully traversed.

According to the Examiner, with the exception of the short range radio frequency (RF) circuitry, Walker discloses all of the limitations set forth in independent Claims 1 and 10. Applicant respectfully disagrees. First, to the extent that Walker discloses a biometric interface, biometric information is used to control access to a device such as a smartcard. For example, Walker states that "the device may include a biometric interface, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint." (Walker, at 5:58-61, emphasis added). Contrastingly, independent Claims 1 and 10 each recite that "the biometric information

is associated with the payment information." Moreover, biometric information must be successfully authenticated in order for a secure module to "generate a key […]; encrypt the key and payment information […]; and provide […] the encrypted key and payment information for use in a transaction." Walker does not associate biometric information with payment information. Walker further does not use biometric information to control the generation, encryption, and transmission of a key and payment information.

Second, instead of automatically generating a key upon successful authentication of the biometric information as set forth in each of independent Claims 1 and 10, Walker requires the cardholder to request generation of a single-use credit card information after the cardholder has gained access to the device. According to Walker, "the cardholder first inputs his PIN or biometric data to access the device […]. If access is granted, the device responds by querying the cardholder on display whether it should generate a single-use credit card number […]. The cardholder responds by requesting generation of a credit card number (for example, by keying "YES")." (Walker, at 6:18-25, emphasis added). Thus, Walker does not teach or suggest "generat[ing] a key when the biometric information read by the biometric reading device is successfully authenticated; encrypt[ing] the key and the payment information stored in memory; and provid[ing], via the short range RF circuitry, the encrypted key and payment information for use in a transaction," as recited in each of independent Claims 1 and 10.

In addition, Walker describes generating a single-use credit card number, which "is distinct from the unchanging account number identifying the particular cardholder." (Walker, at 6:66-7:1). The single-use credit card number is formed by concatenating an encrypted nonce, an initialization vector, and the account number. Thus, contrary to the Examiner's rejection, Walker does not teach or suggest "provid[ing…] the encrypted key and payment information for use in a transaction," as set forth in independent Claims 1 and 10. As such, neither Walker nor Holmes, whether considered independently or in combination, disclose "memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information; a biometric module configured to read biometric information; an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory;

and a secure module configured to: generate a key when the biometric information read by the biometric reading device is successfully authenticated; encrypt the key and the payment information stored in memory; and provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction," as set forth in independent Claims 1 and 10.

For at least the foregoing reasons, independent Claims 1 and 10 are believed to be allowable. The remaining claims depend, either directly or indirectly, on the aforementioned independent claims and are therefore believed to be allowable for the same reasons described above.

CONCLUSION

For all the foregoing reasons, allowance of pending claims 1-4 and 7-16 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: November 30, 2015

/li zhang/
Li Zhang
Reg. No. 70,902

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

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Li Zhang/cindy guido
Attorney Docket Number:	116546-660CT2

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
		Total in USD ($)		**1400**

Electronic Acknowledgement Receipt

EFS ID:	24221293
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Li Zhang/cindy guido
Filer Authorized By:	Li Zhang
Attorney Docket Number:	116546-660CT2
Receipt Date:	30-NOV-2015
Filing Date:	04-MAR-2015
Time Stamp:	21:21:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1400
RAM confirmation Number	11411
Deposit Account	502075
Authorized User	ZHANG, LILY

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

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		response_to_NFOA.PDF	175342 8d17539b211d152233d36ecabd32be795d5b3871	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	4
	Applicant Arguments/Remarks Made in an Amendment	5	11

Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30783 d1c8e2a449ea8baadb124c36fb8f032257b6dc23	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	206125		

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.

Electronic Acknowledgement Receipt

EFS ID:	24221293
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Li Zhang/cindy guido
Filer Authorized By:	Li Zhang
Attorney Docket Number:	116546-660CT2
Receipt Date:	30-NOV-2015
Filing Date:	04-MAR-2015
Time Stamp:	21:21:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$1400
RAM confirmation Number	11411
Deposit Account	502075
Authorized User	ZHANG, LILY

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

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

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

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		response_to_NFOA.PDF	175342 8d17539b211d152233d36ecabd32be795d5b3871	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	4
	Applicant Arguments/Remarks Made in an Amendment	5	11

Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30783 d1c8e2a449ea8baadb124c36fb8f032257b6dc23	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	206125		

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

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

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

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/639,034	Filing Date 03/04/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	11/30/2015	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 14	Minus	** 20	= 0	X $80 =	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $420 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

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

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

LIE
/POLIN ANG/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-660CT2	5934

27189 7590 12/30/2015

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
12/30/2015	ELECTRONIC

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

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

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

docketing@procopio.com
PTONotifications@procopio.com

Office Action Summary	Application No. 14/639,034	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/30/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-4 and 7-16* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-4 and 7-16* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *03/04/2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. This communication is **a Final Office action** in response to Applicant's amended claim 4 on 11/30/2015, in response to Examiner's Non-Final communication on 05/29/2015.

3. Claims 5-6 have been cancelled. Claims 1-16 have been examined in this application. No new information disclosure statement (IDS) has been submitted.

Response to Arguments

4. Applicant's arguments, filed 11/30/2015, with respect to Double Patenting have been considered. The rejection will be held in abeyance pending the indication of allowable subject matter. Applicant will file a terminal disclaimer to obviate the rejection upon the indication of allowable subject matter and provided the double patenting rejection is still maintained and pertinent with respect to the otherwise allowable claims.

5. Applicant's arguments, filed 11/30/2015, with respect to Claim Rejections under 35 U.S.C. §112 with regards to claims 4-6 and 10 have been fully considered and are persuasive; therefore, the rejection in regards to claims 4 and 10 (5-6 have been cancelled) have been withdrawn.

6. Applicant's arguments, filed 11/30/2015, with respect to Rejections under 35 U.S.C. §101 have been fully considered but they are not persuasive. Applicant argues:

> **The Examiner categorized the claimed concept as a fundamental economic practice. Yet the July Update defines fundamental economic practices to as foundational or basic practices that are analogous to abstract ideas that have been identified in previous court cases. Specifically, judicial precedents indicate that creating a contractual relationship,**

hedging, and mitigating settlement risks are abstract ideas that fall into the category of fundamental economic practices. By contrast, Claims 1-16 are set forth a mechanism for securitizing the electronic payment information provided to complete a sales transaction, which bears no similarity to creating a contractual relationship, hedging, or mitigating settlement risks. As such, contrary to the Examiner's assertion, Claims 1-16 are not directed toward an abstract idea.

Notably, independent Claims 1 and 10 recite specialized hardware that is not mere generic computer components or a general purpose computer. For example, independent Claims 1 and 10 each recite a biometric module configured to read biometric information and an authentication module configured to authenticate biometric information. Independent Claims 1 and 10 each further recite a secure module configured generate a key and encrypt the key and payment information in response to a successful authentication of the biometric information, and a short range radio frequency (RF) module configured to transmit the encrypted key and payment information.

But the July Update also stresses that a claim reciting a generic computer component performing a generic computer function is not per se patent ineligible. (July Update, at p. 7). To further clarify computer functions that are "well understood, routine, and conventional" when claimed in a merely generic manner, the July Update provides the following examples:

*** Performing repetitive calculations, * Receiving, processing, and storing data, * Electronically scanning or extracting data from a physical document, * Electronic recordkeeping, * Automated mental tasks, and * Receiving or transmitting data over a network, e.g., using the Internet to gather data.**

Thus, even if assuming arguendo that Claims 1-16 set forth generic computer components, the claimed elements and functions are beyond those recognized by the courts as being well-understood, routine or conventional. Specifically, independent Claims 1 and 10 each recite reading and authenticating biometric information. Independent Claims 1 and 10

each further recite generating a key and encrypting the key and payment information in response to successfully authenticating the biometric information. In addition, the encrypted key and payment information are provided using short range RF circuitry. Accordingly, with reference to the foregoing list of judicially recognized "well understood, routine, and conventional" computer functions.

7. The Examiner respectfully disagrees with the Applicant's arguments. Based on the latest guidelines issued in July 2015, the claims do not contain recitations which amount to significantly more. The claims merely recite a secure way of conducting a transaction utilizing a mobile device which generates a key, encrypts it, and provides the key using a form of communication in order to settle the transaction. The key is generated once the user has supplied biometric information to the mobile device and the device authenticates the biometric data of the user based on stored biometric data. The claimed limitations are argued to recite significantly more because the device is able to read and authenticate the data, the device generating the key automatically, and encrypting the key before providing the key using RF circuitry. Such limitations result in no more than validation of data information and transmission of such data in order to settle a transaction, which does not result in significantly more. All of the limitations recited can simply be carried out utilizing a generic computer / device with executable instructions and any form of communication that is known in the industry including NFC, Bluetooth ®, etc. The simple generation of the key can be performed either by the user requesting the key to be generated after authentication or by the mobile device automatically generating the key; either way the result is the same and such a difference does not result in significantly more since it would be obvious to automate something that is done manually (see In re Venner, 120 USPQ 192,–it has been held that broadly providing a mechanical or automatic

means to replace manual activity which has accomplished the same result involves only routine skill in the art).

8. The guidelines clearly recite that the Examiner may rely on "on the knowledge generally available to those in the art, on the case law precedent, on applicant's own disclosure, or on evidence." As a result, the Examiner has clearly noted that the claims do not amount to significantly more than the abstract idea because one of ordinary skill in the art would readily understand the claim limitations to readily implement them using a generic mobile device or computer with executable code.

9. The courts consider the determination of whether a claim is eligible… to be a question of law. Accordingly, courts do not rely on evidence that a claimed concept is a judicial exception, and in most cases resolve the ultimate legal conclusion on eligibility without making any factual findings. Such cases include, *Alice Corp., Myriad, Mayo, Bilski, Diehr, Flook and Benson.*

10. Also, the Interim Guidelines, see page 3 of "subject matter eligibility," recite that "judicial exceptions need not be old or long-prevalent, and that even newly discovered judicial exceptions are still exceptions, despite their novelty… [the] Supreme Court's cited rationale for considering even "just discovered" judicial exception as exceptions stems from the concern that "without this exception, there would be considerable danger that the grant of patents would 'tie up' the use of such tools and thereby 'inhibit future innovation premised upon them.'"

In conclusion, the claims as a whole merely recite a secure method of authenticating a transaction between two entities utilizing a mobile device, which is a fundamental economic practice. One of ordinary skill in the art would utilize a generic computer or device, input executable code and result at the instant claims; thus rendering the claims **not** patent eligible.

Moreover, the claims do not appear to improve the functioning of the system, device / computer, or effect an improvement in another technology or field; i.e. besides business method or solutions. Furthermore, the steps of capturing user data, generating the key, and sending the encrypted key to settle a transaction do not add a meaningful limitation to the claimed invention as they would be routinely used by those of ordinary skill in the art in order to apply the correlation.

11. Applicant's arguments, filed 11/30/2015, with respect to Rejections under 35 U.S.C. §103 have been fully considered but they are not persuasive. The applicant argues

> **biometric information must be successfully authenticated in order for a secure module to "generate a key [...]; encrypt the key and payment information [...]; and provide [...] the encrypted key and payment information for use in a transaction." Walker does not associate biometric information with payment information. Walker further does not use biometric information to control the generation, encryption, and transmission of a key and payment information. Second, instead of automatically generating a key upon successful authentication of the biometric information as set forth in each of independent Claims 1 and 10, Walker requires the cardholder to request generation of a single-use credit card information after the cardholder has gained access to the device. According to Walker, "the cardholder first inputs his PIN or biometric data to access the device [...]. If access is granted, the device responds by querying the cardholder on display whether it should generate a single-use credit card number [...]. The cardholder responds by requesting generation of a credit card number (for example, by keying "YES")" (Walker, at 6:18-25, emphasis added). Thus, Walker does not teach or suggest "generat[ing] a key when the biometric information read by the biometric reading device is successfully authenticated; encrypt[ing] the key and the payment information stored in memory; and provid[ing], via the short range RF circuitry, the encrypted key and payment information for use in a**

transaction," as recited in each of independent Claims 1 and 10. In addition, Walker describes generating a single-use credit card number, which "is distinct from the unchanging account number identifying the particular cardholder" (Walker, at 6:66-7:1). The single-use credit card number is formed by concatenating an encrypted nonce, an initialization vector, and the account number. Thus, contrary to the Examiner's rejection, Walker does not teach or suggest "provid[ing...] the encrypted key and payment information for use in a transaction."

12. The Examiner disagrees. Walker does teach biometric information in relation to a transaction since the card is used to transmit payment information to the merchant in order to settle a transaction [see Figures 1-3 and related text]. It is clearly recited by Walker that the card is used for a transaction. The card requires the user to "input PIN/Biometric data to access the device" which is used to verify the user, and if the user is granted access, then the card generates the single use credit card number [See figures 1-3 and related text]. The applicant's argument regarding the "key" or card number being generated in Walker after they user asks for it to be generated does not teach "automatically generating." The claims do not teach "automatically" therefore the claim is interpreted as the key being generated in any manner as long as the key is generated. Even assuming arguendo that the key is not generated automatically, it is long been held that broadly providing a mechanical or automatic means to replace manual activity which has accomplished the same result involves only routine skill in the art [see *In re Venner*, 120 USPQ 192]. As a result, it would be obvious to automatically generate the key or single use credit card number in motivation of facilitating user experience. On the other hand, requiring a "yes" input from a user to generate said key would further enhance security measures. The claim again is noted as not reciting how the key is generated and as a result Walker teaches the claimed

limitations. Walker does not teach encrypt the key [...]; however, Holmes does [Abstract, Col. 1, Ln. 60-63, Col. 2, 34-38, Col. 4-5, Ln. 62-, 1-21]. As a result, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walked, to include the teachings of Holmes to encrypt the generated key in motivation of increasing security measures during transfer of the key or single use credit card or information required to process a transaction. Furthermore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the payment information stored in the memory (specified amount of the transaction for example) along with the key before encrypting both in motivation of increasing security measures [Walker, Col. 8, Lines 8-36].

Claim Rejections - 35 USC § 112

13. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claims 4, 10, and 13 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

15. Per claims 4, 10, and 13, the claims are directed to a point of sale (POS) terminal. Claims 1 and 10 are directed to a "A mobile device," see lines 2 on page 36 and line 10 on page 37. The claim limitations directed to other matters than a “mobile device” render the claims indefinite.

Claim Rejections - 35 USC § 101

16. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

17. Claims 1-4, 7-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

18. JUDICIAL EXCEPTIONS TO SECTION 101

19. The Supreme Court held that the patent claims in Alice Corporation Pry. Ltd. v. CLS Bank International, el al. ("Alice Corp. ") are not patent-eligible under 35 U.S.C. § 101. 10. The Supreme Court made clear in Alice Corp. that it applies the framework set forth in Mayo Collaborative Services v. Prometheus Laboratories, Inc., 566 U.S. _ (2012) (Mayo), to analyze all claims directed to laws of nature, natural phenomena, and abstract ideas for subject matter eligibility under 35 U.S.C. § 101. This framework is currently being used by the USPTO to examine claims involving laws of nature, but had not been used for claims involving abstract ideas. Therefore, the following instructions differ from prior USPTO guidance in two ways:

20. 1) Alice Corp. establishes that the same analysis should be used for all types of judicial exceptions, whereas prior USPTO guidance applied a different analysis to claims with abstract ideas (Bilski guidance in MPEP 2106(11) (B)) than to claims with laws of nature (Mayo guidance in MPEP 2106.01).

21. 2) Alice Corp. also establishes that the same analysis should be used for all categories of claims (e.g., product and process claims), whereas prior guidance applied a different analysis to

product claims involving abstract ideas (relying on tangibility in MPEP 2106(II) (A)) than to process claims (Bilski guidance).

22. ALICE V. CLS BANK: TWO-PART ANALYSIS

23. Following Alice Corp, all claims (product and process) having an abstract idea must be analyzed using the following two-part analysis set forth in Mayo. For additional guidance, see "2014 Interim Guidance on Patent Subject Matter Eligibility" December 16, 2014. This memorandum is located at:

24. http://www.gpo.gov/fdsys/pkg/FR-2014-12-16/pdf/2014-29414.pdf

25. and is publicly available at:

26. http://www.uspto.gov/patents/law/exam/interim .guidance subject matter eligibility.jsp

27. First, a determination whether the claim is directed to a judicial exception (i. e., abstract idea).

28. Examples of abstract ideas referenced in Alice Corp. include:

29. Fundamental economic practices;

30. Certain methods of organizing human activities;

31. [A]n idea of itself; and,

32. Mathematical relationships/formulas.

33. Second, a determination whether any element, or combination of elements, in the claim are sufficient to ensure that the claim amounts to significantly more than the judicial exception (i.e., the abstract idea) itself.

34. Limitations referenced in Alice Corp. that may be enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

35. Improvements to another technology or technical fields;

36. Improvements to the functioning of the computer itself;

37. Meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment.

38. Limitations referenced in Alice Corp. that are not enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

39. Adding the words "apply it" (or an equivalent) with an abstract idea, or mere instructions to implement an abstract idea on a computer;

40. Requiting no more than a genetic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry. See also, MPEP 2106(1).

41. Claims 1-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

42. Claim(s) 1-16 are directed to an abstract idea of payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency, which is a fundamental economic practice. The additional element(s) or combination of elements in the

claim(s) other than the abstract idea(s) per se amount(s) to no more than significantly more than the abstract idea itself. The method steps amount to mere instructions to implement the idea on a generic computer structure that serves to perform generic computer functions that are well-understood, routine, and conventional activities previously known to the pertinent industry, do not add meaningful limitations to the method as they would be routinely used by those of ordinary skill in the art in order to apply the correlation and yield predictable results. The functions performed by the "module(s)" appear to be conventional and routine carried out by a general purpose computer. Moreover, the claims do not appear to improve the functioning of the "module(s)" or effect an improvement in another technology or field; i.e. besides business method or solutions. The claims do not recite limitations beyond to provide grounds for an eligible application. One of ordinary skill in the art is able to readily understand the invention and carry out the recited limitations in order to apply the correlation using a generic computer or computers with instructions.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

44. Claims 1-4, 8-13, 15-16 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,163,771 to Walker et al. (herein after referred to as simply Walker), in view of U.S. Patent 6,848,048 to Holmes (herein after referred to as simply Holmes).

45. Per claim 1, Walker teaches all of the following limitations:

a. A mobile device, comprising [Abstract]:

b. Walker does not teach short range radio frequency (RF) circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to modify the teachings of Walker to include the teaching of Holmes to include a short range radio frequency in motivation of establishing a communication protocol to transfer data (see ISO/IEC 14443).

c. Memory (memory) configured to store biometric authentication information (biometric information) and payment information (account number), wherein the biometric authentication information is associated with the payment information [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

d. a biometric module configured to read biometric information [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

e. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory (processor); and [Walker Col. 6, Ln. 14-35 and Figures 1-3 and 6].

f. a secure module configured to (processor) [Walker, Abstract]:

g. generate a key (generates a single use credit card number) when the biometric information read by the biometric reading device is successfully authenticated [Col. 6, Ln. 14-38 and Figures 1-3];

h. Walker does not explicitly teach encrypt the key and the payment information stored in memory [Col. 4, Ln. 5-21, Col. 6, Ln. 61-67, Col. 8, Ln. 9-36 and Figures 1-8]; however, Holmes teaches encrypt the key […] [Abstract, Col. 1, Ln. 60-63, Col. 2, 34-38, Col. 4-5, Ln. 62-, 1-21]

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walked, to include the teachings of Holmes to encrypt the generated key in motivation of increasing security measures during transfer of the key or single use credit card or information required to process a transaction. Furthermore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the payment information stored in the memory (specified amount of the transaction for example) along with the key before encrypting both in motivation of increasing security measures [Walker, Col. 8, Lines 8-36].

i. Walker teaches provide […] the encrypted key and payment information (single – use credit card number, which the payment information (account number) is embedded in) for use in a transaction (ability to send information between two parties, considered a transaction) [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Walker does not explicitly teach provide, via the short range RF circuitry (medium over which information may be transferred ... radio frequency "RF") […]; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to allow the transfer of the

encrypted key via short range RF circuitry as defined by known standards (ISO/IEC 14443) in motivation of increasing security measures.

46. Per claims 2 and 11, Walker teaches wherein the biometric module is configured to read biometric information provided by a user to complete the transaction [Walker, Col. 5, Ln. 59-61 and Figures 1-3].

47. Per claims 3 and 12, Walker teaches wherein the payment information is associated with a primary account number (account number) [Col. 6, Ln. 14-35, 54-59, Col. 7, Ln. 27-36 and Figures 1-3 and 6].

48. Per claim 4, Walker teaches [...] payment information [...] [Col. 8, Ln. 33-60]

Walker does not explicitly teach wherein the secure module is configured to provide the encrypted key [...] to a point of sale (POS) device [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Holmes teaches wherein the secure module is configured to provide the encrypted key [...]to a point of sale (POS) device (cash register), and wherein the POS device is configured to receive the encrypted key [...] [Col. 2, Ln. 38-53, Figures 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to transmit the encrypted key to a point of sale terminal or cash register in motivation of completing the transaction.

49. Per claims 8 and 15, Walker teaches wherein the payment information (account number) is stored in a memory accessible only by the secure module (central processor 101) [Col. 6-7, Ln. 61-, 1-3 and Figures 1-3].

50. Per claims 9 and 16, Walker does not explicitly teach wherein the short range RF circuitry comprises a radio frequency identification (RFID) device; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes in order to utilize radio frequency identification as defined by known standards (ISO/IEC 14443) in motivation of increasing security measures.

51. Per claim 10, Walker teaches

a. A system, comprising [Abstract]:

b. a mobile device, comprising [Abstract]:

c. Walker does not teach short range radio frequency (RF) circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to modify the teachings of Walker to include the teaching of Holmes to include a short range radio frequency in motivation of establishing a communication protocol to transfer data (see ISO/IEC 14443).

d. memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

e. a biometric module configured to read biometric information [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

f. an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and [Walker Col. 6, Ln. 14-35 and Figures 1-3 and 6]

g. a secure module configured to (processor) [Walker, Abstract]:

h. generate a key when the biometric information read by the biometric reading device is successfully authenticated encrypt the key and the payment information stored in memory; and [Col. 6, Ln. 14-38 and Figures 1-3];

i. Walker does not explicitly teach encrypt the key and the payment information stored in memory; however, Holmes teaches encrypt the key […] [Abstract, Col. 1, Ln. 60-63, Col. 2, 34-38, Col. 4-5, Ln. 62-, 1-21]

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walked, to include the teachings of Holmes to encrypt the generated key in motivation of increasing security measures during transfer of the key or single use credit card or information required to process a transaction. Furthermore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the payment information stored in the memory (specified amount of the transaction for example) along with the key before encrypting both in motivation of increasing security measures [Walker, Col. 8, Lines 8-36].

j. Walker teaches provide […] the encrypted key and payment information (single – use credit card number, which the payment information (account number) is embedded

in) for use in a transaction (ability to send information between two parties, considered a transaction) [Col. 6-7, Ln. 61-, 1-25, Col. 8, Ln. 36-54 and Figures 1-4 and 9].

Walker does not explicitly teach provide, via the short range RF circuitry (medium over which information may be transferred ... radio frequency "RF") […]; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings of Holmes to allow the transfer of the encrypted key via short range RF circuitry as defined by known standards (ISO/IEC 14443) in motivation of increasing security measures.

j. Walker does not explicitly teach a point of sale (POS) (cash register) device configured to; however, Holmes does [Col. 2, Ln. 38-53, Figures 1-3]:

It would have been obvious to one of ordinary skill in the art to combine the teaching of Walker to include the teaching of Holmes to include a POS device at a merchant in motivation of conducting transactions.

k. Walker teaches […] secure module (processor) […] [Abstract, Col. 8, Ln. 19-35 and Figure 1-3]

Walker does not explicitly teach receive […] the encrypted key […]; however, Holmes does, [Abstract, Col. 1, Ln. 60-63, Col. 2, 34-53, Col. 4-5, Ln. 62-, 1-21 and figures 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teaching of Holmes to include the receiving of the

encrypted key by the POS (cash register) in motivation of processing the transaction through the RF communication interface with the user device.

Furthermore, it would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include allowing the POS or register to receive the payment information (account number) along with the encrypted key in motivation of increasing security measures.

l. Walker teaches transmit, to a central database, the encrypted key and payment information [Col. 8, Ln. 33-60]; and

m. a central database configured to validate the key and the payment information [Abstract, Col. 8, Ln. 33-67 and Figures 1-9].

52. Claims 7 and 14 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Walker, in view of Holmes, as applied to claims 1 and 10 above, in further view of U.S. Patent Application Publication 2002/0112177 to Voltmer et al. (herein after referred to as simply Voltmer).

53. Per claims 7 and 14, Walker in view of Holmes do not explicitly teaches wherein the biometric authentication information is stored separately from the payment information [Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3]

Voltmer teaches storing separately a plurality of information [Paragraphs 009-0091 and Figures 12A and 12B].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, in view of Holmes, to include the teachings of Voltmer to store the data in partitions or

separately in motivation of increasing security measures or facilitating the upload of information from the memory.

Double Patenting

54. Claims 1-4, and 7-16 are provisionally rejected on the ground of nonstatutory double patenting as being unpatentable over claim1-16 of Pending Application Number 14/659502. Although the claims at issue are not identical, they are not patentably distinct from each other because all of the limitations are the same except for the instant Application reciting "generate a key when the biometric information read by the biometric reading device is successfully authenticated" whereas the Pending Application (14/659502) recites "generate a key when the biometric information read by the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory." Generating the key after authentication is requires that the biometric information is matched otherwise authentication is not possible; therefore the claims are not patentably distinct from each other.

Conclusion

55. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is cited in the Notice of References Cited (form PTO-892).

56. 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).

57. 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.

58. Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on MON - FRI: 7:30AM-5PM EST Every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Hayes can be reached on (571)272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/
Patent Examiner, Art Unit 3685
12/09/2015

/JOHN HAYES/
Supervisory Patent Examiner, Art Unit 3685

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14639034	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC- SEARCHED		
Symbol	Date	Examiner
G06Q	5/8/2015	EO
H04L	5/8/2015	EO

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
705		5/8/2015	EO

SEARCH NOTES		
Search Notes	Date	Examiner
consulted Calvin Hewitt	5/15/2015	EO

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
S1	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:26
S2	1	("6163771").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:27
S5	16	(biometric near1 data) near2 stored near2 (separately or different)	US-PGPUB; USPAT	OR	ON	2015/05/18 15:53
S6	5	"7911643"	US-PGPUB; USPAT	OR	ON	2015/05/18 15:59
S8	0	(separatly near1 stor$3) with data	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S9	12789	(stor$3 near1 data) with separately	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S10	1434	S9 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S11	1011	S10 and ((information or data) near4 (separately))	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S15	919	S11 and (memory)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:07
S19	0	S15 and (stor$3 near4 saperately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:08
S20	498	(authentication near4 stor$3 near4 separately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:13
S21	34	S20 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:16
S22	48796	(stor$4 near3 information separately) same (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S24	29064	(stor$4 near3 information separately) with (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S25	5880	S24 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S26	51	S25 and @pd<"20020101"	US-PGPUB;	OR	ON	2015/05/18 16:26

			USPAT			
S27	1	"20020112177"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:32
S28	1	"20020077993"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:40
S29	10379	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near4 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S30	7730	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near2 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S31	4128	((generate) near2 (key pin code token password)) with ((encrypt) near3 (key pin code token password))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:22
S32	3286	((generate) near2 (key pin code token password)) with ((encrypt) near2 (key pin code token password))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:22
S33	1736	S32 and (transaction financial account)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S34	1134	S33 and @pd<"20120101"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S35	234	S34 and (RFID RD infrared)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S37	63	S35 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:24
S38	850	"5590197"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:44
S39	1	("5590197").PN.	US-PGPUB; USPAT	OR	OFF	2015/06/12 16:44
S40	0	("("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" | "6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" | "5742618" | "6276607" | "6570487" |	US-PGPUB; USPAT	OR	OFF	2015/09/30 16:19

		"8004410").PN.").PN.				
S42	66	("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" | "6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" | "5742618" | "6276607" | "6570487" | "8004410").PN.	US-PGPUB; USPAT	OR	ON	2015/09/30 16:20

12/9/2015 12:23:02 PM
C:\Users\eoussir\Documents\EAST\Workspaces\14639034_Mobile device RFID transaction biometric POS.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14639034	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

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

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

CLAIM		DATE								
Final	Original	05/18/2015	12/09/2015							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	-							
	6	✓	-							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							

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	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

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	20070022058	A1	2007-01-25	Labrou et al.	
	2					

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

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	/Noel C. Gillespie/	Date (YYYY-MM-DD)	2016-05-09
Name/Print	Noel C. Gillespie	Registration Number	47596

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:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Noel C. Gillespie/cindy guido
Attorney Docket Number:	116546-660CT2

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:	25725164
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Noel C. Gillespie/cindy guido
Filer Authorized By:	Noel C. Gillespie
Attorney Docket Number:	116546-660CT2
Receipt Date:	09-MAY-2016
Filing Date:	04-MAR-2015
Time Stamp:	18:02:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$180
RAM confirmation Number	5039
Deposit Account	502075
Authorized User	GILLESPIE, NOEL C.

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

Charge any Additional Fees required under 37 CFR 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)

Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)

Charge any Additional Fees required under 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	Information Disclosure Statement (IDS) Form (SB08)	TO_BE_FILED_116546_660CT2.PDF	612012 8980940cf09428c5c30314df8355fb10b986b403	no	4
Warnings:					
Information:					
A U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form. You may remove the form to add the required data in order to correct the Informational Message or if you chose not to, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Fee Worksheet (SB06)	fee-info.pdf	30729 5b1bcb42c9653328eb9316d815b1aa96ef0bb027	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	642741		

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.

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	March 4, 2015	Francisco Martinez de Velasco Cortina	116546-660CT2	5934

EXAMINER	
OUSSIR, EL MEHDI	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
June 30, 2016	EFS WEB

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

PRE-APPEAL BRIEF ACCOMPANYING PRE-APPEAL BRIEF REQUEST FOR REVIEW

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

Sir:

Pursuant to the Pre-Appeal Brief Conference Pilot Program and further to the Examiner's Final Office Action dated December 30, 2015, Applicant files this Pre-Appeal Brief Request for Review. This Request is accompanied by the filing of a Notice of Appeal.

ARGUMENTS

Applicant turns now to the rejections at issue:

Claims 4, 10, and 13 stand rejected under 35 U.S.C. §112(b), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. In particular, the Action claims that while claims 1 and 10 are directed to a mobile device, claims 4, 10 and 13 have limitations directed to other matters. Applicant addressed this rejection in the prior response and assumes that it is included by mistake. The rejection makes no note of what the other matters are or how they may be different from those addressed in the last response, and in response Applicant's arguments indicates that this rejection was to be withdrawn.

Claims 1-16 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Applicant traverses the rejection because the claims are not directed to an abstract idea, and even if they were, they do add significantly more.

The first step of the two part Mayo test is to determine whether the claim is directed to an . . . abstract idea. *See The 2014 Interim Guidance on Patent Subject Matter Eligibility* at Page 10. If it is determined that the claim is directed to an abstract idea, then the second part of the Mayo test is to determine whether any element, or combination of elements, in the claim is sufficient to ensure that the claims amount to significantly more than the abstract idea. *See Id.* at 20. Fundamental to the Mayo test is the premise that an analysis of the claim limitations must take place. As noted in *The 2014 Interim Guidance* on page 11, "[a] claim is directed to a judicial exception when . . . an abstract idea is recited (i.e., set forth or described) in the claim (emphasis added)." This requires an actual analysis and indication of where in the claim, i.e., what limitations combine to describe or set forth the abstract idea. Only then can one examine the remaining claim elements to ascertain whether they add significantly more than the abstract idea. As noted in *Enfish, LLC, v. Microsoft Corporation, et al., Slip Op. (2016)*, it is not sufficient to simply ask whether a claim involves a patent-ineligible concept, rather the proper inquiry asks whether the character of the claims as a whole and considered in light of the specification are directed to excluded subject matter. *See Id.* at page 10. The court went on to explain that it is improper to simply summarize the entire claim at a high level of abstraction as

being directed to, e.g., an abstract idea, untethered from the actual language of the claims. *See Id.* at page 14.

Here, as is often the case with such Alice rejections, the Action fails to properly identify the abstract idea through analyzing and identifying the limitation or limitations that describe or set forth the abstract idea. Not only is this an incorrect application of the first step of the *Mayo* test, as noted in *Enfish*, it prevents any meaningful application of the second step. Moreover, the claims are not directed to an abstract idea, even if the Mayo test is applied correctly.

The Office Action's entire analysis is contained in paragraph 42, which states in part: "Claim(s) 1-16 are directed to an abstract idea of payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency, which is a fundamental economic practice. The additional element(s) or combination of elements in the claim(s) other than the abstract idea(s) per se amount(s) to no more than significantly more than the abstract idea itself."

Thus, the actual analysis of the claim limitations required by Mayo/Alice is missing. Moreover, while the rejection refers to the broad category of abstract ideas referred to as fundamental economic practices included in *The 2105 Interim Guidance*, the "'directed to' inquiry . . . cannot simply ask whether the claims *involve* a patent-ineligible concept, because essentially every routinely patent eligible claim involving physical products and actions *involves* a law of nature of nature and/or natural phenomenon . . . (original emphasis)." *See Enfish* at page 10, citing to *Mayo*,132 S. Cy. At 1923. Rather, the task of the examiner is to go beyond the broad categories and determine whether the claims are similar to an identified patent-ineligible concept. The *Guidelines* direct the Examiner to look at examples of what the courts have found to be abstract ideas and by way of comparison determine if the claims are directed to a similar abstract idea.

To be clear: "payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency," is NOT one of the examples, nor is it even abstract on its face – i.e., the way the Action characterizes the abstract idea makes clear that the claims are NOT directed to an abstract idea.

Here the claims are directed to an improved mobile device that can engage in a secure transaction by ensuring that a biometric received by the device is associated with payment information included in the device before sending any such payment information. Or as stated in the Action, the claimed device provides "increased security measures." Moreover, the device can upon authentication of the relationship of the biometric with the payment information generated a key that can be encrypted with the payment information for further increased security. So while related to financial transactions, the claims are not directed to an improvement in the financial transaction itself, as in, e.g., *buySAFE*. Rather the claims are directed to an improvement in the device and are necessarily, therefore rooted in technology. Thus, and as in *Enfish*, the claims cannot properly be said to be directed to an abstract idea when the first step of the *Mayo/Alice* test is applied.

Further, assuming *arguendo* that the claim is directed to an abstract idea, Applicant respectfully submits that the claim as a whole amounts to significantly more than the judicial exception. The Action states "[t]he functions performed by the 'module(s)' appear to be conventional and routine carried out by a general purpose computer. Moreover, the claims do not appear to improve the functioning of the 'module(s)' or effect an improvement in another technology or field; i.e. besides business method or solutions."

First, the Enfish court has rightly held that "we are not persuaded that the invention's ability to run on a general-purpose computer dooms the claims." *See Enfish* at page 16. The proper analysis is not whether software runs on a general purpose computer, but whether the claims are directed to an improvement in the computer. *See Id.* The Action says the claims do not improve the functioning of the modules, but this is clearly erroneous. The claims are clearly directed to the functioning of the modules - and this is all that is required under §101. Whether the claims are directed to "activities previously known to the pertinent industry," or "would be routinely used by those of ordinary skill in the art in order to apply the correlation and yield predictable results," is an analysis to be performed under section §102 and §103 and in no way mean that the claims are not directed to improvements in the performance of the modules, which they inarguable are.

Claims 1-4, 8-13, and 15-16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker et al. (U.S. Patent No. 6,163,771) in view of Holmes (U.S. Patent No.

6,848,048). **Claims 7 and 14** stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker in view of Holmes in further view of Voltmer.

According to the Action, with the exception of the short range radio frequency (RF) circuitry, Walker discloses all of the limitations set forth in independent Claims 1 and 10. Applicant respectfully disagrees. First, to the extent that Walker discloses a biometric interface, biometric information is used to control access to a device such as a smartcard. For example, Walker states that "the device may include a biometric interface, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint." (Walker, at 5:58-61, emphasis added). Contrastingly, independent Claims 1 and 10 each recite that "the biometric information is associated with the payment information" and that the biometric information is NOT used for access to the device, but rather to cause, when the biometric information is authenticated as being associated with the account information, a secure module to "generate a key [...]; encrypt the key and payment information [...]; and provide [...] the encrypted key and payment information for use in a transaction."

Walker does not associate biometric information with payment information. In Walker after the user access the device (step 351), using a PIN or biometric, and responds to a query (step 355) from the device so as to cause a single-use credit card number is generated (step 360). Nowhere does it say that the biometric is authenticated as being associated with payment information as alleged in the Action. Further, instead of automatically generating a key upon successful authentication of the biometric information as set forth in each of independent Claims 1 and 10, Walker requires the cardholder to request generation of a single-use credit card information (step 355) after the cardholder has gained access to the device. Thus, Walker does not teach or suggest "generat[ing] a key when the biometric information read by the biometric reading device is successfully authenticated; encrypt[ing] the key and the payment information stored in memory; and provid[ing], via the short range RF circuitry, the encrypted key and payment information for use in a transaction (emphasis added)," as recited in each of independent Claims 1 and 10.

In short, Walker uses the biometric to access the device. Nowhere does Walker indicate that biometric information is associated with payment information; nowhere does Walker say that the biometric information read by the device is authenticated as being associated with

payment information; and nowhere does Walker say that upon authentication of biometric information a key is generated, encrypted with the payment information, and then transmitted.

In view of the above, Applicant submits that the rejections of **Claims 1-16** are in error for at least the above-stated reasons and requests that these rejections be withdrawn.

Claims 1-4 and 7-16 stand provisionally rejected on the ground of nonstatutory double patenting, but the Final Office Action indicates that this rejection will be held in abeyance at this time.

Respectfully submitted,
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

Date: June 30, 2016

/Noel C. Gillespie/
Noel C. Gillespie
Reg. No. 47,596

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

Doc Code: AP.PRE.REQ

PTO/AIA/33 (03-13)
Approved for use through 07/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
116546-660CT2

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on _____

Signature _____

Typed or printed name _____

Application Number	Filed
14/639,034	March 4, 2015

First Named Inventor: Francisco Martinez de Velasco Cortina

Art Unit	Examiner
3685	OUSSIR, EL MEHDI

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant.

☑ attorney or agent of record. Registration number 47596.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Noel C. Gillespie/
Signature

Noel C. Gillespie
Typed or printed name

6192381900
Telephone number

June 30 2016
Date

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

PTO/AIA/31 (03-14)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

NOTICE OF APPEAL FROM THE EXAMINER TO THE PATENT TRIAL AND APPEAL BOARD

Docket Number (Optional): 116546-660CT2

I hereby certify that this correspondence is being facsimile transmitted to the USPTO, EFS-Web transmitted to the USPTO, or deposited with the United States Postal Service with sufficient postage in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, on Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____.

Signature _____

Typed or printed name _____

In re Application of: Francisco Martinez de Velasco Cortina

Application Number	Filed
14/639,034	March 4, 2015

For: SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Art Unit	Examiner
3685	OUSSIR, EL MEHDI

Applicant hereby **appeals** to the Patent Trial and Appeal Board from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 800.00

☐ Applicant asserts small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by 50%, and the resulting fee is: $ _____

☐ Applicant certifies micro entity status. See 37 CFR 1.29. Therefore, the fee shown above is reduced by 75%, and the resulting fee is: $ _____
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

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

☑ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 502075.

☑ Payment made via EFS-Web.

☑ A petition for an extension of time under 37 CFR 1.136(a) (PTO/AIA/22 or equivalent) is enclosed.
For extensions of time in reexamination proceedings, see 37 CFR 1.550.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant

☑ attorney or agent of record
Registration number 47596

☐ attorney or agent acting under 37 CFR 1.34
Registration number _____

Signature /Noel C. Gillespie/

Typed or printed name Noel C. Gillespie

Telephone Number 6192381900

Date June 30 2016

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of _____ forms are submitted.

This collection of information is required by 37 CFR 41.20(b)(1) and 41.31. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

Privacy Act Statement

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

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

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

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Noel C. Gillespie/cindy guido
Attorney Docket Number:	116546-660CT2

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of Appeal	1401	1	800	800
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
			Total in USD ($)	**2200**

Electronic Acknowledgement Receipt

EFS ID:	26232833
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Noel C. Gillespie/cindy guido
Filer Authorized By:	Noel C. Gillespie
Attorney Docket Number:	116546-660CT2
Receipt Date:	30-JUN-2016
Filing Date:	04-MAR-2015
Time Stamp:	18:33:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2200
RAM confirmation Number	070116INTEFSW18342700
Deposit Account	1017
Authorized User	cindy guido
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Pre-Brief Conference request	Pre_AppeaL_Brief_Accompanying_Pre_Appeal_Brief_Request__For_Review.PDF	128169 59651c4500291fffcce6c95aea9fe905a1462c59c	no	6
Warnings:					
Information:					
2	Pre-Brief Conference request	Pre_Appeal_Brief_Request_For_Review.PDF	188930 5e7be48017d29a2c0133e0d168a542679ccc7631	no	2
Warnings:					
Information:					
3	Notice of Appeal Filed	Notice_of_Appeal.PDF	236019 9a4139a1ea0acdf901363ba5c24ca54a61b0f68e	no	2
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32516 4ee1aee8674a58485fe0f789fc7056cebdb186da	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	585634		

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-660CT2	5934

27189 7590 07/21/2016

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

MAIL DATE	DELIVERY MODE
07/21/2016	PAPER

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

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

Notice of Panel Decision from Pre-Appeal Brief Review	Application No.	Applicant(s)
	14/639,034	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

This is in response to the Pre-Appeal Brief Request for Review filed 30 June, 2016.

1. ☐ **Improper Request** – The Request is improper and a conference will not be held for the following reason(s):

☐ The Notice of Appeal has not been filed concurrent with the Pre-Appeal Brief Request.
☐ The request does not include reasons why a review is appropriate.
☐ A proposed amendment is included with the Pre-Appeal Brief request.
☐ Other: .

The time period for filing a response continues to run from the receipt date of the Notice of Appeal or from the mail date of the last Office communication, if no Notice of Appeal has been received.

2. ☒ **Proceed to Board of Patent Appeals and Interferences** – A Pre-Appeal Brief conference has been held. The application remains under appeal because there is at least one actual issue for appeal. Applicant is required to submit an appeal brief in accordance with 37 CFR 41.37. The time period for filing an appeal brief will be reset to be one month from mailing this decision, or the balance of the two-month time period running from the receipt of the notice of appeal, whichever is greater. Further, the time period for filing of the appeal brief is extendible under 37 CFR 1.136 based upon the mail date of this decision or the receipt date of the notice of appeal, as applicable.

☒ The panel has determined the status of the claim(s) is as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: *1-4, 7-16*.
Claim(s) withdrawn from consideration: _____.

3. ☐ **Allowable application** – A conference has been held. The rejection is withdrawn and a Notice of Allowance will be mailed. Prosecution on the merits remains closed. No further action is required by applicant at this time.

4. ☐ **Reopen Prosecution** – A conference has been held. The rejection is withdrawn and a new Office action will be mailed. No further action is required by applicant at this time.

All participants:		
(1) *EL MEHDI OUSSIR*.		(3) *John Hayes*.
(2) *Steven Kim*.		(4)_____.
/STEVEN KIM/ Primary Examiner, Art Unit 3685	/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	/JOHN HAYES/ Supervisory Patent Examiner, Art Unit 3685

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIALS AND APPEALS BOARD

In re application of: NEOLOGY, INC. Docket No: 116546-660CT2

Appln. No.: 14/639,034 Group Art Unit: 3685

Confirmation No.: 5934 Examiner: OUSSIR, EL MEHDI

Filed: March 4, 2015

For: SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

In accordance with the provisions of 37 C.F.R. § 41.37, Appellant respectfully submits this Appeal Brief in response to the Advisory Action dated July 21, 2016 and the Final Office Action ("Office Action") dated December 30, 2015.

Table of Contents

I. REAL PARTY IN INTEREST 2
II. RELATED APPEALS, INTERFERENCES, AND TRIALS 3
III. SUMMARY OF THE CLAIMED SUBJECT MATTER 4
IV. ARGUMENT 6
V. CONCLUSION 13
CLAIMS APPENDIX 14
EVIDENCE APPENDIX 17

I. REAL PARTY IN INTEREST

Neology, Inc. of Poway, California, is the real party in interest.

II. RELATED APPEALS, INTERFERENCES, AND TRIALS

U.S. Application 14/585,057 (Attorney Ref. 116546-6601C1) received a Notice of Panel Decision from Pre-Appeal Brief Review from the USPTO on November 30, 2016. A Notice of Appeal was filed on November 9, 2016. An Appeal Brief has not yet been filed for this application, therefore no decision has been received on this appeal. As no decision was issued by the Board, no attachments relating to this appeal are being included with this Appeal Brief.

U.S. Application 14/659,502 (Attorney Ref. 116546-661CT2) received a Notice of Panel Decision from Pre-Appeal Brief Review from the USPTO on November 30, 2016. A Notice of Appeal was filed on November 16, 2016. An Appeal Brief has not yet been filed for this application, therefore no decision has been received on this appeal. As no decision was issued by the Board, no attachments relating to this appeal are being included with this Appeal Brief.

III. SUMMARY OF THE CLAIMED SUBJECT MATTER

The summary of the invention in connection with claims 1-4 and 7-16 in relation to exemplary embodiments are set forth below. The paragraph and line numbers refer to the paragraph and line numbers of the specification as filed.

The present embodiments provide systems and methods for improved management and profitability of take-out ordering through order sharing.

1. A mobile device, comprising:

short range radio frequency (RF) circuitry (¶¶ [0013] - [0014]);

memory (FIG. 2, ¶ [0014], line 14) configured to store biometric authentication information and payment information (¶ [0069]), wherein the biometric authentication information is associated with the payment information (¶¶ [0072] - [0073]);

a biometric module configured to read biometric information (¶ [0067]);

an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory (¶ [0073]); and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is successfully authenticated (¶ [0053], *"Secure Identification"*);

encrypt the key and the payment information stored in memory (¶ [0053], *"Secure Identification"* and *"Secure Transaction"*); and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction (¶ [0053], *"Secure Transaction"* and *"Secure Data Base"*).

10. A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry (¶¶ [0013] - [0014]);

memory (FIG. 2, ¶ [0014], line 14) configured to store biometric authentication information and payment information (¶ [0069]), wherein the biometric authentication information is associated with the payment information (¶¶ [0072] - [0073]);

a biometric module configured to read biometric information (¶ [0067]);

an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory (¶ [0073]); and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is successfully authenticated(¶ [0053], "*Secure Identification*");

encrypt the key and the payment information stored in memory (¶ [0053], "*Secure Identification*" and "*Secure Transaction*"); and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction (¶ [0053], "*Secure Transaction*" and "*Secure Data Base*"); and

a point of sale (POS) device configured to:

receive, from the secure module, the encrypted key and payment information (¶¶ [0053] and [0059]-[0064]); and

transmit, to a central database, the encrypted key and payment information; and

a central database configured to validate the key and the payment information (¶ [0053], "*Secure Transaction*" and "*Secure Data Base*").

IV. ARGUMENT

By way of summary, Claims 1-4 and 7-16 are pending in the present application and stand rejected. **Claims 4, 10, and 13** stand rejected under 35 U.S.C. §112(b), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. **Claims 1-4 and 7-16** stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. **Claims 1-4, 8-13, and 15-16** stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker et al. (U.S. Patent No. 6,163,771) in view of Holmes (U.S. Patent No. 6,848,048). **Claims 7 and 14** stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker in view of Holmes in further view of Voltmer. **Claims 1-4 and 7-16** stand provisionally rejected on the ground of nonstatutory double patenting, but the Final Office Action indicates that this rejection will be held in abeyance at this time. Appellant respectfully submits that each of these rejections is in error for at least the reasons set forth below.

