IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

MOBILITY IP HOLDINGS, INC., *Plaintiff,* v. SAMSUNG ELECTRONICS CO, LTD. AND SAMSUNG ELECTRONICS AMERICA, INC., *Defendants.*	§ § § § § § § § § § § § §	Case No. 2:26-cv-157 Jury Trial Demanded

PLAINTIFF'S COMPLAINT

Plaintiff **Mobility IP Holdings, Inc.** ("Mobility IP") files this suit against Defendants Samsung Electronics Co., Ltd. ("SEC") and Samsung Electronics America, Inc. ("SEA") for infringement of United States Patent Nos. 8,151,345; 8,548,924; 8,766,772; 8,933,807; 10,235,513; 10,706,412; and 10,762,187 and alleges, with personal knowledge as to its own actions and on information and belief as to the actions of others, as follows:

THE PARTIES

1. Plaintiff Mobility IP is a Texas corporation that holds all right, title, and interest in United States Patent Nos. 8,151,345 ("'345 Patent"); 8,548,924 ("'924 Patent"); 8,766,772 ("'772 Patent"); 8,933,807 ("'807 Patent"); 10,235,513 ("'513 Patent"); 10,706,412 ("'412 Patent"); and 10,762,187 ("'187 Patent") (collectively, "Asserted Patents"). *See* Exhibits 1–7. Mobility IP has a principal place of business at 1917 Palomar Oaks Way, Suite 110, Carlsbad, California 92008.

2. Defendant SEC is a Korea corporation with its principal place of business at 129 Samsung-Ro Yeongtong-gu, Suwon-Si, Gyeonggi-do, 16677 Republic of Korea. SEC may be

APPLE 1031

served pursuant to Fed. R. Civ. P. 4(f)(1). In addition, or in the alternative, SEC may be served through its registered agent Ms. Jenni Chun at 19 Chapin Rd., Bldg. D, Pine Brook, NJ 07058. *See, e.g.*, Exhibit 8.

3. Defendant SEA is a New York corporation with its principal place of business at 85 Challenger Road, Ridgefield Park, New Jersey 07660. SEA has been registered to do business in the state of Texas since June 10, 1996 and may be served through its registered agent, CT Corporation System, at 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

4. SEA is a wholly owned subsidiary of SEC (SEC and SEA collectively "Samsung" or "Defendants"). Samsung maintains regular and established places of business in this District, including a "flagship campus" at 6625 Excellence Way, Plano, Texas 75023.[1]

JURISDICTION & VENUE

5. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because the action brought by Mobility IP against Samsung arises under the patent laws of the United States, 35 U.S.C. § 1 *et seq*.

6. This Court has personal jurisdiction over Samsung at least because Samsung conducts business in this District and throughout the state of Texas.

7. This Court also has personal jurisdiction over Samsung because Samsung has committed acts of patent infringement in this District and throughout Texas, including selling, and offering for sale, products and services that infringe Mobility IP's Asserted Patents.

8. This Court also has personal jurisdiction over Samsung because Samsung has placed infringing products and services into the stream of commerce, with the expectation they

[1] Samsung, *Samsung Electronics America to Open Flagship North Texas Campus*, available at https://news.samsung.com/us/samsung-electronics-america-open-flagship-north-texas-campus/ (last visited Feb. 17, 2026).

will be purchased and used by customers in Texas and in this District, such that customers in Texas and in this District have purchased and used, and continue to purchase and use, Samsung's infringing products and services, which has allowed Samsung to derive substantial benefits from infringing acts in Texas and in this District.

9. Venue is proper in this District against Samsung pursuant to 28 U.S.C. §§ 1391 and 1400(b).

10. Venue is proper in this District against Defendant SEC under 28 U.S.C. § 1391(c)(3) because SEC is a foreign corporation that is not a resident of the United States.

11. Venue is proper in this District against Defendant SEA under 28 U.S.C. §§ 1391 and 1400(b) because SEA is subject to the personal jurisdiction of this Court as set forth above, has committed patent infringement in this District, and maintains regular and established places of business in this District, including a "flagship campus" at 6625 Excellence Way, Plano, Texas 75023.