Rejection under 35 U.S.C. 112(b) – Claims 4, 10, and 13

Claims 4, 10, and 13 stand rejected under 35 U.S.C. §112(b), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. In particular, the Action claims that while claims 1 and 10 are directed to a mobile device, claims 4, 10 and 13 have limitations directed to other matters. Applicant addressed this rejection in the response dated November 30, 2015 and assumes that it is included by mistake. The rejection makes no note of what the other matters are or how they may be different from those addressed in the response dated November 30, 2015, and in

response to Applicant's arguments, the Examiner indicated that this rejection was to be withdrawn.

Rejection under 35 U.S.C. 101 – Claims 1-16

Claims 1-4 and 7-16 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Applicant traverses the rejection because the claims are not directed to an abstract idea, and even if they were, they do add significantly more.

The first step of the two part Mayo test is to determine whether the claim is directed to an . . . abstract idea. See The 2014 Interim Guidance on Patent Subject Matter Eligibility at Page 10. If it is determined that the claim is directed to an abstract idea, then the second part of the Mayo test is to determine whether any element, or combination of elements, in the claim is sufficient to ensure that the claims amount to significantly more than the abstract idea. See Id. at 20. Fundamental to the Mayo test is the premise that an analysis of the claim limitations must take place. As noted in The 2014 Interim Guidance on page 11, "[a] claim is directed to a judicial exception when . . . an abstract idea is *recited (i.e., set forth or described) in the claim* (emphasis added)." This requires an actual analysis and indication of where in the claim, i.e., what limitations combine to describe or set forth the abstract idea. Only then can one examine the remaining claim elements to ascertain whether they add significantly more than the abstract idea. As noted in Enfish, LLC, v. Microsoft Corporation, et al., Slip Op. (2016), it is not sufficient to simply ask whether a claim involves a patent-ineligible concept, rather the proper inquiry asks whether the character of the claims as a whole and considered in light of the specification are directed to excluded subject matter. See Id. at page 10. The court went on to explain that it is improper to simply summarize the entire claim at a high level of abstraction as being

directed to, e.g., an abstract idea, untethered from the actual language of the claims. See Id. at page 14.

Here, as is often the case with such Alice rejections, the Action fails to properly identify the abstract idea through analyzing and identifying the limitation or limitations that describe or set forth the abstract idea. Not only is this an incorrect application of the first step of the Mayo test, as noted in Enfish, it prevents any meaningful application of the second step. Moreover, the claims are not directed to an abstract idea, even if the Mayo test is applied correctly.

The Office Action's entire analysis is contained in paragraph 42, which states in part: "Claim(s) 1-16 are directed to an abstract idea of payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency, which is a fundamental economic practice. The additional element(s) or combination of elements in the claim(s) other than the abstract idea(s) per se amount(s) to no more than significantly more than the abstract idea itself."

Thus, the actual analysis of the claim limitations required by Mayo/Alice is missing. Moreover, while the rejection refers to the broad category of abstract ideas referred to as fundamental economic practices included in The 2105 Interim Guidance, the "'directed to' inquiry . . . cannot simply ask whether the claims involve a patent-ineligible concept, because essentially every routinely patent eligible claim involving physical products and actions involves a law of nature of nature and/or natural phenomenon . . . (original emphasis omitted)." See Enfish at page 10, citing to Mayo,132 S. Cy. At 1923. Rather, the task of the examiner is to go beyond the broad categories and determine whether the claims

are similar to an identified patent-ineligible concept. The Guidelines direct the Examiner to look at examples of what the courts have found to be abstract ideas and by way of comparison determine if the claims are directed to a similar abstract idea.

To be clear: "payment transaction using a mobile device to complete the transaction with a point of sale terminal utilizing security measures to increase security measures and operate using a short range radio frequency," is NOT one of the examples, nor is it even abstract on its face – i.e., the way the Action characterizes the abstract idea makes clear that the claims are NOT directed to an abstract idea.

Here the claims are directed to an improved mobile device that can engage in a secure transaction by ensuring that a biometric received by the device is associated with payment information included in the device before sending any such payment information. Or as stated in the Action, the claimed device provides "increased security measures." Moreover, the device can upon authentication of the relationship of the biometric with the payment information generated a key that can be encrypted with the payment information for further increased security. So while related to financial transactions, the claims are not directed to an improvement in the financial transaction itself, as in, e.g., buySAFE. Rather the claims are directed to an improvement in the device and are necessarily, therefore rooted in technology. Thus, and as in Enfish, the claims cannot properly be said to be directed to an abstract idea when the first step of the Mayo/Alice test is applied.

Further, assuming arguendo that the claim is directed to an abstract idea, Applicant respectfully submits that the claim as a whole amounts to significantly more than the judicial exception. The Action states "[t]he functions performed by the 'module(s)' appear to be conventional and routine carried out by a general purpose computer. Moreover, the

claims do not appear to improve the functioning of the 'module(s)' or effect an improvement in another technology or field; i.e. besides business method or solutions."

First, the Enfish court has rightly held that "we are not persuaded that the invention's ability to run on a general-purpose computer dooms the claims." See Enfish at page 16. The proper analysis is not whether software runs on a general purpose computer, but whether the claims are directed to an improvement in the computer. See Id. The Action says the claims do not improve the functioning of the modules, but this is clearly erroneous. The claims are clearly directed to the functioning of the modules - and this is all that is required under §101.

In the Action's own words the claimed modules with key together increase the security of one transaction. It is simply evident on the fact of the claim that the mobile device with the claimed authentication module and secure module is not merely reciting a fundamental economic practice.

Rejection under 35 U.S.C. 103(a) – Claims 1-16

Claims 1-4, 8-13, and 15-16 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker et al. (U.S. Patent No. 6,163,771) in view of Holmes (U.S. Patent No. 6,848,048). Claims 7 and 14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker in view of Holmes in further view of Voltmer.

According to the Action, with the exception of the short range radio frequency (RF) circuitry, Walker discloses all of the limitations set forth in independent Claims 1 and 10. Applicant respectfully disagrees. First, to the extent that Walker discloses a biometric interface, biometric information is used to control access to the device and not the provisioning of transaction information as in the claims. For example, Walker states that

"the device may include a biometric interface, and be activated by the input of a suitable biometric record such as the cardholder's fingerprint." (Walker, at 5:58-61, emphasis added). Contrastingly, independent Claims 1 and 10 each recite that "the biometric information is associated with the payment information" and that the biometric information is NOT used for access to the device, but rather to cause, when the biometric information is authenticated as being associated with the account information, a secure module to "generate a key [...]; encrypt the key and payment information [...]; and provide [...] the encrypted key and payment information for use in a transaction."

Walker does not associate biometric information with payment information. In Walker after the user access the device (step 351) using a PIN or biometric, then the user must respond to a query (step 355) from the device so as to cause a single-use credit card number to be generated (step 360). Nowhere does it say that the biometric is authenticated as being associated with payment information as alleged in the Action. Further, instead of automatically generating a key and providing transaction information upon successful authentication of the biometric information as set forth in each of independent Claims 1 and 10, Walker requires the cardholder to request generation of a single-use credit card information (step 355) after the cardholder has gained access to the device. Thus, Walker does not teach or suggest "generat[ing] a key when the biometric information read by the biometric reading device is successfully authenticated; encrypt[ing] the key and the payment information stored in memory; and provid[ing], via the short range RF circuitry, the encrypted key and payment information for use in a transaction (emphasis added)," as recited in each of independent Claims 1 and 10.

In short, Walker uses the biometric to access the device. Nowhere does Walker indicate that biometric information is associated with payment information; nowhere does Walker say that the biometric information read by the device is authenticated as being associated with payment information; and nowhere does Walker say that upon authentication of biometric information a key is generated, encrypted with the payment information, and then transmitted.

In view of the above, Applicant submits that the rejections of Claims 1-16 are in error for at least the above-stated reasons and requests that these rejections be withdrawn.

Double Patenting

Claims 1-4 and 7-16 stand provisionally rejected on the ground of nonstatutory double patenting, but the Final Office Action indicates that this rejection will be held in abeyance at this time. Upon the indication of allowable subject matter, and provided the double patenting rejection is still maintained and pertinent with respect to the otherwise allowable claims, Applicant will submit a terminal disclaimer to obviate that double patenting rejection.

V. CONCLUSION

The statutory fee (37 C.F.R. §41.37(a) and 1.17(c)) is being remitted. The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 50-2075. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/ Noel C. Gillespie /
Noel C. Gillespie
Registration No. 47,596

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900 (Phone)
(619) 235-0398 (Fax)

27189
CUSTOMER NUMBER

Date: January 30, 2017

CLAIMS APPENDIX

CLAIMS 1-16 ON APPEAL:

1. A mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

a biometric module configured to read biometric information;

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

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is successfully authenticated;

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

2. The mobile device of claim 1, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

3. The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. The mobile device of claim 1, wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device.

5. (Canceled)

6. (Canceled)

7. The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the secure module.

9. The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

a biometric module configured to read biometric information;

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

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is successfully authenticated

encrypt the key and the payment information stored in memory; and

provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

a point of sale (POS) device configured to:

receive, from the secure module, the encrypted key and payment information; and

transmit, to a central database, the encrypted key and payment information; and

a central database configured to validate the key and the payment information.

11. The system of claim 10, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

12. The system of claim 10, wherein the payment information is associated with a primary account number.

13. The system of claim 10, wherein the POS device includes an RF reader.

14. The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. The system of claim 10, wherein the payment information is stored in a memory accessible only by the secure module.

16. The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

EVIDENCE APPENDIX

Pursuant to 37 C.F.R. § 41.37(c)(1)(ix), submitted herewith are copies of any evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 or any other evidence entered by the Examiner and relied upon by Appellant in the appeal.

NONE.

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Noel C. Gillespie/cindy guido
Attorney Docket Number:	116546-660CT2

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 5 months with $0 paid	1255	1	3000	3000
Miscellaneous:				
			Total in USD ($)	**3000**

Electronic Acknowledgement Receipt

EFS ID:	28212213
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Noel C. Gillespie/cindy guido
Filer Authorized By:	Noel C. Gillespie
Attorney Docket Number:	116546-660CT2
Receipt Date:	30-JAN-2017
Filing Date:	04-MAR-2015
Time Stamp:	21:07:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$3000
RAM confirmation Number	013117INTEFSW21085300
Deposit Account	502075
Authorized User	cindy guido
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	APPEAL_BRIEF__116546-660CT2_TBF.PDF	98959 5d603defe5487dec5a9ed91781099297ec365762	no	17
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30708 fa9939ba96f8a3b78c0d899c06d48b3b0d52fd16	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	129667		

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	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

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	20060020558	A1	2006-01-26	Bonalle	
	2					

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

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)	2017-03-01
Name/Print	Daniel K. Robertson	Registration Number	48,077

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:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Daniel K. Robertson/cindy guido
Attorney Docket Number:	116546-660CT2

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:	28520590
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Daniel K. Robertson/cindy guido
Filer Authorized By:	Daniel K. Robertson
Attorney Docket Number:	116546-660CT2
Receipt Date:	02-MAR-2017
Filing Date:	04-MAR-2015
Time Stamp:	17:50:22
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	030317INTEFSW17512600
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	Information Disclosure Statement (IDS) Form (SB08)	IDS-_116546-660CT2.PDF	611980 838a61dc8469aaff51e3350dc509e4e67b40e904	no	4
Warnings:					
Information:					
A U.S. Publication Number Citation is required in the Information Disclosure Statement (IDS) form. You may remove the form to add the required data in order to correct the Informational Message or if you chose not to, the image of the form will be processed and be made available within the Image File Wrapper (IFW) system. However, no data will be extracted from this form. Any additional data such as Foreign Patent Documents or Non Patent Literature will be manually reviewed and keyed into USPTO systems.					
2	Fee Worksheet (SB06)	fee-info.pdf	30689 3f9e0df4a4a18a7ac845b1e25ab6e0ac6a8ef8dd	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	642669		

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

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

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

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

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	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

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	7911643	B2	2011-03-22	Yamada	
	2	6934861	B2	2005-08-23	Haala	
	3	5590197	A	1996-12-31	Chen	

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	20040128249	A1	2004-07-01	Hoffman	

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							

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

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	Appeal Brief filed April 18, 2017 for US patent application no. 14/659,502.	
	2	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/659,502.	
	3	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.	
	4	US Office Action dated May 16, 2016 received in US patent application no. 14/659,502.	
	5	Response to Office Action filed on December 23, 2015 for US patent application no. 14/659,502.	
	6	US Office Action dated June 22, 2015 received in US patent application no. 14/659,502.	
	7	Response to Office Action filed on May 2, 2017 for US patent application no. 15/372,317.	
	8	US Office Action dated February 2, 2017 received in US patent application no. 15/372,317.	
	9	Response to Office Action filed on November 18, 2016 for US patent application no. 14/321,781.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

	10	US Office Action dated May 19, 2016 received in US patent application no. 14/321,781.	
	11	Response to Office Action filed on December 24, 2015 for US patent application no. 14/321,781.	
	12	US Office Action dated June 24, 2015 received in US patent application no. 14/321,781.	
	13	US Notice of Allowance dated April 11, 2014 received in US patent application no. 14/022,135.	
	14	Response to Office Action filed on March 14, 2014 for US patent application no. 14/022,135.	
	15	US Office Action dated March 7, 2014 received in US patent application no. 14/022,135.	
	16	Response to Office Action filed on February 3, 2014 for US patent application no. 14/022,135.	
	17	US Office Action dated December 5, 2013 received in US patent application no. 14/022,135.	
	18	Response to Office Action filed on April 26, 2017 for US patent application no. 14/724,593.	
	19	US Office Action dated February 17, 2017 received in US patent application no. 14/724,593.	
	20	Pre-Brief Appeal Conference Decision dated December 12, 2016 and received in US patent application no. 14/724,593.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

	21	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.	
	22	US Office Action dated May 6, 2016 received in US patent application no. 14/724,593.	
	23	Response to Office Action filed on January 7, 2016 for US patent application no. 14/724,593.	
	24	US Office Action dated August 4, 2015 received in US patent application no. 14/724,593.	
	25	US Notice of Allowance dated December 3, 2014 received in US patent application no. 14/028,469.	
	26	Supplemental response to Office Action filed on October 31, 2014 for US patent application no. 14/028,469.	
	27	Response to Office Action filed on October 14, 2014 for US patent application no. 14/028,469.	
	28	US Office Action dated August 18, 2014 received in US patent application no. 14/028,469.	
	29	US Office Action dated July 9, 2014 received in US patent application no. 14/028,469.	
	30	Response to Office Action filed on June 13, 2014 for US patent application no. 14/028,469.	
	31	US Office Action dated April 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	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

	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 February 9, 2017 for US patent application no. 14/585,057.	
	37	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/585,057.	
	38	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.	
	39	US Office Action dated May 9, 2016 received in US patent application no. 14/585,057.	
	40	Response to Office Action filed on January 7, 2016 for US patent application no. 14/585,057.	
	41	US Office Action dated October 7, 2015 received in US patent application no. 14/585,057.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

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	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

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)	2017-05-25
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:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Daniel K. Robertson/gloria mimi choi
Attorney Docket Number:	116546-660CT2

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:	29312361
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Daniel K. Robertson/gloria mimi choi
Filer Authorized By:	Daniel K. Robertson
Attorney Docket Number:	116546-660CT2
Receipt Date:	25-MAY-2017
Filing Date:	04-MAR-2015
Time Stamp:	13:56:02
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	052617INTEFSW13574600
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	Information Disclosure Statement (IDS) Form (SB08)	IDS_SB08_TBF_116546-660CT2.PDF	613032 5e118c98669dc9c593c2e4f820e98ccb4b51d646	no	8
Warnings:					
Information:					
2		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:					
3		NPL_15372317_Rejections_and_Amendments.PDF	559675 6e2132f6156a8e358b3740650cfc594605ad2c68	yes	19

Multipart Description/PDF files in .zip description

Document Description	Start	End
Non Patent Literature	1	11

	Non Patent Literature		12	19	
Warnings:					
Information:					
4		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:					
5		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:					
6		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:					
7		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:					
8		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:					
9	Fee Worksheet (SB06)	fee-info.pdf	30747 b5c6511e1ad59fb7320cdb811fb16262138a122a	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	22005050		

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-660CT2	5934

27189 7590 06/16/2017

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
06/16/2017	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. 14/639,034	Applicant(s) MARTINEZ DE VELASCO CORTINA ET AL.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/30/2017*.

☐ 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) *1-4 and 7-16* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☐ Claim(s) *1-4 and 7-16* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *03/04/2015* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *12/30/2015*.

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. In view of the appeal brief filed on **January 30, 2017**, PROSECUTION IS HEREBY REOPENED. New grounds of rejections are set forth below.

3. To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

4. A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

5. Claims 1-4, 7-16 have been examined in this application. Information disclosure statements (IDS) filled on 05/09/2016, 03/02/2017, and 05/25/2017 have been considered.

Response to Arguments

6. Applicant's arguments, see page 6, filed 01/30/2017, with respect to claim rejections under 35 U.S.C. §112(b) have been fully considered but are not persuasive.

7. Applicant's arguments, see pages 7-10, filed 01/30/2017, with respect to claim rejections under 35 U.S.C. §101 have been fully considered and are persuasive; therefore the rejection is withdrawn.

8. Applicant's arguments, see pages 10-12, filed 01/30/2017, with respect to claim rejections under 35 U.S.C. §103 have been fully considered and are partially persuasive. Furthermore, the claims are rejected under a new grounds of rejection.

Applicant argues:

I. Walker doesn't teach associating biometric information with the payment information.

A. New ground of rejection renders the argument moot.

Examiner notes that without conceding that Walker does not teach the association of biometric data with the payment information in light of furthering prosecution, a new ground of rejection is made in view of U.S. Patent Application Publication 2006/0020558 to Bonalle et al. ("Bonalle").

II. Walker does not teach automatically generating a key and providing transaction information.

B. The claims do not recite "automatically" nor would that overcome Walker.

The Examiner disagrees with Applicant's arguments that the reference to Walker does not teach "automatically generating a key and providing transaction information upon successful authentication of the biometric information... in Claims 1 and 10." Applicant points to Walker's Step 355 in Figure 3B and notes that Walker requires the user to provide a request for the generation of the single use credit card number. Although this is true, it is only true for this single embodiment to Walker. Applicant has dismissed the all other teachings and recitation of

what Walker's invention is directed to. For example, Figure 10 in walker discloses explicitly that the user first inputs their biometric data, the user is authenticated, and in Step 1003, the device searches for a single use card number; which is done without any further input from the user. In other words, after the user is authenticated to the device, the device displays a single use credit card number to the user without the user doing anything; which is in line with how the Applicant seems to disclose "automatically" generating...

Even if Walker did not teach automatically generating a single use credit card number after the user is authenticated, one of ordinary skill in the art would obviously make such a step an automated. Most importantly, the claim does not recite "automatically" nor does the specification disclose "automatically" doing anything. Simply automating something does not result in the claim limitation as being non-obvious. If a new combination of old elements is to be patentable, the elements must cooperate in such manner as to produce a new, unobvious, and unexpected result; see *In re Venner*, 120 USPQ 192 (CCPA 1958), *In re Smith*, 73 USPQ 394 (CCPA 1947).

In conclusion, Walker teaches what the Applicant is referring to as "automatically generating a key and providing transaction information upon successful authentication of the biometric information." See Figures 3, 5-7, and 10 and related text. The Examiner notes that in Walker, a user inputs biometric data into a device that is used to settle a transaction. Once the user is authenticated the card then generates a credit card number based on numerous data. The generated credit card number is then provided for settlement of a transaction. Most importantly, the generated credit card data includes many key variables which are utilized to settle the transaction; such as: a) a nonce, b) an initialization variable (I.V.), c) a transaction amount, and

d) a merchant identifier. The device first encrypts the nonce, then the device encrypts the combination of the nonce, the I.V. value, and account number to generate an encrypted credit card number. The "key" as recited in Claim 1, is first generated before being encrypted along with the payment information. This "key" is mapped as being the initialization variable which is generated for every transaction. The encryption of such data is done as a whole, meaning the I.V. and nonce and account number are all encrypted and transmitted or provided to the merchant. The reference explicitly teaches that at least two parts of data are encrypted, and one of ordinary skill in the art can encrypt as many pieces of information as they see fit since that would simply increase security measures. See Walker, Col. 7, Ln. 25-51; Col. 8, Ln. 1-30; Col. 10, Ln. 15-21 and Figures 4-8 and related text. Furthermore, there is no indication in the disclosure as to what the Applicant defines as generating a "key." The disclose does not in any form indicate how the key is generated not alone that the key is generated automatically.

Specification

9. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Applicant should point to the portion(s) in the specification where it is clearly recited how the encryption of the "key and the payment information stored in memory" is carried out. It is not clear how the key and payment information is encrypted not is there a relationship between the generated key and the encryption of the key. If the key is generated, then how is it being encrypted along with the payment information?

Priority Date

10. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, 365(c), or 386(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 5 U.S.C. 119(e) or under 35 U.S.C. 120, 121, 365(c), or 386(c) as follows:

The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original non-provisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of 35 U.S.C. 112(a) or the first paragraph of pre-AIA 35 U.S.C. 112, except for the best mode requirement. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994)

The disclosure of the prior-filed application, Application No. 60/394,241 fails to provide adequate support or enablement in the manner provided by 35 U.S.C. 112(a) or pre-AIA 35 U.S.C. 112, first paragraph for one or more claims of this application. The disclosure in Application 60/394,241 does not include at least the association of the biometric module with the payment information; recited in at least claims 1, 11, and 18. Applications 10/615,026 and 11/279,912 were also determined as lacking support for at least the association of the biometric module with the payment information. Application 10/615,026 was filled on July 09, 2003 and Application 11/279,912 was filled on April 17, 2006. Although multiple other applications were filled as continuations following the 11/279,912 filling, all of these applications do not have support in the manner required to claim priority to such filling dates. Applications 12/688,666, 13/175,768, 13/350,665, and 14/022,135 do not have support for the claimed limitations;

therefore the earlier priority date is determined to be July 01, 2014 based on Application 14/321,781, which discloses claims similar to those of the instant Application.

Claim Rejections - 35 USC § 112

11. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

12. Claims 1 and 10 and all of their dependent claims are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention. Claims 1 and 10 recite "generating a key…" and "encrypting the key…" and "provide... the encrypted key and payment information." The specification was examined carefully, yet there is no mention of a key being generated or even how such a key is generated. The specification does disclose "keys" but these keys are not generated and are simply "keys" that are stored in memory. Also, the specification does not mention the encryption of such a generated key or keys not alone encrypting both the key and the payment information. The specification only recites the keys are encrypted keys not that the keys are first generated and are

encrypted (two distinct recitations) and how such keys are being encrypted. The specification also recites the types of encryptions utilizes and not how the keys are first generated before being encrypted. Lastly, the specification simply recites that a "chip can have a cryptographic block with 4 exchange encrypted keys with up to 256 bits." Again, this is not the same as generating a key, then encrypting that key and providing support of how both steps are carried out. See at least ¶ 0047, 0052, 0058, 0085, 0088, 0106, 0108-0109, 0120. Furthermore, the "provide... the encrypted key and payment information" limitation is not supported by the specification nor is there any mention of two pieces of information being provided individually or separately for use in a transaction. Although the specification discloses that a transaction can be carried out with a POS it does not recite, in any shape or form, that the transaction information includes the encrypted key and transaction information.

13. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claim elements "a biometric module configured to read… an authentication module configured to authenticate… a secure module configured to..." in claims 1 and 10 are limitations that invoke 35 U.S.C. 112, sixth paragraph. However, the written description fails to disclose the corresponding structure, material, or acts for the claimed function. The specification describes a "RF Communications Device (e.g., Cellular Telephone" that includes a modulator, converter, encoder, decoder, an instruction sequencer, a security management unit, and a cryptographic

block ¶ 0013-0014. Further, the specification describes in ¶ 0070-0073 a "POS device" including "a fingerprint reader"/"fingerprint scanner," and a chip (see also Figures, 1, 2, and 5). The specification does not describe any structure corresponding to these devices or components used by the devices. Because these limitations invoke 112(f), the specification must clearly link the recited functions to the corresponding structure. For computer-implemented means-plus-function limitations, the corresponding structure includes both the computer and the algorithm that performs the recited functions. This requirement is described in the notice issued in the Federal Register on March 8, 2011. Specifically, the notice states:

> 3. Computer-Implemented Means-Plus-Function Limitations: For a computer-implemented means-plus-function claim limitation invoking §112, ¶6, the corresponding structure is required to be more than simply a general purpose computer or microprocessor.96 To claim a means for performing a particular computer-implemented function and then to disclose only a general purpose computer as the structure designed to perform that function amounts to pure functional claiming.97
>
> The structure corresponding to a §112, ¶6 claim limitation for a computer-implemented function must include the algorithm needed to transform the general purpose computer or microprocessor disclosed in the specification.98 The corresponding structure is not simply a general purpose computer by itself but the special purpose computer as programmed to perform the disclosed algorithm.99

The notice further states:

> A rejection under §112, ¶2 is appropriate if the specification discloses no corresponding algorithm associated with a computer or microprocessor.103 For example, mere reference to a general purpose computer with appropriate programming without providing an explanation of the appropriate programming,104 or simply reciting "software" without providing detail about the means to accomplish the software function,105 would not be an adequate disclosure of the corresponding structure to satisfy the requirements of §112, ¶2. In addition, merely referencing a specialized computer (e.g., a "bank computer"), some undefined component of a computer system (e.g., "access control manager"), "logic," "code," or elements that are essentially a black box designed to perform the recited function, will not be sufficient because there must be some explanation of how the computer or the computer component performs the claimed function.106

Here, the specification does not recite that the biometric module, authentication module, and a secure module," are associated with any computer, microprocessor, or other structure, where the computer performs the algorithms necessary to carry out the functions of the mobile device. Additionally, the term "device" is a non-structural term.

Applicant may:

(a) Amend the claim so that the claim limitation will no longer be interpreted as a limitation under 35 U.S.C. 112, sixth paragraph; or

(b) Amend the written description of the specification such that it expressly recites what structure, material, or acts perform the claimed function without introducing any new matter (35 U.S.C. 132(a)).

If applicant is of the opinion that the written description of the specification already implicitly or inherently discloses the corresponding structure, material, or acts so that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function, applicant should clarify the record by either:

(a) Amending the written description of the specification such that it expressly recites the corresponding structure, material, or acts for performing the claimed function and clearly links or associates the structure, material, or acts to the claimed function, without introducing any new matter (35 U.S.C. 132(a)); or

(b) Stating on the record what the corresponding structure, material, or acts, which are implicitly or inherently set forth in the written description of the specification, perform the claimed function. For more information, see 37 CFR 1.75(d) and MPEP §§ 608.01(o) and 2181.

Claims 2-4, 7-9 and 11-16 are also rejected as each depends on claims 1 and 10.

15. Claims 1-4, 7-16 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject

matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

16. Claim 1 and 10 recite "generate a key…" and "encrypt the key and the payment information stored in memory…" Generating the "key" is indefinite since no clear recitation of how such key is to be generated is recited nor is there a recitation of how one of ordinary skill in the art is to carry out the encryption of the "key" and the "payment information." Since there are multiple ways to generate keys and encryption information including the generated keys, it is indefinite as to how such limitation are to be carried out. Applicant has failed to particularly point out and distinctly claim the subject matter which the inventor(s) regards as the invention. For at least these reasons the claims and their dependent claims are determined to be indefinite. For purposes of examination any recitation of any generation of any data along with encrypting such data along with other data (such as financial data) will be determined as reading on the claim limitations. All dependent claims of Claims 1 and 10 are also rejected.

17. Claims 1 and 10 recite "generating a key when the biometric information ready by the biometric reading device is successfully authenticated." It is not known whether the biometric device is part of the mobile device, a standalone device, or part of some other device, which is used to read the biometric information because the claim already recited that the mobile device includes a "biometric module." It is indefinite as to how to distinguish between the mobile device including a biometric module that reads biometric data and also another device referred to as the "biometric reading device." It is also indefinite as to how the mobile device, the biometric module, and the biometric reading device all work in conjunction with one another. If the biometric reading device is another device that also reads biometric data, then it is indefinite as

to how such a device is able to access the mobile device's memory, which stores the user's biometric data. For purposes of examination, any device that includes a single biometric reader will be determined as reading on the claim limitations. Claims 2-4, 7-9 and 11-16 are also rejected for their dependence on Claims 1 and 10.

18. Claims 1 and 10 recite "the biometric reading device." There is insufficient antecedent basis for this limitation in the claim. Claims 2-4, 7-9 and 11-16 are also rejected for their dependence on Claims 1 and 10.

19. Claim 10 recites "a central database configured to…" There is insufficient antecedent basis for this limitation in the claim. Claims 11-16 are also rejected for their dependence on Claim 10.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 1-4, 7-16 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,163,771 to Walker et al. (herein after referred to as simply Walker), in view of U.S. Patent 6,848,048 to Holmes (herein after referred to as simply Holmes), in further view of U.S. Patent Application Publication 2006/0020558 to Bonalle et al. (herein after referred to as simply Bonalle).

22. Per claims 1 and 10, Walker teaches all of the following limitations:

a. A mobile device, comprising [Abstract]:

b. Memory (memory) configured to store biometric authentication information (biometric information) and payment information (account number), [...] [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

c. a biometric module configured to read biometric information (device has a biometric reader to receive user biometric data) [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

d. a secure module configured to (processor) [Walker, Abstract]:

e. generate a key (generates a I.V. for every transaction the user wants to carry out, the I.V. is different for every transaction, thus it is generated for every transaction) when the biometric information read by the biometric reading device is successfully authenticated [Col. 5, Ln. 49-67, Col. 6, Ln. 1-38 and Figures 1-9];

Examiner notes that the following is a conditional limitation: "when the biometric information read by the biometric reading device is successfully authenticated."

f. Walker teaches encrypt the key and the payment information stored in memory [Col. 7, Ln. 25-51; Col. 8, Ln. 1-30; Col. 10, Ln. 15-21 and Figures 4-8 and related text]; and

g. Walker teaches provide [...] the encrypted key and payment information for use in a transaction; (the device transmits payment information including IV, CC# and much more to the merchant to settle the transaction) [Col. 2, Ln. 39-53; Col. 4, Ln. 5-15; 50-62; Col. 8, Ln. 61-67; Col. 9, Ln. 1-10].

Examiner notes that the following is an intended use limitation, which does not have much patentable weight: "for use in a transaction."

Walker does not explicitly teach:

h. Walker does not teach radio frequency (RF) cellular circuitry; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings Holmes to explicitly teach a short range RF circuitry which can be incorporated into Walker's smart in motivation of increasing security measures while also enhancing user experience in carrying out a transaction.

i. Walker does not explicitly teach [...] wherein the biometric authentication information is associated with the payment information; however, Bonalle does [Abstract, Paragraph 0047, 0244-0245, 0256].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, which teaches a mobile payment device including a biometric reader configured to authenticate a user by comparing the user's input biometric data to the user's stored biometric data in the device's memory, wherein the device generates a one-time use credit card number for use in a transaction, in view of Holmes which teaches incorporating RF circuitry into Walker's device to include the teachings of Bonalle which teaches that a mobile device utilized for carrying out a transaction will have the biometric data associated with the payment data of the user using the mobile

device in motivation of only allowing the proper user to whom the card belongs to, to carry out a transaction. This results in increased security measures since the mobile card or device is unusable by another user.

j. Walker does not explicitly teach an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; however, Bonalle does [Abstract, Paragraph 0047, 0244-0245, 0256].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, which teaches a mobile payment device including a biometric reader configured to authenticate a user by comparing the user's input biometric data to the user's stored biometric data in the device's memory, wherein the device generates a one-time use credit card number for use in a transaction, in view of Holmes which teaches incorporating RF circuitry into Walker's device to include the teachings of Bonalle which teaches that a mobile device utilized for carrying out a transaction authenticates user biometric data and that the biometric authenticated data is associated with the payment data of the user using the mobile device in motivation of only allowing the proper user to whom the card belongs to, to carry out a transaction. This results in increased security measures since the mobile card or device is unusable by another user.

k. Walker does not explicitly teach […] via the short range RF circuitry […]; however, Holmes does (medium over which information may be transferred ... radio frequency "RF") [Abstract, Col. 2, 34-61, and Figures 1-9].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings Holmes to explicitly teach a short range RF circuitry which can be incorporated into Walker's smart in motivation of increasing security measures while also enhancing user experience in carrying out a transaction.

The Examiner notes that ISO/IEC 14443 is a standard which defines contactless communications using smart cards and integrated circuits and transmission protocols for contactless communications; which is known to one of ordinary skill in the art. This standard is provided as reference to show that RF circuitry is an obvious communication method that is obviously used in mobile devices and standardizes the usage of contactless smart cards.

Per claim 10, Walker teaches:

a. a point of sale (POS) device (terminal / merchant terminal) configured to [Col. 6; Ln. 5-14; Col. 8, Ln. 30-67; Col. 9, Ln. 10-35; Col. 12, Ln. 19-50; and Figures 2-3, 9, 11 and related text]:

b. receive, from the secure module, the encrypted key and payment information; [Col. 6; Ln. 5-14; Col. 8, Ln. 30-67; Col. 9, Ln. 10-35; Col. 12, Ln. 19-50; and Figures 2-3, 9, 11 and related text];

c. transmit, to a central database (CC Issuer), the encrypted key and payment information [Col. 6; Ln. 5-14; Col. 8, Ln. 30-67; Col. 9, Ln. 10-35; Col. 12, Ln. 19-50; and Figures 2-3, 9, 11 and related text]; and

d. a central database configured to validate the key and the payment information [Col. 6; Ln. 5-14; Col. 8, Ln. 30-67; Col. 9, Ln. 10-35; Col. 12, Ln. 19-50; and Figures 2-3, 9, 11 and related text].

Examiner notes that the following is an intended use limitation: "configured to validate the key and the payment information," which does not have much patentable weight.

23. Per claims 2 and 11, Walker teaches wherein the biometric module is configured to read biometric information provided by a user to complete the transaction [Walker, Col. 5, Ln. 59-61 and Figures 1-9].

Examiner notes the following is an intended use limitation which does not have much patentable weight: "configured to read biometric information provided by a user to complete the transaction."

24. Per claims 3 and 12, Walker teaches wherein the payment information is associated with a primary account number (account number) [Col. 6, Ln. 14-35, 54-59, Col. 7, Ln. 27-36 and Figures 1-3 and 6].

25. Per claim 4, Walker teaches wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device (the device transmits payment information including IV, CC# and much more to the merchant's device which is interpreted to be the POS to settle the transaction) [Col. 2, Ln. 39-53; Col. 4, Ln. 5-15; 50-62; Col. 8, Ln. 61-67; Col. 9, Ln. 1-10].

Examiner notes the following limitation is an intended use limitation which does not have much patentable weight: "wherein the transaction module is configured to provide the

transaction information comprising the encrypted key and payment information to a point of sale (POS) device."

26. Per claims 8 and 15, Walker teaches wherein the payment information (account number) is stored in a memory accessible only by the secure module (central processor 101) [Col. 6-7, Ln. 61-, 1-3 and Figures 1-3].

27. Per claims 9 and 16, Walker does not explicitly teach wherein the short range RF circuitry comprises a radio frequency identification (RFID) device; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings Holmes to explicitly teach a short range RF circuitry which can be incorporated into Walker's smart in motivation of increasing security measures while also enhancing user experience in carrying out a transaction.

28. Claims 7 and 14 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Walker, in view of Holmes and Bonalle, as applied to claims 1 and 10 above, in further view of U.S. Patent Application Publication 2002/0112177 to Voltmer et al. (herein after referred to as simply Voltmer).

29. Per claims 7 and 14 Walker in view of Holmes do not explicitly teaches wherein the biometric authentication information is stored separately from the payment information [Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3]. Acknowledgement

Voltmer teaches storing separately a plurality of information [Paragraphs 009-0091 and Figures 12A and 12B].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker which teaches a device that includes a memory / secure memory to include the teachings of Voltmer to explicitly teach storing data in sections or partitions or separately from other data in motivation of increasing security measures or facilitating the upload of information from the memory.

Double Patenting

30. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope

of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

31. Claim 1 of the instant Application is rejected on the ground of nonstatutory double patenting as being unpatentable over Claim 3 of prior U.S. Patent No. 8766772. Although the claims at issue are not identical, they are not patentably distinct from each other. Claim 3 in U.S. Patent 8766772 teaches the claim limitations of the instant Application's Claim 1, but does not teach "a secure module configured to: generate a key when the biometric information read by the biometric reading device is successfully authenticated; encrypt the key and the payment information stored in memory." Walker, U.S. Patent 6163771, teaches such missing limitations; see Col. 5, Ln. 49-67, Col. 6, Ln. 1-38; Col. 7, Ln. 25-51; Col. 8, Ln. 1-30; Col. 10, Ln. 15-21 and Figures 1-9 and related text. It would have been obvious to one of ordinary skill in the art to combine the teachings of U.S. Patent 8766772 and the teachings of Walker in order to generate a value and encrypt such a value along with the payment information before providing them for settlement of the transaction in motivation of increasing security measures.

32. Claims 2-17 are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14/659502 in view of U.S. Patent 6,163,771 to Walker.

This is a provisional obviousness-type nonstatutory double patenting rejection.

33. Although the conflicting claims are not identical, they are not patentably distinct from each other. Claims 1 and 10 of co-pending application 14/659502 recites:

a. mobile device, comprising:

b. short range radio frequency (RF) circuitry;

c. memory configured to store biometric authentication information and payment information;

d. a biometric module configured to read biometric information;

e. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

f. a secure module configured to:

g. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

h. encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction

Claim 10:

j. A system, comprising:

k. a mobile device, comprising:

l. short range radio frequency (RF) circuitry;

m. memory configured to store biometric authentication information and payment information;

n. a biometric module configured to read biometric information;

o. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

p. a secure module configured to:

q. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

r. encrypt the key and the payment information stored in memory; and

s. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

t. a point of sale (POS) device configured to:

u. receive, from the secure module, the encrypted key and payment information; and

v. transmit, to a central database, the encrypted key and payment information; and

w. a central database configured to validate the key and the payment information.

Claims 1 and 10 of co-pending application 14/659502 differ since they fail to recite the authentication module is configured to authenticate the biometric input data is associated with

the payment information. U.S. Patent Application Publication 2006/0020558 to Bonalle et al. ("Bonalle") discloses an authentication module configured to authenticate the biometric information read by the biometric module is associated with the payment information [Abstract, Paragraph 0047, 0244-0245, 0256]. Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of co-pending Application 14/659,502 to include the teachings of Bonalle, which teaches a mobile device utilized for carrying out a transaction will have the biometric data associated with the payment data of the user using the mobile device in motivation of only allowing the proper user to whom the card belongs to, to carry out a transaction. This results in increased security measures since the mobile card or device is unusable by another user.

34. It is well settled that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA 1963). Also note Ex parte Rainu, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

35. Co-pending Applications 14/321781, 14/724593, 14/585057 are also rejected based on the same above rationale.

Conclusion

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed on for PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191.

The examiner can normally be reached on MON - FRI: 7:30AM-5PM EST Every other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Hayes can be reached on (571)272-6708. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/
Patent Examiner, Art Unit 3685
05/27/2017

/MAMON OBEID/
Primary Examiner, Art Unit 3685

/JOHN HAYES/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 14/639,034	Applicant(s)/Patent Under Reexamination MARTINEZ DE VELASCO CORTI	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2003/0018522 A1	01-2003	Denimarck, Paul	G06Q20/40145	705/14.23
*	B	US-2006/0020558 A1	01-2006	Bonalle; David S.	G06Q20/341	705/64
	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.

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	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/E.O/	1	7911643	B2	2011-03-22	Yamada	
/E.O/	2	6934861	B2	2005-08-23	Haala	
/E.O/	3	5590197	A	1996-12-31	Chen	

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

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/E.O/	1	20040128249	A1	2004-07-01	Hoffman	

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							

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

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
/E.O/	1	Appeal Brief filed April 18, 2017 for US patent application no. 14/659,502.	
/E.O/	2	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/659,502.	
/E.O/	3	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.	
/E.O/	4	US Office Action dated May 16, 2016 received in US patent application no. 14/659,502.	
/E.O/	5	Response to Office Action filed on December 23, 2015 for US patent application no. 14/659,502.	
/E.O/	6	US Office Action dated June 22, 2015 received in US patent application no. 14/659,502.	
/E.O/	7	Response to Office Action filed on May 2, 2017 for US patent application no. 15/372,317.	
/E.O/	8	US Office Action dated February 2, 2017 received in US patent application no. 15/372,317.	
/E.O/	9	Response to Office Action filed on November 18, 2016 for US patent application no. 14/321,781.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

/E.O/	10	US Office Action dated May 19, 2016 received in US patent application no. 14/321,781.	
/E.O/	11	Response to Office Action filed on December 24, 2015 for US patent application no. 14/321,781.	
/E.O/	12	US Office Action dated June 24, 2015 received in US patent application no. 14/321,781.	
/E.O/	13	US Notice of Allowance dated April 11, 2014 received in US patent application no. 14/022,135.	
/E.O/	14	Response to Office Action filed on March 14, 2014 for US patent application no. 14/022,135.	
/E.O/	15	US Office Action dated March 7, 2014 received in US patent application no. 14/022,135.	
/E.O/	16	Response to Office Action filed on February 3, 2014 for US patent application no. 14/022,135.	
/E.O/	17	US Office Action dated December 5, 2013 received in US patent application no. 14/022,135.	
/E.O/	18	Response to Office Action filed on April 26, 2017 for US patent application no. 14/724,593.	
/E.O/	19	US Office Action dated February 17, 2017 received in US patent application no. 14/724,593.	
/E.O/	20	Pre-Brief Appeal Conference Decision dated December 12, 2016 and received in US patent application no. 14/724,593.	

EFS Web 2.1.17

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

/E.O/	21	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.	
/E.O/	22	US Office Action dated May 6, 2016 received in US patent application no. 14/724,593.	
/E.O/	23	Response to Office Action filed on January 7, 2016 for US patent application no. 14/724,593.	
/E.O/	24	US Office Action dated August 4, 2015 received in US patent application no. 14/724,593.	
/E.O/	25	US Notice of Allowance dated December 3, 2014 received in US patent application no. 14/028,469.	
/E.O/	26	Supplemental response to Office Action filed on October 31, 2014 for US patent application no. 14/028,469.	
/E.O/	27	Response to Office Action filed on October 14, 2014 for US patent application no. 14/028,469.	
/E.O/	28	US Office Action dated August 18, 2014 received in US patent application no. 14/028,469.	
/E.O/	29	US Office Action dated July 9, 2014 received in US patent application no. 14/028,469.	
/E.O/	30	Response to Office Action filed on June 13, 2014 for US patent application no. 14/028,469.	
/E.O/	31	US Office Action dated April 3, 2014 received in US patent application no. 14/028,469.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

/E.O/	32	Response to Office Action filed on March 14, 2014 for US patent application no. 14/028,469.	
/E.O/	33	US Office Action dated March 6, 2014 received in US patent application no. 14/028,469.	
/E.O/	34	Response to Office Action filed on February 3, 2014 for US patent application no. 14/028,469.	
/E.O/	35	US Office Action dated December 6, 2013 received in US patent application no. 14/028,469.	
/E.O/	36	Appeal Brief filed February 9, 2017 for US patent application no. 14/585,057.	
/E.O/	37	Pre-Brief Appeal Conference Decision dated November 30, 2016 and received in US patent application no. 14/585,057.	
/E.O/	38	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.	
/E.O/	39	US Office Action dated May 9, 2016 received in US patent application no. 14/585,057.	
/E.O/	40	Response to Office Action filed on January 7, 2016 for US patent application no. 14/585,057.	
/E.O/	41	US Office Action dated October 7, 2015 received in US patent application no. 14/585,057.	

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

EXAMINER SIGNATURE			
Examiner Signature	/EL MEHDI OUSSIR/	Date Considered	05/30/2017

*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. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

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)	2017-05-25
Name/Print	Daniel K. Robertson	Registration Number	48077

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

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	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

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
/E.O/	1	20060020558	A1	2006-01-26	Bonalle	
	2					

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/EL MEHDI OUSSIR/	Date Considered	05/30/2017

*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. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

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)	2017-03-01
Name/Print	Daniel K. Robertson	Registration Number	48,077

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14639034	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC- SEARCHED		
Symbol	Date	Examiner
G06Q	5/8/2015	EO
H04L	5/8/2015	EO

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
705		5/8/2015	EO

SEARCH NOTES		
Search Notes	Date	Examiner
consulted Calvin Hewitt	5/15/2015	EO
Consulted John H. and Mamon O on 101/ 103	5/25/2017	EO
Consulted John H. on priority	5/9/2017	EO
Consulted Mohammad N. on priority and 112	5/26/2017	EO

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

/E.O./ Examiner.Art Unit 3685	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14639034	MARTINEZ DE VELASCO CORTINA ET AL.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

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

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

CLAIM		DATE								
Final	Original	05/18/2015	12/09/2015	05/26/2017						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	-	-						
	6	✓	-	-						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	✓	✓						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:26
S2	1	("6163771").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:27
S5	16	(biometric near1 data) near2 stored near2 (separately or different)	US-PGPUB; USPAT	OR	ON	2015/05/18 15:53
S6	5	"7911643"	US-PGPUB; USPAT	OR	ON	2015/05/18 15:59
S8	0	(separatly near1 stor$3) with data	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S9	12789	(stor$3 near1 data) with separately	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S10	1434	S9 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S11	1011	S10 and ((information or data) near4 (separately))	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S15	919	S11 and (memory)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:07
S19	0	S15 and (stor$3 near4 saperately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:08
S20	498	(authentication near4 stor$3 near4 separately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:13
S21	34	S20 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:16
S22	48796	(stor$4 near3 information separately) same (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S24	29064	(stor$4 near3 information separately) with (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S25	5880	S24 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S26	51	S25 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:26
S27	1	"20020112177"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:32
S28	1	"20020077993"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:40
S29	10379	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near4 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S30	7730	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near2 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S31	4128	((generate) near2 (key pin code token	US-PGPUB;	OR	ON	2015/06/12

		password)) with ((encrypt) near3 (key pin code token password))	USPAT			16:22
S32	3286	((generate) near2 (key pin code token password)) with ((encrypt) near2 (key pin code token password))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:22
S33	1736	S32 and (transaction financial account)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S34	1134	S33 and @pd<"20120101"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S35	234	S34 and (RFID RD infrared)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S37	63	S35 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:24
S38	850	"5590197"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:44
S39	1	("5590197").PN.	US-PGPUB; USPAT	OR	OFF	2015/06/12 16:44
S40	0	(("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" | "6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" | "5742618" | "6276607" | "6570487" | "8004410").PN.").PN.	US-PGPUB; USPAT	OR	OFF	2015/09/30 16:19
S42	66	("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" | "6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" |	US-PGPUB; USPAT	OR	ON	2015/09/30 16:20

		"5742618" | "6276607" | "6570487" | "8004410").PN.				
S43	2	"20070022058"	US-PGPUB; USPAT	OR	ON	2016/04/21 15:56
S44	5	(US-20070022058-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2016/12/01 10:38
S45	0	S44 and ((biometric near4 associat$4) with (payment))	US-PGPUB; USPAT	OR	ON	2016/12/01 10:39
S46	39	((biometric near4 associat$4) near4 (payment near2 information))	US-PGPUB; USPAT	OR	ON	2016/12/01 10:39
S47	24	S46 and @pd<"20130909"	US-PGPUB; USPAT	OR	ON	2016/12/01 10:41
S48	5	(US-20070022058-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S49	3	S48 and ((mobile card) near3 (device))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S50	39	((biometric near4 associat$4) near4 (payment near2 information))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S51	34	S50 and ((mobile card) near3 (device))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S52	21	S51 and @pd<"20130909"	US-PGPUB; USPAT	OR	ON	2016/12/01 14:47
S53	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2017/05/24 11:05
S54	1	S53 and (encrypt$4 with key with payment)	US-PGPUB; USPAT	OR	ON	2017/05/24 11:06
S55	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2017/05/25 10:48
S56	0	S55 and (RF near3 device)	US-PGPUB; USPAT	OR	ON	2017/05/25 10:48
S57	1	S55 and (RF with device)	US-PGPUB; USPAT	OR	ON	2017/05/25 10:48
S58	0	(2014/0040628).CCLS.	US-PGPUB; USPAT	OR	OFF	2017/05/25 16:15
S59	0	(2014/0040628).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/05/25 16:15
S60	3	("20140040628").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/05/25 16:16

EAST Search History (Interference)

<This search history is empty>

5/30/2017 2:15:33 PM
C:\Users\eoussir\Documents\EAST\Workspaces\14639034_Mobile device RFID transaction biometric POS.wsp

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-660CT2

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
/E.O/	1	20070022058	A1	2007-01-25	Labrou et al.	
	2					

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1		

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

EXAMINER SIGNATURE

Examiner Signature	/EL MEHDI OUSSIR/	Date Considered	05/30/2017

*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	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-660CT2

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	/Noel C. Gillespie/	Date (YYYY-MM-DD)	2016-05-09
Name/Print	Noel C. Gillespie	Registration Number	47596

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.
14/639,034	03/04/2015	de VELASCO CORTINA, Francisco Martinez	116546-613CT13	5934

EXAMINER	
OUSSIR, El Mehdi	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
December 12, 2017	EFS WEB

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

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

REPLY TO NON-FINAL OFFICE ACTION

Sir:

This paper is submitted in response to the Non-Final Office Action mailed on June 16, 2017. A three-month extension of time is submitted herewith. Please amend the above referenced application as follows:

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

Remarks begin on page 5 of this paper.

LISTING OF THE CLAIMS

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

What is claimed is:

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

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

a biometric reading device ~~module~~ configured to read biometric information;

one or more processors ~~an authentication module~~ configured to authenticate that the biometric information read by the biometric reading device ~~module~~ is associated with the payment information based ~~at least in part~~ on the biometric authentication information stored in memory; and

a security management unit ~~secure module~~ configured to:

encrypt ~~generate~~ a key when the biometric information read by the biometric reading device is successfully authenticated;

encrypt the ~~key and the~~ payment information stored in memory; and

transmit~~provide~~, via the short range RF circuitry, the encrypted key and the encrypted payment information for use in a transaction.

2. (Currently Amended) The mobile device of claim 1, wherein the biometric reading device ~~module~~ is configured to read biometric information provided by a user to complete the transaction.

3. (Original) The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. (Currently Amended) The mobile device of claim 1, wherein the security management unit~~secure module~~ is configured to provide the encrypted key and payment information to a point of sale (POS) device.

5. (Canceled)

6. (Canceled)

7. (Original) The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. (Currently Amended) The mobile device of claim 1, wherein the payment information is stored in a memory accessible only by the security management unit~~secure module~~.

9. (Original) The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. (Currently Amended) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information;

a biometric reading device ~~module~~ configured to read biometric information;

one or more processors ~~an authentication module~~ configured to authenticate that the biometric information read by the biometric reading device ~~module~~ is associated with the payment information based at least in part on the biometric authentication information stored in memory; and

a security management unit ~~secure module~~ configured to:

~~generate~~ encrypt a key when the biometric information read by the biometric reading device is successfully authenticated

encrypt ~~the key and~~ the payment information stored in memory; and

~~provide~~transmit, via the short range RF circuitry, the encrypted key and the encrypted payment information for use in a transaction; and

a point of sale (POS) device configured to:

receive, from the security management unit~~secure module~~, the encrypted key and payment information; and

transmit, to a central database, the encrypted key and payment information; and

a central database configured to validate the key and the payment information.

11. (Currently Amended) The system of claim 10, wherein the biometric reading device ~~module~~ is configured to read biometric information provided by a user to complete the transaction.

12. (Original) The system of claim 10, wherein the payment information is associated with a primary account number.

13. (Original) The system of claim 10, wherein the POS device includes an RF reader.

14. (Original) The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. (Currently Amended) The system of claim 10, wherein the payment information is stored in a memory accessible only by the security management unit~~secure module~~.

16. (Original) The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

REMARKS

Following this amendment, claims 1-4 and 7-16 are pending in the application and are presented for reconsideration and further examination. By the foregoing amendments claims 1, 2, 4, 8, 10, 11, and 15 have been amended. No new matter has been added.

Nonstatutory Double Patenting

Claim 1 stands rejected on the ground of nonstatutory double patenting as being unpatentable over claim 3 of prior U.S. Patent No. 8766772. Claims 2-17 (interpreted as claims 2-16) are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14/659502 in view of U.S. Patent 6,163,771 to Walker.

Not notwithstanding the following remarks and arguments as to the allowability of the pending claims over Walker, claims 1-16 may further change throughout prosecution. Therefore, applicant requests the rejection be held in abeyance until the claims are otherwise in condition for allowance.

Priority Claim

The office action states, "Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under [35 U.S.C.] 119(e) or under 35 U.S.C. 120, 121, 365(c), or 386(c)" because, "[t]he later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original non-provisional application or provisional application)." Office Action, at pg. 6. Specifically, the office action states that "[t]he disclosure in Application 60/394,241 does not include at least the association of the biometric module with the payment information; recited in at least claims 1 and 10. Applicant respectfully disagrees.

Applicant notes that the provisional application 60/394,241 discloses at least,

> This is performed by combining GSM technology with a wireless RF-ID device that can store a person's identification information, including an electronic or biometric "signature" (e.g., fingerprint, facial, iris, or other recognition feature). The RF cellular telephone can thus become a

> person's identification document (e.g., passport, boarding pass) and/or credit card(s) or other card(s) (e.g., mileage cards).

Provisional Specification, at pg. 36, attachment 5, line 15.

The provisional specification further includes the same or similar subject matter, including the figures, as relied up on in the following discussion related to rejections under § 112. For example, the disclosure at pp. 43-50 and various flowcharts throughout, support the disclosure and claims of this application. Accordingly, applicant believes the priority claim is proper.

Rejections Under 35 U.S.C. § 112(a)

Claims 1 and 10 and all of their dependent claims are rejected as failing to comply with the written description requirement. In particular, the office action states,

> Claims 1 and 10 recite "generating a key ... " and "encrypting the key ... " and "provide ... the encrypted key and payment information." The specification was examined carefully, yet there is no mention of a key being generated or even how such a key is generated.

Office Action, at pg. 7. Applicant respectfully traverses the rejections and the characterization of the claims.

To advance prosecution, amended claim 1 recites, inter alia,

> a security management unit configured to:
> encrypt a key when the biometric information read by the biometric reading device is successfully authenticated;
> encrypt the payment information stored in memory; and
> transmit, via the short range RF circuitry, the encrypted key and the encrypted payment information for use in a transaction

Applicant submits that amended claim 1 is supported by the specification. As stated in the Specification, as filed,

> 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.

Specification, at [0014]; see also, Specification, at [0047]. Thus, the claimed "security management unit" can manage storage and transmission of the claimed "key"

and the claimed "payment information" within memory. The Specification further states,

> [a]s 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.

Specification, at [0120]. The "encrypted keys" are thus information, or a key, that is encrypted, as opposed to merely being encryption keys. These keys are encrypted (encrypted keys) and are then stored within the memory (e.g., by the cryptographic block) and later transmitted along with the payment information to the point of sale (POS).

With respect to the payment information and biometrics, the Specification states,

> 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 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.

Specification, at [0053]. Thus, the claimed "mobile device" can encrypt and store payment information in addition to biometric information.

Additionally, the Specification notes that,

> [i]nstead 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.

Specification, at [0070]. Thus, the encrypted payment information and the encrypted key can be provided to complete the transaction based on the biometric information.

For at least the foregoing reasons, applicant submits that amended claim 1 is well supported by the Specification. Accordingly, applicant requests the rejection be withdrawn. Amended claim 10 recites features similar to amended claim 1. Thus for at least the same reasons, applicant requests the rejections of the independent claims and all of associated dependent claims under § 112(b) be withdrawn

Rejections Under 35 U.S.C. § 112(f)

The office action further states, that the "Claim elements 'a biometric module configured to read ... an authentication module configured to authenticate ... a secure module configured to ... a transaction module configured to ..." in claims 2, 11, and 18 are limitations that invoke 35 U.S.C. 112, sixth paragraph. Applicant respectfully disagrees.

Solely to advance prosecution, claims 1 and 10 are amended. Applicant believes that the instant amendments address the issues indicated in the office action.

Accordingly, applicant requests the rejections of claims 1, 10, and all of the dependent claims under § 112(f) be withdrawn.

Rejections Under 35 U.S.C. § 103

Claims 1-4 and 7-16 stand rejected as being unpatentable over U.S. Patent No. 6,163,771 (Walker) in view of U.S. Patent No. 6,848,048 (Holmes) in further view of U.S. Patent No. 5,590,197 (Chen) and US 2006/0020558 (Bonalle). Claims 7 and 14 stand rejected as being unpatentable under Walker, Holmes, and Chen as applied to claims 1 and 10, and further combined with U.S. Pub. No. 2002/0112177 (Voltmer). Applicant respectfully traverses the rejections and the characterization of the claims and the references. Applicant respectfully traverses these rejections and the characterization of the claim and the reference.

The cited reference fails to disclose all of the features of the independent claims, as amended. For example, amended independent claim 1 recites,

> a security management unit configured to:
> encrypt a key when the biometric information read by the biometric reading device is successfully authenticated;

encrypt the payment information stored in memory; and

transmit, via the short range RF circuitry, the encrypted key and the encrypted payment information for use in a transaction

In rejecting claim 1, the office action, stating that Walker discloses,

a secure module configured to (processor) [Walker, Abstract]:

e. generate a key (generates a I.V. for every transaction the user wants to carry out, the I.V. is different for every transaction, thus it is generated for every transaction) when the biometric information read by the biometric reading device is successfully authenticated [Col. 5, Ln. 49-67, Col. 6, Ln. 1-38 and Figures 1-9];

Office Action, at pg. 13. Applicant respectfully disagrees.

Walker discloses a "device for facilitating financial account transactions." Walker, at Abstract. The device of Walker has biometric controls that limit access to the device itself. Walker requires the cardholder to request generation of a "single-use credit card" number after the cardholder has gained access to the device based on biometric information. This requires specific interaction with the device:

> The cardholder first inputs his PIN or biometric data to access the device [...]. If access is granted, the device responds by querying the cardholder on display whether it should generate a single-use credit card number [...]. The cardholder responds by requesting generation of a credit card number (for example, by keying "YES")

Walker, at 6:18-25 (emphasis added). However, Walker does not associate biometric information with payment information as set forth in claim 1. In Walker, the user accesses the device (step 351) using a PIN or biometric, and responds to a query (step 355) from the device causing the generation of a single-use credit card number (step 360). Nowhere does it say that the biometric is authenticated as being associated with payment information as alleged in the office action.

As an additional matter, instead of generating a key upon successful authentication of the biometric information as set forth in each of independent claims 1 and 10, Walker requires the cardholder to request generation of a single-use credit card information (step 355) after the cardholder has gained access to the device. Thus, Walker does not teach or suggest "encrypt[ing], a key when the biometric information read by the biometric reading device is successfully authenticated; encrypt[ing] the payment information stored in memory," as set forth in amended claim 1.

Walker is silent as to any confirmation that the biometric information used to access the device is in any way related to, or associated with specific "financial account identifiers" or the claimed "payment information." Walker is further silent as to any ***authentication*** to that effect. Such authentication is a specific pre-condition for the encrypting. The office action notes as much, stating that "when the biometric information read by the biometric reading device is successfully authenticated," is a conditional limitation (office action, at pg. 13). But Walker is silent to any related requirement. Therefore Walker fails to teach or suggest "the biometric information read by the biometric reading device is successfully authenticated as being associated with the payment information," as set forth in amended claim 1.

Holmes, Chen, and newly introduced Bonalle also fail to disclose or suggest the above noted features, and applicant notes that these references were not cited for such a purpose.

As another example, amended claim 1 recites, inter alia,

> one or more processors configured to authenticate that the biometric information read by the biometric reading device is associated with the payment information based on the biometric authentication information stored in memory.

The suggested combination of references fails to disclose or suggest at least this feature of amended claim 1.

In the response to arguments, the office action introduces Bonalle, stating that,

> Examiner notes that without conceding that Walker does not teach the association of biometric data with the payment information in light of furthering prosecution, a new ground of rejection is made in view of U.S. Patent Application Publication 2006/0020558 to Bonalle et al.("Bonalle").

In rejecting claim 1, the office action further states that "Walker does not explicitly teach [...] wherein the biometric authentication information is associated with the payment information; however, Bonalle does [Abstract, Paragraph 0047, 0244-0245, 0256]. Office Action, at pg. 14. Applicant respectfully disagrees.

As an initial matter, Bonalle is not prior art to this application, given the priority date in 2004. As noted above, priority in this case is proper to July 19, 2002. Thus

Bonalle is not prior art. Even if Bonalle could be considered prior art, Bonalle still fails to disclose or suggest the noted features of claim 1.

Bonalle notes that "the account number ... may be associated with ... biometric data." Bonalle, at [0047]. Bonalle also discloses that "a cardmember may have previously associated a credit card account, a debit card account, and a frequent flier account with his biometric sample." Bonalle, at [0244]. "Later, when cardmember desires to purchase groceries, cardmember may submit his biometric sample while using smartcard 100 for the purchase at access point 15." Bonalle, at [0244].

While the term "biometric" appears throughout Bonalle and can be implemented as a condition for "authorizing" a purchase with the associated credit card, for example, this is not the same as "[authenticating] that the biometric information read by the biometric reading device is associated with the payment information based at least in part on the biometric authentication information stored in memory," as claimed. Moreover, Bonalle is not associated with a mobile device.

Furthermore, there is the matter of the absence of any kind of connection between the purported "authentication" of Bonalle and "encryption" of Walker. Amended claim 1 requires that one is the result of the other. Not only are the disclosures of Walker and Bonalle largely incompatible where this claim feature is concerned, but the office action provides no "rational underpinning" or any reason why one of ordinary skill would look to Bonalle to modify Walker apart from a broad conclusion that "results in increased security measures since the mobile card or device is unusable by another user." Office Action, at pg. 15. This, of course, misses the above-noted elements of amended claim 1.

Holmes and Chen also fail to disclose or suggest the above noted features, and applicant notes that these references were not cited for such a purpose.

The office action further admits that Walker does not teach transmitting the transaction information "via the short range RF circuitry" and instead relies on Holmes. Office Action, at pg. 15. The office action summarily concludes that it would have been obvious to include the cellular circuitry of Holmes for the purpose of "increasing security measures while also enhancing user experience in carrying out a transaction." Office Action, at pg. 16. However, as previously noted in the record, Walker is incapable of

establishing a data transfer protocol of any kind for the purpose of transmitting the transaction data. Accordingly one of ordinary skill would not look to Bonalle to cure the deficiencies of Walker.

For at least the foregoing reasons, the suggested combination of references fails to disclose or suggest all of the features of amended claim 2. Accordingly, applicant requests the rejection be withdrawn.

Amended claim 10 recites features similar to amended claim 1. Thus for at least the same reasons, the suggested combination of references fails to disclose or suggest all of the features of amended claim 10. Accordingly, applicant requests the rejection be withdrawn.

The other dependent claims depend directly or indirectly from amended claims 1 and 10. As dependent claims inherit their patentability from their respective independent claims, the other dependent claims are allowable over the suggested combination of references for at least their dependence on an allowable claims. Accordingly, applicant requests the rejections under § 103 be withdrawn.

CONCLUSION

Applicant has endeavored to address all of the examiner's concerns as expressed in the outstanding Office Action. Accordingly, amendments to the claims, the reasons therefor, and arguments in support of the patentability of the pending claims are presented above. In light of the above amendments and remarks, reconsideration and withdrawal of the outstanding rejections is specifically requested. Although the present communication includes alterations to the claims and characterizations of claim scope and the referenced art, no acquiescence, disclaimer or estoppel is intended or should be inferred thereby. Applicant is not conceding in this application that the previously pending claims are not patentable over the cited references. Rather, any amendments are only being made to expedite prosecution of the application and are without prejudice to the presentation or assertion in the future of claims relating to the same or similar subject matter. Applicant reserves the right to later submit additional or alternative arguments of patentability that may have not been presented at this time.

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

Dated: December 12, 2017

By: /Eric A. Bernsen/
Eric A. Bernsen
Registration No. 71,624

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:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Eric Anthony Bernsen/Helen Glenister
Attorney Docket Number:	116546-613CT13

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	1253	1	1400	1400
Miscellaneous:				
		Total in USD ($)		**1400**

Electronic Acknowledgement Receipt

EFS ID:	31193165
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Eric Anthony Bernsen/Helen Glenister
Filer Authorized By:	Eric Anthony Bernsen
Attorney Docket Number:	116546-613CT13
Receipt Date:	12-DEC-2017
Filing Date:	04-MAR-2015
Time Stamp:	13:42:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1400
RAM confirmation Number	121217INTEFSW13435600
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		12_12_2017_Resp_to_NFOA_as_filed_116546-613CT13.PDF	102796 074fc7024f0ca47a375c1fd86b28df220988128c	yes	13

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	4
	Applicant Arguments/Remarks Made in an Amendment	5	13

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30797 63480f1884f507e066ea31e2f66ab53a6e4f3377	no	2

Warnings:

Information:

Total Files Size (in bytes):	133593

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/639,034	Filing Date 03/04/2015	☐ To be Mailed

ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **12/12/2017**

	(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))	* 14	Minus	** 20	= 0	X $80 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $420 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

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

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

LIE
SHEILA D. CHAPMAN

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.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:26
S2	1	("6163771").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:27
S5	16	(biometric near1 data) near2 stored near2 (separately or different)	US-PGPUB; USPAT	OR	ON	2015/05/18 15:53
S6	5	"7911643"	US-PGPUB; USPAT	OR	ON	2015/05/18 15:59
S8	0	(separatly near1 stor$3) with data	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S9	12789	(stor$3 near1 data) with separately	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S10	1434	S9 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S11	1011	S10 and ((information or data) near4 (separately))	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S15	919	S11 and (memory)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:07
S19	0	S15 and (stor$3 near4 saperately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:08
S20	498	(authentication near4 stor$3 near4 separately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:13
S21	34	S20 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:16
S22	48796	(stor$4 near3 information separately) same (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S24	29064	(stor$4 near3 information separately) with (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S25	5880	S24 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S26	51	S25 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:26
S27	1	"20020112177"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:32
S28	1	"20020077993"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:40
S29	10379	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near4 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S30	7730	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near2 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S31	4128	((generate) near2 (key pin code token	US-PGPUB;	OR	ON	2015/06/12

		password)) with ((encrypt) near3 (key pin code token password))	USPAT			16:22
S32	3286	((generate) near2 (key pin code token password)) with ((encrypt) near2 (key pin code token password))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:22
S33	1736	S32 and (transaction financial account)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S34	1134	S33 and @pd<"20120101"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S35	234	S34 and (RFID RD infrared)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S37	63	S35 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:24
S38	850	"5590197"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:44
S39	1	("5590197").PN.	US-PGPUB; USPAT	OR	OFF	2015/06/12 16:44
S40	0	(("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" | "6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" | "5742618" | "6276607" | "6570487" | "8004410").PN.").PN.	US-PGPUB; USPAT	OR	OFF	2015/09/30 16:19
S42	66	("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" | "6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" |	US-PGPUB; USPAT	OR	ON	2015/09/30 16:20

		"5742618" | "6276607" | "6570487" | "8004410").PN.				
S43	2	"20070022058"	US-PGPUB; USPAT	OR	ON	2016/04/21 15:56
S44	5	(US-20070022058-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2016/12/01 10:38
S45	0	S44 and ((biometric near4 associat$4) with (payment))	US-PGPUB; USPAT	OR	ON	2016/12/01 10:39
S46	39	((biometric near4 associat$4) near4 (payment near2 information))	US-PGPUB; USPAT	OR	ON	2016/12/01 10:39
S47	24	S46 and @pd<"20130909"	US-PGPUB; USPAT	OR	ON	2016/12/01 10:41
S48	5	(US-20070022058-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S49	3	S48 and ((mobile card) near3 (device))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S50	39	((biometric near4 associat$4) near4 (payment near2 information))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S51	34	S50 and ((mobile card) near3 (device))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S52	21	S51 and @pd<"20130909"	US-PGPUB; USPAT	OR	ON	2016/12/01 14:47
S53	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2017/05/24 11:05
S54	1	S53 and (encrypt$4 with key with payment)	US-PGPUB; USPAT	OR	ON	2017/05/24 11:06
S55	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2017/05/25 10:48
S56	0	S55 and (RF near3 device)	US-PGPUB; USPAT	OR	ON	2017/05/25 10:48
S57	1	S55 and (RF with device)	US-PGPUB; USPAT	OR	ON	2017/05/25 10:48
S58	0	(2014/0040628).CCLS.	US-PGPUB; USPAT	OR	OFF	2017/05/25 16:15
S59	0	(2014/0040628).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/05/25 16:15
S60	3	("20140040628").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/05/25 16:16
S61	0	(("7911643" | "5590197" | "20070022058" | "20060020558" | "20020112177" | "6934861" | "20070022058" | "6848048" | "20040128249" | "6163771").PN.").PN.	US-PGPUB; USPAT	OR	OFF	2017/07/19 11:59

S62	22	("7911643" | "5590197" | "20070022058" | "20060020558" | "20020112177" | "6934861" | "20070022058" | "6848048" | "20040128249" | "6163771").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/07/19 11:59

EAST Search History (Interference)

< This search history is empty>

3/16/2018 7:26:55 PM
C:\Users\eoussir\Documents\EAST\Workspaces\14639034_Mobile device RFID transaction biometric POS.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

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

CLAIMS

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

CLAIM		DATE								
Final	Original	05/18/2015	12/09/2015	05/26/2017	03/16/2018					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	✓					
	5	✓	-	-	-					
	6	✓	-	-	-					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	✓	✓	✓					
	10	✓	✓	✓	✓					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	✓	✓	✓					
	15	✓	✓	✓	✓					
	16	✓	✓	✓	✓					

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 03/22/2018

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
03/22/2018	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):

PTONotifications@procopio.com
docketing@procopio.com

Office Action Summary	Application No. 14/639,034	Applicant(s) Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA 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 12/12/2017.

☐ 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) 1-4 and 7-16 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-4 and 7-16 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 03/04/2015 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions

2. This communication is **a Final Office action** in response to Applicant's response on 12/12/2017 to Examiner's Non-Final communication on 06/16/2017. Claims 1-4, 7-16 have been examined in this Application. All other claims have been cancelled.

3. No new information disclosure statement has been submitted.

Response to Arguments

4. Applicant's arguments, see page 5, filled on 12/12/2017, in regards to the claim rejections under obviousness-type nonstatutory double patenting have been considered and the rejection will be held in abeyance per Applicant's request.

5. Applicant's arguments, do not address the Disclosure objection from the previous action. Therefore the objection stands.

6. Applicant's arguments, see pages 5-6, regarding the priority date have been considered but are not persuasive.

Applicant argues:

> **"the provisional application 60/394241 discloses at least, This is performed by combining GSM technology with a wireless RF-ID device that can store a person's identification information, including an electronic or biometric "signature" (e.g., fingerprint, facial, iris, or other recognition feature). The RF cellular telephone can thus become a person's identification document (e.g., passport, boarding pass) and/or credit card(s) or other card(s) (e.g., mileage cards). Provisional Disclosure, at pg. 36, attachment 5, line 15. The provisional Disclosure further includes the same or similar**

subject matter, including the figures, as relied up on in the following discussion related to rejections under § 112. For example, the disclosure at pp. 43-50 and various flowcharts throughout, support the disclosure and claims of this application. Accordingly, applicant believes the priority claim is proper.

The Examiner disagrees. At best, the above relied upon support for the claimed limitations only recites that wireless communication can be utilized in combination with user authentication information. The portions relied upon do not come close to providing support for at least the following limitations, which the Applicant believes distinguish their claims from other teachings:

"one or more processors configured to authenticate that the biometric information read by the biometric reading device is associated with the payment information based at least in part on the biometric authentication information stored in memory." Claims 2, 11, and 18.

Therefore, the earliest priority date is maintained as being July 01, 2014.

7. Applicant's arguments, see pages 7-8, regarding claim rejections under 35 U.S.C. §112 (a) have been fully considered but are partially persuasive.

I. Amendments overcome the rejections: "generate a key…"

A. Removing the "generate a key" limitation overcomes this rejection.

The Examiner agrees with the Applicant's arguments that by removing the "generate a key" limitation and limitations directed to a generation of a key, the rejection is overcome regarding this matter only. Examiner notes that such generation of a key limitation(s) are not supported by the Disclosure; therefore removal of such limitations overcomes the rejection.

II. The amended claim 1 is supported by the Disclosure.

B. Disclose only supports the claimed "encrypted keys."

The Examiner disagrees with the Applicant's arguments in regards to the Disclosure having support for the claim limitations "encrypt the payment information stored in memory" and "transmit the encrypted key and the encrypted payment information…" The portions of the Disclosure, which the Applicant points to, do not provide support for having the payment information be in an encrypted form not alone transmitting such encrypted payment information. The Disclosure, as noted by the Applicant in their arguments, merely describes that the device requires a user to provide authentication information in order to access data within the device. Also, the device stores the encrypted keys in memory of the device NOT the payment information. The Applicant continues by noting that the user's information must be protected "(e.g., biometrics)." This "feature protects the device from the equipment that reads and writes from the device." This support as the Applicant points out does not overcome the rejection of the claims for failing to have support for the payment information being encrypted.

Applicant further claims that the Disclosure, paragraph 0070, notes that the device provides information to a point of sale via RF communication. The device also requires user authentication in order to allow the user to carry out a transaction, this authentication data "can be stored, for example in the Chip, or at a remote location…" These passages do not disclose "encrypted payment information."

8. Applicant's arguments, see pages 9, regarding claim rejections under 35 U.S.C. §112 (b) have been fully considered but they are not persuasive.

Applicant argues that the claimed "security management unit" is a devices that "checks and validates the cryptographic keys that will be sent to the cryptographic block." As it can be seen, the Applicant has not provided support for the claimed "security management unit" to clarify what is the unit and how one of ordinary skill in the art would be able to claimed limitations directed to such unit. As a result, the claims are rejected for their indefiniteness.

9. Applicant's arguments, see page 8, regarding claim interpretation under 35 U.S.C. §112 (f) have been fully considered but are not persuasive. Applicant argues that the claims have been amended to overcome the interpretation that the claim limitations at issue do not include structure. The Examiner disagrees. The claims still invoke 112, f by reciting functions without providing the structure to perform such functions. For instance, Claim 2 recites "a biometric reading device configured to read" and "a security management unit configured to encrypt." These limitations recite functions such as read and encrypt, yet there is no corresponding structure to carry out these functions.

10. Applicant's arguments, see pages 8-12, regarding claim rejections under 35 U.S.C. §103 (a) have been fully considered but are not persuasive.

I. References fail to teach all features of claim 1.

A. Claim 1 is anticipated by Walker and in light of the other references claim 1 is obviously taught by the combination of all references.

The Examiner disagrees with the Applicant arguments that the references do not teach the claimed limitations of at least claim 1. More specifically, the Applicant has noted that the following limitation is not taught by any of the references: "one or more processors configured to authenticate that the biometric information read by the biometric

reading device is associated with the payment information…" The Examiner disagrees. As the Applicant points out in their arguments, Walker is cited to teach that a user must provide biometric input into the device in order to gain access to the device; wherein the device is a credit card. The device is not a cellular phone or a smart card that is utilized for anything other than settling a transaction. Instead the device is utilized to conduct a transaction since it is a credit card. As a result, the fact that such device requires a user to input a biometric sample in order to determine whether it is that of the user's or not allows the user to use this financial card to settle a transaction when the user has been authenticated and that the financial card, as it is obviously known, includes financial data such as account data to allow a transaction to be completed. Thus, the biometric data of the user is tied or is associated with the payment card since without the authentication there is no way for the user to purchase anything with that card. Also, the card is not usable for anything else other than settling a transaction. See Walker, Col. 2, Ln. 39-53; Col. 4, Ln. 5-15; 50-62; Col. 8, Ln. 61-67; and Col. 9, Ln. 1-10. On page 10 of the Applicant's arguments, the Applicant concedes that the device in Walker is utilized for account transaction. Applicant also further points out that in Walker, the user must input their "PIN or biometric data to access the device…" and if such access is granted, then the final point of the process of Walker is to settle a transaction by providing account information to the merchant; thus completing a generic transaction scheme as is obvious to those of ordinary skill in the art. Without the user being authenticated, the card is not able to transmit any data to a merchant to settle a transaction.

II. Bonalle fails to cure the deficiencies of Walker.

B. Bonalle emphasis without question that it is obvious to associate user authentication data with financial information.

The Examiner disagrees with the Applicant's arguments that the reference to Bonalle does not teach explicitly that biometric data is associated with financial or payment information. Bonalle at least in paragraphs 0047, 0244-0245 and 0256 recites that "the account number (e.g., account data) may be associated with any device… or other identifier… configured to allow the customer to interact or communicate with the system, such as… biometric data." Bonalle continues by reciting: "a card member may have previously associated a credit card account, a debit card account, and a frequent flier account with his biometric sample." One of ordinary skill in the art would understand that Walker's device, which is a payment card, requiring a biometric input to be utilized results in the biometric input being associated with the account data. However, to overcome any confusion, the introduction of Bonalle establishes a clear teaching that association of authentication information, including but not limited to biometric data, with account information is obvious. Perhaps the recitations of the references is not being understood clearly by the Applicant even though a new reference was provided to eliminate any confusion on the fact that associating authentication data with account data is obvious to those of ordinary skill in the art as is presented by the references which date back to at least 1997 and 2004 respectively.

III. Walker does not teach generating a key.

C. The limitation directed to generating a key is removed.

The Examiner disagrees with Applicant's arguments since the claims no longer recite a generation of a key or any key being generated. As a result, the arguments directed to generation of a key are moot. However, Walker clearly teaches generation of data including keys.

Disclosure

11. The Disclosure is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Applicant should point to the portion(s) in the Disclosure where it is clearly recited how the encryption of the "key and the payment information stored in memory" is carried out. It is not clear how the key and payment information is encrypted not is there a relationship between the generated key and the encryption of the key. If the key is generated, then how is it being encrypted along with the payment information?

Priority Date

12. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, 365(c), or 386(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 5 U.S.C. 119(e) or under 35 U.S.C. 120, 121, 365(c), or 386(c) as follows:

The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original non-provisional application or

provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of 35 U.S.C. 112(a) or the first paragraph of pre-AIA 35 U.S.C. 112, except for the best mode requirement. See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994)

The disclosure of the prior-filed application, Application No. 60/394,241 fails to provide adequate support or enablement in the manner provided by 35 U.S.C. 112(a) or pre-AIA 35 U.S.C. 112, first paragraph for one or more claims of this application. The disclosure in Application 60/394,241 does not include at least the association of the biometric module with the payment information; recited in at least claims 1, 11, and 18. Applications 10/615,026 and 11/279,912 were also determined as lacking support for at least the association of the biometric module with the payment information. Application 10/615,026 was filled on July 09, 2003 and Application 11/279,912 was filled on April 17, 2006. Although multiple other applications were filled as continuations pending the 11/279,912 filling, all of these applications do not have support in the manner required to claim priority to such filling dates. Applications 12/688,666, 13/175,768, 13/350,665, 14/022,135 do not have support for the claimed limitations; therefore the earlier priority date is determined to be July 01, 2014.

Claim Rejections - 35 USC § 112

13. The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The Disclosure shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The Disclosure shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

14. Claims 1 and 10 and all of their dependent claims are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the Disclosure in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention. Claims 1 and 10 recite "a biometric reading device…", "encrypt a key…", "encrypt the payment information stored in memory," and "transmit the encrypted key and the encrypted payment information." These claim elements and limitations lack support. The Disclosure was examined carefully, yet there is no mention of such biometric reading device, a key being encrypted or that the payment information is also encrypted.

The Disclosure does disclose "keys" but these keys are not generated and are simply "keys" that are stored in memory. The Disclosure does not mention the encryption of such a key not alone encrypting both the key and the payment information. There is also no support of how the keys are encrypted by the security management unit. Lastly, the Disclosure simply recites that a "chip can have a cryptographic block with 4 exchange encrypted keys with up to 256 bits)." Again, this is not the same as encrypting a key using a security management unit. See at least ¶ 0047, 0052, 0058, 0085, 0088, 0106, 0108-0109, 0120. Furthermore, the transmission of "the encrypted key and the encrypted payment information" is not supported by the Disclosure. Although the Disclosure discloses that a transaction can be carried out with a POS it does not

recite, in any form, that the transaction information includes the encrypted key and encrypted transaction information.

15. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The Disclosure shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The Disclosure shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

16. Claim elements "a biometric reading device configured to read", "security management unit configure to encrypt" in claims 1 and 10 are limitations that invoke 35 U.S.C. 112, sixth paragraph. However, the written description fails to disclose the corresponding structure, material, or acts for the claimed function. The Disclosure describes a "RF Communications Device (e.g., Cellular Telephone" that includes a modulator, converter, encoder, decoder, an instruction sequencer, a security management unit, and a cryptographic block ¶ 0013-0014. Further, the Disclosure describes in ¶ 0070-0073 a "POS device" including "a fingerprint reader"/"fingerprint scanner," and a chip (see also Figures, 1, 2, and 5). This fingerprint reader is associated with the POS not the claimed "mobile device." The mobile device is never recited as having a "biometric reading device." The Disclosure does not describe any structure corresponding to these devices or components used by the devices. Because these limitations invoke 112(f), the Disclosure must clearly link the recited functions to the corresponding structure. For computer-implemented means-plus-function limitations, the corresponding structure includes both the computer and the algorithm that performs the recited functions. This

requirement is described in the notice issued in the Federal Register on March 8, 2011.

Specifically, the notice states:

> 3. Computer-Implemented Means-Plus-Function Limitations: For a computer-implemented means-plus-function claim limitation invoking §112, ¶6, the corresponding structure is required to be more than simply a general purpose computer or microprocessor.96 To claim a means for performing a particular computer-implemented function and then to disclose only a general purpose computer as the structure designed to perform that function amounts to pure functional claiming.97
>
> The structure corresponding to a §112, ¶6 claim limitation for a computer-implemented function must include the algorithm needed to transform the general purpose computer or microprocessor disclosed in the Disclosure.98 The corresponding structure is not simply a general purpose computer by itself but the special purpose computer as programmed to perform the disclosed algorithm.99

The notice further states:

> A rejection under §112, ¶2 is appropriate if the Disclosure discloses no corresponding algorithm associated with a computer or microprocessor.103 For example, mere reference to a general purpose computer with appropriate programming without providing an explanation of the appropriate programming,104 or simply reciting "software" without providing detail about the means to accomplish the software function,105 would not be an adequate disclosure of the corresponding structure to satisfy the requirements of §112, ¶2. In addition, merely referencing a specialized computer (e.g., a "bank computer"), some undefined component of a computer system (e.g., "access control manager"), "logic," "code," or elements that are essentially a black box designed to perform the recited function, will not be sufficient because there must be some explanation of how the computer or the computer component performs the claimed function.106

Here, the Disclosure does not recite that the biometric reading device, and security management unit are associated with any computer, microprocessor, or other structure, where the computer performs the algorithms necessary to carry out the functions of the mobile device. Additionally, the term “device” is a non-structural term (See 35 USC §112 Supplementary Examination Guidelines, slide 40, 4/8/2011.

Applicant may:

(a) Amend the claim so that the claim limitation will no longer be interpreted as a limitation under 35 U.S.C. 112, sixth paragraph; or

(b) Amend the written description of the Disclosure such that it expressly recites what structure, material, or acts perform the claimed function without introducing any new matter (35 U.S.C. 132(a)).

If applicant is of the opinion that the written description of the Disclosure already implicitly or inherently discloses the corresponding structure, material, or acts so that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function, applicant should clarify the record by either:

(a) Amending the written description of the Disclosure such that it expressly recites the corresponding structure, material, or acts for performing the claimed function and clearly links or associates the structure, material, or acts to the claimed function, without introducing any new matter (35 U.S.C. 132(a)); or

(b) Stating on the record what the corresponding structure, material, or acts, which are implicitly or inherently set forth in the written description of the Disclosure, perform the claimed function. For more information, see 37 CFR 1.75(d) and MPEP §§ 608.01(o) and 2181.

Claims 3-5, 8-10, 12-17, 19-24 are also rejected as each depends on claims 2, 11 and 18. For purposes of examination, any device capable of storing biometric data and any teaching of an encrypted data field will be determined as reading on the claimed limitations directed to the "biometric reading device" and "security management unit."

17. Claims 2 and 11 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention. Per claims 2 and 11, the claims recites "wherein the biometric reading device is configured to read biometric information provided by a user to complete the transaction."

However, the claims from which these claims depend, claims 1 and 10, already recite such a limitation: "a biometric reading device configured to read biometric information." Therefore, it is not known how the two different readings of biometric data are related to one another. If the user already provided the biometric data and the device sent the encrypted key and payment information, then how is the user still providing their biometric data as claimed in dependent claims 2 and 11? For at least these reasons the claims are rejected for failing to particularly point out and claim the subject matter that the inventors or joint inventor claim as their invention. One of ordinary skill in the art would not know how to carry the claimed limitations. As a result, for purposes of examination, any teachings of a single biometric reading from a user will be determined as reading on claims 2 and 11.

CLAIM INTERPRETATION

18. The following is a quotation of 35 U.S.C. 112(f):

> (f) Element in Claim for a Combination. – An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

The following is a quotation of pre-AIA 35 U.S.C. 112, sixth paragraph:

> An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.

19. The claims in this application are given their broadest reasonable interpretation using the plain meaning of the claim language in light of the specification as it would be understood by one of ordinary skill in the art. The broadest reasonable interpretation of a claim element (also

commonly referred to as a claim limitation) is limited by the description in the specification when 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, is invoked.

As explained in MPEP § 2181, subsection I, claim limitations that meet the following three-prong test will be interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph:

(A) the claim limitation uses the term "means" or "step" or a term used as a substitute for "means" that is a generic placeholder (also called a nonce term or a non-structural term having no specific structural meaning) for performing the claimed function;

(B) the term "means" or "step" or the generic placeholder is modified by functional language, typically, but not always linked by the transition word "for" (e.g., "means for") or another linking word or phrase, such as "configured to" or "so that"; and

(C) the term "means" or "step" or the generic placeholder is not modified by sufficient structure, material, or acts for performing the claimed function.

Use of the word "means" (or "step") in a claim with functional language creates a rebuttable presumption that the claim limitation is to be treated in accordance with 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph. The presumption that the claim limitation is interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, is rebutted when the claim limitation recites sufficient structure, material, or acts to entirely perform the recited function.

Absence of the word "means" (or "step") in a claim creates a rebuttable presumption that the claim limitation is not to be treated in accordance with 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph. The presumption that the claim limitation is not interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, is rebutted when the claim

limitation recites function without reciting sufficient structure, material or acts to entirely perform the recited function.

20. Claim limitations in this application that use the word "means" (or "step") are being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, except as otherwise indicated in an Office action. Conversely, claim limitations in this application that do not use the word "means" (or "step") are not being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, except as otherwise indicated in an Office action.

This application includes one or more claim limitations that do not use the word "means," but are nonetheless being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, because the claim limitation(s) uses a generic placeholder that is coupled with functional language without reciting sufficient structure to perform the recited function and the generic placeholder is not preceded by a structural modifier. Such claim limitation(s) is/are:

a. "a biometric reading device"

b. "a security management unit"

These claim limitations are in claims 1-4, 7-16.

Because this/these claim limitation(s) is/are being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, it/they is/are being interpreted to cover the corresponding structure described in the specification as performing the claimed function, and equivalents thereof.

If applicant does not intend to have this/these limitation(s) interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph, applicant may: (1) amend the claim limitation(s) to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph (e.g., by reciting sufficient structure to perform the claimed function); or (2)

present a sufficient showing that the claim limitation(s) recite(s) sufficient structure to perform the claimed function so as to avoid it/them being interpreted under 35 U.S.C. 112(f) or pre-AIA 35 U.S.C. 112, sixth paragraph.

Claim Rejections - 35 USC § 101

21. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.
> 35 U.S.C. 101 reads as follows:

22. Claims 1-4, 7-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

JUDICIAL EXCEPTIONS TO SECTION 101

23. The Supreme Court held that the patent claims in Alice Corporation Pry. Ltd. v. CLS Bank International, el al. ("Alice Corp. ") are not patent-eligible under 35 U.S.C. § 101. The Supreme Court made clear in Alice Corp. that it applies the framework set forth in Mayo Collaborative Services v. Prometheus Laboratories, Inc., 566 U.S. _ (2012) (Mayo), to analyze all claims directed to laws of nature, natural phenomena, and abstract ideas for subject matter eligibility under 35 U.S.C. § 101. This framework is currently being used by the USPTO to examine claims involving laws of nature, but had not been used for claims involving abstract ideas. Therefore, the following instructions differ from prior USPTO guidance in the following two ways.

24. Alice Corp. establishes that the same analysis should be used for all types of judicial exceptions, whereas prior USPTO guidance applied a different analysis to claims with abstract

ideas (Bilski guidance in MPEP 2106(11) (B)) than to claims with laws of nature (Mayo guidance in MPEP 2106.01).

25. Alice Corp. also establishes that the same analysis should be used for all categories of claims (e.g., product and process claims), whereas prior guidance applied a different analysis to product claims involving abstract ideas (relying on tangibility in MPEP 2106(II) (A)) than to process claims (Bilski guidance).

ALICE V. CLS BANK: TWO-PART ANALYSIS

26. Following Alice Corp, all claims (product and process) having an abstract idea must be analyzed using the following two-part analysis set forth in Mayo. For additional guidance, see latest "Interim Guidance on Patent Subject Matter Eligibility" released in July, 2015.

27. The following are limitations referenced in Alice Corp. that may be enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

a. Improvements to another technology or technical fields;

b. Improvements to the functioning of the computer itself;

c. Applying the judicial exception with, or by use of, a particular machine; effecting a transformation or reduction of a particular article to a different state or thing; adding a specific limitation other than what is well-understood, routine and conventional in the field, or adding unconventional steps that confine the claim to a particular useful application.

28. Limitations referenced in Alice Corp. that are not enough to qualify as "significantly more" when recited in a claim with an abstract idea include, as non-limiting or non-exclusive examples:

d. Adding the words "apply it" (or an equivalent) with an abstract idea, or mere instructions to implement an abstract idea on a computer;

e. Requiring no more than a genetic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry. See also, MPEP 2106(1).

29. Claims 1-4, 7-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more.

30. Claims 1-4, 7-16 are directed to an abstract idea of essentially conducting a transaction utilizing a mobile device. The claim limitations individually and as a whole do not transform the claim or claims into more than an abstract idea of itself. Concepts tied to an abstract idea of itself include collecting and comparing known information, comparing data to determine a risk level, compare new and stored information and using rules to identify options, obtaining and comparing intangible data, storing gathering and analyzing data and using categories to organize, store and transmit information, and conducting a transaction.

31. Cases tied to the above court decision abstract concepts include at least: *Clasen Immunotherapies Inc. v. Biogen IDEC*, 659 F. 3d 1057 (Fed. Cir. 2011), *buySAFE, Inc. v. Google* 765 F.3d 1350 (Fed. Cir. 2014), *PerkinElmer Inc. v. Intema Ltd.,* 496 Fed. Appx. 65 (Fed. Cir. 2012), *Cybersource Corp. v. Retail Decisions, Inc.,* 654 F.3d 1366 (Fed. Cir. 2011), *SmartGene, Inc. v. Advanced Biological Labs., 555 Fed. Appx. 950 (Fed. Cir. 2014)*, and *Affinity Labs v. Amazon.com* (_ F.3d _, 120 U.S.P.Q.2d 1210 (Fed. Cir. 2016) CAFC Appeal No. 15-2080).

32. More specifically, Claim 1 for instance is directed to a mobile device comprising RF communication means and a memory storing data, the device receives data, analyzed or authenticates the data, manipulates the data through encryption, and transmits the data to settle a transaction. These limitations when considered individually and as a whole amount to mere collection of data and manipulation of data (receiving data, comparing data, determining a risk level based on the data, etc.) to yield a result.

33. The additional element(s) or combination of elements in the claim(s) other than the abstract idea(s) per se amount(s) to no more than significantly more than the abstract idea itself. The claims recite the additional elements of "a mobile device," "RF cellular circuitry," "memory," "biometric reading device," "one or more processors," "security management unit," and "a POS" at a high level of generality and only perform generic functions of communicating data between entities, storing data, obtaining data, processing data and causing a result based on the processing / analyzing of data. Generic computers performing generic computer functions, without an inventive concept, do not amount to significantly more than the abstract idea. The limitations directed to the "a mobile device," "RF cellular circuitry," "memory," "biometric reading device," "one or more processors," "security management unit," and "a POS" are simply generic and are recited to attempt to limit the abstract idea to a particular technological environment. The type of information being manipulated and obtained does not impose meaningful limitations or render the idea less abstract. Looking at the elements as a combination does not add anything more than the elements analyzed individually. Therefore, the claims do not amount to significantly more than the abstract idea itself. The claim is not patent eligible.

34. The claims do not include limitations that meet the criteria required to determine the claims as a whole amounting to significantly more than the judicial exception itself (**see**

paragraph 27, a-c). This is evident by the description; **see at least Paragraphs 0002, 0080-81,** which recite: "An RF Communications Device (e.g., Cellular Telephone)..." "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."

35. As a result, the claims and each claimed limitation amount to mere instructions to implement the idea on generic computers or devices, or routers that serve to perform generic computer functions that are well-understood, routine, and conventional activities previously known in the pertinent industry, which do not add meaningful limitations to the method. The functions performed by the "a mobile device," "RF cellular circuitry," "memory," "biometric reading device," "one or more processors," "security management unit," and "a POS" appear to be conventional and routine carried out by a general purpose computers or devices such as an off the shelf computers, cellular phones, PDAs, smart cards, routers etc. with instructions to process a payment transaction using devices, communication means, and obtaining, sending and receiving of data. The claimed limitations as a whole do not add significantly more to the

abstract idea of using computer technology, software, and data collection / data comparison, communication means to settle a transaction.

36. Moreover, the claims do not appear to improve the functioning of the "a mobile device," "RF cellular circuitry," "memory," "biometric reading device," "one or more processors," "security management unit," and "a POS" or effect an improvement in another technology or field; i.e. besides business method or solutions. The claims do not recite limitations beyond to provide grounds for an eligible application. Accordingly, the Examiner concludes that there are no meaningful limitations in the claims that transform the judicial exception into a patent eligible application such that the claim amounts to significantly more than the judicial exception itself.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

38. Claims 1-4, 7-16 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,163,771 to Walker et al. ("Walker"), in view of U.S. Patent 6,848,048 to Holmes ("Holmes"), in further view of U.S. Patent Application Publication 2006/0020558 to Bonalle et al. ("Bonalle").

39. Per claims 1 and 10, Walker teaches all of the following limitations:

a. A mobile device, comprising [Abstract]:

b. a memory (memory) [...] and configured to store biometric authentication information (biometric information) and payment information (account number), [...] [Walker, Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3, 8];

c. a biometric reading device configured to read biometric information (device has a biometric reader to receive user biometric data) [Walker, Col. 5, Ln. 59-61 and Figures 1-3];

d. a secure module configured to (processor) [Walker, Abstract]:

e. encrypt a key when the biometric information read by the biometric reading device is successfully authenticated [Col. 7, Ln. 25-51; Col. 8, Ln. 1-30; Col. 10, Ln. 15-21 and Figures 4-8 and related text];

Examiner notes that the following is a conditional limitation: "when the biometric information read by the biometric reading device is successfully authenticated."

f. encrypt the payment information stored in memory [Col. 7, Ln. 25-51; Col. 8, Ln. 1-30; Col. 10, Ln. 15-21 and Figures 4-8 and related text]; and

g. transmit [...] the encrypted key and the encrypted payment information for use in a transaction; (the device transmits payment information including IV, CC# and much more to the merchant to settle the transaction) [Col. 2, Ln. 39-53; Col. 4, Ln. 5-15; 50-62; Col. 8, Ln. 61-67; Col. 9, Ln. 1-10].

Examiner notes that the following is an intended use limitation, which does not have much patentable weight: "for use in a transaction."