12. Samsung has previously been party to numerous patent cases in this District and has repeatedly availed itself of the power and benefits of this Court and forum by raising counterclaims seeking a declaratory judgment of noninfringement and invalidity.[2]

13. Defendants SEC and SEA are properly joined under 35 U.S.C. § 299(a)(1) because Defendants have committed the accused acts of patent infringement jointly, severally, and in the alternative with respect to or arising out of the same transaction, occurrence, or series of

[2] *See, e.g.*, *Kim v. Samsung Elecs. Co.*, 2-23-cv-00155 (E.D. Tex. Apr. 5, 2023), *Kim v. Samsung Elecs. Co.*, 2-22-cv-00367 (E.D. Tex. Sept. 21, 2022), *Hardin v. Samsung Elecs. Co.*, 2-22-cv-00344 (E.D. Tex. Sept. 2, 2022), *Smith Interface Techs., LLC v. Samsung Elecs. Co.*, 2-22-cv-00290 (E.D. Tex. Jul. 29, 2022), *Emergent Mobile LLC v. Samsung Elecs. Co.*, 2-22-cv-00107 (E.D. Tex. Apr. 8, 2022), *Scramoge Tech. Ltd. v. Samsung Elecs. Co.*, 2-22-cv-00015 (E.D. Tex. Jan. 10, 2022), *Netlist, Inc. v. Samsung Elecs. Co.*, 2-21-cv-00463 (E.D. Tex. Dec. 20, 2021), *KT Imaging USA, LLC v. Samsung Elecs. Co.*, 4-20-cv-00339 (E.D. Tex. Apr. 20, 2020), *Acorn Semi, LLC v. Samsung Elecs. Co.*, 2-19-cv-00347 (E.D. Tex. Oct. 23, 2019), *Dareltech, LLC v. Samsung Elecs. Co.*, 4-18-cv-00702 (E.D. Tex. Oct. 4, 2018), and *MyMail, Ltd. v. Samsung Elecs. Co.*, 2-18-cv-00017 (E.D. Tex. Jan. 19, 2018).

transactions or occurrences relating to the making, using, importing, selling, and/or offering for sale the same accused Samsung products and services. In addition, joinder is proper under 35 U.S.C. § 299(a)(2) because questions of fact common to both Defendants will arise in this action.

FACTUAL BACKGROUND

Mobile-Device Payments

14. Use of mobile devices such as smartphones to pay for goods and services has become an enormous business that continues to grow, with some analysts estimating a total contactless transaction volume of over a trillion dollars annually in the United States.

15. Samsung is one of the largest smartphone manufacturers in the United States and in the world. Samsung's mobile devices enable users to pay at a point of sale ("POS") terminal by confirming their identity via the mobile device, then placing the mobile device close to a near-field communication ("NFC") receiver located at the POS terminal.[3] Using information stored in the mobile device via the Samsung Wallet or Samsung Pay app,[4] the POS terminal can process the payment without requiring the user to physically present a payment card.

16. Because of the convenience and security of payments using mobile devices, the use of mobile devices has grown substantially since the introduction of payments via mobile device. Mobile device payments are convenient because users typically carry their mobile device with them. Mobile device payments are more secure than card payments because a transaction cannot occur unless the user authenticates themselves on the mobile device, which is a form of protection that does not exist with in-person card transactions.

[3] Samsung, *How to use Samsung Wallet and Pay*, https://youtu.be/q-1dNsPJlnw?t=106
[4] Samsung Pay was formerly a separate app but later was integrated into Samsung Wallet. https://www.samsung.com/us/support/owners/app/samsung-wallet (last visited Feb. 17, 2026).

Mobility IP and Its Patented Inventions

17. Well over a decade before Samsung first introduced its mobile payment technology, the inventors of the Asserted Patents began developing the technology at issue in this case.

18. In the early 2000s, Neology, Inc. began applying for patents that embodied the innovations that resulted from innovations in this space. The United States Patent and Trademark Office ("PTO") has since issued numerous patents to Neology, including the '772 Patent, the '807 Patent, the '513 Patent, the '412 Patent, and the '187 Patent. Neology eventually assigned these patents to Mobility IP.

19. In addition, Neology also acquired patents directed to technology involving the use of secure elements to store transaction information that can be later transmitted via near-field communication ("NFC") and other means. These inventions are reflected in the '345 Patent and the '924 Patent. Neology eventually assigned these patents to Mobility IP.