Walker does not explicitly teach:

h. Walker does not teach short range radio frequency (RF) circuitry; however, **Holmes** does [Col. 2, Ln. 38-53, Fig. 1-3];

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings Holmes to explicitly teach a short range RF circuitry which can be incorporated into Walker's smartcard / device in motivation of increasing security measures while also enhancing user experience in carrying out a transaction.

i. Walker does not teach memory coupled to the short range RF circuitry; however, **Holmes** does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings Holmes to explicitly teach a short range RF circuitry which communicates data that is stored in memory, which can be incorporated into Walker's smartcard / device that includes a memory and a processor and the ability to transmit data to settle a transaction in motivation of increasing security measures while also enhancing user experience in carrying out a transaction.

j. Walker does not explicitly teach [...] wherein the biometric authentication information is associated with the payment information; however, **Bonalle** does [Abstract, Paragraph 0047, 0244-0245, 0256].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, which teaches a mobile payment device including a biometric reader configured to authenticate a user by comparing the user's input biometric data to the user's stored biometric data in the device's memory, wherein the device generates a one-time use credit card number for use in a transaction, in view of Holmes which

teaches incorporating RF circuitry into Walker's device to include the teachings of Bonalle which teaches that a mobile device utilized for carrying out a transaction will have the biometric data associated with the payment data of the user using the mobile device in motivation of only allowing the proper user to whom the card belongs to, to carry out a transaction. This results in increased security measures since the mobile card or device is unusable by another user.

k. Walker does not explicitly teach one or more processors configured to authenticate that the biometric information read by the biometric reading device is associated with the payment information based on the biometric authentication information stored in memory; however, **Bonalle** does [Abstract, Paragraph 0047, 0244-0245, 0256].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker, which teaches a mobile payment device including a biometric reader configured to authenticate a user by comparing the user's input biometric data to the user's stored biometric data in the device's memory, wherein the device generates a one-time use credit card number for use in a transaction, in view of Holmes which teaches incorporating RF circuitry into Walker's device to include the teachings of Bonalle which teaches that a mobile device utilized for carrying out a transaction authenticates user biometric data and that the biometric authenticated data is associated with the payment data of the user using the mobile device in motivation of only allowing the proper user to whom the card belongs to, to carry out a transaction. This results in increased security measures since the mobile card or device is unusable by another user.

l. Walker does not explicitly teach [...] via the short range RF circuitry [...]; however, **Holmes** does (medium over which information may be transferred ... radio frequency "RF") [Abstract, Col. 2, 34-61, and Figures 1-9].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings Holmes to explicitly teach a short range RF circuitry which can be incorporated into Walker's smartcard / device in motivation of increasing security measures while also enhancing user experience in carrying out a transaction.

The Examiner notes that ISO/IEC 14443 is a standard which defines contactless communications using smart cards and integrated circuits and transmission protocols for contactless communications; which is known to one of ordinary skill in the art. This standard is provided as reference to show that RF circuitry is an obvious communication method that is obviously used in mobile devices and standardizes the usage of contactless smart cards.

Per claim 10, Walker teaches:

a. a point of sale (POS) device (terminal / merchant terminal) configured to [Col. 6; Ln. 5-14; Col. 8, Ln. 30-67; Col. 9, Ln. 10-35; Col. 12, Ln. 19-50; and Figures 2-3, 9, 11 and related text]:

b. receive, from the security management unit, the encrypted key and payment information; [Col. 6; Ln. 5-14; Col. 8, Ln. 30-67; Col. 9, Ln. 10-35; Col. 12, Ln. 19-50; and Figures 2-3, 9, 11 and related text];

c. transmit, to a central database (CC Issuer), the encrypted key and payment information [Col. 6; Ln. 5-14; Col. 8, Ln. 30-67; Col. 9, Ln. 10-35; Col. 12, Ln. 19-50; and Figures 2-3, 9, 11 and related text]; and

d. a central database configured to validate the key and the payment information [Col. 6; Ln. 5-14; Col. 8, Ln. 30-67; Col. 9, Ln. 10-35; Col. 12, Ln. 19-50; and Figures 2-3, 9, 11 and related text].

Examiner notes that the following is an intended use limitation: "configured to validate the key and the payment information," which does not have much patentable weight.

40. Per claims 2 and 11, Walker teaches wherein the biometric reading device is configured to read biometric information provided by a user to complete the transaction [Walker, Col. 5, Ln. 59-61 and Figures 1-9].

Examiner notes the following is an intended use limitation which does not have much patentable weight: "configured to read biometric information provided by a user to complete the transaction."

41. Per claims 3 and 12, Walker teaches wherein the payment information is associated with a primary account number (account number) [Col. 6, Ln. 14-35, 54-59, Col. 7, Ln. 27-36 and Figures 1-3 and 6].

42. Per claim 4, Walker teaches wherein the security management unit is configured to provide the encrypted key and payment information to a point of sale (POS) device (the device transmits payment information including IV, CC# and much more to the merchant's device which is interpreted to be the POS to settle the transaction) [Col. 2, Ln. 39-53; Col. 4, Ln. 5-15; 50-62; Col. 8, Ln. 61-67; Col. 9, Ln. 1-10].

Examiner notes the following limitation is an intended use limitation which does not have much patentable weight: "wherein the transaction module is configured to provide the transaction information comprising the encrypted key and payment information to a point of sale (POS) device."

43. Per claims 8 and 15, Walker teaches wherein the payment information (account number) is stored in a memory accessible only by the security management unit (central processor 101) [Col. 6-7, Ln. 61-, 1-3 and Figures 1-3].

44. Per claims 9 and 16, Walker does not explicitly teach wherein the short range RF circuitry comprises a radio frequency identification (RFID) device; however, Holmes does [Col. 2, Ln. 38-53, Fig. 1-3].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker to include the teachings Holmes to explicitly teach a short range RF circuitry which can be incorporated into Walker's smart in motivation of increasing security measures while also enhancing user experience in carrying out a transaction.

45. Claims 7 and 14 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Walker, in view of Holmes and Bonalle, as applied to claims 1 and 10 above, in further view of U.S. Patent Application Publication 2002/0112177 to Voltmer et al. (herein after referred to as simply Voltmer).

46. Per claims 7 and 14 Walker in view of Holmes do not explicitly teaches wherein the biometric authentication information is stored separately from the payment information [Col.5, Ln. 49-67, Col. 6-7, Ln. 61-67, 1-3, Col.8, Ln. 19-25 and Figures 1-3]. Acknowledgement

Voltmer teaches storing separately a plurality of information [Paragraphs 009-0091 and Figures 12A and 12B].

It would have been obvious to one of ordinary skill in the art to combine the teachings of Walker which teaches a device that includes a memory / secure memory to include the teachings of Voltmer to explicitly teach storing data in sections or partitions or separately from other data in motivation of increasing security measures or facilitating the upload of information from the memory.

Double Patenting

47. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with

this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

48. Claim 1 of the instant Application is rejected on the ground of nonstatutory double patenting as being unpatentable over Claim 3 of prior U.S. Patent No. 8766772. Although the claims at issue are not identical, they are not patentably distinct from each other. Claim 3 in U.S. Patent 8766772 teaches the claim limitations of the instant Application's Claim 1, but does not teach "a security management unit configured to: encrypt a key when the biometric information read by the biometric reading device is successfully authenticated; encrypt the payment information stored in memory." Walker, U.S. Patent 6163771, teaches such missing limitations; see Col. 5, Ln. 49-67, Col. 6, Ln. 1-38; Col. 7, Ln. 25-51; Col. 8, Ln. 1-30; Col. 10, Ln. 15-21 and Figures 1-9 and related text. It would have been obvious to one of ordinary skill in the art to combine the teachings of U.S. Patent 8766772 and the teachings of Walker in order to encrypt a value and encrypt such a value along with the payment information before providing them for settlement of the transaction in motivation of increasing security measures.

49. Claims 2-17 are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14/659502 in view of U.S. Patent 6,163,771 to Walker.

This is a provisional obviousness-type nonstatutory double patenting rejection.

50. Although the conflicting claims are not identical, they are not patentably distinct from each other. Claims 1 and 10 of co-pending application 14/659502 recites:

a. mobile device, comprising:

b. short range radio frequency (RF) circuitry;

c. memory configured to store biometric authentication information and payment information;

d. a biometric module configured to read biometric information;

e. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

f. a secure module configured to:

g. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

h. encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction

Claim 10:

j. A system, comprising:

k. a mobile device, comprising:

l. short range radio frequency (RF) circuitry;

m. memory configured to store biometric authentication information and payment information;

n. a biometric module configured to read biometric information;

o. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

p. a secure module configured to:

q. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

r. encrypt the key and the payment information stored in memory; and

s. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

t. a point of sale (POS) device configured to:

u. receive, from the secure module, the encrypted key and payment information; and

v. transmit, to a central database, the encrypted key and payment information; and

w. a central database configured to validate the key and the payment information.

Claims 1 and 10 of co-pending application 14/659502 differ since they fail to recite the authentication module is configured to authenticate the biometric input data is associated with the payment information. U.S. Patent Application Publication 2006/0020558 to Bonalle et al. ("Bonalle") discloses an authentication module configured to authenticate the biometric

information read by the biometric module is associated with the payment information [Abstract, Paragraph 0047, 0244-0245, 0256]. Therefore, it would have been obvious to one of ordinary skill in the art to combine the teachings of co-pending Application 14/659,502 to include the teachings of Bonalle, which teaches a mobile device utilized for carrying out a transaction will have the biometric data associated with the payment data of the user using the mobile device in motivation of only allowing the proper user to whom the card belongs to, to carry out a transaction. This results in increased security measures since the mobile card or device is unusable by another user.

51. It is well settled that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA 1963). Also note Ex parte Rainu, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

52. Co-pending Applications 14/321781, 14/724593, 14/585057 are also rejected based on the same above rationale.

Conclusion

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.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on M-F 9AM - 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John W Hayes can be reached on 5712726708. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/
Patent Examiner, Art Unit 3685
03/16/2018

/MAMON OBEID/
Primary Examiner, Art Unit 3685

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC - Searched*		
Symbol	Date	Examiner
G06Q	5/8/2015	EO
H04L	5/8/2015	EO

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner
705		5/8/2015	EO

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

Search Notes		
Search Notes	Date	Examiner
consulted Calvin Hewitt	5/15/2015	EO
Consulted John H. and Mamon O on 101/ 103	5/25/2017	EO
Consulted John H. on priority	5/9/2017	EO
Consulted Mohammad N. on priority and 112	5/26/2017	EO
Consulted Steven K. 112	03/14/2018	EO
Review of references	03/16/2018	EO
Consulted John H. 101	03/14/2018	EO

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

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 07/12/2018

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
07/12/2018	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):

PTONotifications@procopio.com
docketing@procopio.com

Applicant-Initiated Interview Summary	**Application No.** 14/639,034	**Applicant(s)** Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA Status** No

All participants (applicant, applicants representative, PTO personnel):

(1) EL MEHDI OUSSIR. (3) _____.

(2) Mark W. Catanese (Applicant's Representative). (4) _____.

Date of Interview: 06 July 2018.

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: Walker et al..

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's representative and the Examiner discussed potential claim amendments to try and overcome the outstanding rejections.

In regards to the 112 (a) rejections, the proposed claims were discussed to determined whether they overcome the rejections. Although some recommendations were made, no agreement was reached.

In regards to the 103 rejection, the claims were discussed in light of the art of record. Although no agreement was reached, the Examiner proposed that the claims recite exactly what the Applicant deems as their invention including reciting what triggers the user to input their biometric input. For instance, does a terminal send a request to the mobile device for data using some communication method and how does the mobile device then request the user to input their biometric data...?.

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

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	/MAMON OBEID/ Primary Examiner, Art Unit 3685

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 examiners 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 applicants 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 applicants 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 examiners 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 examiners initials.

DO NOT ENTER E.O.

App Nos.: 14,639,034 Attorney Docket No. 116546-613CT13
Title: SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
Filed: March 4, 2015
Inventor(s): de VELASCO CORTINA, Francisco Martinez
Examiner: OUSSIR, El Mehdi
Art Unit: 3685
Conf. No.: 5934

AGENDA FOR TELEPHONIC INTERVIEW

(NOT INTENDED FOR ENTRY INTO THE RECORD)

Attendees, Date and Type of Interview

A telephonic interview is scheduled for July 6, 2018, at 2:30PM EDT (11:30AM PDT). The interview will be attended by Examiner Oussir and Applicant's Representative Mark W. Catanese (Reg. No. 64,279).

Applicant's Representative will call the Examiner at (571) 270-0191.

Identification of Claims to be Discussed

Claims 1 and 10.

Identification of Art to be Discussed

U.S. Patent No. 6,163,771 ("Walker");

U.S. Patent No. 6,848,048 ("Holmes"); and

U.S. App. Pub. No. 206/0020558 ("Bonalle").

Items to be Discussed

1. Applicant would like to discuss the rejection of the claims under 35 U.S.C. § 112 (a) and the proposed amendment to claim 1 below. Support for claim 1 and the proposed amendments can be found, for example, in at least FIGs. 12 and 13 and paragraphs [0082], [0111], [0119]-[0135], [0151], and [0174] of the published application. Applicant to explain that one skilled in the art would reasonably conclude that the specification describes the proposed claimed features.
2. Applicant would like to discuss the rejection of the claims under 35 U.S.C. § 112 (b) and the claim interpretation as invoking 35 U.S.C. § 112 (f). Applicant believes that the at least the proposed amendments to claim 1 no longer invoke 35 U.S.C. § 112 (f) and overcome the rejections under § 112 (b).

3. Applicant to explain that the proposed amendments to claim 1 overcome the objection to the disclosure and the priority date.
4. Applicant would like to discuss the rejection of the claims under 35 U.S.C. §103 and the proposed amendment to claim 1 below in view of the above cited references. Specifically, Applicant to explain why it believes the cited references do not teach or suggest the proposed amendments to claim 1.
5. Applicant would also like to discuss the rejection of the claims under 35 U.S.C. §101 and the proposed amendment to claim 1. Specifically, Applicant to explain why it believes the proposed amendments to claim 1 are directed to patentable subject matter.

6. Proposed Amendments to Claim 1

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

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and encrypted payment information, wherein the biometric authentication information is associated with a user associated with the encrypted payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processor configured to execute instructions stored in the memory to:

receive the biometric information of the user read by the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the encrypted payment information based on the biometric authentication information stored in memory~~; and~~,

~~a security management unit configured to:~~

~~encrypt~~ retrieve a key ~~when~~ in response to successfully authenticating the biometric information read by the biometric reading device ~~is successfully authenticated;~~,

~~encrypt the payment information stored in memory; and~~

transmit, via the short range RF circuitry, the ~~encrypted~~ key ~~and the encrypted payment information~~, and

grant access to the encrypted payment information stored in the memory for use in a transaction based on the transmitted key and the authentication.

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	14639034	Filing Date	2015-03-04	Docket Number (if applicable)	116546-613CT13	Art Unit	3685
First Named Inventor	Francisco Martinez de Velasco Cortina			Examiner Name	OUSSIR, El Mehdi		

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, 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

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2018-07-23
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.

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT13

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

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

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	1251	1	200	200
Miscellaneous:				
RCE- 1ST REQUEST	1801	1	1300	1300
		Total in USD ($)		**1500**

Electronic Acknowledgement Receipt

EFS ID:	33260003
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	23-JUL-2018
Filing Date:	04-MAR-2015
Time Stamp:	20:53:58
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1500
RAM confirmation Number	072418INTEFSW20574100
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		07_23_2018_Resp_to_FOA_as_filed_116546-613CT13_.PDF	216808 f171d7a99205b83ffa6810ed50330cfb18d40757	yes	26

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Amendment Submitted/Entered with Filing of CPA/RCE	1	1
	Claims	2	5
	Applicant summary of interview with examiner	6	6
	Applicant Arguments/Remarks Made in an Amendment	7	26

Warnings:

Information:

2	Request for Continued Examination (RCE)	116546-613CT13_RCE.PDF	1349967 812d50d95a7bea0cfe05f2c63c7694eeacfd04f5	no	3

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	32551 f174158f401123765697831 9f51369a1baf4053e	no	2

Warnings:

Information:

Total Files Size (in bytes):	1599326

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	de VELASCO CORTINA, Francisco Martinez	116546-613CT13	5934

EXAMINER	
OUSSIR, El Mehdi	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
July 23, 2018	EFS WEB

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

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

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

Sir:

This paper is submitted in response to the Final Office Action mailed on March 22, 2018, Applicant submits the present communication with a Request for Continued Examiner (RCE). Allowance of the above identified application is respectfully requested in view of the following submission, where:

Amendments to the Claims begin on page 2 of this paper.

Interview Summary beings on page 6 of this paper.

Remarks begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

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

What is claimed is:

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

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processor configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuity of the mobile device, wherein the connection is established to conduct a secured transaction between the mobile device and the POS device,

in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory~~; and~~,

~~a security management unit configured to:~~

~~encrypt~~ secure the payment information using a key,

when the biometric information read by the biometric reading device is successfully authenticated~~; encrypt the payment information stored in memory; and~~, transmit to the POS device, via the short range RF circuitry, ~~the encrypted key and the encrypted payment information for use in a~~ information indicative of the authentication, and

retrieve purchase information related to the secured transaction based, in part, on the transmitted information.

2. (Previously Presented) The mobile device of claim 1, wherein the biometric reading device is configured to read biometric information provided by a user to complete the transaction.

3. (Original) The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. (Canceled)

5. (Canceled)

6. (Canceled)

7. (Original) The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. (Currently Amended) The mobile device of claim 1, wherein the payment information is secured ~~stored in a memory accessible only by the security management unit~~with a cryptographic key.

9. (Original) The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. (Currently Amended) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information;

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processor configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuity of the mobile device, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based at least in part on the biometric authentication information stored in memory~~; and~~

~~a security management unit configured to:~~

~~encrypt~~secure the payment information using a key,

when the biometric information read by the biometric reading device is successfully authenticated~~ encrypt the payment information stored in memory; and~~, transmit to the POS device, via the short range RF circuitry, information indicative of the authentication, and

~~the encrypted key and the encrypted payment information for use in a transaction~~retrieve purchase information related to the secured transaction based, in part, on the transmitted information; and

~~a point of sale (POS)~~the POS device configured to:

receive, from the ~~security management unit~~mobile device, the ~~encrypted key and~~ secured payment information and the information indicative of the authentication; and

~~transmit~~retrieve, ~~to~~ from a central database, ~~the encrypted key and payment~~ purchase information based on the received information indicative of authentication; and

a central database configured to validate the key and the payment information based on the information indicative of authentication.

11. (Previously Presented) The system of claim 10, wherein the biometric reading device is configured to read biometric information provided by a user to complete the transaction.

12. (Original) The system of claim 10, wherein the payment information is associated with a primary account number.

13. (Original) The system of claim 10, wherein the POS device includes an RF reader.

14. (Original) The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. (Currently Amended) The system of claim 10, wherein the payment information is ~~stored in a memory accessible only by the security management unit~~secured with a cryptographic key.

16. (Original) The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

INTERVIEW SUMMARY

Applicant thanks Examiner Oussir for the courtesy extended during the telephonic interview conducted in the present application on July 6, 2018 with Mark Catanese ("Interview"). During the Interview, Applicant and Examiner discussed the objections to the priority claim. While no agreement was reached, the Examiner agreed that if the 112 rejections are overcome then the objection to the claim to priority to at least US Application Nos. 14/321,781; 14/022,135; 13/350,665; 13/175,768; 12/688,666; 11/279.912; 10/615,026 would be overcome. The Applicant and Examiner also discussed certain proposed amendments, some of which are reflected in the "Amendments to the Claims" section above. Other features were discussed that the Examiner agreed appeared to overcome the prior art rejections, some of which are incorporated in the claim amendments reflected above. No agreement was reached with respect to patentability. The Examiner expressed that additional search and consideration would be needed. The substance of those discussions is reflected in the remarks below.

REMARKS

The present amendment is in response to the Final Office Action dated March 22, 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, 8, 10, and 15 are amended and claim 4 is cancelled without prejudice or disclaimer. Support for the amendments can be found throughout the application as originally filed. For example, support can be found at least in FIGS. 12-14 and the accompanying text of the application as originally filed. No new matter has been added. Claims 1-3 and 7-16 are pending in the application, claims 5 and 6 having been previously cancelled without prejudice or disclaimer. Claims 1 and 10 are the independent claims.

In response to the Office Action, Applicant respectfully traverses all of the rejections and requests reconsideration of the above-captioned application in view of the following comments.

B. Nonstatutory Double Patenting

Claim 1 stands rejected on the ground of nonstatutory double patenting as being unpatentable over claim 3 of prior U.S. Patent No. 8,766,772. Claims 2-17 (interpreted as claims 2-16) are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14/659,502 in view of U.S. Patent 6,163,771 ("Walker").

Applicant respectfully requests reconsideration of these rejections in view of the foregoing claim amendments. Furthermore, not notwithstanding the following remarks and arguments as to the allowability of the pending claims over Walker, the claims may further change throughout prosecution. Therefore, Applicant respectfully requests the double patenting rejection be held in abeyance until the claims are otherwise in condition for allowance.

C. Objection to the Disclosure

The Office Action objects to the disclosure of the application. Specifically, the Office Action alleges that it is not "clearly recited how encryption of the 'key and the payment information' stored in the memory is carried out." *Office Action, p. 8.* Applicant does not necessarily agree with the rejection; however, in the interest of advancing prosecution and without acquiescing to the merits of the object, Applicant has amended claims 1 and 10 as set forth in the "Amendments to the Claims" section above. Applicant respectfully submits that claims 1 and 10 no longer recite the objected to phrase. Accordingly, as agreed in the Interview, Applicant respectfully submits that this object is moot and requests the objection be withdrawn.

D. Priority Date

The Office Action states, "Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under [35 U.S.C.] 119(e) or under 35 U.S.C. 120, 121, 365(c), or 386(c)" because, "[t]he later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original non-provisional application or provisional application)." *Office Action, at pg. 8.* Applicant does not necessarily agree with the rejection; however, in the interest of advancing prosecution and without acquiescing to the merits of the object, Applicant has amended claims 1 and 10 as set forth in the "Amendments to the Claims" section above. As acknowledged in the Office Action, "[t]he disclosure of the invention in the parent application and in the later filed application must be sufficient to comply with the requirements of 35 U.S.C. 112(a) or the first paragraph of pre-AIA 35 U.S.C. 112, except for the best mode requirement." *Office Action, p. 9.* Thus, for the reasons set forth below with respect to the rejections under 35 U.S.C. § 112(a), Applicant respectfully submits that the priority claim is proper and that the priority date is to be July 9, 2002.

Additionally, as discussed during the interview, Applicant submits that the disclosure in US Application Nos. 14/321,781; 14/022,135; 13/350,665; 13/175,768; 12/688,666; 11/279.912; 10/615,026 (collectively "the parent utility applications") are substantially the same as the disclosure of the present application

and only differ with respect to formatting and clerical changes. Accordingly, Applicant respectfully submits that, to the extent that the present application complies with 35 U.C.S. § 112 supports the amended claims, the parent utility applications also provide sufficient support under § 112. Thus, to the extent the Examiner maintains the rejection of priority to the provisional application no. 60/394,241 (a point the Applicant does not concede), the claim to priority to the parent utility applications is proper and the priority date is to be July 9, 2003 at the latest, e.g., the date US Application No. 10/615,026 ("the '026 parent application") was filed.

E. Claim Rejections - 35 U.S.C. § 112(a)

Claims 1 and 10 and all of their dependent claims are rejected as failing to comply with the written description requirement. Applicant does not necessarily agree with the rejection; however, in the interest of in the interest of advancing prosecution and without acquiescing to the merits of the object, Applicant has amended claim 1 to recite, a mobile device comprising:

> short range radio frequency (RF) circuitry;
>
> a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;
>
> a biometric reading device configured to read biometric information; and
>
> one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processor configured to execute instructions stored in the memory to:
>
> establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuity of the mobile device, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,
>
> in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device,
>
> authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on

> the biometric authentication information stored in memory,
>
> secure the payment information using a key,
>
> when the biometric information read by the biometric reading device is successfully authenticated, transmit to the POS device, via the short range RF circuitry, information indicative of the authentication, and
>
> retrieve purchase information related to the secured transaction based, in part, on the transmitted information.

Applicant respectfully submits that the amendments to claim 1 are supported by the application as originally filed. For example, support of the amendments can be found in at least FIGs. 12-14 and the accompanying text and paragraphs [0059]-[0072] of the application as originally filed. Furthermore, support for the amendments can be found, for example, in pages 36-47 of US Provisional Application No. 60/394,241 (hereinafter "Parent Provisional Application") from which the present application claims priority.

For example, claim 1 recites, *inter alia*, "a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information." Support for these features can be found, for example, in at least FIG. 12 and 13 and paragraphs [0059]-[0075] of the application as originally filed. For example, [0068] states "the RF device 1222 includes a chip and an RF antenna" and "EEPROM memory 1348 [that] stores data." *See also, Parent Provisional Application, pp. 45 and 46* (depicting figures of the RF devices that are substantially the same as FIGS. 12 and 13 of the present application including EEPROM memory storing data of a RF device). Additionally, paragraph [0069] states "the chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel mileage card information)." *See also, Parent Provisional Application, p. 40 and 44* ("the RF chip carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel milage card information)"). Furthermore, paragraph [0061] and [0062] state "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)" and "[t]he 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)." *See also, Parent Provisional Application, pp. 36-37.* Accordingly, Applicant respectfully submits that one skilled in the art would understand the specification as providing sufficient support for the above-identified features.

Claim 1 also recites, *inter alia*, "a biometric reading device configured to read biometric information." Support for this feature can be found, for example, in at least FIGs. 12 and 13 and paragraphs [0066]-[0068] and [0070]-[0073] of the application as originally filed. For example, paragraph [0066]-[0067] state "[t]he POS 1210 can include an RF reader/writer 31 and a fingerprint digital scanning device 1232" and "In an alternative embodiment, the RF cellular telephone can include a fingerprint digital scanner 1223." *See also paragraph [0070] of the application as originally filed* (stating "the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone"); *see also, Parent Provisional Application, pp. 37-38* ("the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone" and "the RF cellular telephone can include a fingerprint digital scanner").

The Office Action refers to the description of one embodiment at paragraphs [0070]-[0073] to allege that the biometric reader, e.g., fingerprint reader or scanner is actually associated with the POS and not the mobile device; however, the Office Action ignores the part of paragraph [0070] that states "[i]n an alternative embodiment, the user could imprint their fingerprint into a fingerprint reading device included on the RF cellular telephone [as opposed to a fingerprint reading device in a POS]." The Office Action also ignores the immediately following paragraph [0074], which states "[a]lthough 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," as well as the disclosure in figure 12 and the accompanying description, which as described above clearly indicate that the mobile device can include the digital scanning device. Accordingly, Applicant respectfully submits that one skilled in the art would understand the specification as providing sufficient support for the above-identified features.

Claim 1 also recites, *inter alia*, "establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS is within an operating range of the short range RF circuity of the mobile device, wherein the connection is established to conduct a secure transaction between the mobile device and the POS." Support for this feature can be found, for example, in at least [0060] and [0071] of the application as originally filed. For example, paragraph [0060] states "[a]s 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." Similarly, paragraph [0071] states "a user carries an RF cellular telephone and approaches an RF reader/writer (e.g., in a hotel), which is continuously scanning." *See also, Parent Provisional Application, p. 38* ("In step 1, the customer carries an RF cellular telephone and enters a hotel. As soon as the customer comes into POS range (e.g., 5 feet), the hotel's RF reader identifies the customer, credit card information, and hotel rewards card information. (The RF reader is continuously scanning.)"). Accordingly, Applicant respectfully submits that one skilled in the art would understand the specification as providing sufficient support for the above-identified features, at least because as the RF reader/writer at the POS is continuously scanning such scanning would cause a communicative connection between the short range RF circuity of the mobile device and the RF reader/writer of the POS.

Claim 1 also recites, *inter alia*, "in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device." Support for this feature can be found, for example, in at least paragraphs [0060], [0071], and [0072] of the application as originally filed. For example, paragraph [0060] states "[a]s 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)." Similarly, paragraph [0072] explains that at step 1410, which follows step 1405 where the RF cellular telephone approaches the RF reader/writer, the user "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 1222." *See also, Parent Provisional Application, p. 39* ("In step 3, the customer reviews the transaction, and then, if the customer wants to complete the transaction, the customer imprint a fingerprint into the fingerprint scanner."). Accordingly, Applicant respectfully submits that one skilled in the art would understand the specification as providing sufficient support for the above-identified features.

Claim 1 also recites, *inter alia*, "authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory." Support for this feature can be found, for example, in at least paragraphs [0065], [0066], [0064], [0069], [0070], [0072], and [0073] of the application as originally filed. For example, paragraph [0072] states "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)." *See also, Parent Provisional Application, pp. 37 and 39* (explaining for example, "a fingerprint reader to verify that the holder of the RF cellular telephone is the owner of the RF cellular telephone" and "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"). Furthermore, the RF cellular telephone includes a "chip [that] carries authentication information (e.g., fingerprint) and transaction information (e.g., credit card information, airline, or hotel mileage card information)." *See Application as originally filed, para. [0069] and Parent Provisional Application, p. 40 and 44.* Accordingly, Applicant respectfully submits that one skilled in the art would understand the specification as providing sufficient support for the above-identified features.

Claim 1 also recites, *inter alia*, "secure the payment information using a key." Support for this feature can be found, for example, in at least paragraphs [0033], [0053], [0068], [0069], [0064], [0069], [0070], [0072], [0073], [0088] and [0120][1] of

[1] Applicant notes that, while various embodiments of RF identification mechanisms are described in the application as originally filed, one skilled in the art would recognize that the features of one embodiment may be interchanged and utilized in other embodiments described in the application as

the application as originally filed. For example, [0033] states "[a]n 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," where payment or transaction information is one such type of information stored on the RF device (*see, e.g., para. [0069]). See also, Parent Provisional Application, p. 30* ("the information contained in the device you can not be able to altered without you being able to determine by who and for what purpose and for this we use highly secure chip with a hardware programmable cryptographic block with credit and debit exchange keys. "). Furthermore, paragraphs [0068] and [0069] state "[t]he RF cellular telephone also may include a cryptographic programmable block chip 1349 to enhance security." *See also, Parent Provisional Application, pp. 40 and 46* ("The RF cellular telephone also may include a cryptographic programmable block chip to enhance security." Thus, the specification clearly discloses that information stored in the mobile device, such as payment or transaction information can be secured, e.g., via encryption. Accordingly, Applicant respectfully submits that one skilled in the art would understand the specification as providing sufficient support for the above-identified features.

Claim 1 also recites, *inter alia*, "when the biometric information read by the biometric reading device is successfully authenticated, transmit to the POS device, via the short range RF circuitry, information indicative of the authentication." Support for this feature can be found, for example, in at least paragraphs [0060] and [0073] of the application as originally filed. For example, paragraph [0073] states "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." Regarding the Parent Provisional Application, as discussed above, the RF cellular telephone is described as storing the biometric information and comprising a fingerprint reader. Thus, one skilled in the art would recognize, in this embodiment, the authentication of

originally filed. *See, e.g., Application as originally filed, paras. [0003], [0016], [0018], and [0054] and Parent Provisional Application, p. 2.*

the biometric information at the RF cellular telephone would be communicated to the POS using the connection via the short range RF circuity. Otherwise, the transaction would not proceed as claimed. Accordingly, Applicant respectfully submits that one skilled in the art would understand the specification as providing sufficient support for the above-identified features.

Claim 1 also recites, *inter alia*, "retrieve information related to the secured transaction based, in part, on the transmitted information." Support for this feature can be found, for example, paragraph [0073] states after the RF cellular telephone is used to verify the authentication information, "this information is presented to a point of sale or access control device to retrieve purchase information." *See also, Parent Provisional Application, p. 36-41*. Accordingly, Applicant respectfully submits that one skilled in the art would understand the specification as providing sufficient support for the above-identified features.

For at least the foregoing reasons, applicant submits that amended claim 1 is well supported by the application as originally filed. Accordingly, applicant requests the rejection be withdrawn. Amended claim 10 recites features similar to amended claim 1. Thus for at least the same reasons, applicant requests the rejections of the independent claims and all of associated dependent claims under § 112(a) be withdrawn.

F. Claim Interpretation

In the Office Action, claims 1-4 and 7-16 are interpreted under 35 U.S.C. § 112(f) or pre-AIA 35 U.S.C. § 112, sixth paragraph. Applicant traverses the interpretation.

Applicant disagrees that Claims 1-4 and 7-16 fall within the scope of 35 U.S.C. §112(f), as means plus function claims. However, without acquiescing to the merits of the interpretation and in the interest of advancing prosecution, Applicant has amended Claims 1-4 and 7-16 to recite "one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processor configured to execute instructions stored in the memory . . ." perform the functions recited in claims 1-4 and 7-16.

Per MPEP § 2181, "a claim limitation that does not use the term 'means' or 'step' will trigger the rebuttable presumption that 35 U.S.C. 112(f) . . . does not apply . . . ." This "presumption may be overcome if the claim limitation uses a generic placeholder (a term that is simply a substitute for the term 'means'). *Id.* Applicant submits that the terms "memory" and "processor" as recited in claims 1-4 and 7-16 are each structural terms with specific structural meanings understood to have sufficiently definite meaning by persons of ordinary skill in the art.

Furthermore, Applicant submits that the term "a biometric reading device" as recited in claims 1-4 and 7-16 is a structural term with specific structural meaning understood to have sufficient definite meaning by persons of ordinary skill in the art. For example, paragraphs [0066] and [0067] of the application as filed describes "a fingerprint digital scanning device," "fingerprint digital scanner," "fingerprint reading device," and "finger print scanner." *See also id. at paras. [0070], [0072], and [0073].* Furthermore, paragraph [0064] states "any other biometric identifier (e.g., a voice print, iris recognition, facial recognition) could be used." Thus, one skilled in the art would understand the specific structural meaning of the term "biometric reading device."

Accordingly, as agreed during the Interview, Applicant submits that claims 1-4 and 7-16 fall outside of the scope of 35 U.S.C. § 112(f) or pre-AIA 35 U.S.C. § 112, sixth paragraph.

G. ***Claim Rejections - 35 U.S.C. § 112(b)***

Claims 1 and 10 stand rejected under 35 U.S.C. § 112(b). Specifically, the Office Action states "Claim elements 'a biometric reading device configured to read', 'security management unit configured to encrypt' in claims 1 and 10 are limitations that invoke 35 U.S.C. 112, sixth paragraph. However, the written description fails to disclose the corresponding structure, material, or acts for the claimed function." *Office Action, p. 11.* Applicant respectfully traverses these rejections.

However, in the interest of in the interest of advancing prosecution and without acquiescing to the merits of the object, Applicant has amended claims 1 and 10as set forth in the "Amendments to the Claims" section above. Particularly, claims 1 and 10 have been amended to remove the phrase "security management unit configured to

encrypt," thereby rendering the rejection of this phrase as moot. Furthermore, as explained above, the term "a biometric reading device" does not invoke and falls outside the scope of 35 U.S.C. § 112(f), at least because "a biometric reading device" is a structural term with specific structural meaning understood to have sufficient definite meaning by persons of ordinary skill in the art. Furthermore, paragraphs [0066] and [0067] describe that the biometric reading device may be a fingerprint digital scanning device in some embodiments that reads a user's fingerprint. *See also, id. at paras. [0070]-0074].*

Furthermore, the Office Action states "[t]his fingerprint reader is associated with the POS not the claimed 'mobile device.' The mobile device is never recited as having a 'biometric reading device." Applicant respectfully submits that this statement is flatly incorrect. For example, the application as originally filed, with reference to FIG. 12, states "the RF **cellular telephone** can ***include*** **a finger print scanner 1223**." *Id. at para. [0067], see also id. at paras. [0070].*

For at least the foregoing reasons, Applicant submits that amended claims 1 and 10 are well supported by the application as originally filed. Accordingly, Applicant requests the rejections of the independent claims and all of associated dependent claims under § 112(b) be withdrawn.

H. Claim Rejections - 35 U.S.C. § 101

Claims 1-4 and 7-16 stand rejected under 35 U.S.C. § 101 as being directed to a judicial exception, namely the abstract idea of conducting a transaction utilizing a mobile device. The Office Action goes on to state that the above claims do not include significantly more, because the elements of the claims allegedly do not contain an "inventive concept" sufficient to "transform" the claimed abstract idea into a patent eligible application.

Applicant respectfully traverses these rejections. However, without acquiescing to the merits of the grounds of the Examiner's rejection, and in the interest of advancing prosecution, Applicant has amended independent claims 1 and 10 as reflected in the "Amendments to the Claims" section. Applicant respectfully submits that amended claims 1 and 10 recite patent eligible subject matter pursuant to 35 U.S.C. § 101.

Regarding amended claim 1, Applicant respectfully submits that claim 1 is not directed to the alleged abstract idea. The Federal Circuit has instructed that "the claims are considered in their entirety to ascertain whether ***their character as a whole*** is directed to excluded subject matter." *McRO, Inc., v. Bandai Namco Games America, Inc.,* 837 F.3d 1299, 1312 (Fed. Cir. 2016) (emphasis added). The Federal Circuit explained that it is improper to simply summarize the entire claim at a high level of abstraction as being directed to, e.g., an abstract idea, untethered from the actual language of the claims. See *Enfish, LLC, v. Microsoft Corporation, et al.,* 822 F.3d 1327, 1337 (Fed. Cir. 2016). The Office Action alleges that the claims are directed to the abstract idea of conducting a transaction utilizing a mobile device. However, amended claim 1 is not directed to merely processing physical checks. Rather, claim 1 is directed to a mobile device comprising:

> short range radio frequency (RF) circuitry;
>
> a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;
>
> a biometric reading device configured to read biometric information; and
>
> one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processor configured to execute instructions stored in the memory to:
>
> establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuity of the mobile device, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,
>
> in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device,
>
> authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory,
>
> secure the payment information using a key,
>
> when the biometric information read by the biometric reading device is successfully authenticated,

> transmit to the POS device, via the short range RF circuitry, information indicative of the authentication, and
>
> retrieve purchase information related to the secured transaction based, in part, on the transmitted information.

Applicant respectfully submits that the Office Action improperly summarizes the claim at a high level of abstraction and fails to consider the claim as a whole. Noteably, the alleged abstract idea fails to consider several of the claimed features. Particularly, in addition to claiming a mobile device for conducting a transaction, claim 1 also recites that the mobile device includes "short range radio frequency (RF) circuitry" and "a biometric reading device configured to read biometric information." Furthermore, the claimed mobile device establishes a connection with a POS via the short range RF circuitry, reads biometric information provided by the user via the biometric reading device, authenticates the user to perform a secure transaction, and transmits information to the POS. Accordingly, Applicant respectfully submits that claim 1, when considered as a whole including each and every feature recited in the claim, is ***not directed*** to the alleged abstract idea of conducting a transaction with a mobile device, but ***merely involves*** the alleged abstract idea. *See MPEP 2106.04(II).*

The Office Action attempts the requisite analysis by addressing the claim limitations in paragraph 32; however, in order to arrive at the conclusion that the claims are abstract, the Office Action first genericizes each limitation to make it appear as though each limitation is directed to abstract functions such as encryption, storing data, transmission, etc. But that is not the analysis that is required, i.e., one cannot take abstractions of the actual limitations. And clearly, making each limitation abstract is going to lead to a determination that the claim as a whole is abstract.

While the courts have rendered many opinions with conclusions like: a claim directed to merely receiving data or comparing data or determining a risk level are abstract and therefore unpatentable. But the decisions do not hold that therefore any claim or limitation that involves, e.g., comparing data or retrieving data is abstract. In fact, once the correct analysis is performed, such a finding should almost never be the case – this is why it is called an exception the law of patentability. The claims at issue here clearly do not pre-empt any use of encryption, or storing data, or receiving data, or

authenticating data, etc. Therefore, the test for an *exception* laid out by the Supreme Court in *Alice* would, by design fail here, i.e., under *Alice* the claims are not directed to an abstract idea.

An analysis of the claims at issue in one of the example cases, *Cybersource*, provided in the Office Action makes the point clear. Here is a claim at issue in that case:

> Claim 3, as amended during reexamination, reads:
>
> 3. A method for verifying the validity of a credit card transaction over the Internet comprising the steps of:
>
> a) obtaining information about other transactions that have utilized an Internet address that is identified with the [ ] credit card transaction;
>
> b) constructing a map of credit card numbers based upon the other transactions and;
>
> c) utilizing the map of credit card numbers to determine if the credit card transaction is valid.

The court rightly determined that the limitations say nothing more than obtain credit card numbers and store them in a map and then use those numbers to compare to a newly obtained credit card number, i.e., compare one credit card number to another. The case literally stands for the principal that just comparing data is not patentable - even if you use the Internet. It *does not* mean that any claim that involves comparing data is abstract. And it certainly does not mean that one can isolate a step of comparing data in a claim, determine that isolated limitation is abstract under *Cybersource*, then do the same thing to all the other limitations, and then conclude that since each individual limitation is directed to an abstract idea, the entire claim is directed to an abstract idea. That is not what is meant by look at the claim limitations individually and as a whole and is the exact type of analysis that would lead to the exception swallowing the whole of patentability as warned against in *Alice*.

That the analysis in the Office Action runs entirely counter to *Alice*, the other cases that came after, and the patent office guidance allegedly based thereon is reflected perfectly in paragraph 36 of the Office Action in which it is alleged: “Moreover, the claims do not appear to improve the functioning of the "a mobile device," "RF cellular circuitry," "memory," "biometric reading device," "one or more processors," "security management unit," and "a POS" or effect an improvement in another

technology or field . . . ." Clearly what the Office Action is alleging is that the RF circuitry just does what RF circuitry is supposed to do, and the memory does what memory is supposed to do, and the biometric reading unit does what the biometric reading device is supposed to do, therefore they are all generic and cannot support patentability. But one of skill in the art would recognize after reading the specification, in fact anyone would that including the biometric reader and the security unit in the device and configured them to work with the RF circuitry, memory, and processors as described and claimed clearly improves the operation of the mobile device by allowing it to be used in a mobile transaction. In fact paragraphs [0062] and [0063] describe all kinds of benefits that result from the this improvement.

Assuming, *arguendo*, that the claims are directed to the abstract idea, Applicant respectfully submits that claims include significantly more than the abstract idea, at least because the elements of claim 1 are not routine or conventional. "An inventive concept can be found in the unconventional and non-generic ***combination*** of known elements." *Subject Matter Eligibility Examples: Business Methods, Example 34, p. 4* (describing *BASCOM Global Internet v. AT&T Mobility LLC*, 119 USPQ2d 1236 (Fed. Cir. 2016)) (https://www.uspto.gov/sites/default/files/documents/ieg-bus-meth-exs-dec2016.pdf) (emphasis in original); see *also Amdocs (Isr.) Ltd. V. Openet Telecom, Inc.*, 841 F.3d 1288 (finding eligibility where "the claim's enhancing limitation necessarily requires that these generic component operate in an unconventional manner"). Here, amended claim 1 may utilize arguably generic components, but these components operate in an unconventional manner to achieve an improvement in a technological or Internet-centric application (as described above). For example, the features of claim 1 are unconventional at least because, as described below, they have not been disclosed by the prior art.

Furthermore, the Office Action alleges that "the claims and each claimed limitation amount to mere instructions to implement the idea on generic computers or devices, or routers that serve to perform generic computer functions that are well-understood, routine, and conventional activities previously known in the pertinent industry." *Office Action, p. 21.* Applicant respectfully disagrees.

Applicant respectfully submits that that Office Action fails to meets the burden under MPEP 2106.05(d)(I) to establish that the claimed combination of features are re well-understood, routine, and conventional activities. "As set forth in MPEP § 2106.05(d)(I), an examiner should conclude that an element (or combination of elements) represents well-understood, routine, conventional activity only when the examiner can readily conclude that the element(s) is widely prevalent or in common use in the relevant industry." *See Changes in Examination Procedure Pertaining to Subject Matter Eligibility, Recent Subject Matter Eligibility Decision (Berkheimer v. HP, Inc.) Memo, p. 3* (citing *Berkheimer v. HP Inc.*, 881 F.3d 1360 (Fed. Cir. 2018)) (https://uspto.gov/sites/default/files/documents/memo-berkheimer-20180419.PDF) (hereinafter "*Berkheimer Memo*"). "The mere fact that something is disclosed in a piece of prior art, for example, does not mean it was well-understood, routine, and conventional." *Berkheimer*, 881 F.3d at 1369. As explained in the *Berkheimer Memo*, "an additional element (or combination of elements) is ***not*** well-understood, routine or conventional unless the examiner finds, and expressly supports a rejection in writing with, one or more of the following: ***unless*** the examiner finds, ***and expressly supports*** a rejection in writing with, one or more of the following:

> (1) A citation to an express statement in the specification or to a statement made by an applicant during prosecution that demonstrates the well-understood, routine, conventional nature of the additional element(s);"
>
> (2) "A citation to one or more of the court decisions discussed in MPEP § 2106.05(d)(II) as noting the well-understood, routine, conventional nature of the additional element(s);"
>
> (3) "A citation to a publication that demonstrates the well-understood, routine, conventional nature of the additional element(s);" or
>
> (4) "A statement that the examiner is taking official notice of the well-understood, routine, conventional nature of the additional element(s)."

Berkheimer Memo at pp. 3-5 (emphasis added).

Here, the Office Action conclusory states "the functions performed by the [various features recited in claim 1] ***appear*** to be conventional and routine carried out

by a general purpose computer or devices." *Office Action, p. 21* (emphasis added). The Office Action fails to explain or provide any reasoning why the claimed combination of features are allegedly conventional and routine. Furthermore, the Office Action does not provide any evidence meeting the requirements of items (1)-(4) of the *Berkheimer Memo* to show that the combination of features are well-understood, routine or conventional. Accordingly, Applicant respectfully submits that the claimed combination of features recited in amended claim 1 is not well-understood, routine or conventional.

Accordingly, for at least the reasons set forth above, Applicant respectfully submits that amended claim 1 is directed to patent eligible subject matter. Independent claim 10 has been amended to recite features similar to claims 1. Thus for at least the same reasons, Applicant respectfully submits the claim 10 is also directed to patent eligible subject matter. The dependent claims depend directly or indirectly from claims 1 and 10. As dependent claims inherit their patentability from their respective independent claim, the other dependent claims are patent eligible for at least their dependence on an allowable claim and their respective additional novel features. Accordingly, Applicant requests that the Office reconsider and withdraw these rejections.

I. Claim Rejections – 35 U.S.C. § 103

Claims 1-4 and 7-16 stand rejected as being unpatentable over Walker in view of U.S. Patent No. 6,848,048 ("Holmes") in further view of US 2006/0020558 (Bonalle). Claims 7 and 14 stand rejected as being unpatentable under Walker, Holmes, and Chen as applied to claims 1 and 10, and further combined with U.S. Pub. No. 2002/0112177 (Voltmer). 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 and 10 as presented herein.

Without acquiescing to the merits of the grounds of the rejections, and in the interest of advancing prosecution, Applicant has amended Claim 1 to recite:

> establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuity of the mobile

> device, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,
>
> in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device.

Applicant respectfully submits that Walker does not teach or suggest at least "in response to establishing the connection [with the POS], prompt the user to provide biometric information to the biometric reading device," as claimed in amended claim 1.

As discussed during the Interview, Walker describes that a "cardholder first inputs his PIN or biometric data to access [a] device (step 351)" and "[i]f access is granted, the device response by querying the cardholder on display 102 whether it should generate a single-use credit card number (step 355)." *Walker, Col. 6, ll. 18-22*. The single-user credit card number is "recognized as a conventional credit card number," and this number is transmitted to the merchant. *Id. at Col. 6, ll. 36-40.* However, as agreed during the Interview, Walker merely describes inputting biometric data to access the device, and fails to teach or suggest that this biometric data is input based on either the device receiving a request from a merchant to conduct a transaction or establishing a connect to between the device and the merchant. Accordingly, Applicant respectfully submits that Walker does not teach or suggest at least "establish a connection with a point of sale (POS) device, via the short range RF circuitry . . . to conduct a secure transaction" and "in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device," as recited in claim 1.

Furthermore, in rejecting claim 1, the Office Action conceded that "Walker does not explicitly teach [...] wherein the biometric authentication information is associated with the payment information" or "one or more processors configured to authenticate that the biometric information read by the biometric reading device is associated with the payment information based on the biometric authentication information stored in the memory." *Office Action, pp. 24 and 25*. However, the Office Action alleges that Bonalle discloses these features.

Applicant respectfully disagrees and submits that Bonalle is not prior art to this application. Bonalle was filed on July 1, 2004 and does not claim priority to any earlier

applications. Thus, the priority date of Bonalle is July 1, 2004. Whereas, the present application claims priority to US Provisional App. No. 60/394,241, which was filed on July 9, 2002, before the filing date of Bonalle. Thus Bonalle is not prior art. Furthermore, the '026 parent application was filed on July 9, 2003, which is also prior to the filing date of Bonalle. Thus, to the extent the Examiner maintains his rejection of priority claim to the provisional application (a point that is not conceded), Bonalle would still fail to qualify as prior art

Additionally, Applicant respectfully submits that the other references do not cure the deficiencies of Walker at least with respect to amended claim 1. The other references were cited merely to supposedly show certain features which are unrelated to the above-indicated features of amended claim 1, and these references do not appear to remedy the deficiencies of Walker. Therefore, the combination of the prior art references does not teach or suggest all of the features of independent claim 1. Accordingly, not all of the claim elements were known or taught by the prior art.

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, claim 1 is patentable over the cited references, in combination or individually, and Applicant respectfully requests this rejection be withdrawn.

Independent claim 10 has been amended to recite features similar to claim 1. Thus for at least the same reasons, Applicant respectfully submits the suggested combination of references fail to disclose or suggest all of the features of claim 10. Accordingly, Applicant requests the rejections be withdrawn.

The dependent claims depend directly or indirectly from claims 1 and 10. 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 the rejections under § 103 be withdrawn.

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

Dated: July 23, 2018

By: /Mark W. Catanese/
Mark W. Catanese
Registration No. 64,279
Customer No. 27189

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B Street
Suite 2200
San Diego, CA 92101
Tel 619-238-1900
Fax 619-235-0398
docketing@procopio.com

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/639,034	Filing Date 03/04/2015	☐ 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	07/23/2018	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 13	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	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".	diana A bates
*** 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.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 03/01/2019

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
03/01/2019	ELECTRONIC

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

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

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

PTONotifications@procopio.com
docketing@procopio.com

Office Action Summary	Application No. 14/639,034	Applicant(s) Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA 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 07/23/2018.

☐ 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) 1-3 and 7-16 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-3 and 7-16 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 03/04/2015 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions.

2. This communication is a Non-Final Office Action in response to a request for continued examination on 07/23/2018 as a result of the Final Action mailed on 03/22/2018.

3. Claims 1-3, and 7-16 have been examined in this application.

4. No new information disclosure statement (IDS) has been filed.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on May 19, 2015 has been entered.

Response to Arguments

6. Applicant's arguments, see page 7, filed on 07/23/2018, in regards to the claim rejections under nonstatutory double patenting / obviousness-type nonstatutory double patenting have been considered and the rejection will be held in abeyance per Applicant's request.

7. Applicant's arguments, page 8, regarding the disclosure objection have been considered and are persuasive. The objection is withdrawn.

8. Applicant's arguments, see pages 10-15, regarding claim rejections under 35 U.S.C. §112 (a) have been fully considered but are partially persuasive.

Applicant argues every limitation of claim 1 and indicates where support is found for the limitations. The Examiner agrees that as a result of the claim amendments, most of the claim limitation rejections are overcome. However, there are two limitations, which the Examiner does not find support and disagrees with the Applicant's arguments.

On page 12, the Applicant argues that the claim amendment "establish a connection with a point of sale (POS) device… when the POS device is within an operating range of the short range RF circuitry of the mobile device" is supported by the specification. Applicant points to paragraphs 0060 and 0071 of the disclosure, as originally filed, for support. Thought the paragraphs recite "a user with an RF cellular telephone approaches a POS with an RF reader/write, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone," such support does not amount establishing support for the claim limitation. Determining whether the mobile device is within an operating range and establishing, emphasis added, a connection based on the determination of the range is not supported by the specification. The Applicant also points to the Provisional Application, page 38. Though the specification of the Provisional Application does not include page 38, the Examiner found that the page referenced by the Applicant is in the filed drawings. Applicant argues that "the customer comes into POS range (e.g., 5 feet), the hotel's RF reader identifies the customer, credit card information…" Again, this citation does not result in support for indicating that the devices are within range of communication and based on such indication establishing a connection. Establishing a connection by determining that a user is within an operational range is not disclosed in the specification. For at least these reasons, claims 1-3 and 7-16 are rejected because the claims contains subject matter which was not described in the disclosure in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for

pre-AIA the inventors, at the time the application was filed, had possession of the claimed invention.

Furthermore, in regards to claim limitation "secure the payment information using a key," in claims 1 and 10, Applicant argues that support can be found in paragraphs 0064-0073 and in pages 37 and 30 in the Provisional Application. The Examiner disagrees. At best, the specification, paragraph 0069, recites that "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." This citation along with all other citations do not provide support for "[securing] the payment information using a key." Securing data using keys results in encryption of the data. Merely reciting that the cellular phone "may include a cryptographic programmable block chip" for enhancing security does not amount to securing the payment information using a key. The Provisional Application only recites that a fingerprint reader verifies that the user of the cellular phone is the owner of the cellular phone. Verifying a user or authenticating a user is not the same as securing payment information using a key. The claims and all dependent claims are rejected because the claims contains subject matter which was not described in the disclosure in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventors, at the time the application was filed, had possession of the claimed invention.

9. Applicant's arguments, see pages 15-16, regarding claim interpretation under 35 U.S.C. §112 (f) have been fully considered and are persuasive; therefore the interpretation is withdrawn.

10. Applicant's arguments, see pages 16-17, regarding claim rejections under 35 U.S.C. §112(b) have been fully considered and are persuasive; therefore, the rejections are withdrawn.

11. Applicant's arguments, see pages 17-23, regarding claim rejections under 35 U.S.C. §101 have been fully considered and are persuasive. Based on the latest guidelines (PEG 2019) and the Applicant's arguments, the rejections are withdrawn.

12. Applicant's arguments, see pages 23-25, regarding claim rejections under 35 U.S.C. §103 (a) have been fully considered but are moot because they do not apply to the newly relied upon references.

Claim Objections

13. Claim 1 and 10 are objected to because the claims recite "one or more processors… the one or more processor…" The claim should be amended to recite "one or more processors… the one or more processors…" Appropriate correction is required.

14. Claims 10 is objected to because the claim recites "retrieve, from a central database, purchase information…" and "a central database configured to validate the key and the payment information…" The claim should be amended to recite "the central database configured to validate the key and the payment information…" to prevent any future rejections. Appropriate correction is required.

15. Claims 2 and 11 are objected to because of the following informalities: Claim 2 and 11 recite "wherein the biometric reading device is configured to read biometric information provided by a user to complete the transaction." Claims 1 and 10 recite "a biometric reading device configured to read biometric information." Since claims 1 and 10 already indicate that the device reads biometric information, the dependent claims should recite that the device is reading "…the biometric information provided by a user…" Appropriate correction is required in order to avoid any future rejections.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The Disclosure shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The Disclosure shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

16. Claims 1 and 10 and all of their dependent claims are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the disclosure in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1 and 10 recite "establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuitry of the mobile device," and "secure the payment information using a key."

The specification was examined carefully, wherein Paragraphs 0060 and 0071 of the disclosure, as originally filed, recite "a user with an RF cellular telephone approaches a POS with an RF reader/write, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone." These portions of the specification do not disclose the claim limitation "establish a connection with a point of sale (POS) device, via the

short range RF circuitry, when the POS device is within an operating range of the short range RF circuitry of the mobile device."

The only portions _____ are the only portions that disclose any relevance to the connection. However, these portions do not disclose the claim limitation: " "

In regards to claim limitation "secure the payment information using a key," in claims 1 and 10, the specification discloses at Paragraph 0069 that "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." The specification also recites "a "chip can have a cryptographic block with 4 exchange encrypted keys with up to 256 bits)." These citations along with all other citations do not provide support for "secure the payment information using a key." Claims 8 and 15 recite "wherein the payment information is secured with a cryptographic key." The claims are rejected for the same rational as above.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 1-3, 7-16 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,934,689 to Ritter et al. ("Ritter"), in view of U.S. Patent Application Publication 2002/0157029 to French et al. ("French"), in further view of U.S. Patent 6,163,771 to Walker et al. ("Walker").

18. Per claims 1 and 10, Ritter teaches all of the following limitations:

a. A mobile device, comprising [Abstract, Col. 4, Ln. 46-51 and Figure 1]:

b. short range radio frequency (RF) circuitry [Col. 4, Ln. 46-67; Col. 5, Ln. 1-9 and Figure 1];

c. a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information [Abstract, Col.5, Ln. 56-67; Col. 7, Ln. 51-67; Col. 8, Ln. 1-6; and Figure 1];

d. a biometric reading device configured to read biometric information [abstract, Col. 5, Ln. 62-67; Col. 6, Ln. 1-6; Col. 9, Ln. 1-15 and Figure 1]; and

e. one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processor configured to execute instructions stored in the memory to [Abstract, Col. 4, Ln. 46-67; Col.5, Ln. 10-18; Col. 5, Ln. 58-67; and Figures 1]:

f. establish a connection with a point of sale (POS) device, via the short range RF circuitry, when then the POS device is within an operating range of the short range RF circuitry of the mobile device, wherein the connection is established to conduct a secured transaction between the mobile device and the POS device [Abstract, Col. 4, Ln. 46-67; Col. 6, Ln. 49-67 and Figure 1],

g. authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory [Abstract, Col.5, Ln. 56-67; Col. 6, Ln. 1-11; Col. 7, Ln. 51-67; and Figure 1],

h. secure the payment information using a key [Col. 3, Ln. 1-8; Col. 7, Ln. 41-50; Col. 8, Ln. 64-67],

i. when the biometric information ready by the biometric reading device is successfully authenticated, transmit to the POS device, via the short range RF circuitry, information indicative of the authentication [Abstract, Col. 5, Ln. 56-67; Col. 6, Ln. 1-11; Col. 6, Ln. 39-58 and Figure 1], and

j. retrieve purchase information related to the secured transaction based, in part, on the transmitted information [Col. 3, Ln. 1-8; Col. 8, Ln. 7-17 and Figure 3].

k. Although Ritter teaches a user carrying out a transaction with a POS using their mobile device, wherein the user must provide biometric authentication information in order to advance a transaction with the POS utilizing wireless / RF communication as shown above [Abstract, Col. 4, Ln. 14-67], Ritter does not explicitly disclose in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device.

French explicitly teaches in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device [Paragraphs 0065-0067, 0130-0132 and Figure 12].

It would have been obvious to one or ordinary skill in the art at the time of the invention to combine the teachings of Ritter, which teaches requiring a user to perform a biometric authentication on their mobile device in order to be authenticated and subsequently allow the user to complete a transaction with a terminal utilizing RF communication, in order to include the teachings of French to explicitly disclose that the

user is prompted for the authentication information when the user establishes a connection with the POS or merchant in motivation of enhancing user experience by providing the prompt for the authentication information in order to facilitate the process of conducting the transaction.

Per claim 10, Ritter teaches:

a. a point of sale (POS) device configured to [Abstract, Col. 4, Ln. 38-45 and Figure 1]:

b. receive, from the mobile device, the secured payment information and the information indicative of the authentication [Abstract, Col. 6, Ln. 1-11; Col. 6, Ln. 39-67; Col. 8, Ln. 7-17; Col. 8, Ln. 64-67 and Figure 1]; and

c. Although Ritter in view of French teach settlement of a transaction between a mobile device and a merchant or point of sale and performing authentication checks using multiple entities and databases, Ritter in view of French do not explicitly disclose retrieve, from a central database, purchase information based on the received information indicative of authentication.

Walker teaches retrieve, from a central database, purchase information based on the received information indicative of authentication [Abstract, Col. 6, Ln. 38-53; Col. 8, Ln. 34-65; Figures 3-4, and 12]; and

It would have been obvious to one or ordinary skill in the art at the time of the invention to combine the teachings of Ritter in view of French, which teach a mobile device in communication with a POS conducting a transaction and having the POS

transmit a settlement request to a clearing point or clearing house using encryption techniques once requirements have been met, to include the teachings of Walker to explicitly teach retrieving purchase information from a central authority based on authentication of in motivation deterring fraudulent transactions in order to increase security measures.

d. Ritter in view of French teach settling a transaction between entities, including sending from a POS to a clearing point or clearing house a request to settle the transaction. However, Ritter in view of French do not explicitly disclose a central database configured to validate the key and the payment information based on the information indicative of authentication.

Walker teaches a central database configured to validate the key and the payment information based on the information indicative of authentication [Abstract, Col. 6, Ln. 38-53; Col. 8, Ln. 34-65; Figures 3-4, and 12].

It would have been obvious to one or ordinary skill in the art at the time of the invention to combine the teachings of Ritter in view of French, which teach a mobile device in communication with a POS conducting a transaction and having the POS transmit a settlement request to a clearing point or clearing house using encryption techniques in order to settle a transaction, to include the teachings of Walker to explicitly teach validating by the issuer the key and payment information in motivation of settling the transaction and returning a transaction response to the merchant / POS.

19. Per claims 2 and 11, Ritter teaches wherein the biometric reading device is configured to read biometric information provided by a user to complete the transaction [Col. 5, Ln. 56-67; Col. 6, Ln. 1-6].

20. Per claims 3 and 12, Ritter teaches wherein the payment information is associated with a primary account number [Abstract, Col. 7, Ln. 51-67 and Figure 1].

21. Per claims 7 and 14 Ritter teaches wherein the biometric authentication information is stored separately from the payment information [Col. 5, Ln. 56-62; Col. 7, Ln. 51-64 and elements 12-15 and 17 in Figure 1].

22. Per claims 8 and 15, Ritter teaches wherein the payment information is secured with a cryptographic key [Col. 3, Ln. 1-8; Col. 7, Ln. 41-50; Col. 8, Ln. 64-67].

23. Per claims 9 and 16, Ritter teaches wherein the short range RF circuitry comprises a radio frequency identification (RFID) device [Col. 4, Ln. 46-67; Col. 5, Ln. 1-9; and Figure 1].

24. Per claim 13, Ritter teaches wherein the POS device includes an RF reader [Col. 4, Ln. 46-67; Col. 5, Ln. 1-9; Col. 5, Ln. 25-30 and Figure 1].

Double Patenting

25. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*,

140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claim 1 of the instant Application is rejected on the ground of nonstatutory double patenting as being unpatentable over Claim 3 of prior U.S. Patent No. 8766772. Although the claims at issue are not identical, they are not patentably distinct from each other. Claim 3 in U.S. Patent 8766772 teaches the claim limitations of the instant Application's Claim 1, but does not teach "secure the payment information using a key." Ritter, U.S. Patent 6934689, teaches such missing limitations; see abstract, Col. 3, Ln. 1-8; Col. 7, Ln. 41-50; Col. 8, Ln. 64-67 and Figure 1. It would have been obvious to one of ordinary skill in the art at the time of the invention to

combine the teachings of U.S. Patent 8766772 and the teachings of Ritter to teach securing the payment information utilizing a key before providing the information to another entity to advance a transaction in motivation of increasing security measures.

26. Claims 2-17 are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14/659502 in view of U.S. Patent 6,163,771 to Walker.

This is a provisional obviousness-type nonstatutory double patenting rejection.

Although the conflicting claims are not identical, they are not patentably distinct from each other. Claims 1 and 10 of co-pending application 14/659502 recites:

a. mobile device, comprising:

b. short range radio frequency (RF) circuitry;

c. memory configured to store biometric authentication information and payment information;

d. a biometric module configured to read biometric information;

e. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

f. a secure module configured to:

g. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

h. encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction

Claim 10:

j. A system, comprising:

k. a mobile device, comprising:

l. short range radio frequency (RF) circuitry;

m. memory configured to store biometric authentication information and payment information;

n. a biometric module configured to read biometric information;

o. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

p. a secure module configured to:

q. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

r. encrypt the key and the payment information stored in memory; and

s. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

t. a point of sale (POS) device configured to:

u. receive, from the secure module, the encrypted key and payment information; and

v. transmit, to a central database, the encrypted key and payment information; and

w. a central database configured to validate the key and the payment information.

Claims 1 and 10 of co-pending application 14/659502 differ from the instant claims since they fail to recite that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory. Ritter discloses an authenticating that the biometric information is associated with the user associated with the payment information based on the biometric authentication information stored in memory. See Ritter at Abstract, Col.5, Ln. 56-67; Col. 6, Ln. 1-11; Col. 7, Ln. 51-67; and Figure 1. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of co-pending Application 14/659,502 to include the teachings of Ritter, which teaches a mobile device authenticating a user based on biometric input and settling a transaction using payment information associated with the user of the mobile device in motivation of only allowing the proper user to whom the device belongs to settle a transaction based on associating the biometric input with the stored input and the user with the payment information; resulting in increased security measures.

It is well settled that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA 1963). Also note Ex parte Rainu, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

Co-pending Applications 14/321781, 14/724593, 14/585057 are also rejected based on the same above rationale.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed on for PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on M-F 9AM - 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Neha W. Patel can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/

El Mehdi Oussir
Patent Examiner, Art Unit 3685
02/26/2019

Notice of References Cited	Application/Control No. 14/639,034	Applicant(s)/Patent Under Reexamination Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-7911643-B2	03-2011	Yamada; Makoto	H04N1/33307	358/1.15
*	B	US-5590197-A	12-1996	Chen; James F.	G06Q20/04	380/30
*	C	US-20070022058-A1	01-2007	Labrou; Yannis	G06Q20/32	705/67
*	D	US-20020193142-A1	12-2002	Stavenow, Bengt	G06F21/41	455/556.1
*	E	US-20020194499-A1	12-2002	Audebert, Yves Louis Gabriel	H04L63/0853	726/35
*	F	US-20020123325-A1	09-2002	Cooper, Gerald M.	H04L63/0492	455/411
*	G	US-20020112171-A1	08-2002	Ginter, Karl L.	G06F21/10	713/185
*	H	US-20020157029-A1	10-2002	French, Jennifer	G06F21/31	726/21
*	I	US-6934689-B1	08-2005	Ritter; Rudolf	G06Q20/04	705/16
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

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

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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06Q	5/8/2015	EO
H04L	5/8/2015	EO
G06Q20	02/15/2019	EO

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
705		5/8/2015	EO

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

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

Search Notes		
Search Notes	**Date**	**Examiner**
consulted Calvin Hewitt	5/15/2015	EO
Consulted John H. and Mamon O on 101/ 103	5/25/2017	EO
Consulted John H. on priority	5/9/2017	EO
Consulted Mohammad N. on priority and 112	5/26/2017	EO
Consulted Steven K. 112	03/14/2018	EO
Review of references	03/16/2018	EO
Consulted John H. 101	03/14/2018	EO
East search update	02/13/2019	EO
Consulted Steven Kim 101	02/13/2019	EO
IP.COM search	02/13/2019	EO
EAST search update	02/15/2019	EO
IP.COM search	02/18/2019	EO
Consulted Steven Kim 101 / 103	02/19/2019	EO
Consulted Mohammad N. 112	02/21/2019	EO

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

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

CLAIMS

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

CLAIM		DATE								
Final	Original	05/18/2015	12/09/2015	05/26/2017	03/16/2018	02/26/2019				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	✓	✓	✓				
	3	✓	✓	✓	✓	✓				
	4	✓	✓	✓	✓	-				
	5	✓	-	-	-	-				
	6	✓	-	-	-	-				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9	✓	✓	✓	✓	✓				
	10	✓	✓	✓	✓	✓				
	11	✓	✓	✓	✓	✓				
	12	✓	✓	✓	✓	✓				
	13	✓	✓	✓	✓	✓				
	14	✓	✓	✓	✓	✓				
	15	✓	✓	✓	✓	✓				
	16	✓	✓	✓	✓	✓				

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L7	1	("8766772").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/26 13:14
S98	3	(contactless near2 (payment transaction) and biometric) and @ay< "2003"	US-PGPUB; USPAT	OR	OFF	2019/02/21 17:21
S97	1	("6934689").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 17:11
S96	1	("20020157029").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 15:00
S95	1	("20020112171").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 14:58
S94	0	(2002/0112171).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 14:57
S93	2	("20020123325").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 21:15
S92	5	("0797,359").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 21:14
S91	24	("1239630").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 21:13
S90	1	("20020194499").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/15 20:54
S89	1	("20020157029").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/15 20:41
S88	0	(2002/0157029).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/15 20:41

S87	154	(prompt$4 dialog$3 form window popup pop$up) near2 (biometric pin code iris fingerprint authenticat$4 password passcode) with (location connect$4 area vicinity range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:32
S86	92	(prompt$4 dialog$3 form window popup pop$up) near2 (biometric pin code iris fingerprint authenticat$4 password passcode) with (location area vicinity range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:29
S85	8880	(prompt$4 dialog$3 form window popup pop$up) with (location area vicinity range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:26
S84	30	S83 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 20:24
S83	730	S81 same (biometric pin code iris fingerprint authenticat$4 password passcode)	US-PGPUB; USPAT	OR	ON	2019/02/15 20:24
S82	326	S81 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 20:23
S81	5053	(prompt$4 dialog$3 form window popup pop$up) with (range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:22
S80	11	S79 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:42
S79	1910	S76 and ((prompt$4) near6 (biometric iris pin code password))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:42
S78	2422	S75 and ((prompt$4) near6 (biometric iris pin code password))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:42
S77	13	S76 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:39
S76	2479	S75 and ((prompt$4) with (user customer) with (biometric iris pin code password))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:38
S75	76623	(detect$4 determin$5) with (device mobile) with (rf bluetooth nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:36
S74	68297	(detect$4 determin$5) with (device mobile) with (rf bluetooth nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:36
S73	18	S72 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:30
S72	2518	S71 and ((mobile electronic) near3 (device phone pda))	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:30
S71	2980	S70 and ((prompt$4) with (user	US-PGPUB;	OR	OFF	2019/02/15

		customer) with (biometric iris pin code password))	USPAT			19:26
S70	108452	((establish$3) near6 (connection link)) with (rf bluetooth nfc wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 19:25
S69	82023	((establish$3) near6 (connection link)) with (rf bluetooth nfc wireless)	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:25
S68	3	S64 and ((prompt$4) with (input biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S67	5	S64 and ((prompt$4 ask$4) with (input biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S66	7	S64 and ((prompt$4 ask$4 requir$4) with (input biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S65	7	S64 and (prompt$4 ask$4 requir$4)	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S64	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S63	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	OFF	2019/02/15 16:19

EAST Search History (Interference)

< This search history is empty>

2/ 26/ 2019 2:25:46 PM
C:\ Users\ eoussir\ Documents\ EAST\ Workspaces\ 14639034_Mobile device RFID transaction biometric POS.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 04/09/2019

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
04/09/2019	ELECTRONIC

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

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

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

PTONotifications@procopio.com
docketing@procopio.com

Applicant-Initiated Interview Summary	**Application No.** 14/639,034	**Applicant(s)** Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA (FITF) Status** No

All participants (applicant, applicants representative, PTO personnel):

(1) EL MEHDI OUSSIR. (3) _____.

(2) Mark W. Catanese (Applicant's Representative). (4) _____.

Date of Interview: 03 April 2019.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☑112 ☐102 ☑103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: Ritter/French.

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's representative and the Examiner discussed proposed claim amendments to try and overcome claim rejections. Specifically, the 112(a) rejections were discussed. Examiner explained why the rejections were issued. Potential claim amendments were presented to try and overcome the rejections. No specific agreement was reached, but the Examiner noted that further review of the amendments and specification would be made. Per 103, the reference to French was argued as not teaching prompting a user for data in response to a communication. Examiner noted that French explicitly taught the limitation. No agreement was reached..

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

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	/NEHA PATEL/ Supervisory Patent Examiner, Art Unit 3685

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 examiners 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 applicants 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 applicants 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 examiners 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 examiners initials.

Do Not Enter E. O.

App Nos.: 14/639,034 Attorney Docket No. 116546-613CT13
Title: SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
Filed: March 4, 2015
Inventor(s): de VELASCO CORTINA, Francisco Martinez
Examiner: OUSSIR, El Mehdi
Art Unit: 3685
Conf. No.: 5934

AGENDA FOR TELEPHONIC INTERVIEW

(NOT INTENDED FOR ENTRY INTO THE RECORD)

Attendees, Date and Type of Interview

A telephonic interview is scheduled for April 3, 2019, at 2:00PM EDT (11:00AM PDT). The interview will be attended by Examiner Oussir and Applicant's Representative Mark W. Catanese (Reg. No. 64,279).

Applicant's Representative will call the Examiner at (571) 270-0191.

Identification of Claims to be Discussed

Claims 1 and 10.

Identification of Art to be Discussed

U.S. Patent No. 6,934,689 ("Ritter");

U.S. App. Pub. No. 2002/0157029 ("French"); and

U.S. Patent No. 6,163,771 ("Walker").

Items to be Discussed

1. Applicant would like to discuss the rejection of the claims under 35 U.S.C. § 112 (a) and the proposed amendment to claim 1 below. Applicant to explain that one skilled in the art would reasonably conclude that the specification describes the claimed features.
2. Applicant would like to discuss the rejection of the claims under 35 U.S.C. §103 and the proposed amendment to claim 1 below in view of the above cited references. Specifically, Applicant to explain why it believes the cited references do not teach or suggest the claimed features.

Proposed Amendments to Claim 1

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

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more ~~processor~~ processors configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuity of the mobile device, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in the memory,

secure the payment information using a key,

when the biometric information read by the biometric reading device is successfully authenticated, transmit to the POS device, via the short range RF circuitry, information indicative of the authentication, and

~~retreive~~retrieve purchase information related to transaction based, in part, on the transmitted information.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	de VELASCO CORTINA, Francisco Martinez	116546-613CT13	5934

EXAMINER	
OUSSIR, El Mehdi	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
April 18, 2019	EFS WEB

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

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

RESPONSE TO OFFICE ACTION

Sir:

This paper is submitted in response to the Non-Final Office Action mailed on March 1, 2019. Allowance of the above identified application is respectfully requested in view of the following submission, where:

Amendments to the Claims begin on page 2 of this paper.

Interview Summary begins on page 6 of this paper.

Remarks begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

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

What is claimed is:

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

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more ~~processor~~ processors configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry~~, when the POS device is within an operating range of the short range RF circuity of the mobile device~~, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

obtain at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device,

in response to ~~establishing the connection~~obtaining at least a portion of the payment information, prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory,

secure the payment information using a key,

when the biometric information read by the biometric reading device is successfully authenticated, transmit to the POS device, via the short range RF circuitry, information indicative of the authentication, and

~~retreive~~retrieve purchase information related to transaction based, in part, on the transmitted information.

2. (Currently Amended) The mobile device of claim 1, wherein the biometric reading device is configured to read the biometric information provided by a user to complete the transaction.

3. (Original) The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. (Canceled)

5. (Canceled)

6. (Canceled)

7. (Original) The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. (Previously Amended) The mobile device of claim 1, wherein the payment information is secured with a cryptographic key.

9. (Original) The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. (Currently Amended) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information;

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more ~~processor~~ processors configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuity of the mobile device, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based at least in part on the biometric authentication information stored in memory

secure the payment information using a key,

when the biometric information read by the biometric reading device is successfully authenticated, transmit to the POS device, via the short range RF circuitry, information indicative of the authentication, and

~~retreive~~retrieve purchase information related to the secured transaction based, in part, on the transmitted information; and

the POS device configured to:

receive, from the mobile device, the secured payment information and the information indicative of the authentication; and

retrieve, from a central database, purchase information based on the received information indicative of authentication; and

[[a]]the central database configured to validate the key and the payment information based on the information indicative of authentication.

11. (Currently Amended) The system of claim 10, wherein the biometric reading device is configured to read the biometric information provided by a user to complete the transaction.

12. (Original) The system of claim 10, wherein the payment information is associated with a primary account number.

13. (Original) The system of claim 10, wherein the POS device includes an RF reader.

14. (Original) The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. (Previously Amended) The system of claim 10, wherein the payment information is secured with a cryptographic key.

16. (Original) The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

17. (New) The system of claim 1, wherein the one or more processors are configured to execute the instructions to retrieve information to complete the secure transaction based, in part, on the transmitted information.

INTERVIEW SUMMARY

Applicant thanks Examiner Oussir for the courtesy extended during the telephonic interview conducted in the present application on April 3, 2019 with Mark Catanese ("Interview"). During the Interview, Applicant and Examiner discussed the rejection of the claims in view of certain proposed amendments, some of which are reflected in the "Amendments to the Claims" section above. Other features were discussed that the Examiner, but no agreement was reached with respect to patentability. The substance of those discussions is reflected in the remarks below.

REMARKS

The present amendment is in response to the Final Office Action dated March 1, 2019. 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, 2, 10, and 11 are amended and new claim 17 is added. Support for the amendments can be found throughout the application as originally filed. For example, support can be found at least in FIGS. 12-14 and the accompanying text of the application as originally filed. No new matter has been added. Claims 1-3 and 7-16 are pending in the application, claims 4-6 having been previously cancelled without prejudice or disclaimer. Claims 1 and 10 are the independent claims.

In response to the Office Action, Applicant respectfully traverses all of the rejections and requests reconsideration of the above-captioned application in view of the following comments.

B. Claim Objections

In the Office Action, claims 1, 2, 10, and 11 are objected too. Without acquiescing to the merits of the objections and in the interest of advancing prosecution, Applicant has amended claims 1, 2, 10, and 11 as suggested in the Office Action. Accordingly, Applicant respectfully submits that amended claims 1, 2, 10, and 11 overcome the objections and requests the objections be withdrawn.

C. Claim Rejections - 35 U.S.C. § 112(a)

Claims 1 and 10 and all of their dependent claims stand rejected as failing to comply with the written description requirement. Particularly, the Office Action asserted that features (A) "establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuity of the mobile device" and (B) "secure the payment information using a key" are unsupported by the application as originally filed. Applicant respectfully traverses each of these rejections.

Regarding feature (A), Applicant does not necessarily agree with the rejection; however, in the interest of advancing prosecution and without acquiescing to the merits of the object, Applicant has amended claim 1 as discussed during the interview and as reflected in the "Amendments to the Claims" section, thereby rendering the rejection of this feature as moot.

Turning to feature (B), the Office Action alleged that in the Response to Final Office Action filed on July 23, 2018 "Applicant argues that support [for this feature] can be found in paragraphs 0064-0073 and in pages 37 and 30 in the Provisional Application." *Office Action, p. 4.* However, this assertion is not a complete characterization of the remarks set forth by the Applicant and over simplifies that Applicant's remarks as well as the application as filed in order to make it appear as though the application as filed does not provide support for the feature of "[securing] payment information using a key."

For example, while Applicant cited to "at least FIGs. 12-14 and the accompanying text and paragraphs [0059]-[0072] of the application as originally filed" and pages 36-47 of the US Provisional Application No. 60/394,241 (hereinafter "Parent Provisional Application.)" (*Response to Final Office Action, p. 10*), Applicant also explained that:

> Support for this feature can be found, for example, in at least **paragraphs [0033], [0053], [0068], [0069], [0064], [0069], [0070], [0072], [0073], [0088] and [0120]**[1] of the application as originally filed. For example, **[0033]** states "[a]n 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**," where payment or transaction information is one such type of information stored on the RF device (*see, e.g., para. [0069]). See also, **Parent Provisional Application, p. 30*** ("the information contained in the device you can not be able to altered without you being able to determine by who and for what purpose and for this we use highly secure chip with a hardware programmable cryptographic block with credit and debit exchange keys. "). Furthermore, paragraphs [0068] and [0069] state "[t]he RF cellular telephone also may include a cryptographic

[1] Applicant notes that, while various embodiments of RF identification mechanisms are described in the application as originally filed, one skilled in the art would recognize that the features of one embodiment may be interchanged and utilized in other embodiments described in the application as originally filed. *See, e.g., Application as originally filed, paras. [0003], [0016], [0018], and [0054] and Parent Provisional Application, p. 2.*

> programmable block chip 1349 to enhance security." *See also, Parent Provisional Application, pp. 40 and 46* ("The RF cellular telephone also may include a cryptographic programmable block chip to enhance security.")

Id. at pp. 13-14 (emphasis added).

Additionally, paragraph [0053] of the application as filed describes a "**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**" and a "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." (emphasis added); *see also Parent Provisional Application, p. 30*. Applicant also notes that paragraph [0088] of the application as originally filed describes various data encryption standards, such as DES, 3DES, MD5, and a Federal Information Processing Standard (PIPS) 140-certified random number generator for generating secure encryption keys. *See also Data Encryption Standard, Wikipedia.Org,* available at https://en.wikipedia.org/wiki/Data_Encryption_Standard (explaining that DES is a symmetric-key algorithm for the encryption of electronic data). Further still, paragraph [0109] states:

> [t]he 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.

(emphasis added); *see also, Internet Key Exchange, Wikipedia.Org,* available at https://en.wikipedia.org/wiki/Internet_Key_Exchange (explaining that IKE is a protocol to exchange a shared session secure from which cryptographic keys are derived).

Thus, clearly the application describes more than "[m]erely reciting that the cellular phone 'may include a cryptographic programmable block chip' for enhancing secure" as asserted at pages 4 and 7 of the Office Action. For example, at least the above sections of the application as filed describe various cryptographic and encryption methods that provide can be implemented to secure data and transactions (e.g., data exchanges).

Accordingly, Applicant respectfully submits that that the application as originally filed provides sufficient support in compliance with 112(a) for the feature of "[securing] the payment information using a key."

Applicant notes that "[t]o satisfy the written description requirement, a patent specification must describe the claimed invention ***in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention***." *MPEP 2163(I)* (citing *Moba, B.V. v. Diamond Automation, Inc.*, 325 F.3d 1306, 1319 (Fed. Cir. 2003); *Vas-Cath, Inc. v. Mahurkar*, 935 F.2d 1555, 1563 (Fed. Cir. 1991)) (emphasis added).

As described above, the application as originally filed describes that encryption of data using a sundry of cryptographic methods, such as for example, credit and debit exchange keys, a cryptographic programmable block, encryption keys, DES, 3DES, MD5, a Federal Information Processing Standard (PIPS) 140-certified random number generator for generating secure encryption keys, IKE protocol, etc. Additionally, the application as originally filed as detailed above describes that both secure transactions (e.g., data exchanges between devices) can be protected using encryption keys and that a central data base may be secured using encryption. Accordingly, one skilled in the art would reasonably conclude that the application as originally filed provides sufficient detail to support securing data either stored in a memory and/or exchanged between device using keys, such as encryption keys.

Furthermore, that the various citations to the paragraphs of the application as originally filed are from different sections of the application is irrelevant. Applicant submits that there is nothing in the application as originally filed to restrict the above cited paragraphs describing the various data encryption algorithms and processes to a specific embodiment. In fact, the paragraph [0003] of the application as originally filed

clearly states that "[t]hose 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." *See also, paragraphs [0016], [0018], and [0054] of the application as originally filed; and Parent Provisional Application, p. 2* (stating that that "systems ad method can be used in numerous embodiments, including, but not limited to: . . . RF Cellular Telephone and Method of Use."). Thus, one skilled in the art would reasonably conclude that the application as originally filed provides sufficient detail to support securing data either stored in a memory and/or exchanged between device using keys, such as encryption keys in connection with the RF Communication Device and Method thereof as described in connection with FIGS. 12-14.

Accordingly, in view of the above, Applicant submits that the application as originally filed provides sufficient detail that one skilled in the art can reasonably conclude that the application describes "[securing] the payment information," as recited in amended claim 1.

For at least the foregoing reasons, Applicant submits that amended claim 1 is well supported by the application as originally filed. Accordingly, Applicant requests the rejection be withdrawn. Amended claim 10 recites features similar to amended claim 1. Thus for at least the same reasons, applicant requests the rejections of the independent claims and all of associated dependent claims under § 112(a) be withdrawn.

D. Claim Rejections – 35 U.S.C. § 103

Claims 1-3 and 7-16 stand rejected as being unpatentable over US. Patent 6,934,689 ("Ritter") in view of U.S. Patent App. Pub. No. 2002/0157029 ("French"), in further view of US Patent 6,163,771 (Walker). 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 and 10 as presented herein.

In rejecting claim 1, the Office Action conceded that "Ritter does not explicitly disclose in response to establishing the connection, prompt the user to provide

biometric information to the biometric reading device." *Office Action, p. 9*. However, the Office Action asserted that French discloses this feature.

Applicant respectfully disagrees and submits that French does not teach or suggest "in response to ***establishing the connection [to conduct the secure transaction],*** prompt the user to provide biometric information to the biometric reading device," as previously recited in claim 1.

French describes "a system and method to authenticate a network user's identity using a hierarchy of information queries." *French, para. [0058]*. French describes that "a user who wants to access information or process a transaction over a network is prompted to submit information to authentication process 10 through client 110." *Id. at para. [0065]*. Thus, French at best describes that when a user "wants" to process a transaction over a network, the user is prompted to submit information. There is nothing in French that describes whether this prompt is in response to a connection with another device or if a connection with the other device is already established and the user simply elects this time to process a transaction. Thus, French does not teach or suggest at least "in response to *establishing the connection,* prompt the user to provide biometric information to the biometric reading device," as previously recited in claim 1.

Furthermore, Applicant notes, even if the feature "to conduct a secure transaction" is interpreted as an intended use phrase (a point the Applicant does not concede), such features still serve to limit the claim at least because the phrase "to conduct a secure transaction" results in a manipulative difference between the claim 1 and the prior art. *See MPEP 2112.02(II)*. That is, the timing of the prompt is based on the establishing a connection with a POS device for a specific purpose, opposed to a general connection with another device.

However, without acquiescing to the merits of the grounds of the rejections, and in the interest of advancing prosecution, Applicant has amended Claim 1 to recite, in part, "obtain at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device, [and] in response to obtaining at least a portion of the payment information, prompt the user to provide biometric information to the biometric reading device." Support for the amendments

can be found, for example, in at least FIG. 14 and paragraphs [0060] and [0070]-[0074] of the application as originally filed. *See also, Parent Provisional Application, pp. 36-42*.

Applicant respectfully submits that the cited references do not teach or suggest at least the above-identified features as recited in amended claim 1.

For example, Ritter describes "[i]f the customer would like to pay the total amount of the payment transaction by means of his mobile device 1, he switches on his mobile device 1, and, to be on the safe side, in an embodiment variant, is requested by an authentication module 12 of the mobile device 1" (*Ritter, Col. 5, ll. 51-56*), and only after successful authentication selecting the function "payment transaction" and establishing a communication with a payment terminal 2 *(id. at Col. 6, ll. 7-64*). Thus, Ritter describes unlocking a device 1 by authenticating the user which is followed by establishing a connection with the payment terminal 2. Accordingly, Applicant respectfully submits that Ritter does not teach or suggest at least "obtain at least a portion of the payment information relevant to the secure transaction **based on establishing the connection with POS device**, [and] **in response to obtaining at least a portion of the payment information, prompt** the user to provide biometric information to the biometric reading device," as recited in claim 1. (emphasis added).

Additionally, Applicant respectfully submits that the other references do not cure the deficiencies of Ritter at least with respect to amended claim 1. The other references were cited merely to supposedly show certain features which are unrelated to the above-indicated features of amended claim 1, and these references do not appear to remedy the deficiencies of Ritter. For example, as described above, French describes that a user who wants to process a transaction over a network is prompted to submit information to authentication process 10 through client 110, but does not appear to disclose obtaining at least part of the information related to the transaction and then prompting the user to authenticate themselves in response to obtaining the information. Furthermore, Walker is similar to Ritter, in that Walker merely describes authenticating a user to gain access to a device. *See, e.g., Walker, Col. 6, ll. 18-22.* Therefore, the combination of the prior art references does not teach or suggest all of

the features of independent claim 1. Accordingly, not all of the claim elements were known or taught by the prior art.

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, claim 1 is patentable over the cited references, in combination or individually, and Applicant respectfully requests this rejection be withdrawn.

Independent claim 10 has been amended to recite features similar to claim 1. Thus for at least the same reasons, Applicant respectfully submits the suggested combination of references fail to disclose or suggest all of the features of claim 10. Accordingly, Applicant requests the rejections be withdrawn.

The dependent claims depend directly or indirectly from claims 1 and 10. 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 the rejections under § 103 be withdrawn.

E. Nonstatutory Double Patenting

Claim 1 stands rejected on the ground of nonstatutory double patenting as being unpatentable over claim 3 of prior U.S. Patent No. 8,766,772. Claims 2-17 (interpreted as claims 2, 3, and 7-16) are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14/659,502 in view of Walker.

Applicant respectfully requests reconsideration of these rejections in view of the foregoing claim amendments. Furthermore, not notwithstanding the following remarks and arguments as to the allowability of the pending claims over Walker, the claims may further change throughout prosecution. Therefore, Applicant respectfully requests the double patenting rejection be held in abeyance until the claims are otherwise in condition for allowance.

F. New Claim

New dependent claim 17 has been added. Applicant submits the new dependent claim depends from independent claim 1. As dependent claims inherit their patentability from their respective dependent claim, the new dependent claim is allowable for at least their dependence on an allowable claim and its respective additional novel features. Accordingly, Applicant respectfully submits that new dependent claim 17 is 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

Dated: April 18, 2019

By: /Mark W. Catanese/
Mark W. Catanese
Registration No. 64,279
Customer No. 27189

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B Street
Suite 2200
San Diego, CA 92101
Tel 619-238-1900
Fax 619-235-0398
docketing@procopio.com

Electronic Acknowledgement Receipt

EFS ID:	35764737
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	18-APR-2019
Filing Date:	04-MAR-2015
Time Stamp:	14:21:15
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		116546-613CT13_Resp_to_NFOA_dated_Mar_1_AS_FILED_04_18_2019.PDF	146625 68648a2f37afad91b8fba7f289e7a42f9a2006fe	yes	15

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	5
	Applicant summary of interview with examiner	6	6
	Applicant Arguments/Remarks Made in an Amendment	7	15
Warnings:			
Information:			
	Total Files Size (in bytes):	146625	

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

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 08/01/2019

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
08/01/2019	ELECTRONIC

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

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

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

PTONotifications@procopio.com
docketing@procopio.com

Office Action Summary	Application No. 14/639,034	Applicant(s) Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (FITF) Status No

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

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 04/18/2019.

☐ 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) 1-3 and 7-17 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) 1-3 and 7-17 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 03/04/2015 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

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

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions

2. This communication is **a Final Office action** in response to Applicant's response on 04/18/2019 to Examiner's Non-Final communication on 03/01/2019.

3. Claims 1-3, and 7-17 have been examined in this application. Claim 17 is newly presented.

4. No new information disclosure statement (IDS) has been filed.

Response to Arguments

5. Applicant's arguments, filed on 04/18/2019, page 7, in regards to claim objections have been fully considered and the objections are withdrawn.

6. Applicant's arguments regarding claim rejections under nonstatutory double patenting / obviousness-type nonstatutory double patenting have been considered and the rejection will be held in abeyance per Applicant's request.

7. Applicant's arguments, see pages 7-11, regarding claim rejections under 35 U.S.C. §112 (a) have been fully considered but are partially persuasive.

I. Claims have been amended to overcome the rejection directed to establishing a connection with a POS device via RF circuitry when the POS device is within operating range of the mobile device.

A. Claims are still directed to "establishing a connection with a point of sale…" and support for such a limitation is not found.

The Examiner disagrees with the Applicant's arguments. The amendments merely cancel the conditional limitation of when the two devices are in proximity to one another. However, the claims still recite establishing a connection between the mobile device and a POS. The specification was examined carefully, wherein Paragraphs 0060 and 0071 of the disclosure, as originally filed, recite "a user with an RF cellular telephone approaches a POS with an RF reader/write, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone." These portions of the specification do not disclose the claim limitation "establish a connection with a point of sale (POS) device, via the short range RF circuitry."

II. Support for securing the payment information using a key can be found Paragraphs 0033, 0053, 0068, 0069, 0064, 0070, 0072-0073, 0088, and 0120.

B. The specification does not recite that payment information is secured using a key.

The Examiner disagrees with the Applicant's arguments. The Applicant is relying on the explanation of encryption technology and how it is used to protect information instead of pointing out where support is found for securing payment information using a key. For instance the Applicant argues: "information in the central database 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 takes to the field… it also extends and expands the verification of both individual and vehicle identity… Applicant also notes… various data encryption standards… for generating secure encryption keys…" All of the arguments and support relied upon is directed to encryption at a high level and does not specify that a specific

encryption technique is used **nor** does the specification describe what information is being encrypted using such specific encryption.

The cited portions and the arguments filed by the Applicant do not provide any support for the claim limitation of "secure the payment information using a key." Support simply indicating just what the claim recites would overcome the rejection, but instead, the support relied upon merely recites how keys can be generated and the benefit of using encryption techniques.

8. Applicant's arguments, see pages 11-14, regarding claim rejections under 35 U.S.C. §103 (a) have been fully considered but are not persuasive.

I. References do not teach obtaining payment information after establishing an RF connection and prompting the user to provide biometric information.

A. Ritter in view of French teach the claimed limitations.

The Examiner disagrees with the Applicant's arguments that the references do not teach the claim limitations directed to "[obtaining] at least a portion of the payment information relevant to the secure transaction based on establishing the connection with the POS device," and prompting the user to provide biometric information to the biometric reading device in response to obtaining at least a portion of the payment information.

Ritter clearly teaches "obtain at least a portion of the payment information relevant to the secure transaction based on establishing the connection with the POS device." See Ritter at least at Abstract, Col. 2, Ln. 59-67; Col. 6, Ln. 29-33; and Col. 7, Ln. 25-32 and Claim 2. The mobile device receives data from the terminal, wherein the

data comprises transaction data in response to the mobile device and the terminal establishing a wireless connection.

Although Ritter teaches a user carrying out a transaction with a POS using their mobile device, authenticating the user using biometric information, and providing by the POS to the mobile device transaction information using a wireless / RF communication, Ritter does not explicitly disclose in response to obtaining at least a portion of the payment information, prompt the user to provide biometric information to the biometric reading device.

French teaches in response to obtaining at least a portion of the payment information, prompt the user to provide biometric information to the biometric reading device Paragraphs. French is directed to settling a transaction based on sending and receiving of data between devices and enforcing multiple authentication measures. The biometric authentication is performed after transaction data is received and thus French teaches the claimed limitation. See French at least at Paragraphs 0065, 0067, 0130-0135 and Figure 12. It would have been obvious to one or ordinary skill in the art at the time of the invention to combine the teachings of Ritter, which teaches requiring a user to perform a biometric authentication on their mobile device in order to be authenticated and subsequently allow the user to complete a transaction with a terminal utilizing RF communication, in order to include the teachings of French to explicitly disclose that the user is prompted for the authentication information in response to obtaining at least a portion of the payment information in motivation of enhancing user experience by providing the prompt for the authentication information in order to facilitate the process of conducting the transaction and optimize security measures.

Also, it would be obvious to one of ordinary skill in the art to combine the teachings of Ritter in view of French to teach requesting biometric data at any point during a transaction between two devices communicating wirelessly in motivation of providing security measures when conducting a transaction.

Claim Objections

9. Claims and 10 objected to because of the following informalities: The claims recite: "obtain at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device." The claims must recite "... establish the connection with the POS device." Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The Disclosure shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The Disclosure shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 1 and 10 and all of their dependent claims are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the disclosure in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint

inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1 and 10 recite "establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuitry of the mobile device," and "secure the payment information using a key."

The specification was examined carefully, wherein Paragraphs 0060 and 0071 of the disclosure, as originally filed, recite "a user with an RF cellular telephone approaches a POS with an RF reader/write, the RF reader/writer identifies the user and obtains any relevant information stored on the RF cellular telephone." These portions of the specification do not disclose the claim limitation "establish a connection with a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuitry of the mobile device."

In regards to claim limitation "secure the payment information using a key," in claims 1 and 10, the specification discloses at Paragraph 0069 that "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." The specification also recites "a "chip can have a cryptographic block with 4 exchange encrypted keys with up to 256 bits)." These citations along with all other citations do not provide support for "secure the payment information using a key." Claims 8 and 15 recite "wherein the payment information is secured with a cryptographic key." The claims are rejected under the same rational as above.