20. Mobility IP is the sole and exclusive owner of all right, title and interest to and in, or is the exclusive licensee with the right to sue for, the Asserted Patents and holds the exclusive right to take all actions necessary to enforce its rights to the Asserted Patents, including the filing of this patent infringement lawsuit. Mobility IP also has the right to recover all damages for past, present, and future infringement of the Asserted Patents and to seek injunctive relief as appropriate under the law.

Samsung's Use of the Patented Technology

21. Samsung markets itself as a leading provider of mobile devices in the United States such as smartphones, tablets, and watches. The ecosystem of Samsung products spans billions of mobile devices. The mobile device products Samsung sells in the United States include at least the following: Samsung Galaxy A Series; Samsung Galaxy Note Series (until 2021); Samsung Galaxy

S Series; Samsung Galaxy Xcover Series; Samsung Galaxy Z Fold Series; the Samsung Galaxy Z Flip Series; Samsung Galaxy Watch Series; and Samsung Galaxy Tab series (referred to collectively as the "Accused Instrumentalities").[5] Each of the mobile device lines includes one or more different models of mobile devices. Throughout this complaint, if an exemplary mobile device is discussed, such as the Samsung Galaxy S23 Ultra,[6] it should be understood that the accusations against the exemplary mobile device are also applicable to all other Samsung mobile devices sold in the United States in the past six years.

22. Near Field Communication ("NFC") can be used to facilitate mobile payments when an NFC-equipped device (such as a smartphone or an electronic wearable like a watch) is placed near a contactless merchant terminal allowing the devices to exchange payment data.

23. Contactless merchant terminal adoption in the U.S. has been expedited by card issuer security requirements. Card issuers in the United States set an October 2015 deadline for merchants to upgrade payment terminals capable of accepting credit cards with embedded chips for security, and many of these upgraded terminals have NFC capability built in. In December 2015, approximately 2.36 million contactless terminals were in service in the United States. As a result of the COVID-19 pandemic, there has been a sharp rise in adoption of contactless payment in the United States and all over the globe. By 2024, public reporting estimates that contactless payments accounted for approximately 25% of all card transactions in the United States.[7]

24. Each of the Accused Instrumentalities include a processor, a secure element, biometric security, a display, a cellular radio, and an NFC radio.

---

[5] https://www.samsung.com/us/business/mobile/phones/; https://tsar3000.com/list-of-all-samsung-galaxy-models-by-series-and-release-date/ (last visited Feb. 17, 2026).
[6] https://www.samsung.com/us/smartphones/galaxy-s23-ultra-lite-no-3-party/ (last visited Feb. 17, 2026).
[7] Clearly Payments, *The Contactless Payments Market Overview in USA for 2024*, https://www.clearlypayments.com/blog/the-contactless-payments-market-overview-in-usa-for-2024/ (last visited Feb. 17, 2026).

25. On September 28, 2015, Samsung launched its Samsung Pay mobile payment service that enabled its users to make a payment—"Users can simply swipe up, scan their fingerprint and pay."[8] The smartphone first authenticates the user using biometrics such as a fingerprint reader or facial recognition. After authentication, the user places smartphone near a POS terminal. The smartphone then transmits transaction information (such as card information) to the POS terminal via NFC to complete the transaction.

26. By making, using, offering to sell, and/or selling the Accused Instrumentalities, Samsung has infringed and is infringing the asserted patents as described in further detail below.

Causes of Action

Count I: Infringement of U.S. Patent No. 8,151,345 ("'345 Patent")

27. All preceding factual allegations above are incorporated as if fully set forth herein.

28. The USPTO duly and legally issued U.S. Patent No. 8,151,345 ("'345 Patent") to C. Douglas Yeager as the named inventor. All right, title, and interest in the '345 Patent have been assigned to Mobility IP.

29. The '345 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

30. Samsung has directly infringed and continues to directly infringe the '345 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '345 Patent. For example, claim 23 of the '345 Patent[9] recites:

[8] Samsung, *Samsung Mobile Payment Service – Samsung Pay, Available Starting Today in the U.S.*, (Sep. 28, 2015), https://news.samsung.com/global/samsung-mobile-payment-service-samsung-pay-available-starting-today-in-the-u-s; *see also* Samsung UK, *How to set-up Samsung Pay on your Galaxy phone,* https://youtu.be/Aw2zbFUIGls?t=28.