Claims 1 and 10 recite "obtain at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device." The specification

does not have any support for such a claim limitation. At best, Figure 14 recites at step 1405 that a "user with RF cell phone approaches RF reader. RF reader identifies user and obtains relevant transaction information." The claims are directed to the mobile device obtaining the payment information not the POS. Figure 14 clearly indicates that the POS is the entity obtaining the "relevant transaction information" and not the mobile device. The Figures is contrary to what the claim recites. All dependent claims are rejected on mere dependence on the rejected claims.

> The following is a quotation of 35 U.S.C. 112(b):
> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.
>
> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 10-17 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

12. Per claim 10, the claim are directed to a system comprising: a mobile device and a POS device. The claim however recites, "the central database configured to validate the key and the payment information based on the information indicative of authentication," wherein the central database is outside the scope of the claimed system. As a result of the central database being outside of the claimed system, the claim is determined to be indefinite and amounts to merely an intended use limitation not having patentable weight. For purposes of examination, any teaching of a transaction being carried out using a mobile device and a POS will be determined as reading on the claim limitation.

Dependent claims 11-16 are rejected for mere dependence on claim 10.

13. Per claim 17, the claim recites "wherein the one or more processors are configured to execute the instructions to retrieve information to complete the secure transaction based, in part, on the transmitted information." The claim is indefinite because it is not known what information is being retrieved since at least claim 1 recites multiple types of information (i.e. biometric authentication information, payment information, information indicative of the authentication, purchase information, and transmitted information). For purposes of examination, any teaching of any information will be determined as reading on the claim limitation.

Claim Rejections - 35 USC § 103

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

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1-3, 7-16 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,934,689 to Ritter et al. ("Ritter"), in view of U.S. Patent Application Publication 2002/0157029 to French et al. ("French"), in further view of U.S. Patent 6,163,771 to Walker et al. ("Walker").

15. Per claims 1 and 10, Ritter teaches all of the following limitations:

a. A mobile device, comprising [Abstract, Col. 4, Ln. 46-51 and Figure 1]:

b. short range radio frequency (RF) circuitry [Col. 4, Ln. 46-67; Col. 5, Ln. 1-9 and Figure 1];

c. a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information [Abstract, Col.5, Ln. 56-67; Col. 7, Ln. 51-67; Col. 8, Ln. 1-6; and Figure 1];

d. a biometric reading device configured to read biometric information [abstract, Col. 5, Ln. 62-67; Col. 6, Ln. 1-6; Col. 9, Ln. 1-15 and Figure 1]; and

e. one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory to [Abstract, Col. 4, Ln. 46-67; Col.5, Ln. 10-18; Col. 5, Ln. 58-67; and Figures 1]:

f. establish a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secured transaction between the mobile device and the POS device [Abstract, Col. 4, Ln. 46-67; Col. 6, Ln. 49-67 and Figure 1],

g. obtain at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device [Abstract, Col. 2, Ln. 59-67; Col. 6, Ln. 29-33; and Col. 7, Ln. 25-32 and Claim 2],

h. authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory [Abstract, Col.5, Ln. 56-67; Col. 6, Ln. 1-11; and Figure 1],

i. secure the payment information using a key [Col. 3, Ln. 1-8; Col. 7, Ln. 41-50; Col. 8, Ln. 64-67],

j. when the biometric information ready by the biometric reading device is successfully authenticated, transmit to the POS device, via the short range RF circuitry, information indicative of the authentication [Abstract, Col. 5, Ln. 56-67; Col. 6, Ln. 1-11; Col. 6, Ln. 39-58 and Figure 1], and

Examiner notes that the following limitation is a conditional limitation, which does not have to occur, resulting in the claim not having much patentable weight: "when the biometric information ready by the biometric reading device is successfully authenticated, transmit to the POS device, via the short range RF circuitry, information indicative of the authentication."

k. retrieve purchase information related to the secured transaction based, in part, on the transmitted information [Col. 3, Ln. 1-8; Col. 7, Ln. 1-3; Col. 7, Ln. 25-65 and Figure 1].

l. Although Ritter teaches a user carrying out a transaction with a POS using their mobile device, authenticating the user using biometric information, and providing by the POS to the mobile device transaction information using a wireless / RF communication as shown above [Abstract, Col. 4, Ln. 14-67], Ritter does not explicitly disclose in response to obtaining at least a portion of the payment information, prompt the user to provide biometric information to the biometric reading device.

French teaches in response to obtaining at least a portion of the payment information, prompt the user to provide biometric information to the biometric reading device [Paragraphs 0065, 0067, 0130-0135 and Figure 12].

It would have been obvious to one or ordinary skill in the art at the time of the invention to combine the teachings of Ritter, which teaches requiring a user to perform a biometric authentication on their mobile device in order to be authenticated and subsequently allow the user to complete a transaction with a terminal utilizing RF communication, in order to include the teachings of French to explicitly disclose that the user is prompted for the authentication information in response to obtaining at least a portion of the payment information in motivation of enhancing user experience by providing the prompt for the authentication information in order to facilitate the process of conducting the transaction and optimize security measures.

Also, it would be obvious to one of ordinary skill in the art to prompt the user to provide the biometric information at any point during the transaction in motivation of increasing security measures.

Per claim 10, Ritter teaches:

a. a point of sale (POS) device configured to [Abstract, Col. 4, Ln. 38-45 and Figure 1]:

b. receive, from the mobile device, the secured payment information and the information indicative of the authentication [Abstract, Col. 6, Ln. 1-11; Col. 6, Ln. 39-67; Col. 8, Ln. 7-17; Col. 8, Ln. 64-67 and Figure 1]; and

c. Although Ritter in view of French teach settlement of a transaction between a mobile device and a merchant or point of sale and performing authentication checks using multiple entities and databases, Ritter in view of French do not explicitly disclose

retrieve, from a central database, purchase information based on the received information indicative of authentication.

Walker teaches retrieve, from a central database, purchase information based on the received information indicative of authentication [Abstract, Col. 6, Ln. 38-53; Col. 8, Ln. 34-65; Figures 3-4, and 12]; and

It would have been obvious to one or ordinary skill in the art at the time of the invention to combine the teachings of Ritter in view of French, which teach a mobile device in communication with a POS conducting a transaction and having the POS transmit a settlement request to a clearing point or clearing house using encryption techniques once requirements have been met, to include the teachings of Walker to explicitly teach retrieving purchase information from a central authority based on authentication of in motivation deterring fraudulent transactions in order to increase security measures.

d. Ritter in view of French teach settling a transaction between entities, including sending from a POS to a clearing point or clearing house a request to settle the transaction. However, Ritter in view of French do not explicitly disclose the central database configured to validate the key and the payment information based on the information indicative of authentication.

Walker teaches a central database configured to validate the key and the payment information based on the information indicative of authentication [Abstract, Col. 6, Ln. 38-53; Col. 8, Ln. 34-65; Figures 3-4, and 12].

It would have been obvious to one or ordinary skill in the art at the time of the invention to combine the teachings of Ritter in view of French, which teach a mobile

device in communication with a POS conducting a transaction and having the POS transmit a settlement request to a clearing point or clearing house using encryption techniques in order to settle a transaction, to include the teachings of Walker to explicitly teach validating by the issuer the key and payment information in motivation of settling the transaction and returning a transaction response to the merchant / POS.

Examiner notes that the following limitation is an intended use limitation and does not have any patentable weights because it is outside the scope of the claim: "the central database configured to validate the key and the payment information based on the information indicative of authentication."

16. Per claims 2 and 11, Ritter teaches wherein the biometric reading device is configured to read biometric information provided by a user to complete the transaction [Col. 5, Ln. 56-67; Col. 6, Ln. 1-6].

17. Per claims 3 and 12, Ritter teaches wherein the payment information is associated with a primary account number [Abstract, Col. 7, Ln. 51-67 and Figure 1].

18. Per claims 7 and 14 Ritter teaches wherein the biometric authentication information is stored separately from the payment information [Col. 5, Ln. 56-62; Col. 7, Ln. 51-64 and elements 12-15 and 17 in Figure 1].

19. Per claims 8 and 15, Ritter teaches wherein the payment information is secured with a cryptographic key [Col. 3, Ln. 1-8; Col. 7, Ln. 41-50; Col. 8, Ln. 64-67].

20. Per claims 9 and 16, Ritter teaches wherein the short range RF circuitry comprises a radio frequency identification (RFID) device [Col. 4, Ln. 46-67; Col. 5, Ln. 1-9; and Figure 1].

21. Per claim 13, Ritter teaches wherein the POS device includes an RF reader [Col. 4, Ln. 46-67; Col. 5, Ln. 1-9; Col. 5, Ln. 25-30 and Figure 1].

22. Per claim 17, Ritter teaches wherein the one or more processors are configured to execute the instructions to retrieve information to complete the secure transaction based, in part, on the transmitted information [Col. 3, Ln. 1-8; Col. 5, Ln. 56-67; Col. 6, Ln. 1-11; Col. 6, Ln. 39-58 ; Col. 7, Ln. 1-3; Col. 7, Ln. 25-65 and Figure 1].

Double Patenting

23. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claim 1 of the instant Application is rejected on the ground of nonstatutory double patenting as being unpatentable over Claim 3 of prior U.S. Patent No. 8766772. Although the claims at issue are not identical, they are not patentably distinct from each other. Claim 3 in U.S. Patent 8766772 teaches the claim limitations of the instant Application's Claim 1, but does not teach "secure the payment information using a key." Ritter, U.S. Patent 6934689, teaches such missing limitations; see abstract, Col. 3, Ln. 1-8; Col. 7, Ln. 41-50; Col. 8, Ln. 64-67 and Figure 1. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of U.S. Patent 8766772 and the teachings of Ritter to teach securing the payment information utilizing a key before providing the information to another entity to advance a transaction in motivation of increasing security measures.

24. Claims 2-17 are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14/659502 in view of U.S. Patent 6,163,771 to Walker.

This is a provisional obviousness-type nonstatutory double patenting rejection.

Although the conflicting claims are not identical, they are not patentably distinct from each other. Claims 1 and 10 of co-pending application 14/659502 recites:

a. mobile device, comprising:

b. short range radio frequency (RF) circuitry;

c. memory configured to store biometric authentication information and payment information;

d. a biometric module configured to read biometric information;

e. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

f. a secure module configured to:

g. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

h. encrypt the key and the payment information stored in memory; and

i. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction

Claim 10:

j. A system, comprising:

k. a mobile device, comprising:

l. short range radio frequency (RF) circuitry;

m. memory configured to store biometric authentication information and payment information;

n. a biometric module configured to read biometric information;

o. an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

p. a secure module configured to:

q. generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

r. encrypt the key and the payment information stored in memory; and

s. provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and

t. a point of sale (POS) device configured to:

u. receive, from the secure module, the encrypted key and payment information; and

v. transmit, to a central database, the encrypted key and payment information; and

w. a central database configured to validate the key and the payment information.

Claims 1 and 10 of co-pending application 14/659502 differ from the instant claims since they fail to recite that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory. Ritter discloses an authenticating that the biometric information is associated with the user associated with the payment information based on the biometric authentication information stored in memory. See Ritter at Abstract, Col.5, Ln. 56-67; Col. 6, Ln. 1-11; Col. 7, Ln. 51-67; and Figure 1. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of co-pending Application 14/659,502 to include the teachings of Ritter, which teaches a mobile device

authenticating a user based on biometric input and settling a transaction using payment information associated with the user of the mobile device in motivation of only allowing the proper user to whom the device belongs to settle a transaction based on associating the biometric input with the stored input and the user with the payment information; resulting in increased security measures.

It is well settled that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA 1963). Also note Ex parte Rainu, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

Co-pending Applications 14/321781, 14/724593, 14/585057 are also rejected based on the same above rationale.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed on for PTO-892.

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.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on M-F 9AM - 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Neha W. Patel can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov.

Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/

El Mehdi Oussir
Patent Examiner, Art Unit 3685
07/26/2019

/NEHA PATEL/
Supervisory Patent Examiner, Art Unit 3685

Notice of References Cited	Application/Control No. 14/639,034	Applicant(s)/Patent Under Reexamination Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20020123325-A1	09-2002	Cooper, Gerald M.	H04L63/0492	455/411
*	B	US-20020112171-A1	08-2002	Ginter, Karl L.	G06F21/10	713/185
*	C	US-20020157029-A1	10-2002	French, Jennifer	G06F21/31	726/21
*	D	US-6934689-B1	08-2005	Ritter; Rudolf	G06Q20/04	705/16
*	E	US-20060204048-A1	09-2006	Morrison; Robert A.	G06F21/31	382/115
*	F	US-20070198436-A1	08-2007	Weiss; Kenneth P.	G06F21/32	705/75
*	G	US-9858566-B2	01-2018	Mardikar; Upendra S.	G06Q20/1085	1/1
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

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

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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

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

CLAIMS

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

CLAIM		DATE								
Final	Original	05/18/2015	12/09/2015	05/26/2017	03/16/2018	02/26/2019				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	✓	✓	✓				
	3	✓	✓	✓	✓	✓				
	4	✓	✓	✓	✓	-				
	5	✓	-	-	-	-				
	6	✓	-	-	-	-				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9	✓	✓	✓	✓	✓				
	10	✓	✓	✓	✓	✓				
	11	✓	✓	✓	✓	✓				
	12	✓	✓	✓	✓	✓				
	13	✓	✓	✓	✓	✓				
	14	✓	✓	✓	✓	✓				
	15	✓	✓	✓	✓	✓				
	16	✓	✓	✓	✓	✓				
	17					✓				

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06Q	5/8/2015	EO
H04L	5/8/2015	EO
G06Q20	02/15/2019	EO

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
705		5/8/2015	EO

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

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

Search Notes		
Search Notes	**Date**	**Examiner**
consulted Calvin Hewitt	5/15/2015	EO
Consulted John H. and Mamon O on 101/ 103	5/25/2017	EO
Consulted John H. on priority	5/9/2017	EO
Consulted Mohammad N. on priority and 112	5/26/2017	EO
Consulted Steven K. 112	03/14/2018	EO
Review of references	03/16/2018	EO
Consulted John H. 101	03/14/2018	EO
East search update	02/13/2019	EO
Consulted Steven Kim 101	02/13/2019	EO
IP.COM search	02/13/2019	EO
EAST search update	02/15/2019	EO
IP.COM search	02/18/2019	EO
Consulted Steven Kim 101 / 103	02/19/2019	EO
Consulted Mohammad N. 112	02/21/2019	EO
Consulted Steven Kim 112	07/26/2019	EO
EAST SEARCH	07/26/2019	EO

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S133	6	S132 and ((request$3 receiv$3 obtain$3 prompt$3) near5 (user) near5 (biometric iris fingerprint))	US-PGPUB; USPAT	OR	ON	2019/07/26 18:02
S132	13	S128 AND (establish$3 (communication link)) and ((receiv$3 transmit$4 send$3) near5 (data information))	US-PGPUB; USPAT	OR	ON	2019/07/26 17:58
S130	3	S128 and ((promp$3) with (biometric passcode password PIN))	US-PGPUB; USPAT	OR	ON	2019/07/26 17:54
S129	9	S128 and ((promp$3 receiv$3) with (biometric passcode password PIN))	US-PGPUB; USPAT	OR	ON	2019/07/26 17:54
S128	16	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$ or US-20020193142-$ or US-20020194499-$ or US-20020123325-$ or US-20020112171-$ or US-20020157029-$ or US-20060204048-$ or US-20070198436-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$ or US-6934689-$ or US-9858566-$).did.	US-PGPUB; USPAT	OR	ON	2019/07/26 17:53

EAST Search History (Interference)

< This search history is empty>

7/ 26/ 2019 8:25:45 PM
C:\ Users\ eoussir\ Documents\ EAST\ Workspaces\ 14639034_Mobile device RFID transaction biometric POS.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

USPTO Automated Interview Request (AIR)

Oct 11 2019

This paper requesting to schedule and/or conduct an interview is appropriate because:

This submission is requested to be accepted as an authorization for this interview to communicate via the internet. Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with the undersigned concerning scheduling of the interview via video conference, instant messaging, or electronic mail, and to conduct the interview in accordance with office practice including video conferencing.

Name(s):
Mark W. Catanese

S-signature:
/Mark W Catanese/

Registration Number:
64279

U.S. Application Number:
14639034

Confirmation Number:
5934

E-mail Address:
mark.catanese@procopio.com

Phone Number:
+1 6195153213

Proposed Time of Interview:
10-22-2019 1:00 PM ET

Alternative Proposed Time(s) of Interview:
10-22-2019 2:00 PM ET

Alternative Proposed Time(s) of Interview:
10-23-2019 1:00 PM ET

Prefered Interview Type:
Telephonic

I am the applicant or applicant's representative for this application.

Topic for Discussion:
Applicant would like to discuss the nature of the rejection of the claims and the references cited in the office action in view of proposed amendments to claim 1 (to be provided prior to the interview)

UNITED STATES
PATENT AND TRADEMARK OFFICE

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 14/639,034	Filing Date 03/04/2015	☐ 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

AMENDMENT	10/31/2019	(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))	* 13	Minus	** 20	= 0		x $100 =	0
	Independent (37 CFR 1.16(h))	* 2	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

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 $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".	/VIKKI GRAY/
*** 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.

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

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

Application Number	14639034	Filing Date	2015-03-04	Docket Number (if applicable)	116546-613CT13	Art Unit	3685
First Named Inventor	Francisco Martinez de Velasco Cortina			Examiner Name	El Mehdi OUSSIR		

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, 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

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2019-10-31
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.
14/639,034	03/04/2015	de VELASCO CORTINA, Francisco Martinez	116546-613CT13	5934

EXAMINER	
OUSSIR, El Mehdi	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
October 31, 2019	EFS WEB

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

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

RESPONSE TO OFFICE ACTION

Sir:

This paper is submitted in response to the Final Office Action mailed on August 1, 2019. Allowance of the above identified application is respectfully requested in view of the following submission, where:

Amendments to the Claims begin on page 2 of this paper.

Interview Summary begins on page 6 of this paper.

Remarks begin on page 7 of this paper.

AMENDMENTS TO THE CLAIMS

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

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

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

~~obtain at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device,~~

~~in response to obtaining at least a portion of the payment information,~~ prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory,

generate a key when the biometric information read by the biometric reading device is successfully authenticated,

secure the payment information ~~using a key~~stored in the memory, and

~~when the biometric information read by the biometric reading device is successfully authenticated,~~ transmit to the POS device, via the short range RF circuitry, ~~information indicative of the authentication, and~~

~~retrieve purchase information related to transaction based, in part, on the transmitted information~~the generated key and secured payment information for use in the secure transaction.

2. (Previously Presented) The mobile device of claim 1, wherein the biometric reading device is configured to read the biometric information provided by a user to complete the transaction.

3. (Original) The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. (Canceled)

5. (Canceled)

6. (Canceled)

7. (Original) The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. (Currently Amended) The mobile device of claim 1, wherein the ~~payment information~~memory is secured with a cryptographic key.

9. (Original) The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. (Previously Presented) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information;

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, ~~when the POS device is within an operating range of the short range RF circuity of the mobile device,~~ wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based at least in part on the biometric authentication information stored in memory

generate a key when the biometric information read by the biometric reading device is successfully authenticated,

secure the payment information ~~using a key~~stored in the memory, and

~~when the biometric information read by the biometric reading device is successfully authenticated,~~ transmit to the POS device, via the short range RF circuitry, ~~information indicative of the authentication, and~~

~~retrieve purchase information related to the secured transaction based, in part, on the transmitted information; and~~the key and the payment information for us in the secure transaction;

the POS device ~~configured~~ comprising at least one memory and at least one processors operably coupled to the memory, the POS device configured to execute instructions stored in the at least one memory to:

receive, from the mobile device, the secured payment information and the ~~information indicative of the authentication~~ key; and

retrieve, from [[a]]the central database, purchase information based on the received key and payment information indicative of authentication; and

the central database comprising at least one memory and at least one processors operably coupled to the memory, the central database configured to execute instruction stored in the memory to validate the key and the payment information based on the information indicative of authentication.

11. (Previously Presented) The system of claim 10, wherein the biometric reading device is configured to read the biometric information provided by a user to complete the transaction.

12. (Original) The system of claim 10, wherein the payment information is associated with a primary account number.

13. (Original) The system of claim 10, wherein the POS device includes an RF reader.

14. (Original) The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. (Currently Amended) The system of claim 10, wherein the ~~payment information~~ memory is secured with a cryptographic key.

16. (Original) The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

17. (~~Previously Presented~~Cancelled) ~~The system of claim 1, wherein the one or more processors are configured to execute the instructions to retrieve information to complete the secure transaction based, in part, on the transmitted information.~~

INTERVIEW SUMMARY

Applicant thanks Examiner Oussir for the courtesy extended during the telephonic interview conducted in the present application on October 28, 2019 with Mark Catanese ("Interview"). During the Interview, Applicant and Examiner discussed the rejection of the claims in view of certain proposed amendments, some of which are reflected in the "Amendments to the Claims" section above. Other features were discussed that the Examiner, but no agreement was reached with respect to patentability. The substance of those discussions is reflected in the remarks below.

Applicant also thanks Examiner Oussir for the courtesy extended during the follow-up telephonic interview conducted in the present application on October 31, 2019 with Mark Catanese ("Second Interview"). During the Second Interview, Applicant and Examiner discussed the rejection of claim 10 under 35 U.S.C. § 112(b) in view of certain amendments proposed by the Examiner, which are reflected in the "Amendments to the Claims" section above. No agreement was reached with respect to patentability. The substance of those discussions is reflected in the remarks below.

REMARKS

The present amendment is in response to the Final Office Action dated August 1, 2019. 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, 8, 10, and 15 are amended and claim 17 is cancelled without prejudice or disclaimer. Support for the amendments can be found throughout the application as originally filed. For example, support can be found at least in paragraphs [0033], [0053], [0065]-[0073], [0088], [0108]-[0109], and [0120] of the application as originally filed. No new matter has been added. Claims 1-3 and 7-16 are pending in the application, claims 4-6 having been previously cancelled without prejudice or disclaimer. Claims 1 and 10 are the independent claims.

In response to the Office Action, Applicant respectfully traverses each and every one of the rejections as set forth in the Office Action. However, in the interest of advancing prosecution, certain amendments have been made as set forth in the "AMENDMENTS TO THE CLAIMS, section, and Applicant requests reconsideration of the above-captioned application in view of the following comments and amendments as set forth herein.

B. Claim Objections

The Office Action states that "Claims [*sic*] and 10 [*sic*] object to because of the following informalities: The claims recite: 'obtain at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device.'" *Office Action, p. 6.*

Applicant respectfully notes that claim 10 as previously presented did not recite "at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device, but that claim 1 did recite this feature. Thus, Applicant assumes the Office Acton intended to object to claim 1. In any event, without acquiescing to the merits of the objections and in the interest of advancing prosecution, Applicant has amended claims 1 and 10 as set forth in the "AMENDMENTS TO THE CLAIMS" section. Accordingly, Applicant respectfully submits that amended claims 1 and 10 overcome the objections and requests the objections be withdrawn.

C. Claim Rejections - 35 U.S.C. § 112(a)

Claims 1 and 10 and all of their dependent claims stand rejected as failing to comply with the written description requirement. Particularly, the Office Action asserted that features (A) "establish a connection with a point of sale (POS) device. . . "; (B) "secure the payment information using a key"; and (C) "obtain at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device" are unsupported by the application as originally filed.

Applicant respectfully traverses each of the rejections and does not agree with the characterizations as set forth in the Office Action. However, in an interest to advance prosecution and without acquiescing to the rejections, Applicant has amended the claims as set forth in the "AMENDMENTS TO THE CLAIMS" section. Applicant respectfully submits that the application as originally filed provides sufficient detail that one skilled in the art can reasonably conclude that the application describes provides written description support for the amended claims.

Regarding feature (A), as agreed to during the Interview, Applicant submits that the application as filed describes "sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention." *MPEP 2163(I)* (citing *Moba, B.V. v. Diamond Automation, Inc.*, 325 F.3d 1306, 1319 (Fed. Cir. 2003); *Vas-Cath, Inc. v. Mahurkar*, 935 F.2d 1555, 1563 (Fed. Cir. 1991)) (emphasis added). For example, paragraphs [0059]-[0061] and [0070]-[0071] of the application as filed describes that an RF reader/writer of a POS device is continuously scanning and that the RF communication device creates a communication (or connection) with the POS via the RF circuitry. *See also paras. [0065]-[0068] of the application as filed* (describing that POS 1210 includes an RF reader/writer that an RF cellular telephone 1205 includes an RF device having a chip and an RF antenna).

Accordingly, as agreed to during the Interview, Applicant respectfully submits that that the application as originally filed provides sufficient support in compliance with 112(a) for the feature of "establish a connection with a point of sale (POS) device . . . ," as recited in claim 1.

Turning to feature (B), Applicant does not agree with the rejection and submits that the claimed feature is supported in the application as originally filed; however, in the interest of advancing prosecution and without acquiescing to the merits of the rejection, Applicant has amended claim 1 as discussed during the interview to recite "secure the payment information stored in the memory."

As agreed to during the Interview, Applicant respectfully submits that that the application as originally filed provides sufficient support in compliance with 112(a) for the feature of "establish a connection with a point of sale (POS) device . . . ," as recited in claim 1. For example, support for the claimed feature can be found in paragraphs [0033], [0053], [0069], and [0065]-[0075] of the application as originally filed.

Furthermore, in the Decision on Appeal issued in co-pending Application 14/659,502 (which Applicant notes shares a common specification with the present application), the Patent Trial and Appeal Board ("Board") cited to paragraphs [0065]-[0075] as providing support for features as claimed in the co-pending Application 14/659,502, that is "encrypt the key and the payment information stored in memory." *See Ex parte Francisco Martinez de Velasco,* Appeal 2017-011851, Decision on Appeal in App. No. 14/659,502, p. 2 (PTAB, May 10, 2019) (hereinafter "Decision"). Notably, the Board explained the application as filed describes:

> Disclosed embodiments include cryptographic "credit and debit exchange keys" that provide for security of payment information and for protecting use of "personal information (e.g., biometrics) contained in [a] device." Spec. ¶ 53. A key is generated when an individual's biometric stored in the device, such as a fingerprint, is matched with the output of a biometric reader, e.g., at a point of sale. Spec. ¶¶ 65-73. Encryption using the key enables protecting both the individual's biometric information and stored payment information, such as a credit card number, for a point of sale transaction. *Id.*

Id. at p. 2.

Accordingly, Applicant respectfully submits that that the application as originally filed provides sufficient support in compliance with 112(a) for the feature of "[securing] the payment information stored in the memory."

Turning to feature (C), Applicant does not agree with the rejection and submits that the claimed feature is supported in the application as originally filed; however, in the interest of advancing prosecution and without acquiescing to the merits of the rejection, Applicant has amended claim 1 as reflected in the "AMENDMENTS TO THE CLAIMS" section, thereby rendering this rejection as moot.

For at least the foregoing reasons, Applicant submits that amended claim 1 is well supported by the application as originally filed. Accordingly, Applicant requests the rejection be withdrawn. Amended claim 10 recites features similar to amended claim 1. Thus for at least the same reasons, applicant submits that claim 10 is supported by the application as originally filed, and the rejection be withdrawn.

The dependent claims depend directly or indirectly from claims 1 and 10. 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 the rejections under § 112(a) be withdrawn.

At page 7, the Office Action states "Claims 8 and 15 recites 'wherein the payment information is secured with a cryptographic key.' The claims are rejected under the same rational as above."

Applicant does not agree with the rejection; however, in the interest of advancing prosecution and without acquiescing to the merits of the object, Applicant has amended claims 8 and 15 as reflected in the "Amendments to the Claims" section to recite "wherein the memory is secured with a cryptographic key." Applicant respectfully submits that, for at least the same reasons as set forth above with respect to feature (B) recited in claims 1 and 10, the application as filed provides sufficient support for amended claims 8 and 15. Therefore, Applicant requests the rejection be withdrawn.

D. Claim Rejections - 35 U.S.C. § 112(b)

Claims 10-17 stand rejected under 35 U.S.C. § 112(b) as allegedly being indefinite. Applicant respectfully traverses each of the rejections and does not necessarily agree with the characterizations as set forth in the Office Action.

With respect to claim 10, the Office Action stated "[p]er claim 10, the claim are directed to a system comprising: a mobile device and a POS device. The claim however recites, 'the central database configured to validate the key and the payment information based on the information indicative of authentication,' wherein the central database is outside the scope of the claimed system." *Office Action, p. 8.*

Applicant does not necessarily agree with the rejection. However, in the interest of advancing prosecution and without acquiescing to the merits of the object, Applicant has amended claim 10 to incorporate the amendments proposed by the Examiner during the Second Interview as reflected in the "Amendments to the Claims" section. Accordingly, Applicant respectfully submits that claim 10 is not indefinite and is in compliance with 112(b). Applicant request the rejection be withdrawn.

Dependent claims 11-16 depend from claim 10. 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 the rejections under § 112(b) be withdrawn.

Regarding claim 17, Applicant does not agree with the rejection and submits that the claim 17 is not indefinite; however, in the interest of advancing prosecution and without acquiescing to the merits of the rejection, Applicant has cancelled claim 17 without prejudice or disclaimer, thereby rendering this rejection as moot. Accordingly, Applicant request the rejection be withdrawn.

E. Claim Rejections – 35 U.S.C. § 103

Claims 1-3 and 7-16 stand rejected as being unpatentable over US. Patent 6,934,689 ("Ritter") in view of U.S. Patent App. Pub. No. 2002/0157029 ("French"), in further view of US Patent 6,163,771 (Walker). 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 and 10 as presented herein.

Without acquiescing to the merits of the grounds of the rejections, and in the interest of advancing prosecution, Applicant has amended claim 1 to recite, in part, "generate a key when the biometric information read by the biometric reading device is successfully authenticated."

Support for the amendments can be found, for example, in at least paragraph [0033], [0053], [0065]-[0073], [0088], [0108]-[0109], and [0120] of the application as originally filed. For example, as described above, in the Decision, the Board cited to paragraphs [0065]-[0075] as providing support for features as claimed in the co-pending Application 14/659,502. Notably, the Board explained the application as filed describes:

> Disclosed embodiments include cryptographic "credit and debit exchange keys" that provide for security of payment information and for protecting use of "personal information (e.g., biometrics) contained in [a] device." Spec. ¶ 53. A key is generated when an individual's biometric stored in the device, such as a fingerprint, is matched with the output of a biometric reader, e.g., at a point of sale. Spec. ¶¶ 65-73. Encryption using the key enables protecting both the individual's biometric information and stored payment information, such as a credit card number, for a point of sale transaction. *Id.*

Decision, p. 2.

Applicant respectfully submits that the cited references do not teach or suggest at least the above-identified features as recited in amended claim 1.

For example, Ritter describes "[i]f the customer would like to pay the total amount of the payment transaction by means of his mobile device 1, he switches on his mobile device 1, and, to be on the safe side, in an embodiment variant, is requested by an authentication module 12

of the mobile device 1." *Ritter, Col. 5, ll. 51-56*. After successful authentication the user selects the function "payment transaction," which in turn prompts the user "to enter transaction identification information for the respective payment transaction." *Id. at Col. 6, ll. 7-38.* The transaction identification information is then transmitted to the payment terminal 2. *Id. at Col. 6, ll. 39-64*. Ritter also describes that "data transactions via contact interface 11, 21 can be encrypted." *Id at Col. 8, ll. 65-67.* Thus, Ritter at best describes that transaction identification information is transmitted (which may be encrypted) ***after*** the user provides input in response to the prompt to enter the transaction identification information, which in turn is only provided ***after*** the user has selected the payment function ***following*** unlocking the mobile device 1 by successful biometric authentication. Accordingly, Applicant submits that Ritter does not teach or suggest at least "generate a key when the biometric information read by the biometric reading device is successfully authenticated," as recited in claim 1.

Additionally, Applicant respectfully submits that the other references do not cure the deficiencies of Ritter at least with respect to amended claim 1. The other references were cited merely to supposedly show certain features which are unrelated to the above-indicated features of amended claim 1, and these references do not appear to remedy the deficiencies of Ritter. Therefore, the combination of the prior art references does not teach or suggest all of the features of independent claim 1. Accordingly, not all of the claim elements were known or taught by the prior art.

Therefore, 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. Accordingly, claim 1 is patentable over the cited references, in combination or individually, and Applicant respectfully requests this rejection be withdrawn.

Independent claim 10 has been amended to recite features similar to claim 1. Thus for at least the same reasons, Applicant respectfully submits the suggested combination of references fail to disclose or suggest all of the features of claim 10. Accordingly, Applicant requests the rejections be withdrawn.

The dependent claims depend directly or indirectly from one of claims 1 and 10. 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 the rejections under § 103 be withdrawn.

F. Nonstatutory Double Patenting

Claim 1 stands rejected on the ground of nonstatutory double patenting as being unpatentable over claim 3 of prior U.S. Patent No. 8,766,772. Claims 2-17 (interpreted as claims 2, 3, and 7-16) are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 1-16 of copending Application No. 14/659,502 in view of Walker.

Applicant respectfully requests reconsideration of these rejections in view of the foregoing claim amendments. Furthermore, not notwithstanding the following remarks and arguments as to the allowability of the pending claims over the cited referecnes, the claims may further change throughout prosecution. Therefore, Applicant respectfully requests the double patenting rejection be held in abeyance until the claims are otherwise in condition for allowance.

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

Dated: October 31, 2019

By: /Mark W. Catanese/
Mark W. Catanese
Registration No. 64,279
Customer No. 27189

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B Street
Suite 2200
San Diego, CA 92101
Tel 619-238-1900
Fax 619-235-0398
docketing@procopio.com

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT13

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($)
Miscellaneous:				
RCE- 2ND AND SUBSEQUENT REQUEST	1820	1	1900	1900
		Total in USD ($)		**1900**

Electronic Acknowledgement Receipt

EFS ID:	37624182
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	31-OCT-2019
Filing Date:	04-MAR-2015
Time Stamp:	23:57:59
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1900
RAM confirmation Number	E20190UN58352185
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)	116546-613CT13_RCE_TBF_w_Amendment_10_31_2019.PDF	1349955 8a1009055379ff04276572bedbed960c714e3ccb	no	3
Warnings:					
Information:					
2		116546-613CT13_Response_OA_filed_10_31_2019.PDF	125728 1b4806d93fe726cc95739b697655f6fffc361462	yes	13

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Claims	2	5
Applicant summary of interview with examiner	6	6
Applicant Arguments/Remarks Made in an Amendment	7	13

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30718 e26d919d28544c8a3f84520dfd6607745b2f2e36	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1506401		

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 11/01/2019

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
11/01/2019	ELECTRONIC

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

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

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

PTONotifications@procopio.com
docketing@procopio.com

Applicant-Initiated Interview Summary	**Application No.** 14/639,034	**Applicant(s)** Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA (FITF) Status** No

All participants (applicant, applicants representative, PTO personnel):

(1) EL MEHDI OUSSIR. (3) _____.

(2) Mark W. Catanese (Applicant's Representative). (4) _____.

Date of Interview: 28 October 2019.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☑112 ☐102 ☑103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: Ritter, French, Walker.

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's representative and the Examiner discussed potential claim amendments to try and overcome the 112 and 103 rejections. Although No agreement was reached regarding the 103 rejection, the Examiner noted that the 112 rejection regarding the establishing of the connection is overcome. Examiner proposed amending the claims to recite how the "portion of payment information" is exchanged between the device and at what point in the transaction is such information being exchanged. The Examiner also requested support/reference to the specification for all amendments to try and expedite prosecution.
.

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

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

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 examiners 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 applicants 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 applicants 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 examiners 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 examiners initials.

App Nos.: 14/639,034 Attorney Docket No. 116546-613CT13
Title: SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
Filed: March 4, 2015
Inventor(s): de VELASCO CORTINA, Francisco Martinez
Examiner: OUSSIR, El Mehdi
Art Unit: 3685
Conf. No.: 5934

Do Not Enter E.O.

AGENDA FOR TELEPHONIC INTERVIEW

(NOT INTENDED FOR ENTRY INTO THE RECORD)

Attendees, Date and Type of Interview

A telephonic interview is scheduled for October 28, 2019, at 5:00PM ET (2:00PM PT). The interview will be attended by Examiner Oussir and Applicant's Representative Mark W. Catanese (Reg. No. 64,279).

Applicant's Representative will call the Examiner at (571) 270-0191.

Identification of Claims to be Discussed

Claims 1 and 10.

Identification of Art to be Discussed

U.S. Patent No. 6,934,689 ("Ritter");

U.S. App. Pub. No. 2002/0157029 ("French"); and

U.S. Patent No. 6,163,771 ("Walker").

Items to be Discussed

1. Applicant would like to discuss the rejection of the claims under 35 U.S.C. §§ 112 (a) and 112(b) and the proposed amendment to claim 1 below. Applicant to explain that one skilled in the art would reasonably conclude that the specification describes the claimed features.
2. Applicant would like to discuss the rejection of the claims under 35 U.S.C. §103 and the proposed amendment to claim 1 below in view of the above cited references. Specifically, Applicant to explain why it believes the cited references do not teach or suggest the claimed features.

Proposed Amendments to Claim 1

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

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory to:

establish a connection with a RF reader/writer of a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

~~obtain~~exchange at least a portion of the payment information relevant to the secure transaction based on establishing the connection with POS device,

in response to ~~obtaining~~ exchanging at least a portion of the payment information, prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory,

when the biometric information read by the biometric reading device is successfully authenticated, generate information indicative of the authentication;

secure the payment information ~~using a key~~stored in the memory,

~~when the biometric information read by the biometric reading device is successfully authenticated,~~ transmit to the POS device, via the short range RF

circuitry, information indicative of the authentication and the payment information, and

retrieve purchase information related to the transaction based, in part, on the transmitted information.

10. (Currently Amended) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information;

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory to:

establish a connection with a RF reader/writer of a point of sale (POS) device, via the short range RF circuitry, when the POS device is within an operating range of the short range RF circuity of the mobile device, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based at least in part on the biometric authentication information stored in memory.

when the biometric information read by the biometric reading device is successfully authenticated, generate information indicative of the authentication;

secure the payment information ~~using a key~~stored in the memory, ~~when the biometric information read by the biometric reading device is successfully authenticated,~~ transmit to the POS device, via the short range RF circuitry, information indicative of the authentication and the payment information, and

retrieve purchase information related to the secured transaction based, in part, on the transmitted information; and

the POS device configured to:

receive, from the mobile device, the secured payment information and the information indicative of the authentication; and

retrieve, from a central database, purchase information based on the received information indicative of authentication and the payment information; and

the central database configured to validate the ~~key~~information indicative of authentication and the payment information ~~based on the information indicative of authentication~~.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 11/05/2019

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

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
11/05/2019	ELECTRONIC

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

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

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

PTONotifications@procopio.com
docketing@procopio.com

Applicant-Initiated Interview Summary	**Application No.** 14/639,034	**Applicant(s)** Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA (FITF) Status** No

All participants (applicant, applicants representative, PTO personnel):

(1) EL MEHDI OUSSIR. (3) _____.

(2) Mark W. Catanese (Applicant's Representative).. (4) _____.

Date of Interview: 31 October 2019.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☑112 ☐102 ☐103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 10.

Identification of prior art discussed: NA.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

See Continuation Sheet.

Applicant recordation instructions: 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

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

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 examiners 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 applicants 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 applicants 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 examiners 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 examiners initials.

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: Applicant's representative requested further review of a claim rejections under 112 for claim 10. Specifically, claim 10 was rejected for being indefinite because the claim recites limitations carried out by a central database. The central database is outside the scope of claim 10 because claim 10 is directed to a system comprising a mobile device and a POS. Agreement was reached that if the claims were amended to recite "a POS comprising a memory storing instructions and a processor executing the instruction to cause the processor to perform..." and "a central database comprising memory and instructions and a processor to execute the instructions to cause the processor to perform..." then the rejection would be withdrawn. Furthermore, claim 1 was addressed and the Examiner proposed amending the claim to positively recite the "when..." claim limitation since it is a conditional limitation that does not have to be carried out. Applicant agrees. Also the last limitation of claim 1 was received and agreement was reached that it could be removed since the retrieval of purchase information is done by the POS after the device transmits information to the POS indicative of the authentication. No agreement was reached; however Applicant noted that they would try and resolve the concern.

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-613CT13

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5627544	A	1997-05-06	SNODGRASS CHARLES K et al.	
	2	5819234	A	1998-10-06	SLAVIN et al.	
	3	5940006	A	1999-08-17	MACLELLAN et al.	
	4	6089284	A	2000-07-18	KAEHLER DAVID L et al.	
	5	6570488	B2	2003-05-27	Kucharczyk et al.	
	6	6934689	B1	2005-08-23	Ritter et al.	
	7	7081819	B2	2006-07-25	Martinez de Velasco Cortina et al.	
	8	7096363	B2	2006-08-22	Kon et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	9	7987501	B2	2011-07-26	Miller et al.	
	10	8237568	B2	2012-08-07	Martinez de Velasco Cortina et al.	
	11	8325044	B2	2012-12-04	Martinez de Velasco Cortina et al.	
	12	8587436	B2	2013-11-19	Martinez de Velasco Cortina et al.	
	13	9558385	B2	2017-01-31	Martinez de Velasco Cortina et al.	
	14	9858566	B2	2018-01-02	Mardikar et al.	
	15	6796490	B1	2004-09-28	Drummond	

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	20020073416	A1	2002-06-13	Ramsey Catan	
	2	20020112171	A1	2002-08-15	Ginter et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	3	20020123325	A1	2002-09-05	Cooper	
	4	20020157029	A1	2002-10-24	French et al.	
	5	20020193142	A1	2002-12-19	Stavenow et al.	
	6	20020194499	A1	2002-12-19	Audebert et al.	
	7	20030018522	A1	2003-01-23	Denimarck et al.	
	8	20030019929	A1	2003-01-30	Stewart et al.	
	9	20030055738	A1	2003-03-20	Alie	
	10	20030112120	A1	2003-06-19	Siefert	
	11	20030137403	A1	2003-07-24	Carrender et al.	
	12	20030149662	A1	2003-08-07	Shore	
	13	20060204048	A1	2006-09-14	Morrison	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	14	20070198436	A1	2007-08-23	Weiss	

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

FOREIGN PATENT DOCUMENTS Remove

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

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

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Ewa Syta, S. K. (2010). RFID-based Authentication Middleware for Mobile Devices. IEEE, 1-10. Retrieved from http://www.cs.ccsu.edu/-stan/research/pervasive/pubs/hicss201 Orfidam .pdf (10 pages)	
	2	US Notice of Allowance dated July 24, 2019 received in US patent application no. 16/051,751 (16 pages)	
	3	US Notice of Allowance dated June 4, 2019 received in US patent application no. 16/051,751 (22 pages)	
	4	Response to Office Action filed on April 30, 2019 in US Patent Application no. 16/051,751. (11 pages)	
	5	US Applicant Interview Summary dated April 22, 2019 received in US patent application no. 16/051,751	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	6	US Office Action dated February 4, 2019 received in US Patent Application no. 16/051,751. (21 pages)	
	7	Preliminary Amendment filed on August 28, 2018 in US Patent Application no. 16/051,751. (9 pages)	
	8	US Office Action dated October 24, 2019 received in US patent application no. 14/724,593. (29 pages)	
	9	Notice of Appeal dated April 10, 2019 filed in US patent application no. 14/724,593. (4 pages)	
	10	US Office Action dated January 11, 2019 received in US patent application no. 14/724,593. (48 pages)	
	11	Response to Office Action filed on September 11, 2018 for US patent application no. 14/724,593 (24 pages)	
	12	US Office Action dated July 12, 2018 received in US patent application no. 14/724,593. (45 pages)	
	13	Response to Office Action filed on January 10, 2018 for US patent application no. 14/724,593 (17 pages).	
	14	US Applicant Interview Summary dated December 6, 2017 received in US patent application no. 14/724,593. (3 pages)	
	15	US Office Action dated July 28, 2017 received in US patent application no. 14/724,593. (36 pages)	
	16	US Notice of Allowance dated May 28, 2019 received in US patent application no. 14/659,502 (31 pages)	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	17	Patent Board Decision mailed May 10, 2019 received in US patent application no. 14/659,502 (11 pages).	
	18	Reply Brief filed September 26, 2017 for US patent application no. 14/659,502 (13 pages).	
	19	Examiner's Answer to Appeal Brief dated July 26, 2017 received in US patent application no. 14/659,502.(28 pages).	
	20	US Applicant Interview Summary dated December 20, 2019 received in US patent application no. 14/585,057 (3 pages).	
	21	US Office Action dated September 19, 2019 received in US patent application no. 14/585,057 (21 pages)	
	22	Response to Office Action filed on April 30, 2019 for US Patent application no. 14/585,057 (20 pages)	
	23	Patent Board Decision dated March 4, 2019 for US patent application no. 14/585,057. (11 pages)	
	24	Reply Brief filed dated August 21, 2017 in the US Patent application no. 14/585,057 (11 pages)	
	25	Examiner's Answer to Appeal Brief dated June 21, 2017 received in US patent application no. 14/585,057 (24 pages)	
	26	Advisory Action dated December 16, 2019 received in US Patent Application 14/321,781 (7 pages)	
	27	Response to Office Action mailed December 3, 2019 for US Patent application 14/321,781 (30 pages)	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	28	US Office Action dated October 4, 2019 received in US patent application no. 14/321,781. (21 pages)	
	29	Response to Office Action filed on June 7, 2019 for US patent application no. 14/321,781. (31 pages)	
	30	US Office Action dated March 7, 2019 received in US patent application no. 14/321,781. (19 pages)	
	31	Response to Office Action filed on August 14, 2018 for US patent application no. 14/321,781. (28 pages)	
	32	US Office Action dated March 22, 2018 received in US patent application no. 14/321,781. (37 pages)	
	33	Response to Office Action filed on December 5, 2017 for US patent application no. 14/321,781. (16 pages)	
	34	US Office Action dated June 5, 2017 received in US patent application no. 14/321,781. (51 pages)	

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

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

CERTIFICATION STATEMENT

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

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

OR

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

See attached certification statement.

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

☒ A certification statement is not submitted herewith.

SIGNATURE

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

Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2020-01-06
Name/Print	Mark W. Catanese	Registration Number	64279

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

Privacy Act Statement

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

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

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

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

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

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

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

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

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

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

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

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	de VELASCO CORTINA, Francisco Martinez	116546-613CT13	5934

EXAMINER	
OUSSIR, El Mehdi	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
January 6, 2020	EFS WEB

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

INFORMATION DISCLOSURE STATEMENT

In accordance with 37 CFR Sections 1.97 and 1.98, the items identified in this Information Disclosure Statement ("IDS") are brought to the attention of the Office. The items are listed on the attached form.

Copies of these references are not being provided pursuant to 37 CFR §1.98(d), as these references were cited in application Serial No 14/321,781, from which priority is being claimed. It is requested that the information provided herein be made of record in this application.

This statement is being filed with filing, and therefore no fees are due, however, the Commissioner is hereby authorized to charge any fees required by the filing of these papers, and to credit any overpayment to Procopio's Deposit Account No. 50-2075.

Respectfully submitted,
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

Dated: January 6, 2020

By: /Mark W. Catanese/
Mark W. Catanese
Registration No. 64,279
Customer No. 27189

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B Street
Suite 2200
San Diego, CA 92101
Tel 619-238-1900
Fax 619-235-0398
docketing@procopio.com

Electronic Acknowledgement Receipt

EFS ID:	38218357
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	06-JAN-2020
Filing Date:	04-MAR-2015
Time Stamp:	20:45:01
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	Information Disclosure Statement (IDS) Form (SB08)	116546-613CT13_SUPP_IDS_SB08_.PDF	1036247 024fce4b829b066b5fa9bd40dcf33685d3135939	no	9
Warnings:					

Information:					
2	Transmittal Letter	116546-613CT13_Statement_of_non-NPL_as_filed_01_06_2020.PDF	54688 a9ac85e8a2a678b47f66547af992743dcd92a734	no	1
Warnings:					
Information:					
			Total Files Size (in bytes):	1090935	

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

New Applications Under 35 U.S.C. 111

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

National Stage of an International Application under 35 U.S.C. 371

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

New International Application Filed with the USPTO as a Receiving Office

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

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 01/08/2020

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
01/08/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTONotifications@procopio.com
docketing@procopio.com

Office Action Summary	Application No. 14/639,034	Applicant(s) Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

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 10/31/2019.

☐ 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) 1-3 and 7-16 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-3 and 7-16 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 03/04/2015 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☑ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

This communication is a Non-Final Office Action in response to a request for continued examination on 10/31/2019 as a result of the Final Action mailed on08/01/2019.

Claims 1-3, and 7-16 have been examined in this application.

No new information disclosure statement (IDS) has been filed.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on May 19, 2015 has been entered.

Response to Arguments

Applicant's arguments regarding claim rejections under nonstatutory double patenting / obviousness-type nonstatutory double patenting have been considered, however the rejection is maintained.

Claim Objections

Claim 1 recites "prompt the user to provide biometric information to the biometric reading device." The claims must recite "in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device."

See claim 10, which recites the above required amendment to claim 1.

Per claim 10, the claim recites "transmit to the POS device, via the short range RF circuitry," in a first limitation then recites "the key and the payment information for us in the secure transaction;" as a separate limitation. The claim must be amended to combine these limitations. Also, the claim must be amended to recite "for use" instead of "for us."

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The Disclosure shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

The following is a quotation of the first paragraph of pre-AIA 35 U.S.C. 112:

> The Disclosure shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 8 and 15 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the disclosure in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for pre-AIA the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 8 and 15 recite "wherein the memory is secured with a cryptographic key." It is not known how a memory can be secured with a cryptographic key. Data in the memory is secured using encryption techniques, wherein a memory is a hardware or physical device that stored data. The specification discloses using encryption techniques to encrypt data, however, it does not recite that the actual memory is secured or encrypted with a cryptographic key. Also, it

is not known how such memory is secured with a cryptographic key when claims 1 and 10 already recite "secure the payment information stored in the memory."

> The following is a quotation of 35 U.S.C. 112(b):
> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.
>
> The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:
> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-3, and 7-16 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Claims 1 and 10 recite "a memory coupled to the short range RF circuitry" and "memory configured to store biometric authentication information…" However, both claims also recite "authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in memory."

As a result, it is not known whether the recited first memory is the same or different than the memory recited as storing "the biometric authentication information." Therefore, the claims and all dependent claims are determined to be indefinite.

Claim 10 also recites "the POS device comprising at least one memory and at least one processors operably coupled to the memory, the POS device configured to execute instructions stored in the at least one memory" and "the central database comprising at least one memory and at least one processors operably coupled to the memory, the central database configured to

execute instruction stored in the memory." The claim limitations as indicated above recite a first "at least one memory" and a second "the memory," resulting in the claim being indefinite because it is not known whether "the memory" is referring back to the "at least one memory" or to another memory.

All dependent claims are rejected for at least mere dependence on the rejected claims.

Per Claims 8 and 15 recite "wherein the memory is secured with a cryptographic key." It is not known to which memory the recited "the memory" is referring to.

Also, it is not known whether the payment information stored in the memory is secured with a cryptographic key, claims 1 and 10 recite secure the payment information stored in the memory, or whether the memory itself is secured with a cryptographic key. Thus, the claims are indefinite.

Per claims 2 and 11, the claims recite "wherein the biometric reading device is configured to read the biometric information provided by a user to complete the transaction." Claims 1 and 10, already recite "a user" being prompted to provide biometric information, therefore, it is not known whether the "a user" in claims 2 and 11 is another user different than the user prompted to provide biometric data in claims 1 and 10.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible

harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the claims at issue are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO internet Web site contains terminal disclaimer forms which may be used. Please visit http://www.uspto.gov/forms/. The filing date of the application will determine what form should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1 and 10 of the instant Application are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over Claim 4 and 11 of

co-pending Application No. 14/659502 in view of U.S. Patent Application Publication 2002/0157029 to French et al. ("French").

Although the claims at issue are not identical, they are not patentably distinct from each other. Claim 4 and 11 of the co-pending Application 14/659502 teaches the claim limitations of the instant Application's Claim 1 and 10, but does not teach "establish a connection with a point of sale…" and "prompt the user to provide biometric information to the biometric reading device."

French teaches establishing a connection and prompting a user for biometric information; see French at least at Paragraphs 0065-0067, 0130-0135 and Figure 12. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the claims of co-pending Application 14/659502 to include the teachings of French to teach establishing a connection and prompting a user for biometric information in motivation of increasing security measures.

Claims 1 and 10 are provisionally rejected on the ground of obviousness-type non-statutory double patenting as being unpatentable over claims 5 and 11 of co-pending Application No. 14/321781 in view of French.

Although the conflicting claims are not identical, they are not patentably distinct from each other. Claims 5 and 11 of co-pending application 14/321781 recite:

Claim 1: A mobile device, comprising: short range radio frequency (RF) circuitry; memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information; a biometric module configured to read biometric information; an authentication module configured

to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and a secure module configured to: generate a key when the biometric information read by the biometric reading device is successfully authenticated; encrypt the key and the payment information stored in memory; and provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

Claim 5: wherein the secure module is configured to provide the encrypted key and payment information to a point of sale (POS) device, and wherein the POS device is configured to receive the encrypted key and payment information from the secure module, and transmit the encrypted key and payment information to a central database.

Claim 11: A system, comprising: a mobile device, comprising: short range radio frequency (RF) circuitry; memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with the payment information; a biometric module configured to read biometric information; an authentication module configured to authenticate that the biometric information read by the biometric module is associated with the payment information based at least in part on the biometric authentication information stored in memory; and a secure module configured to: generate a key when the biometric information read by the biometric reading device is successfully authenticated encrypt the key and the payment information stored in memory; and provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction; and a point of sale (POS) device configured to: receive, from the secure module, the encrypted key and payment information; and transmit, to a central database, the encrypted key

and payment information; and a central database configured to validate the key and the payment information.

Claims 5 and 11 of co-pending application 14/321781 differ from the instant claims since they fail to recite "establish a connection with a point of sale…" and "prompt the user to provide biometric information to the biometric reading device."

French teaches establishing a connection and prompting a user for biometric information; see French at least at Paragraphs 0065-0067, 0130-0135 and Figure 12. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the claims of co-pending Application 14/659502 to include the teachings of French to teach establishing a connection and prompting a user for biometric information in motivation of increasing security measures.

It is well settled that the omission of an element and its function is an obvious expedient if the remaining elements perform the same function as before. In re Karlson, 136 USPQ 184 (CCPA 1963). Also note Ex parte Rainu, 168 USPQ 375 (Bd. App. 1969). Omission of a reference element whose function is not needed would be obvious to one of ordinary skill in the art.

Co-pending Applications 14/724593, 14/585057 and Patent 8766772 are also rejected for at least the above rationale.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed on for PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on M-F 9AM - 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Neha W. Patel can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/

El Mehdi Oussir
Patent Examiner, Art Unit 3685
01/03/2020

Examiner-Initiated Interview Summary	**Application No.** 14/639,034	**Applicant(s)** Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA (FITF) Status** No

All participants (applicant, applicant's representative, PTO personnel):

(1) EL MEHDI OUSSIR. (3) _____.

(2) Mark Catanese (Applicant's Representatative). (4) _____.

Date of Interview: 02 January 2020.

Type: ☑ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☑ No.
If Yes, brief description: _____.

Issues Discussed ☐ 101 ☐ 112 ☐ 102 ☐ 103 ☐ Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: NA.

Identification of prior art discussed: NA.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

See Continuation Sheet.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: The Examiner initiated an interview with the Applicant's representative to try and explain the outstanding rejections and potential amendments to try and overcome the rejections. As a result of the holiday season, the Examiner has agreed to issue the Office Action in order to provide the Applicant with a thorough explanation of the rejection and allow for a timely response to the rejections.

The Examiner is available to hold future interviews to the discuss the current Office Action.

Notice of References Cited	Application/Control No. 14/639,034	Applicant(s)/Patent Under Reexamination Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20020073416-A1	06-2002	Ramsey Catan, Carolyn	G06Q20/04	725/6
*	B	US-20020112177-A1	08-2002	Voltmer, William H.	G06F21/32	726/26
*	C	US-6796490-B1	09-2004	Drummond; Jay Paul	G06Q20/32	235/379
*	D	US-6044382-A	03-2000	Martino; Rocco L.	G06F9/466	348/E7.081
*	E	US-6049710-A	04-2000	Nilsson; B. G.	H04M3/42204	379/88.03
*	F	US-6259405-B1	07-2001	Stewart; Brett B.	H04M15/8033	342/457
*	G	US-20010044900-A1	11-2001	Uchida, Kaoru	G06F21/32	713/186
*	H	US-20020010684-A1	01-2002	Moskowitz, Scott A.	G06F21/10	705/75
*	I	US-20020040327-A1	04-2002	Owa, Tsunayuki	G06Q10/10	705/26.1
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06Q	5/8/2015	EO
H04L	5/8/2015	EO
G06Q20	02/15/2019	EO

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
705		5/8/2015	EO

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

Search Notes		
Search Notes	**Date**	**Examiner**
consulted Calvin Hewitt	5/15/2015	EO
Consulted John H. and Mamon O on 101/ 103	5/25/2017	EO
Consulted John H. on priority	5/9/2017	EO
Consulted Mohammad N. on priority and 112	5/26/2017	EO
Consulted Steven K. 112	03/14/2018	EO
Review of references	03/16/2018	EO
Consulted John H. 101	03/14/2018	EO
East search update	02/13/2019	EO
Consulted Steven Kim 101	02/13/2019	EO
IP.COM search	02/13/2019	EO
EAST search update	02/15/2019	EO
IP.COM search	02/18/2019	EO
Consulted Steven Kim 101 / 103	02/19/2019	EO
Consulted Mohammad N. 112	02/21/2019	EO
Consulted Steven Kim 112	07/26/2019	EO
EAST SEARCH	07/26/2019	EO
Consulted Mohammad N. 112	01/03/2020	EO
East search update	01/03/2020	EO
IP.com / google search / NPL search	01/03/2020	EO
Review co-pending applications / patents	01/03/2020	EO

Interference Search			
US Class/CPC Symbol	**US Subclass/CPC Group**	**Date**	**Examiner**

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/18/2015	12/09/2015	05/26/2017	03/16/2018	02/26/2019	01/03/2020			
	1	✓	✓	✓	✓	✓	✓			
	2	✓	✓	✓	✓	✓	✓			
	3	✓	✓	✓	✓	✓	✓			
	4	✓	✓	✓	✓	-	-			
	5	✓	-	-	-	-	-			
	6	✓	-	-	-	-	-			
	7	✓	✓	✓	✓	✓	✓			
	8	✓	✓	✓	✓	✓	✓			
	9	✓	✓	✓	✓	✓	✓			
	10	✓	✓	✓	✓	✓	✓			
	11	✓	✓	✓	✓	✓	✓			
	12	✓	✓	✓	✓	✓	✓			
	13	✓	✓	✓	✓	✓	✓			
	14	✓	✓	✓	✓	✓	✓			
	15	✓	✓	✓	✓	✓	✓			
	16	✓	✓	✓	✓	✓	✓			
	17					✓	-			

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L9	9	8 and @pd<"20020709"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:18
L8	1476	7 and (transaction purchas$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:18
L7	2030	6 and (generat$3 with (key code OTP pin password account))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:17
L6	3586	5 and ((establish$3 with (RF (radio near2 frequency) NFC Bluetooth (wireless))) near6 (connection))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:17
L5	97107	((prompt$3 pop-up pop$up) with (password authenticat$3 PIN biometric code OTP))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:16
L4	83423	((prompt$3 pop-up pop$up) with (password authenticat$3 PIN biometric code OTP))	US-PGPUB; USPAT	OR	ON	2020/01/04 13:15
L3	5	2 and ((prompt$3 pop-up pop$up) with (password authenticat$3 PIN biometric code OTP))	US-PGPUB; USPAT	OR	ON	2020/01/04 13:15
L2	19	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$ or US-20020193142-$ or US-20020194499-$ or US-20020123325-$ or US-20020112171-$ or US-20020157029-$ or US-20060204048-$ or US-20070198436-$ or US-20020073416-$ or US-20020112177-$).did. or (US-6848048-$ or US-	US-PGPUB; USPAT	OR	ON	2020/01/04 13:14

		6163771-$ or US-7911643-$ or US-5590197-$ or US-6934689-$ or US-9858566-$ or US-6796490-$).did.				
L1	8	"8766772"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 12:38
S146	2	S145 and (biometric near6 (associat$4 tied tying) near6 (financial account payment))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/26 17:45
S145	19	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$ or US-20020193142-$ or US-20020194499-$ or US-20020123325-$ or US-20020112171-$ or US-20020157029-$ or US-20060204048-$ or US-20070198436-$ or US-20020073416-$ or US-20020112177-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$ or US-6934689-$ or US-9858566-$ or US-6796490-$).did.	US-PGPUB; USPAT	OR	ON	2019/09/26 17:43
S144	1	("8766772").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/09/23 12:54
S143	1	("6796490").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/09/17 17:42
S142	1	("20020112177").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/09/12 13:06
S141	4	S140 AND @PD< "20020709"	US-PGPUB; USPAT	OR	ON	2019/09/12 12:05
S140	974	S139 and (((mobile cellular electronic pda portable) near2 (device phone)) with ((biometric fingerprint) near2 (reader scan scanner device input)))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:56
S139	133856	((user purchaser) near4 (select selection choos$3 selecting pick$3) near6 (product item media))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:53
S138	110882	((user purchaser) near2 (select selection choos$3 selecting pick$3) near6 (product item media))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:52
S137	2	S134 and ((user purchaser) near2 (select selection choos$3 selecting pick$3) near6 (product item media))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:42
S136	7	S134 and ((user purchaser) near2 (select selection choos$3 selecting pick$3))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:41
S135	9	S134 and ((user purchaser) near6 (select selection choos$3 selecting pick$3))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:41

S134	16	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$ or US-20020193142-$ or US-20020194499-$ or US-20020123325-$ or US-20020112171-$ or US-20020157029-$ or US-20060204048-$ or US-20070198436-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$ or US-6934689-$ or US-9858566-$).did.	US-PGPUB; USPAT	OR	ON	2019/09/12 11:39

EAST Search History (Interference)

< This search history is empty>

1/4/2020 1:21:56 PM
C:\Users\eoussir\Documents\EAST\Workspaces\14639034_Mobile device RFID transaction biometric POS V2.wsp

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed	PTO/SB/25 PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION AND TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	14639034
Filing Date	04-Mar-2015
First Named Inventor	Francisco Martinez de Velasco Cortina
Attorney Docket Number	116546-613CT13
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Neology, Inc.	100 %

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

14659502 filed on 03/16/2015

14321781 filed on 07/01/2014

14724593 filed on 05/28/2015

14585057 filed on 12/29/2014

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

8766772

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicants claims the following fee status:

○ Small Entity

○ Micro Entity

◉ Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 64279

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/Mark W. Catanese/

Name	Mark W. Catanese

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT13

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 14639034

Filing Date: 04-Mar-2015

Applicant/Patent under Reexamination: Martinez de Velasco Cortina

Electronic Terminal Disclaimer filed on January 13, 2020

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	38281163
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	13-JAN-2020
Filing Date:	04-MAR-2015
Time Stamp:	19:51:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	E20201CJ51305992
Deposit Account	502075
Authorized User	Helen Glenister

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	40499 ec4cc4569e405b27bac5e24f6a211ca83c103c33	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30509 16a48265b3ce68edb762681d8fff4b14ad6b785e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	71008		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	de VELASCO CORTINA, Francisco Martinez	116546-613CT13	5934

EXAMINER	
OUSSIR, El Mehdi	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
January 13, 2020	EFS WEB

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Mail Stop AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO OFFICE ACTION

Sir:

This paper is submitted in response to the Non-Final Office Action mailed on January 8, 2020. Allowance of the above identified application is respectfully requested in view of the following submission, where:

Amendments to the Claims begin on page 2 of this paper.

Interview Summary begins on page 5 of this paper.

Remarks begin on page 6 of this paper.

A **Terminal Disclaimer** is submitted herewith.

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	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, El Mehdi
Attorney Docket Number	116546-613CT13

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	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, El Mehdi
	Attorney Docket Number	116546-613CT13

	1	US Office Action dated January 8, 2020 received in US patent application no. 14/321,781(21 pages)	
	2	Appeal Brief filed June 10, 2019 filed in US patent application no. 14/724,593. (46 pages)	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, El Mehdi
	Attorney Docket Number	116546-613CT13

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2020-01-13
Name/Print	Mark W. Catanese	Registration Number	64279

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT13

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	1806	1	240	240
		Total in USD ($)		**240**

Electronic Acknowledgement Receipt

EFS ID:	38282160
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	13-JAN-2020
Filing Date:	04-MAR-2015
Time Stamp:	19:56:20
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$240
RAM confirmation Number	E20201CJ57216046
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		116546-613CT13_Resp_to_NFOA_dated_Jan_8_as_filed_01_13_2020.PDF	102957 e4fc32aa6e40566100317095a485232fcbaadcf1	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Applicant Arguments/Remarks Made in an Amendment	6	8
	Applicant summary of interview with examiner	5	5
	Claims	2	4
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1

Warnings:

Information:

2	Information Disclosure Statement (IDS) Form (SB08)	116546-613CT13_SIDS_filed_with_Response_01_13_2020.PDF	612148 99bab371f2217b62fc7d1b0ef435c5e38bad7f5a	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.

3	Non Patent Literature	116546-613CT_IDS_NPL_NFOA_dated_Jan_8__2020_from_14321781.PDF	866347 a1aea59e5bc8e9692fc57ca95ae9d8e9c369d69d	no	21

Warnings:

Information:

4	Non Patent Literature	116546-613CT15_Appeal_Brief_as_filed_06_10_2019.PDF	2068900 ef3462173c6d00a41dba4bd53221a3db46e1ef32	no	46

Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30651 6137a61a8f496108f450b833bb21851ecd2185ff	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	3681003		

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.

REMARKS

The present amendment is in response to the Non-Final Office Action dated January 8, 2020. 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 and 10 are amended and claims 2, 8, 11 and 15 are cancelled without prejudice or disclaimer. Support for the amendments can be found throughout the application as originally filed. No new matter has been added. Claims 1, 3, 7, 9, 10, 12-14, and 16 are pending, claims 4-6 and 17 having been previously cancelled without prejudice or disclaimer. Claims 1 and 10 are the independent claims.

In response to the Office Action, Applicant respectfully traverses each and every one of the rejections as set forth in the Office Action. However, in the interest of advancing prosecution, certain amendments have been made as set forth in the "AMENDMENTS TO THE CLAIMS, section, and Applicant requests reconsideration of the above-captioned application in view of the following comments and amendments as set forth herein.

B. Claim Objections

The Office Action objected to claims 1 and 10.

Applicant has amended the claims as set forth in the "AMENDMENTS TO THE CLAIMS" section. Accordingly, as agreed to during the Interview, Applicant respectfully submits that amended the claims overcome the objections and requests the objections be withdrawn.

C. Claim Rejections - 35 U.S.C. § 112(a)

Claims 8 and 15 stand rejected as failing to comply with the written description requirement.

Applicant respectfully traverses each of the rejections and does not agree with the characterizations as set forth in the Office Action. However, in an interest to advance prosecution and without acquiescing to the rejections, Applicant has amended the claims as set forth in the "AMENDMENTS TO THE CLAIMS" section. More particularly, claims 8 and 15 have been cancelled without prejudice and disclaimer, thereby rendering the rejection moot. Therefore, Applicant requests the rejection be withdrawn.

D. Claim Rejections - 35 U.S.C. § 112(b)

Claims 1-3 and 7-16 stand rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention.

Applicant respectfully traverses each of the rejections and does not agree with the characterizations as set forth in the Office Action. However, in an interest to advance prosecution and without acquiescing to the rejections, Applicant has amended the claims as set forth in the "AMENDMENTS TO THE CLAIMS" section. More particularly, claims 1 and 10 have been amended, as discussed during the Interview, in a manner that which the Examiner agreed overcomes the current rejections. Additionally, claims 2, 8, 11, and 15 have been cancelled without prejudice and disclaimer, thereby rendering the objection moot. Accordingly, as agreed to during the Interview, Applicant respectfully submits that amended the claims overcome the rejections and requests the rejections be withdrawn.

E. Nonstatutory Double Patenting

Claims 1 and 10 stand provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over Claim 4 and 11 of co-pending Application No. 14/659,502 in view of U.S. Patent Application Publication 2002/0157029 ("French"). Claims 1 and 10 are provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over claims 5 and 11 of co-pending Application No. 14/321,781 in view of French. The Office Action also states that "Co-pending Applications 14/724593, 14/585057 and Patent 8766772 are also rejected for at least the above rationale," (*Office Action, p. 9*), which is by the Applicant to mean that the claims also stand provisionally rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over copending Applications 14/724,593 and 14/585,057, and stand rejected on the ground of obviousness-type nonstatutory double patenting as being unpatentable over Patent 8,766,772.

Applicant acknowledges the double patenting rejection with respect to US Application Nos. 14/659,502; 14/321,781; 14/724,593; and 14/585,057 and US Patent No. 8,766,772. Without acquiescing to the merits of the grounds of the rejection and in the interest of advancing prosecution, Applicant has filed a Terminal Disclaimer herewith. Applicant respectfully requests withdrawal of the rejections and that the claims are in condition for allowance.

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

Dated: January 13, 2020

By: /Mark W. Catanese/
Mark W. Catanese
Registration No. 64,279
Customer No. 27189

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B Street
Suite 2200
San Diego, CA 92101
Tel 619-238-1900
Fax 619-235-0398
docketing@procopio.com

INTERVIEW SUMMARY

Applicant thanks Examiner Oussir for the courtesy extended during the telephonic interview conducted in the present application on January 10, 2020 with Mark Catanese ("Interview"). During the Interview, Applicant and Examiner discussed the rejection of the claims in view of certain proposed amendments, which are reflected in the "Amendments to the Claims" section above, that the Examiner agreed overcome the current rejections. Applicant agreed to file a Terminal Disclaimer to overcome the double patenting rejections. Examiner indicated that the amendments and Terminal Disclaimer should place the application in condition for allowance subject to further consideration. The substance of those discussions is reflected in the remarks below.

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A mobile device, comprising:

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in the memory,

generate a key when the biometric information read by the biometric reading device is successfully authenticated,

secure the payment information stored in the memory, and

transmit to the POS device, via the short range RF circuitry, the generated key and secured payment information for use in the secure transaction.

2. (Cancelled)

3. (Original) The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Original) The mobile device of claim 1, wherein the biometric authentication information is stored separately from the payment information.

8. (Cancelled)

9. (Original) The mobile device of claim 1, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

10. (Previously Presented) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

a memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information;

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

~~in response to establishing the connection,~~ prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based at least in part on the biometric authentication information stored in the memory

generate a key when the biometric information read by the biometric reading device is successfully authenticated,

secure the payment information stored in the memory, and

transmit to the POS device, via the short range RF circuitry, the key and the payment information for [[us]]use in the secure transaction;

the POS device comprising at least one memory and at least one ~~processors~~ processor operably coupled to the at least one memory of the POS device, the at least one processor of the POS device configured to execute instructions stored in the at least one memory of the POS device to:

receive, from the mobile device, the secured payment information and the key; and

retrieve, from the central database, purchase information based on the received key and payment information indicative of authentication; and

the central database comprising at least one memory and at least one ~~processors~~ processor operably coupled to the memory of the central database, the at least one processor of the central database configured to execute ~~instruction~~ instructions stored in the memory of the central database to:

receive, from the POS, the secured payment information and the generated key; and

validate the key and the payment information based on the information indicative of authentication.

11. (Cancelled)

12. (Original) The system of claim 10, wherein the payment information is associated with a primary account number.

13. (Original) The system of claim 10, wherein the POS device includes an RF reader.

14. (Original) The system of claim 10, wherein the biometric authentication information is stored separately from the payment information.

15. (Cancelled)

16. (Original) The system of claim 10, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

17. (Cancelled)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 01/16/2020

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
01/16/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTONotifications@procopio.com
docketing@procopio.com

Applicant-Initiated Interview Summary	**Application No.** 14/639,034	**Applicant(s)** Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA (FITF) Status** No

All participants (applicant, applicants representative, PTO personnel):

(1) EL MEHDI OUSSIR. (3) _____.

(2) Mark W. Catanese (Applicant's Representative). (4) _____.

Date of Interview: 10 January 2020.

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 and 10.

Identification of prior art discussed: NA.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner and the Applicant's representative discussed claim amendments to overcome the objections and 112 rejections in the last Office Action. Agreement was reached to overcome the objections and rejections by amending the claims appropriately and canceling all other claims..

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

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

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 examiners 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 applicants 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 applicants 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 examiners 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 examiners initials.

DO NOT ENTER E.O.

App Nos.: 14/639,034 Attorney Docket No. 116546-613CT13
Title: SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
Filed: March 4, 2015
Inventor(s): de VELASCO CORTINA, Francisco Martinez
Examiner: OUSSIR, El Mehdi
Art Unit: 3685
Conf. No.: 5934

AGENDA FOR TELEPHONIC INTERVIEW

(NOT INTENDED FOR ENTRY INTO THE RECORD)

Attendees, Date and Type of Interview

A telephonic interview is scheduled for January 10, 2020, at 4:00PM ET (1:00PM PT). The interview will be attended by Examiner Oussir and Applicant's Representative Mark W. Catanese (Reg. No. 64,279).

Applicant's Representative will call the Examiner at (571) 270-0191.

Identification of Claims to be Discussed

Independent Claims 1 and 10 and dependent claims 2, 8, 11, and 15.

Identification of Art to be Discussed

None

Items to be Discussed

1. Applicant would like to discuss the objections of the claims and the proposed amendment to claims 1 and 10 below and representative claims below.
2. Applicant would also like to discuss the rejection of the claims under 35 U.S.C. §§ 112 (a) and 112(b) and the proposed amendments to claims 1 and 10 below and representative claims below.

Proposed Amendments

1. (Currently Amended) A mobile device, comprising:

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in the memory,

generate a key when the biometric information read by the biometric reading device is successfully authenticated,

secure the payment information stored in the memory, and

transmit to the POS device, via the short range RF circuitry, the generated key and secured payment information for use in the secure transaction.

2. (Previously Presented) The mobile device of claim 1, wherein the biometric reading device is configured to read the biometric information provided by a user to complete the transaction.

8. (Previously Presented) The mobile device of claim 1, wherein the memory is secured with a cryptographic key.

10. (Currently Amended) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

a memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information;

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory to:

establish a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

in response to establishing the connection, prompt the user to provide biometric information to the biometric reading device,

authenticate that the biometric information read by the biometric reading device is associated with the user associated with the payment information based at least in part on the biometric authentication information stored in the memory

generate a key when the biometric information read by the biometric reading device is successfully authenticated,

secure the payment information stored in the memory, and

transmit to the POS device, via the short range RF circuitry, the key and the payment information for [[us]]use in the secure transaction;

the POS device comprising at least one memory and at least one processors operably coupled to the at least one memory of the POS device, the POS device configured to execute instructions stored in the at least one memory of the POS device to:

receive, from the mobile device, the secured payment information and the key; and

retrieve, from the central database, purchase information based on the received key and payment information indicative of authentication; and

the central database comprising at least one memory and at least one processors operably coupled to the memory of the central database, the central database configured to execute

~~instruction~~ instructions stored in the memory of the central database to validate the key and the payment information based on the information indicative of authentication.

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	14639034
Filing Date	04-Mar-2015
First Named Inventor	Francisco Martinez de Velasco Cortina
Attorney Docket Number	116546-613CT13
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Neology, Inc.	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

8766772

8933807

9558385

10235513

10445719

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

○ Small Entity

○ Micro Entity

◉ Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 64279

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/Mark W. Catanese/
Name	Mark W. Catanese

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT13

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 14639034

Filing Date: 04-Mar-2015

Applicant/Patent under Reexamination: Martinez de Velasco Cortina

Electronic Terminal Disclaimer filed on March 25, 2020

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	38967546
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	25-MAR-2020
Filing Date:	04-MAR-2015
Time Stamp:	18:18:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	E20203OI18341239
Deposit Account	502075
Authorized User	Helen Glenister
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: 37 CFR 1.16 (National application filing, search, and examination fees) 37 CFR 1.17 (Patent application and reexamination processing fees)	

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	35324 157e5e549412e7336f4e63614dc2ec3c9d2e08c5	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30509 63eb47dcecd6ef07967003708024ec0471c7a7ff	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	65833		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

27189 7590 04/06/2020

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 04/06/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

TITLE OF INVENTION: SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	07/06/2020

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 04/06/2020

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

TITLE OF INVENTION: SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1000	$0.00	$0.00	$1000	07/06/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
OUSSIR, EL MEHDI	3685	705-071000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 04/06/2020

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER	
OUSSIR, EL MEHDI	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 04/06/2020

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/639,034	Applicant(s) Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to Interviews with Applicant's Representative begining on 03/24/2020.
   ☐ 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 1,3,7,10 and 12-14 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information , please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☑ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☑ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☑ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/EL MEHDI OUSSIR/
Examiner, Art Unit 3685

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application is being examined under the pre-AIA first to invent provisions.

This communication is in response to Applicant's response on January 13, 2020 in response to Examiner's Non-Final Office Action filed on January, 08, 2020. This communication is further in response to the multiple telephone and e-mail communications with Applicant's representative, Mark W. Catanese, on March 24, 2020, and March 25, 2020.

As a result of the communications with Applicant's representative, the following claims have been amended and are hereby entered by Examiner amendments.

Claims 1, 3, 7, 10 and 12-14 are entered. All other claims are cancelled.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in interviews and e-mail confirmations from the Applicant's representative on March 24, 2020, and March 25, 2020.

The application has been amended as follows:

a. Please replace all previous claims with attached amended claims, wherein:

b. Claims 1, 3, 7, 10 and 12-14 are pending.

c. Claims 2, 4-6, 8-9, 11, and 15-17 are cancelled.

Final Claims

1. (Currently Amended) A mobile device, comprising:

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory that, when executed by the one or more processors, causes the one or more processors to perform operations of[[to]]:

~~establish~~ establishing a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

~~prompt~~ prompting the user to provide biometric information to the biometric reading device,

~~authenticate~~ authenticating that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in the memory,

~~generate~~ in response to the authentication, generating a key ~~when the biometric information read by the biometric reading device is successfully authenticated~~,

~~secure~~ securing the payment information stored in the memory, and

~~transmit~~ transmitting to the POS device, via the short range RF circuitry, the ~~generated~~ key and the secured payment information for use in the secure transaction.

2. (Cancelled)

3. (Original) The mobile device of claim 1, wherein the payment information is associated with a primary account number.

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Currently Amended) The mobile device of claim 1, wherein the biometric authentication information is stored separately from the secured payment information.

8. (Cancelled)

9. (Cancelled)

10. (Currently Amended) A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

a memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information;

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory that, when executed by the one or more processors, causes the one or more processors to perform operations of[[to]]:

~~establish~~ establishing a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

~~prompt~~ prompting the user to provide biometric information to the biometric reading device,

~~authenticate~~ authenticating that the biometric information read by the biometric reading device is associated with the user associated with the payment information based at least in part on the biometric authentication information stored in the memory,

~~generate~~ in response to authenticating, generating a key ~~when the biometric information read by the biometric reading device is successfully authenticated~~,

~~secure~~ securing the payment information stored in the memory, and

~~transmit~~ transmitting to the POS device, via the short range RF circuitry, the key and the secured payment information for use in the secure transaction;

the POS device comprising at least one memory and at least one processor operably coupled to the at least one memory of the POS device, the at least one memory of the POS device storing instructions that, when executed by the at least one processor of the POS device

causes the at least one processor of the POS device to perform operations of ~~configured to execute instructions stored in the at least one memory of the POS device to~~:

~~receive~~ receiving, from the mobile device, the secured payment information and the key; and

~~retrieve, from the central database, purchase~~ transmitting the ~~generated~~ key and the secure payment information based ~~on the received key and payment information indicative of authentication~~ to a central database; and

the central database comprising at least one memory and at least one processor operably coupled to the memory of the central database, the at least one memory of the central database storing instructions that, when executed by the at least one processor of the central database causes the at least one processor of the central database to perform operations of ~~configured to execute instructions stored in the memory of the central database to~~:

~~receive~~ receiving, from the POS, the secured payment information and the ~~generated~~ key; and

~~validate~~ validating the key and the secured payment information ~~based on the information indicative of authentication~~ to complete the secured transaction.

11. (Cancelled)

12. (Original) The system of claim 10, wherein the payment information is associated with a primary account number.

13. (Original) The system of claim 10, wherein the POS device includes an RF reader.

14. (Currently Amended) The system of claim 10, wherein the biometric authentication information is stored separately from the secured payment information.

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

Reasons for Allowance

Claims 1, 3, 7, 10 and 12-14 are allowed.

The following is an Examiner's statement of reasons for allowance:

Applicant's arguments, filed 01/13/2020, see page 6, regarding claim objections have been fully considered and in light of the above entered Examiner amendments are thus persuasive; therefore the objections are withdrawn.

Applicant's arguments, see page 6-7, regarding claim rejections under 35 U.S.C. §112 have been fully considered and in light of the above entered Examiner amendments are thus persuasive; therefore the rejections are withdrawn.

Applicant's arguments, see page 7, regarding the double patenting rejection have been fully considered. Applicant has submitted a terminal disclaimer on 01/13/2020 to overcome the rejection. Furthermore, Applicant's representative in an interview on 03/25/2020 agreed that an additional terminal disclaimer will be submitted for the following patents: 8,766,772, 8,933,807, 9,558,385, 10,235,513, and 10,445,719. The terminal disclaimer was approved and entered on 03/25/2020.

The claims are directed to settlement of a transaction using a mobile device comprising Radio Frequency (RF) cellular circuitry, an antenna, a biometric reading device, a point of sale (POS) device, and a central database. The mobile device establishes a connection with the POS using the RF communication before prompting a user for their biometric information. The

biometric information is associated with the user associated with the payment information based on biometric information stored in the memory of the mobile device. The mobile device then authenticates the biometric input and in response generates a key. The mobile device secures the payment information that is stored in the mobile device's memory before transmitting the generated key and the secure payment information to the POS. The POS receives the data and transmits it to the central database, wherein the central database then validates the data to complete the secured transaction.

Utilizing biometric authentication to provide access to a device and further utilize the device to complete a transaction is known in the art. U.S. Patent 6,163,771 to Walker ("Walker") teaches that a user provides their biometric information to a portable payment device, the payment device authenticates the received biometric data and if it is authenticated, provides the user with a prompt on whether they would like to complete a transaction, wherein the portable device generates a single use credit card number. If the user selects "YES," then the portable device generates the single use credit card number and displays the number or sends the number to a point of sale device. See Walker at least at Col. 5, Ln. 48-67; Col. 6, Ln. 1-67 and Col. 7, Ln. 1-67 and Figures 1, 3, and 10.

U.S. Patent 6,796,490 to Drummond et al. ("Drummond") teaches utilizing wireless communication to transmit data between a devices in order to settle a transaction. Specifically, Drummond teaches a wireless ATM system (30) comprises one or more wireless ATMs (32, 34, 36) that are operative to wirelessly communicate with a wireless ATM server (38). The wireless ATMs each include a wireless network interface (41). The wireless ATM server includes a corresponding wireless access point or wireless hub (40). Wireless transmission between the

wireless ATMs and wireless ATM server is secured with a wireless encryption protocol. The wireless ATM server is operative to communicate with at least one host banking system (46) through at least one public or private network (44). The wireless ATM server is operative to route transaction and event messages between the host banking system and each of the wireless ATMs using a message gateway router (43). The wireless ATM server further includes a firewall (42). See Col. 5, Ln. 1-67; Col. 6, Ln. 1-67 and Figures 3-5.

U.S. Patent 6,848,048 to Holmes ("Holmes") teaches specifically using RF cellular circuitry as a communication method for devices to send and receive data. See Holmes Col. 2, Ln. 28-53 and Figures 1-3.

U.S. Patent Application Publication 2002/0157029 to French et al. ("French") teaches network authentication system provides verification of the identity or other attributes of a network user to conduct a transaction, access data or avail themselves of other resources. The user is presented with a hierarchy of queries based on wallet-type (basic identification) and non-wallet type (more private) information designed to ensure the identity of the user and prevent fraud, false negatives and other undesirable results. A preprocessing stage may be employed to ensure correct formatting of the input information and clean up routine mistakes (such as missing digits, typos, etc.) that might otherwise halt the transaction. Queries can be presented in interactive, batch processed or other format. The authenticator can be configured to require differing levels of input or award differing levels of authentication according to security criteria. The user inputs the first type of information requested into client 110. Data may be queried from the user through textual questions, graphical user interfaces (GUIs), hyper text markup (HTML) forms or any other suitable mechanisms, either in a real-time interactive environment or through a batch submission. Selection of the input mode may depend upon various factors such as

resource loading and availability, business model, user and system traffic and transaction criticality. French also specifically discloses that the user is associated with purchase or transaction data. See French, Paragraphs 0137-0156, and Figures 2-3.

U.S. Patent 6,934,689 to Ritter et al. ("Ritter") teaches a payment transaction method and payment transaction system in which payment transactions between customers with portable mobile devices, for example mobile radio telephones, and a plurality of payment terminals are carried out at a service point, the payment terminal responsible for a payment transaction informing a respective customer about the total transaction amount and the transaction identification of the payment transaction, the transaction identification comprising a payment terminal identification, the mobile device transmitting, via a contactless device interface, the transaction identification, entered in the mobile device by the customer, to the payment terminal, identified through the payment terminal identification, the payment terminal transmitting, after receipt of the transaction identification, a payment request comprising a service point identification, the payment terminal identification and the total transaction amount, via the contactless device interface to the mobile device, and a payment record which comprises the payment request and a customer identification, being prepared in the mobile device and being transmitted from the mobile device via the contactless device interface to the payment terminal. It is clearly taught by Ritter that a transaction can be carried out between two devices using wireless radio frequency communication, wherein the data communicated between the devices is in a secure form. Ritter requires a user to provide a biometric input and the biometric input is authenticated before the transaction is settled. Furthermore, Ritter's transaction method requires two phases, wherein in the first phase transaction identification id determined or entered by the user and sent to the point of sale terminal which is assigned to the user device. The second phase

focuses on the financial aspect of the transaction, wherein the point of sale sends to the mobile device a request for payment transaction. Once the customer accepts the payment request, the mobile device generates the payment request and sends it to the point of sale. The point of sale then forwards the request to a clearing point. See Ritter at least at Col. 2, Ln. 45-67; Col. 3, Ln. 1-67; Col. 7, Ln. 1-67 and Col. 8, Ln. 1-67 and Figure 1.

A search was conducted to determine if any non-patent literature (NPL) relates to the claims. The NPL found is by Smart Card Alliance (Alliance, 2002). The reference discloses the use of both information a user knows (a PIN), something the user has (a smart card), and something the user is (biometric data). Using a PIN, smart, and biometric data to advance a transaction results in increased security level or measures. The reference discloses at a general level on how utilizing such data increases security measures.

Other references, which are noted in the notice of reference cited form PTO-892, disclose various methods and systems of settling a transaction using security measures.

The references as mentioned above or those not relied upon but are cited, do not teach solely or in combination all of the claim limitations as disclosed in claims 1 and 10.

The references do not teach the following claim limitations:

A mobile device, comprising:

short range radio frequency (RF) circuitry;

a memory coupled to the short range RF circuitry and configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information; and

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory that, when executed by the one or more processors, causes the one or more processors to perform operations of[[to]]:

establishing a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

prompting the user to provide biometric information to the biometric reading device,

authenticating that the biometric information read by the biometric reading device is associated with the user associated with the payment information based on the biometric authentication information stored in the memory,

in response to the authentication, generating a key,

securing the payment information stored in the memory, and

transmitting to the POS device, via the short range RF circuitry, the key and the secured payment information for use in the secure transaction.

And

A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

a memory configured to store biometric authentication information and payment information, wherein the biometric authentication information is associated with a user associated with the payment information;

a biometric reading device configured to read biometric information;

one or more processors operably coupled to the memory, short range RF circuitry, and the biometric reading device, the one or more processors configured to execute instructions stored in the memory that, when executed by the one or more processors, causes the one or more processors to perform operations of[[to]]:

establishing a connection with a point of sale (POS) device, via the short range RF circuitry, wherein the connection is established to conduct a secure transaction between the mobile device and the POS device,

prompting the user to provide biometric information to the biometric reading device,

authenticating that the biometric information read by the biometric reading device is associated with the user associated with the payment information based at least in part on the biometric authentication information stored in the memory,

in response to authenticating, generating a key,

securing the payment information stored in the memory, and

transmitting to the POS device, via the short range RF circuitry, the key and the secured payment information for use in the secure transaction;

the POS device comprising at least one memory and at least one processor operably coupled to the at least one memory of the POS device, the at least one memory of the POS

device storing instructions that, when executed by the at least one processor of the POS device causes the at least one processor of the POS device to perform operations of:

receiving, from the mobile device, the secured payment information and the key; and

transmitting the key and the secure payment information based to a central database; and

the central database comprising at least one memory and at least one processor operably coupled to the memory of the central database, the at least one memory of the central database storing instructions that, when executed by the at least one processor of the central database causes the at least one processor of the central database to perform operations of:

receiving, from the POS, the secured payment information and the key; and

validating the key and the secured payment information to complete the secured transaction.

Applicant's arguments submitted through the prosecution history provide further support for the reasons for allowance.

In conclusion, a prima facie case of obviousness with respect to the claims cannot be made and that the claims are patentably distinct from the prior art. Therefore, the limitations lacking in the prior art, in combination with the other limitations clearly claimed for patent, are novel and unobvious.

Further prior art, foreign prior art, and NPL searches were conducted; however, no relevant prior art was found.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EL MEHDI OUSSIR whose telephone number is (571)270-0191. The examiner can normally be reached on M-F 9AM - 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Neha W. Patel can be reached on 571-270-1492. The fax phone number for the organization where this application or proceeding is assigned is 571-270-1191.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Sincerely,

/El Mehdi Oussir/

El Mehdi Oussir
Patent Examiner, Art Unit 3685
03/27/2020

Examiner-Initiated Interview Summary	**Application No.** 14/639,034	**Applicant(s)** Martinez de Velasco Cortina et	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA (FITF) Status** No

All participants (applicant, applicant's representative, PTO personnel):

(1) EL MEHDI OUSSIR. (3) _____.

(2) Mark W. Catanese (Applicant's Representative). (4) _____.

Date of Interview: 24 March 2020.

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: 1,3,7,10 and 12-14.

Identification of prior art discussed: NA.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

See Continuation Sheet.

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Continuation of Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: The Examiner and the Applicant's representative discussed claim amendments to overcome 112 issues and objections along with other issues. Applicant's representative requested that the proposed amendments be approved by the Applicant. No specific agreement was reached. Also, Applicant representative requested that the requested Terminal Disclaimer for the newly 5 identified patents be approved by the Applicant. No specific agreement reached.

On 03/25/2020, Examiner received approval of the proposed claim amendments from Applicant and also confirmation of filing a terminal disclaimer for the identified 5 patents at issue. Further amendments were discussed and agreement was reached. The Examiner agreed to entering the amendments through Examiner Amendments.

Notice of References Cited	Application/Control No. 14/639,034	Applicant(s)/Patent Under Reexamination Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 1 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6848048-B1	01-2005	Holmes; William S.	G06F21/64	713/162
*	B	US-6163771-A	12-2000	Walker; Jay S.	G06Q20/04	705/18
*	C	US-7911643-B2	03-2011	Yamada; Makoto	H04N1/33307	358/1.15
*	D	US-5590197-A	12-1996	Chen; James F.	G06Q20/04	380/30
*	E	US-20070022058-A1	01-2007	Labrou; Yannis	G06Q20/32	705/67
*	F	US-20030018522-A1	01-2003	Denimarck, Paul	G06Q30/0267	705/14.23
*	G	US-20060020558-A1	01-2006	Bonalle; David S.	G06Q20/382	705/64
*	H	US-20020193142-A1	12-2002	Stavenow, Bengt	G06F21/41	455/556.1
*	I	US-20020194499-A1	12-2002	Audebert, Yves Louis Gabriel	H04L63/0853	726/35
*	J	US-20020123325-A1	09-2002	Cooper, Gerald M.	H04L63/0492	455/411
*	K	US-20020112171-A1	08-2002	Ginter, Karl L.	G06F21/10	713/185
*	L	US-20020157029-A1	10-2002	French, Jennifer	G06F21/31	726/21
*	M	US-6934689-B1	08-2005	Ritter; Rudolf	G06Q20/04	705/16

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	Alliance, S. C. (2002, May). Gemalto.com. Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems . Princeton Junction, NJ, USA. Retrieved from https://www.gemalto.com/press-site/gemplus/2002/security/Smart_Card_Biometric_paper.pdf (Year: 2002)
	V	IEEE. (1997, March 24). IEEE xplore. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=570830 (Year: 1997)
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 14/639,034	Applicant(s)/Patent Under Reexamination Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 2 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20060204048-A1	09-2006	Morrison; Robert A.	G06F21/32	382/115
*	B	US-20070198436-A1	08-2007	Weiss; Kenneth P.	G06Q20/401	705/75
*	C	US-9858566-B2	01-2018	Mardikar; Upendra S.	H04W12/06	1/1
*	D	US-20020073416-A1	06-2002	Ramsey Catan, Carolyn	G07C9/37	725/6
*	E	US-20020112177-A1	08-2002	Voltmer, William H.	G06Q20/40145	726/26
*	F	US-6796490-B1	09-2004	Drummond; Jay Paul	G06Q20/32	235/379
*	G	US-6044382-A	03-2000	Martino; Rocco L.	G06F9/466	348/E7.081
*	H	US-6049710-A	04-2000	Nilsson; B. G.	H04M3/42204	379/88.03
*	I	US-6259405-B1	07-2001	Stewart; Brett B.	H04M15/8033	342/457
*	J	US-20010044900-A1	11-2001	Uchida, Kaoru	G06Q20/40	713/186
*	K	US-20020010684-A1	01-2002	Moskowitz, Scott A.	G06F21/10	705/75
*	L	US-20020040327-A1	04-2002	Owa, Tsunayuki	G06Q10/10	705/26.1
*	M	US-20030149662-A1	08-2003	Shore, Jon	G06Q20/04	705/39

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.

Notice of References Cited	Application/Control No. 14/639,034	Applicant(s)/Patent Under Reexamination Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	Art Unit 3685	Page 3 of 3

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20030112120-A1	06-2003	K., Seifert Mark	G05B19/0425	340/5.53
*	B	US-8766772-B2	07-2014	Martinez de Velasco Cortina; Francisco	H04W12/00	340/5.8
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

CPC						
Symbol					**Type**	**Version**
G06Q	/	20	/	3674	F	2013-01-01
G06Q	/	20	/	3278	I	2013-01-01
H04W	/	4	/	80	A	2018-02-01
H04W	/	12	/	06	A	2013-01-01
H04W	/	12	/	00	A	2013-01-01
H04W	/	12	/	08	A	2013-01-01

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
	/		/					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 7	
/EL MEHDI OUSSIR/ Examiner, Art Unit 3685 (Primary Examiner)	27 March 2020 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 14

U.S. Patent and Trademark Office — Part of Paper No.: 20200327

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

INTERNATIONAL CLASSIFICATION					
CLAIMED					
G06Q20/36	/	20	/	36	
G06Q20/32	/	20	/	32	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**
705	71

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 7	
/EL MEHDI OUSSIR/ Examiner, Art Unit 3685 (Primary Examiner)	27 March 2020 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 14

U.S. Patent and Trademark Office

Part of Paper No.: 20200327

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	**Art Unit**
	EL MEHDI OUSSIR	3685

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	4	10												
-	2	-	11												
2	3	5	12												
-	4	6	13												
-	5	7	14												
-	6	-	15												
3	7	-	16												
-	8	-	17												
-	9														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 7	
/EL MEHDI OUSSIR/ Examiner, Art Unit 3685 (Primary Examiner)	27 March 2020 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 14

U.S. Patent and Trademark Office Part of Paper No.: 20200327

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

CPC - Searched*		
Symbol	**Date**	**Examiner**
G06Q	5/8/2015	EO
H04L	5/8/2015	EO
G06Q20	02/15/2019	EO
G06Q20	03/24/2020	EO

CPC Combination Sets - Searched*		
Symbol	**Date**	**Examiner**

US Classification - Searched*			
Class	**Subclass**	**Date**	**Examiner**
705		5/8/2015	EO

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	**Date**	**Examiner**

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

consulted Calvin Hewitt	5/15/2015	EO
Consulted John H. and Mamon O on 101/ 103	5/25/2017	EO
Consulted John H. on priority	5/9/2017	EO
Consulted Mohammad N. on priority and 112	5/26/2017	EO
Consulted Steven K. 112	03/14/2018	EO
Review of references	03/16/2018	EO
Consulted John H. 101	03/14/2018	EO
East search update	02/13/2019	EO
Consulted Steven Kim 101	02/13/2019	EO
IP.COM search	02/13/2019	EO
EAST search update	02/15/2019	EO
IP.COM search	02/18/2019	EO
Consulted Steven Kim 101 / 103	02/19/2019	EO
Consulted Mohammad N. 112	02/21/2019	EO
Consulted Steven Kim 112	07/26/2019	EO
EAST SEARCH	07/26/2019	EO
Consulted Mohammad N. 112	01/03/2020	EO
East search update	01/03/2020	EO
IP.com / google search / NPL search	01/03/2020	EO
Review co-pending applications / patents	01/03/2020	EO
Consulted M. Nilforoush 112s	03/24/2020	EO
NPL Search / Google / ((MOBILE DEVICE BIOMETRIC AUTHENTICATION RADIO FREQUENCY TRANSACTION WITH POS) OR (BIOMETRIC READING DEVICE)) before:priority: 20030101 after:priority:19900101	03/24/2020	EO
GOOGLE patents / IP search	03/24/2020	EO
Interference search / EAST search update	03/24/2020	EO
Search inventor, title, claims, applicant	03/24/2020	EO

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14/639,034	Martinez de Velasco Cortina et al.
	Examiner	Art Unit
	EL MEHDI OUSSIR	3685

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
G06Q	20	03/24/2020	EO

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	

Bibliographic Data

Application No: 14/639,034

Foreign Priority claimed: ○ Yes ◉ No

35 USC 119 (a-d) conditions met: ☐ Yes ☑ No ☐ Met After Allowance

Verified and Acknowledged: /El Mehdi Oussir/ (Examiner's Signature) | EO (Initials)

Title: SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
03/04/2015	705	3685	116546-613CT13
RULE			

APPLICANTS

NEOLOGY, INC., Poway, CA, UNITED STATES

INVENTORS

Francisco Martinez de Velasco Cortina La Jolla, CA, UNITED STATES

Manfred Rietzler Marktoberdorf, GERMANY

CONTINUING DATA

This application is a CON of 14321781 07/01/2014

14321781 is a CON of 14022135 09/09/2013 PAT 8766772

14022135 is a CON of 13350665 01/13/2012 PAT 8587436

13350665 is a CON of 13175768 07/01/2011 PAT 8237568

13175768 is a CON of 12688666 01/15/2010 PAT 8004410

12688666 is a CON of 11279912 04/17/2006 PAT 7671746

11279912 is a CON of 10615026 07/09/2003 PAT 7081819

10615026 has PRO of 60394241 07/09/2002

FOREIGN APPLICATIONS

IF REQUIRED, FOREIGN LICENSE GRANTED**

03/24/2015

STATE OR COUNTRY

UNITED STATES

ADDRESS

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

525 B STREET

SUITE 2200

SAN DIEGO, CA 92101

UNITED STATES

FILING FEE RECEIVED

$5,740

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S166	6	S164 AND (biometric)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/03/24 13:01
S165	56	((("Rietzler") near3 ("Manfred"))).INV.	USPAT	OR	ON	2020/03/24 13:00
S164	6	S163 AND (biometric with transaction)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/03/24 13:00
S163	32	((("Martinez") near3 ("de") near3 ("Velasco") near3 ("Cortina") near3 ("Francisco"))).INV.	USPAT	OR	ON	2020/03/24 13:00
S162	6	S160 AND (biometric with transaction)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/03/24 12:59
S161	6	S160 AND (biometric with transaction)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/03/24 12:54
S160	100	S159 and (RF (radio near2 frequency) RFID)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/03/24 12:53
S159	101	((("NEOLOGY") near3 ("INC"))).AS,AANM.	USPAT	OR	ON	2020/03/24 12:53
S158	5	S157 and (RF (radio near2 frequency) RFID)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/03/24 12:53
S157	7	S156 AND (biometric with transaction)	US-PGPUB;	OR	ON	2020/03/24

			USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			12:52
S156	28	("20010044900" | "20020010684" | "20020040327" | "20020112171" | "20020123325" | "20020157029" | "20020193142" | "20020194499" | "20030019929" | "20030055738" | "20030112120" | "20030137403" | "20030149662" | "5627544" | "5819234" | "5940006" | "6044382" | "6049710" | "6089284" | "6259405" | "6570488" | "6934689" | "7081819" | "7096363" | "7987501" | "8237568" | "8325044" | "9558385").PN.	US-PGPUB; USPAT	OR	ON	2020/03/24 12:51
S155	9	S154 and @pd<"20020709"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:18
S154	1476	S153 and (transaction purchas$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:18
S153	2030	S152 and (generat$3 with (key code OTP pin password account))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:17
S152	3586	S151 and ((establish$3 with (RF (radio near2 frequency) NFC Bluetooth (wireless))) near6 (connection))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:17
S151	97107	((prompt$3 pop-up pop$up) with (password authenticat$3 PIN biometric code OTP))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 13:16
S150	83423	((prompt$3 pop-up pop$up) with (password authenticat$3 PIN biometric code OTP))	US-PGPUB; USPAT	OR	ON	2020/01/04 13:15
S149	5	S148 and ((prompt$3 pop-up pop$up) with (password authenticat$3 PIN biometric code OTP))	US-PGPUB; USPAT	OR	ON	2020/01/04 13:15
S148	19	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$	US-PGPUB; USPAT	OR	ON	2020/01/04 13:14

		or US-20020193142-$ or US-20020194499-$ or US-20020123325-$ or US-20020112171-$ or US-20020157029-$ or US-20060204048-$ or US-20070198436-$ or US-20020073416-$ or US-20020112177-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$ or US-6934689-$ or US-9858566-$ or US-6796490-$).did.				
S147	8	"8766772"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/01/04 12:38
S146	2	S145 and (biometric near6 (associat$4 tied tying) near6 (financial account payment))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/09/26 17:45
S145	19	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$ or US-20020193142-$ or US-20020194499-$ or US-20020123325-$ or US-20020112171-$ or US-20020157029-$ or US-20060204048-$ or US-20070198436-$ or US-20020073416-$ or US-20020112177-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$ or US-6934689-$ or US-9858566-$ or US-6796490-$).did.	US-PGPUB; USPAT	OR	ON	2019/09/26 17:43
S144	1	("8766772").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/09/23 12:54
S143	1	("6796490").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/09/17 17:42
S142	1	("20020112177").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/09/12 13:06
S141	4	S140 AND @PD<"20020709"	US-PGPUB; USPAT	OR	ON	2019/09/12 12:05
S140	974	S139 and (((mobile cellular electronic pda portable) near2 (device phone)) with ((biometric fingerprint) near2 (reader scan scanner device input)))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:56
S139	133856	((user purchaser) near4 (select selection choos$3 selecting pick$3) near6 (product item media))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:53
S138	110882	((user purchaser) near2 (select selection choos$3 selecting pick$3) near6 (product item media))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:52
S137	2	S134 and ((user purchaser) near2 (select selection choos$3 selecting pick$3) near6 (product item media))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:42

S136	7	S134 and ((user purchaser) near2 (select selection choos$3 selecting pick$3))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:41
S135	9	S134 and ((user purchaser) near6 (select selection choos$3 selecting pick$3))	US-PGPUB; USPAT	OR	ON	2019/09/12 11:41
S134	16	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$ or US-20020193142-$ or US-20020194499-$ or US-20020123325-$ or US-20020112171-$ or US-20020157029-$ or US-20060204048-$ or US-20070198436-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$ or US-6934689-$ or US-9858566-$).did.	US-PGPUB; USPAT	OR	ON	2019/09/12 11:39
S133	6	S132 and ((request$3 receiv$3 obtain$3 prompt$3) near5 (user) near5 (biometric iris fingerprint))	US-PGPUB; USPAT	OR	ON	2019/07/26 18:02
S132	13	S128 AND (establish$3 (communication link)) and ((receiv$3 transmit$4 send$3) near5 (data information))	US-PGPUB; USPAT	OR	ON	2019/07/26 17:58
S130	3	S128 and ((promp$3) with (biometric passcode password PIN))	US-PGPUB; USPAT	OR	ON	2019/07/26 17:54
S129	9	S128 and ((promp$3 receiv$3) with (biometric passcode password PIN))	US-PGPUB; USPAT	OR	ON	2019/07/26 17:54
S128	16	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$ or US-20020193142-$ or US-20020194499-$ or US-20020123325-$ or US-20020112171-$ or US-20020157029-$ or US-20060204048-$ or US-20070198436-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$ or US-6934689-$ or US-9858566-$).did.	US-PGPUB; USPAT	OR	ON	2019/07/26 17:53
S122	1	("9858566").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/05/13 16:23
S121	19	S120 and (biometric)	USPAT	OR	ON	2019/05/13 15:52
S120	185	((("MARTINEZ") near3 ("DE") near3 ("VELASCO") near3 ("CORTINA") near3 ("Francisco")) OR (("RIETZLER") near3 ("Manfred"))).INV.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	ON	2019/05/13 15:52
S119	30	((("Martinez") near3 ("de") near3 ("Velasco") near3 ("Cortina") near3 ("Francisco"))).INV.	USPAT	OR	ON	2019/05/13 15:52
S118	3	S117 and (generate near2 key)	USPAT	OR	ON	2019/05/13 15:51
S117	34	S114 and (biometric)	USPAT	OR	ON	2019/05/13 15:51
S116	1	S115 and (biometric)	USPAT	OR	ON	2019/05/13 15:51
S115	7	S114 and (RF with circuitry)	USPAT	OR	ON	2019/05/13 15:51
S114	95	((("Neology") near3	USPAT	OR	ON	2019/05/13

		("Inc"))).AS,AANM.				15:50
S113	1	("20070198436").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/05/13 15:41
S109	8	("0000002" | "0000004" | "20020035690" | "20080141032" | "20100313026" | "20130166912" | "20140068268" | "20140075192").PN.	US-PGPUB; USPAT	OR	ON	2019/05/10 16:49
S108	1	("20060204048").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/05/10 14:16
S107	1	("20040034784").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/05/10 14:15
S106	18	S105 AND ((G06Q20/3676 OR G06Q20/3821 OR G06Q20/385 OR G06Q20/40 OR G06Q20/40145 OR G06Q30/06 OR G06Q40/02 OR G06Q50/22 OR G06Q20/401 OR G06Q20/102 OR G06Q20/3674 OR G06Q20/382 OR G06Q10/06 OR G06Q10/10 OR G06Q20/20 OR G06Q20/206 OR G06Q20/3672 OR G06Q20/4012 OR G06Q30/02 OR G06Q10/103 OR G06Q20/341 OR G06Q20/347 OR G06Q20/367 OR G06Q40/04 OR G06Q50/24).CPC.)	US-PGPUB; USPAT	OR	ON	2019/05/09 17:41
S105	57	S104 and @pd<"20120709"	US-PGPUB; USPAT	OR	ON	2019/05/09 17:41
S104	168	S102 and ((authomatic automatically) near5 (generate generating))	US-PGPUB; USPAT	OR	ON	2019/05/09 17:40
S103	0	S102 and (authomatic$5 near4 generat$4)	US-PGPUB; USPAT	OR	ON	2019/05/09 17:40
S102	2624	S100 and (generat$3 with (authenticat$3) with (biometric finger print iris))	US-PGPUB; USPAT	OR	ON	2019/05/09 17:39
S101	0	S100 and (generat$3 with (response and "to"))	US-PGPUB; USPAT	OR	ON	2019/05/09 17:39
S100	360414	(generat$3 near3 (code OTP PIN (random near2 number)))	US-PGPUB; USPAT	OR	ON	2019/05/09 17:38
S99	1	("8766772").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/26 13:14
S98	3	(contactless near2 (payment transaction) and biometric) and @ay<"2003"	US-PGPUB; USPAT	OR	OFF	2019/02/21 17:21
S97	1	("6934689").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 17:11
S96	1	("20020157029").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 15:00
S95	1	("20020112171").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 14:58
S94	0	(2002/0112171).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/21 14:57

S93	2	("20020123325").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 21:15
S92	5	("0797,359").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 21:14
S91	24	("1239630").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 21:13
S90	1	("20020194499").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/15 20:54
S89	1	("20020157029").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/15 20:41
S88	0	(2002/0157029).CCLS.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/02/15 20:41
S87	154	(prompt$4 dialog$3 form window popup pop$up) near2 (biometric pin code iris fingerprint authenticat$4 password passcode) with (location connect$4 area vicinity range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:32
S86	92	(prompt$4 dialog$3 form window popup pop$up) near2 (biometric pin code iris fingerprint authenticat$4 password passcode) with (location area vicinity range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:29
S85	8880	(prompt$4 dialog$3 form window popup pop$up) with (location area vicinity range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:26
S84	30	S83 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 20:24
S83	730	S81 same (biometric pin code iris fingerprint authenticat$4 password passcode)	US-PGPUB; USPAT	OR	ON	2019/02/15 20:24
S82	326	S81 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 20:23

S81	5053	(prompt$4 dialog$3 form window popup pop$up) with (range approach$3 proximate proximal proximity geofenc$3 close) near4 (rf bluetooth beacon rfid nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 20:22
S80	11	S79 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:42
S79	1910	S76 and ((prompt$4) near6 (biometric iris pin code password))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:42
S78	2422	S75 and ((prompt$4) near6 (biometric iris pin code password))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:42
S77	13	S76 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:39
S76	2479	S75 and ((prompt$4) with (user customer) with (biometric iris pin code password))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:38
S75	76623	(detect$4 determin$5) with (device mobile) with (rf bluetooth nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	ON	2019/02/15 19:36
S74	68297	(detect$4 determin$5) with (device mobile) with (rf bluetooth nfc (radio near2 frequency))	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:36
S73	18	S72 and @pd<"20020709"	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:30
S72	2518	S71 and ((mobile electronic) near3 (device phone pda))	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:30
S71	2980	S70 and ((prompt$4) with (user customer) with (biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:26
S70	108452	((establish$3) near6 (connection link)) with (rf bluetooth nfc wireless)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2019/02/15 19:25
S69	82023	((establish$3) near6 (connection link)) with (rf bluetooth nfc wireless)	US-PGPUB; USPAT	OR	OFF	2019/02/15 19:25
S68	3	S64 and ((prompt$4) with (input biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S67	5	S64 and ((prompt$4 ask$4) with (input biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S66	7	S64 and ((prompt$4 ask$4 requir$4) with (input biometric iris pin code password))	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S65	7	S64 and (prompt$4 ask$4 requir$4)	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S64	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	OFF	2019/02/15 17:53
S63	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-	US-PGPUB; USPAT	OR	OFF	2019/02/15 16:19

		5590197-$).did.				
S62	22	("7911643" | "5590197" | "20070022058" | "20060020558" | "20020112177" | "6934861" | "20070022058" | "6848048" | "20040128249" | "6163771").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2017/07/19 11:59
S61	0	(("7911643" | "5590197" | "20070022058" | "20060020558" | "20020112177" | "6934861" | "20070022058" | "6848048" | "20040128249" | "6163771").PN.").PN.	US-PGPUB; USPAT	OR	OFF	2017/07/19 11:59
S60	3	("20140040628").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/05/25 16:16
S59	0	(2014/0040628).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2017/05/25 16:15
S58	0	(2014/0040628).CCLS.	US-PGPUB; USPAT	OR	OFF	2017/05/25 16:15
S57	1	S55 and (RF with device)	US-PGPUB; USPAT	OR	ON	2017/05/25 10:48
S56	0	S55 and (RF near3 device)	US-PGPUB; USPAT	OR	ON	2017/05/25 10:48
S55	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2017/05/25 10:48
S54	1	S53 and (encrypt$4 with key with payment)	US-PGPUB; USPAT	OR	ON	2017/05/24 11:06
S53	7	(US-20070022058-$ or US-20030018522-$ or US-20060020558-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2017/05/24 11:05
S52	21	S51 and @pd<"20130909"	US-PGPUB; USPAT	OR	ON	2016/12/01 14:47
S51	34	S50 and ((mobile card) near3 (device))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S50	39	((biometric near4 associat$4) near4 (payment near2 information))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S49	3	S48 and ((mobile card) near3 (device))	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S48	5	(US-20070022058-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2016/12/01 14:46
S47	24	S46 and @pd<"20130909"	US-PGPUB; USPAT	OR	ON	2016/12/01 10:41
S46	39	((biometric near4 associat$4) near4 (payment near2 information))	US-PGPUB; USPAT	OR	ON	2016/12/01 10:39

S45	0	S44 and ((biometric near4 associat$4) with (payment))	US-PGPUB; USPAT	OR	ON	2016/12/01 10:39
S44	5	(US-20070022058-$).did. or (US-6848048-$ or US-6163771-$ or US-7911643-$ or US-5590197-$).did.	US-PGPUB; USPAT	OR	ON	2016/12/01 10:38
S43	2	"20070022058"	US-PGPUB; USPAT	OR	ON	2016/04/21 15:56
S42	66	("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" | "6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" | "5742618" | "6276607" | "6570487" | "8004410").PN.	US-PGPUB; USPAT	OR	ON	2015/09/30 16:20
S40	0	(("6175922" | "6268796" | "7031946" | "7310734" | "6848048" | "5974500" | "6275157" | "6334059" | "6698653" | "6753759" | "6793134" | "6950013" | "7671746" | "7980378" | "8126449" | "6163771" | "20030074317" | "4529870" | "5787174" | "6098879" | "6157333" | "6203952" | "6758405" | "7080819" | "7487538" | "7844505" | "5590197" | "20050149764" | "20100095130" | "5552789" | "5864580" | "5874896" | "6025780" | "6140941" | "6211790" | "6340116" | "6850147" | "6975834" | "7225337" | "7911643" | "20100094754" | "6052068" | "6073840" | "6104281" | "6388579" | "6427504" | "8041815" | "8401539" | "8548927" | "20020109580" | "6111506" | "6167333" | "6182894" | "6269292" | "6617961" | "20030200227" | "6025784" | "6360208" | "6894615" | "7533809" | "20020089434" | "5657008" | "5742618" | "6276607" | "6570487" | "8004410").PN.").PN.	US-PGPUB; USPAT	OR	OFF	2015/09/30 16:19
S39	1	("5590197").PN.	US-PGPUB; USPAT	OR	OFF	2015/06/12 16:44
S38	850	"5590197"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:44
S37	63	S35 and (biometric)	US-PGPUB;	OR	ON	2015/06/12

			USPAT			16:24
S35	234	S34 and (RFID RD infrared)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S34	1134	S33 and @pd<"20120101"	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S33	1736	S32 and (transaction financial account)	US-PGPUB; USPAT	OR	ON	2015/06/12 16:23
S32	3286	((generate) near2 (key pin code token password)) with ((encrypt) near2 (key pin code token password))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:22
S31	4128	((generate) near2 (key pin code token password)) with ((encrypt) near3 (key pin code token password))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:22
S30	7730	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near2 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S29	10379	((generate create) near2 (key pin code token password OTP)) same ((encrypt) near4 (key pin code token password OTP))	US-PGPUB; USPAT	OR	ON	2015/06/12 16:21
S28	1	"20020077993"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:40
S27	1	"20020112177"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:32
S26	51	S25 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:26
S25	5880	S24 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S24	29064	(stor$4 near3 information separately) with (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S22	48796	(stor$4 near3 information separately) same (authentication)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:25
S21	34	S20 and (biometric)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:16
S20	498	(authentication near4 stor$3 near4 separately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:13
S19	0	S15 and (stor$3 near4 saperately)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:08
S15	919	S11 and (memory)	US-PGPUB; USPAT	OR	ON	2015/05/18 16:07
S11	1011	S10 and ((information or data) near4 (separately))	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S10	1434	S9 and @pd<"20020101"	US-PGPUB; USPAT	OR	ON	2015/05/18 16:06
S9	12789	(stor$3 near1 data) with separately	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S8	0	(separatly near1 stor$3) with data	US-PGPUB; USPAT	OR	ON	2015/05/18 16:05
S6	5	"7911643"	US-PGPUB; USPAT	OR	ON	2015/05/18 15:59
S5	16	(biometric near1 data) near2 stored near2 (separately or different)	US-PGPUB; USPAT	OR	ON	2015/05/18 15:53
S2	1	("6163771").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:27

S1	1	("6848048").PN.	US-PGPUB; USPAT	OR	OFF	2015/05/18 08:26

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S176	11	((RF) (Radio frequency)) with (biometric) with (cellular with circuitry)	US-PGPUB; USPAT	OR	ON	2020/03/24 13:10
S175	10	(mobile near6 device) with (biometric near3 device) with (generate near5 key) with (encrypt$3 with key)	US-PGPUB; USPAT	OR	ON	2020/03/24 13:08
S174	50	S173 and (RF (radio) (RFID) (wireless))	US-PGPUB; USPAT	OR	ON	2020/03/24 13:06
S173	51	S172 and (establish same connection)	US-PGPUB; USPAT	OR	ON	2020/03/24 13:06
S172	239	S171 and (biometric)	US-PGPUB; USPAT	OR	ON	2020/03/24 13:05
S171	662	S170 and (generat$3 with key)	US-PGPUB; USPAT	OR	ON	2020/03/24 13:05
S170	1023	(encrypt$3) with (key) with (payment near3 information)	US-PGPUB; USPAT	OR	ON	2020/03/24 13:05
S169	10	S168 AND ((H04W84/12 OR H04W12/06 OR H04W12/08 OR H04W4/80 OR H04W48/16 OR H04W4/027 OR H04W52/0254 OR H04W52/0258 OR H04W52/143 OR H04W52/282 OR H04W52/283 OR H04W52/285 OR H04W76/27 OR H04W88/06 OR G06Q10/103 OR G06Q10/20).CPC.)	US-PGPUB; USPAT	OR	ON	2020/03/24 13:04
S168	15	((RF) (Radio frequency)) with (cellular near5 circuitry) with (POS POC (Computing near4 device))	US-PGPUB; USPAT	OR	ON	2020/03/24 13:03
S167	3	((RF) (Radio frequency)) with (biometric) with (cellular near5 circuitry)	US-PGPUB; USPAT	OR	ON	2020/03/24 13:02
S127	27	S126 and (generat$4 with key with biometric)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:55
S126	83	S124 and (stor$3 near4 biometric near4 information)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:55
S125	15	S124 and (store near2 biometric near2 information)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:55
S124	11100	S123 and (short near2 range near2 radio)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:54
S123	826132	(mobile near2 device)	US-PGPUB; USPAT	OR	ON	2019/05/13 15:54

3/27/2020 10:14:29 AM
C:\Users\eoussir\Documents\EAST\Workspaces\14639034_Mobile device RFID transaction biometric POS V2.wsp

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, El Mehdi
Attorney Docket Number	116546-613CT13

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]

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, El Mehdi
	Attorney Docket Number	116546-613CT13

	1	US Office Action dated January 8, 2020 received in US patent application no. 14/321,781(21 pages)	
	2	Appeal Brief filed June 10, 2019 filed in US patent application no. 14/724,593. (46 pages)	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/EL MEHDI OUSSIR/	Date Considered	03/27/2020

*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. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, El Mehdi
Attorney Docket Number	116546-613CT13

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2020-01-13
Name/Print	Mark W. Catanese	Registration Number	64279

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

SEARCH TERMS

MOBILE DEVICE BIOMETRIC AUTHENTICATION RADIO FREQUENCY TRANSACTION WITH POS

BIOMETRIC READING DEVICE

+ Synonym

+ Add term

SEARCH FILTERS

Date Priority

1980-01-01 2003-01-01

Inventor

Assignee

Patent Office Language

Status Type

Litigation

About 36,852 results Download Add to collection Side-by-side

Sort by Relevance Group by None Deduplicate by Family Results / page 10

Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification System

Google Scholar www.garnetbot.com Albrecht S White Peter May

Published 2002

... Credential users must understand the care, usage, and context of the ID card and be provided with clear instructions on how the credential interfaces with **reading** systems ... **Biometric** capture Image processing Template storage Image Template Storage **device** (card or database) ...

Smartcards and Biometrics: An Overview

Google Scholar www.rulencardtrack.com Brocklander R Computers Fraud & Security Bulletin

Published 1999

... An alarm circuitry: this circuitry must process the information from the fraud sensors and act appropriately • Memory to store sensitive data, eg cryptographic keys, **biometric** template ... Passive probing: **reading** information, generally from the database ...

Evaluation of microbial health risks associated with the reuse of source-separated human urine

Google Scholar www.diva-portal.org Höglund C

Published 2001

Page 1. Evaluation of microbial health risks associated with the reuse of source-separated human urine Caroline Höglund Royal Institute of Technology (KTH) Department of Biotechnology, Applied Microbiology Swedish Institute ...

Multiplex pyrosequencing

Google Scholar academic.oup.com Ronaghi M Nucleic acids research

Published 2001

... Hybridization at the upstream region requires a DNA polymerase for **reading** through the variable region such as DNA sequencing techniques (1 – 4), while hybridization on the variable region may require ligase or nucleases (5 – 9). DNA sequencing has been the most ...

Psychophysiologic responses to combat imagery of Vietnam veterans with posttraumatic stress disorder versus other anxiety disorders.

Google Scholar psycnet.apa.org Pitman R Journal of abnormal psychology

Published 1990

... restriction tape. The subject was informed that a series of scripts would be presented after this tape. Each script

Top 1000 results by filing date

Relative count of top 3 values

Assignees Inventors CPCs

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-613CT13

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5627544	A	1997-05-06	SNODGRASS CHARLES K et al.	
	2	5819234	A	1998-10-06	SLAVIN et al.	
	3	5940006	A	1999-08-17	MACLELLAN et al.	
	4	6089284	A	2000-07-18	KAEHLER DAVID L et al.	
	5	6570488	B2	2003-05-27	Kucharczyk et al.	
	6	6934689	B1	2005-08-23	Ritter et al.	
	7	7081819	B2	2006-07-25	Martinez de Velasco Cortina et al.	
	8	7096363	B2	2006-08-22	Kon et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	9	7987501	B2	2011-07-26	Miller et al.	
	10	8237568	B2	2012-08-07	Martinez de Velasco Cortina et al.	
	11	8325044	B2	2012-12-04	Martinez de Velasco Cortina et al.	
	12	8587436	B2	2013-11-19	Martinez de Velasco Cortina et al.	
	13	9558385	B2	2017-01-31	Martinez de Velasco Cortina et al.	
	14	9858566	B2	2018-01-02	Mardikar et al.	
	15	6796490	B1	2004-09-28	Drummond	

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	20020073416	A1	2002-06-13	Ramsey Catan	
	2	20020112171	A1	2002-08-15	Ginter et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	3	20020123325	A1	2002-09-05	Cooper	
	4	20020157029	A1	2002-10-24	French et al.	
	5	20020193142	A1	2002-12-19	Stavenow et al.	
	6	20020194499	A1	2002-12-19	Audebert et al.	
	7	20030018522	A1	2003-01-23	Denimarck et al.	
	8	20030019929	A1	2003-01-30	Stewart et al.	
	9	20030055738	A1	2003-03-20	Alie	
	10	20030112120	A1	2003-06-19	Siefert	
	11	20030137403	A1	2003-07-24	Carrender et al.	
	12	20030149662	A1	2003-08-07	Shore	
	13	20060204048	A1	2006-09-14	Morrison	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	14	20070198436	A1	2007-08-23	Weiss	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Ewa Syta, S. K. (2010). RFID-based Authentication Middleware for Mobile Devices. IEEE, 1-10. Retrieved from http://www.cs.ccsu.edu/-stan/research/pervasive/pubs/hicss201 Orfidam .pdf (10 pages)	
	2	US Notice of Allowance dated July 24, 2019 received in US patent application no. 16/051,751 (16 pages)	
	3	US Notice of Allowance dated June 4, 2019 received in US patent application no. 16/051,751 (22 pages)	
	4	Response to Office Action filed on April 30, 2019 in US Patent Application no. 16/051,751. (11 pages)	
	5	US Applicant Interview Summary dated April 22, 2019 received in US patent application no. 16/051,751	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	6	US Office Action dated February 4, 2019 received in US Patent Application no. 16/051,751. (21 pages)	
	7	Preliminary Amendment filed on August 28, 2018 in US Patent Application no. 16/051,751. (9 pages)	
	8	US Office Action dated October 24, 2019 received in US patent application no. 14/724,593. (29 pages)	
	9	Notice of Appeal dated April 10, 2019 filed in US patent application no. 14/724,593. (4 pages)	
	10	US Office Action dated January 11, 2019 received in US patent application no. 14/724,593. (48 pages)	
	11	Response to Office Action filed on September 11, 2018 for US patent application no. 14/724,593 (24 pages)	
	12	US Office Action dated July 12, 2018 received in US patent application no. 14/724,593. (45 pages)	
	13	Response to Office Action filed on January 10, 2018 for US patent application no. 14/724,593 (17 pages).	
	14	US Applicant Interview Summary dated December 6, 2017 received in US patent application no. 14/724,593. (3 pages)	
	15	US Office Action dated July 28, 2017 received in US patent application no. 14/724,593. (36 pages)	
	16	US Notice of Allowance dated May 28, 2019 received in US patent application no. 14/659,502 (31 pages)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	17	Patent Board Decision mailed May 10, 2019 received in US patent application no. 14/659,502 (11 pages).	
	18	Reply Brief filed September 26, 2017 for US patent application no. 14/659,502 (13 pages).	
	19	Examiner's Answer to Appeal Brief dated July 26, 2017 received in US patent application no. 14/659,502.(28 pages).	
	20	US Applicant Interview Summary dated December 20, 2019 received in US patent application no. 14/585,057 (3 pages).	
	21	US Office Action dated September 19, 2019 received in US patent application no. 14/585,057 (21 pages)	
	22	Response to Office Action filed on April 30, 2019 for US Patent application no. 14/585,057 (20 pages)	
	23	Patent Board Decision dated March 4, 2019 for US patent application no. 14/585,057. (11 pages)	
	24	Reply Brief filed dated August 21, 2017 in the US Patent application no. 14/585,057 (11 pages)	
	25	Examiner's Answer to Appeal Brief dated June 21, 2017 received in US patent application no. 14/585,057 (24 pages)	
	26	Advisory Action dated December 16, 2019 received in US Patent Application 14/321,781 (7 pages)	
	27	Response to Office Action mailed December 3, 2019 for US Patent application 14/321,781 (30 pages)	

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

	28	US Office Action dated October 4, 2019 received in US patent application no. 14/321,781. (21 pages)	
	29	Response to Office Action filed on June 7, 2019 for US patent application no. 14/321,781. (31 pages)	
	30	US Office Action dated March 7, 2019 received in US patent application no. 14/321,781. (19 pages)	
	31	Response to Office Action filed on August 14, 2018 for US patent application no. 14/321,781. (28 pages)	
	32	US Office Action dated March 22, 2018 received in US patent application no. 14/321,781. (37 pages)	
	33	Response to Office Action filed on December 5, 2017 for US patent application no. 14/321,781. (16 pages)	
	34	US Office Action dated June 5, 2017 received in US patent application no. 14/321,781. (51 pages)	

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/EL MEHDI OUSSIR/	Date Considered	03/27/2020

*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. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-613CT13

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2020-01-06
Name/Print	Mark W. Catanese	Registration Number	64279

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	de VELASCO CORTINA, Francisco Martinez	116546-613CT13	5934

EXAMINER	
OUSSIR, El Mehdi	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
April 16, 2020	EFS WEB

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

MAIL STOP ISSUE FEE
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Though Applicant agrees with the conclusion of patentability contained in the communication dated April 6, 2020, Applicant respectfully disagrees with the reasons for allowance set forth therein. For example, while Applicant does not disagree with the characterizations set forth in the reasons for allowance, Applicant submits that the instant application is not limited to only those characterizations. Rather, the claims are to be read in light of the characterizations as set forth in the specification, and not only those stated in the reasons for allowance.

The Commissioner is hereby authorized to charge any underpayment or credit any overpayment to Procopio's Deposit Account No. 50-2075.

Respectfully submitted,

Dated: April 16, 2020

By: /Mark W. Catanese/
Mark W. Catanese
Reg. No. 64,279

Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101
(619) 238-1900
Customer No. 27189

Document Description: Issue Fee Payment (PTO-85B)

Issue Fee Transmittal Form

Application Number	Filing Date	First Named Inventor	Atty. Docket No.	Confirmation No.
14639034	04-Mar-2015	Francisco Martinez de Velas	116546-613CT13	5934

TITLE OF INVENTION :

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

Entity Status	Application Type	Art Unit	Class - Subclass	EXAMINER
Regular Undiscounted	Utility under 35 USC 111(a)	3685	071000	EL MEHDI OUSSIR

Issue Fee Due	Publication Due	Total Fee(s) Due	Date Due	Prev. Paid Fee
$1000	$0	$1000	06-Jul-2020	$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 **in 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, CORY, HARGREAVES
2. & SAVITCH LLP
3. MARK W. CATANESE

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**	04-16-2020
Name	Mark William Catanese	**Registration Number**	64279

WEB IFEE 1.0

FEE ADDRESS INDICATION FORM

Application Number	14639034	Art Unit	3685
Filing Date	04-Mar-2015	Examiner Name	EL MEHDI OUSSIR
First Name Inventor	Francisco Martinez de Velasco Cortina	Attorney Doc. Number	116546-613CT13

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**	04-16-2020
Name	Mark William Catanese	**Registration Number**	64279

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT13

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:	39171881
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	16-APR-2020
Filing Date:	04-MAR-2015
Time Stamp:	15:56:08
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	E20204FF56053931
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	Amendment after Notice of Allowance (Rule 312)	116546-613CT13_Comments_on_Statement_of_Allowability_.pdf	50880 6d0ad293e620d29194a06102727bff936616e8f3	no	1
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	Web85b.pdf	46566 29c7f9c984ccf7fba2feaabc060b31e81c612f7e	no	2
Warnings:					
Information:					
3	Maintenance Fee Address Change	web85feeaddress.pdf	33163 a22f37d4964e2f143b917b763b20a0003a03ffca	no	1
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	31927 d6da73abe3bae7479eb1a105b4854c176a8ffdb4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	162536		

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 (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

U.S.PATENTS						
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	6016476	A	2000-01-18	Maes	
	2	6089284	A	2000-07-18	Kaehler	
	3	7096363	B2	2006-08-22	Kon	
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S.PATENT APPLICATION PUBLICATIONS						
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	20030004827	A1	2003-01-02	Wang	
	2	20040044627	A1	2004-03-04	Russell	
	3	20040049451	A1	2004-03-11	Beraardi	
If you wish to add additional U.S. Published Application citation information please click the Add button.						
FOREIGN PATENT DOCUMENTS						

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

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

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Alliance, S. C, Gemalto.com. Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identificatioin Systems, Princeton Junction, NJ, USA. Retrieved from https://www.gemalto.com/press-site/gernplus/2002/security/Smart_Card_Biometric_paper.pdf (2002) (22 pages)	☐
	2	US Office Action dated April 13, 2020 received in US Patent Application no. 16/519,961 (38 pages)	☐
	3	Notice of Allowance and Examiner Initiated Interview Summary dated April 8, 2020 received in US Patent application no. 14/724,593 (48 pages)	☐
	4	US Applicant Interview Summary dated January 22, 2020 received in US patent application no. 14/724,593 (7 pages)	☐
	5	US Applicant Interview Summary dated January 22, 2020 received in US patent application no. 14/585,057 (7 pages)	☐
	6	Notice of Allowance and Examiner Initiated Interview Summary dated April 2, 2020 received in US Patent application no. 14/321,781 (41 pages)	☐

If you wish to add additional non-patent literature document citation information please click the Add button

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

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	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2020-04-20
Name/Print	Mark W. Catanese	Registration Number	64279

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	14639034	Filing Date	2015-03-04	Docket Number (if applicable)	116546-613CT13	Art Unit	3685
First Named Inventor	Francisco Martinez de Velasco Cortina			Examiner Name	El Mehdi OUSSIR		

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, 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 QPIDS Statement

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

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2020-04-20
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.

Doc Code: PET.AUTO Document Description: Petition automatically granted by EFS-Web	PTO/SB/140 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**PETITION TO WITHDRAW AN APPLICATION FROM ISSUE AFTER PAYMENT OF THE ISSUE FEE UNDER 37 CFR 1.313(c)**
Application Number	14639034
Filing Date	04-Mar-2015
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	EL MEHDI OUSSIR
Attorney Docket Number	116546-613CT13
Title	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

An application may be withdrawn from issue for further action upon petition by the applicant. To request that the Office withdraw an application from issue, applicant must file a petition under this section including the fee set forth in § 1.17(h) and a showing of good and sufficient reasons why withdrawal of the application from issue is necessary.

APPLICANT HEREBY PETITIONS TO WITHDRAW THIS APPLICATION FROM ISSUE UNDER 37 CFR 1.313(c).

A grantable petition requires the following items:
(1) Petition fee; and
(2) One of the following reasons:
(a) Unpatentability of one or more claims, which must be accompanied by an unequivocal statement that one or more claims are unpatentable, an amendment to such claim or claims, and an explanation as to how the amendment causes such claim or claims to be patentable;
(b) Consideration of a request for continued examination in compliance with § 1.114 (for a utility or plant application only); or
(c) Express abandonment of the application. Such express abandonment may be in favor of a continuing application, but not a CPA under 37 CFR 1.53(d).

Petition Fee

○	Small Entity
○	Micro Entity
◉	Regular Undiscounted

Reason for withdrawal from issue

○ One or more claims are unpatentable ◉ Consideration of a request for continued examination (RCE) (List of Required Documents and Fees) ○ Applicant hereby expressly abandons the instant application (any attorney/agent signing for this reason must have power of attorney pursuant to 37 CFR 1.32(b)).
RCE request,submission, and fee. ☐ I certify, in accordance with 37 CFR 1.4(d)(4) that : The RCE request ,submission, and fee have already been filed in the above-identified application on ☒ Are attached.
THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES I certify, in accordance with 37 CFR 1.4(d)(4) that I am: ◉ An attorney or agent registered to practice before the Patent and Trademark Office who has been given power of attorney in this application. ○ An attorney or agent registered to practice before the Patent and Trademark Office, acting in a representative capacity. ○ A sole inventor ○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application ○ A joint inventor; all of whom are signing this e-petition

Signature	/Mark W. Catanese/
Name	Mark W. Catanese
Registration Number	64279

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	de VELASCO CORTINA, Francisco MARTINEZ	116546-613CT13	5934

EXAMINER	
OUSSIR, El Mehdi	
ART UNIT	PAPER NUMBER
3685	
SUBMISSION DATE	DELIVERY MODE
April 20, 2020	EFS WEB

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

INFORMATION DISCLOSURE STATEMENT

In accordance with 37 CFR Sections 1.97 and 1.98, the items identified in this Information Disclosure Statement ("IDS") are brought to the attention of the Office. The items are listed on the attached form.

Copies of these references are not being provided pursuant to 37 CFR §1.98(d), as these references were cited in application Serial No 14/321,781, from which priority is being claimed. It is requested that the information provided herein be made of record in this application.

This statement is being filed with filing, and therefore no fees are due, however, the Commissioner is hereby authorized to charge any fees required by the filing of these papers, and to credit any overpayment to Procopio's Deposit Account No. 50-2075.

Respectfully submitted,
PROCOPIO, CORY, HARGREAVES & SAVITCH LLP

Dated: April 20, 2020

By: /Mark W. Catanese/
Mark W. Catanese
Registration No. 64,279
Customer No. 27189

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B Street
Suite 2200
San Diego, CA 92101
Tel 619-238-1900
Fax 619-235-0398
docketing@procopio.com

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT13

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
PETITION FEE- 37 CFR 1.17(H) (GROUP III)	1464	1	140	140
RCE- 2ND AND SUBSEQUENT REQUEST	1820	1	1900	1900
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2040**

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

Decision Date : April 20, 2020

In re Application of :

Francisco Martinez de Velasco Cortina

DECISION ON PETITION
UNDER CFR 1.313(c)(2)

Application No : 14639034

Filed : 04-Mar-2015

Attorney Docket No : 116546-613CT13

This is an electronic decision on the petition under 37 CFR 1.313(c)(2), filed April 20, 2020 , to withdraw the above-identified application from issue after payment of the issue fee.

The petition is **GRANTED.**

The above-identified application is withdrawn from issue for consideration of a submission under 37 CFR 1.114 (request for continued examination). See 37 CFR 1.313(c)(2).

Petitioner is advised that the issue fee paid in this application cannot be refunded. If, however, this application is again allowed, petitioner may request that it be applied towards the issue fee required by the new Notice of Allowance.

Telephone inquiries concerning this decision should be directed to the Patent Electronic Business Center (EBC) at 866-217-9197.

This application file is being referred to Technology Center AU 3685 for processing of the request for continuing examination under 37 CFR 1.114 .

Office of Petitions

Electronic Acknowledgement Receipt

EFS ID:	39196768
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	20-APR-2020
Filing Date:	04-MAR-2015
Time Stamp:	16:57:37
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$2040
RAM confirmation Number	E20204JG57322248
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)

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)	116546-613CT13_RCE_to_file_with_QPIDS_04_17_2020.PDF	1349971 c5346c32c28ad10f80287fb364ac7c7d789914b3	no	3
Warnings:					
Information:					
2	Petition automatically granted by EFS	petition-request.pdf	31549 65a6915765169389e96fac7bf487a3608df12c71	no	2
Warnings:					
Information:					
3	Quick Path Information Disclosure Statement	116456-613CT13_QPIDS_filed_04_20_2020.PDF	202425 5e1de18d0060f904098d68e618f538256845bda8	no	2
Warnings:					
Information:					
4	Quick Path Information Disclosure Statement	116546-613CT13_SIDS_up_to_April_.PDF	1034903 e8272f73f7d580ccdf42ea3fd732bfe1c28bba04	no	1
Warnings:					
Information:					
5	Other Reference-Patent/App/Search documents	116546-613CT13_IDS_Statement_of_non-submit_NPL_filed_04_17_2020.pdf	53121 0629ab7e268d41cd0547491fe4679b9f7037349c	no	1
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	32399 055443fbb556977543210f8a6b1edb7a5ea9fd39	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	2704368

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/25 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A PROVISIONAL DOUBLE PATENTING REJECTION OVER A PENDING "REFERENCE" APPLICATION**
Application Number	14639034
Filing Date	04-Mar-2015
First Named Inventor	Francisco Martinez de Velasco Cortina
Attorney Docket Number	116546-613CT13
Title of Invention	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
Neology, Inc.	100%

The owner(s) of percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of any patent granted on pending reference Application Number(s)

16519961 filed on 07/23/2019

as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and any patent granted on the reference application are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term of any patent granted on said reference application, "as the term of any patent granted on said reference application may be shortened by any terminal disclaimer filed prior to the grant of any patent on the pending reference application," in the event that any such patent granted on the pending reference application: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as shortened by any terminal disclaimer filed prior to its grant.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○	I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

○ Small Entity

○ Micro Entity

◉ Regular Undiscounted

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 47596

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/Mark W. Catanese/
Name	Mark W. Catanese

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	14639034
Filing Date:	04-Mar-2015
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Filer:	Mark William Catanese/Helen Glenister
Attorney Docket Number:	116546-613CT13

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
STATUTORY OR TERMINAL DISCLAIMER	1814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 14639034

Filing Date: 04-Mar-2015

Applicant/Patent under Reexamination: Martinez de Velasco Cortina

Electronic Terminal Disclaimer filed on April 24, 2020

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	39244262
Application Number:	14639034
International Application Number:	
Confirmation Number:	5934
Title of Invention:	SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS
First Named Inventor/Applicant Name:	Francisco Martinez de Velasco Cortina
Customer Number:	27189
Filer:	Mark William Catanese/Helen Glenister
Filer Authorized By:	Mark William Catanese
Attorney Docket Number:	116546-613CT13
Receipt Date:	24-APR-2020
Filing Date:	04-MAR-2015
Time Stamp:	17:00:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	E20204NH00228517
Deposit Account	502075
Authorized User	Helen Glenister

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

37 CFR 1.16 (National application filing, search, and examination fees)

37 CFR 1.17 (Patent application and reexamination processing fees)

37 CFR 1.19 (Document supply fees)

37 CFR 1.20 (Post Issuance fees)

37 CFR 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	34092 90982060d0f79c560fb2edb139ffa10a129096c5	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30509 97cc17fa8dd6b5944b98c70dc65215c2e17c6ab5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64601		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



United States Patent and Trademark Office

Office of the Chief Financial Officer

Document Code:WFEE

User :71167

Sale Accounting Date:05/05/2020

Sale Item Reference Number	Effective Date
14639034	04/20/2020

Document Number	Fee Code	Fee Code Description	Amount Paid	Payment Method
I202055I07484609	1806	SUBMISSION- INFORMATION DISCLOSURE STMT	$240.00	Deposit Account

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	03/04/2015	Francisco Martinez de Velasco Cortina	116546-613CT13	5934

27189 7590 05/27/2020

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

EXAMINER
OUSSIR, EL MEHDI

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
05/27/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTONotifications@procopio.com
docketing@procopio.com

Corrected ***Notice of Allowability***	**Application No.** 14/639,034	**Applicant(s)** Martinez de Velasco Cortina et al.	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA (FITF) Status** No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to Quick Path IDS request on 04/20/2020.
   ☐ 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 1,3,7,10 and 12-14 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information , please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/EL MEHDI OUSSIR/ Examiner, Art Unit 3685	/MAMON OBEID/ Primary Examiner, Art Unit 3685

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT
(Not for submission under 37 CFR 1.99)

Application Number	14639034
Filing Date	2015-03-04
First Named Inventor	Francisco Martinez de Velasco Cortina
Art Unit	3685
Examiner Name	OUSSIR, EL MEHDI
Attorney Docket Number	116546-613CT13

U.S.PATENTS

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	6016476	A	2000-01-18	Maes	
	2	6089284	A	2000-07-18	Kaehler	
	3	7096363	B2	2006-08-22	Kon	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

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	20030004827	A1	2003-01-02	Wang	
	2	20040044627	A1	2004-03-04	Russell	
	3	20040049451	A1	2004-03-11	Beraardi	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

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								

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	Alliance, S. C, Gemalto.com. Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identificatioin Systems, Princeton Junction, NJ, USA. Retrieved from https://www.gemalto.com/press-site/gernplus/2002/security/Smart_Card_Biometric_paper.pdf (2002) (22 pages)	☐
	2	US Office Action dated April 13, 2020 received in US Patent Application no. 16/519,961 (38 pages)	☐
	3	Notice of Allowance and Examiner Initiated Interview Summary dated April 8, 2020 received in US Patent application no. 14/724,593 (48 pages)	☐
	4	US Applicant Interview Summary dated January 22, 2020 received in US patent application no. 14/724,593 (7 pages)	☐
	5	US Applicant Interview Summary dated January 22, 2020 received in US patent application no. 14/585,057 (7 pages)	☐
	6	Notice of Allowance and Examiner Initiated Interview Summary dated April 2, 2020 received in US Patent application no. 14/321,781 (41 pages)	☐
If you wish to add additional non-patent literature document citation information please click the Add button			

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

EXAMINER SIGNATURE			
Examiner Signature	/EL MEHDI OUSSIR/	Date Considered	05/14/2020

*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. /E.O/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14639034
	Filing Date	2015-03-04
	First Named Inventor	Francisco Martinez de Velasco Cortina
	Art Unit	3685
	Examiner Name	OUSSIR, EL MEHDI
	Attorney Docket Number	116546-613CT13

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☐ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Mark W. Catanese/	Date (YYYY-MM-DD)	2020-04-20
Name/Print	Mark W. Catanese	Registration Number	64279

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /E.O/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/639,034	07/07/2020	10706412	116546-613CT13	5934

27189 7590 06/17/2020

PROCOPIO, CORY, HARGREAVES & SAVITCH LLP
525 B STREET
SUITE 2200
SAN DIEGO, CA 92101

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 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.

IR103 (Rev. 10/09)