[9] Claim 23 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

A cellular network adapter for a cellular network device configured with a cellular network application interface comprising;

a secure element comprising a data file;

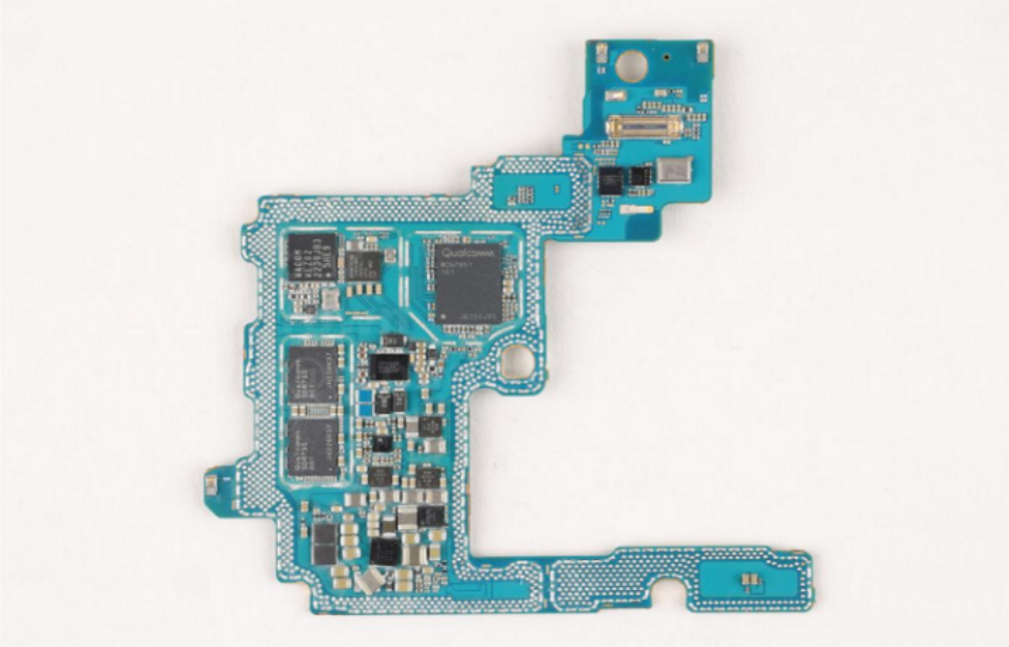
a secure element reader in the cellular network adapter configured to interrogate the secure element by executing file system functions according to ISO 7816-4 and to generate file information from the secure element data file;

a near field communications controller bridge chip to convert the file information to an RF data signal for an external reader; and

a communications controller configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction authorization information and to transmit the transaction authorization information from the cellular network device over a wireless network through the cellular network application interface, wherein the wireless network comprises a cellular network and the secure element reader in the cellular network adapter is configured to await a startup instruction comprising an unpredictable number originating over the cellular wireless network prior to interrogating the secure element.

31. The Accused Instrumentalities meet the recited elements of Claim 23. For example, the Accused Instrumentalities include a secure element. The teardown of an exemplary Samsung Galaxy S23 Ultra is presented below.[10] The motherboard includes a secure element, a near field communications controller bridge chip, and one or more processors that are configured to receive file information from the secure element and to convert the information into transaction authorization information:

[10] *TechInsights Teardown: Samsung Galaxy S23 Ultra*, (Sep. 22, 2023) https://electronics360.globalspec.com/article/20178/techinsights-teardown-samsung-galaxy-s23-ultra



The main board of the Samsung Galaxy S23 Ultra includes the main components that help the phone operate with the cellular connection, Wi-Fi, Bluetooth and more. Source: TechInsights

Main board

The main board includes the heart of the phone with the main applications processor from Qualcomm with an octa-core Snapdragon 8 generation and 8 GB mobile LPDDR5X SDRAM multi-chip memory from Samsung. Other electronic components include:

- 256 GB 3D TLC V-NAND flash and camera power management from Samsung
- NFC and secure element chip, SIM card interface and battery charger from NXP Semiconductors
- Qualcomm 5G RF transceiver and power management IC
- Power management IC from Analog Devices
- Class-D audio amplifier from Cirrus Logic
- Overvoltage protection from ETEK
- OVP load switch from Kinetic Technologies.
- 32-bit ARM Cotex-M0 microcontroller from ST Microelectronics

32. The secure element is used to store electronic payment information.[11] The Accused Instrumentalities follow Europay, Mastercard, and Visa's (EMV's) standards for processing contactless payments.[12]

[11] Samsung Developer, *Samsung eSE SDK*, https://developer.samsung.com/ese/overview.html (last visited Feb. 17, 2026) (describing the "embedded Secure Element (eSE)" of Samsung devices and how they store "payments."); Samsung, *How secure is Samsung Pay*, https://www.samsung.com/uk/support/apps-services/how-secure-is-samsung-pay/ (last visited Feb. 17, 2026) (describing Samsung Pay's use of tokenization to store credit card (transaction) information).

[12] US Payments Forum, *EMV Payment Tokenization Primer and Lessons Learned*, (Jun. 2019), https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf at 24–25; *see also* EMVCo, *EMV Payment Tokenisation: A Guide to Use Cases* (Jan. 16, 2023) at 42–43, found at https://www.emvco.com/emv-technologies/payment-tokenisation/.

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

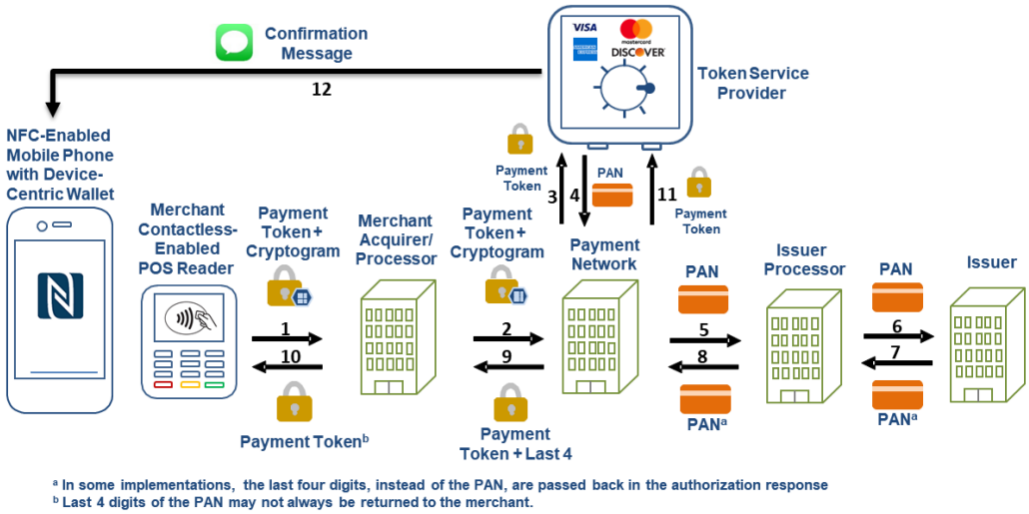


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

33. The cardholder's primary account number (PAN) is sent to a token provider that verifies the card via the card issuer. Once verified, a token known as the Device Account Number is activated and stored in the phone. The Device Account Number is a surrogate that represents the PAN for purposes of payment processing.[13] Thus, the secure element includes a data file.

34. The above-described functionality is initiated by the processor that accessed the transaction information (e.g., the Device Account Number) from the secure element. The information is then combined into a communications data package (the unique cryptogram) based on the transaction information.

35. During a Samsung Pay transaction, the mobile device creates a dynamic cryptogram specific to the transaction. The cryptogram is created using the token (based on the credit card), token key, transaction data, etc. according to the EMV contactless specification.[14] The dynamic cryptogram, token, and other data is transmitted via NFC from the mobile device to the terminal. Each of the Accused Instrumentalities allows the emulation of ISO 7816-4 cards.[15]

36. The Accused Instrumentalities include a communications controller configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction authorization information and to transmit the transaction authorization information from the cellular network device over a wireless network through the cellular network application interface, wherein the wireless network comprises a cellular network and the secure element reader in the cellular network adapter is configured to await a startup instruction comprising an unpredictable number originating over the cellular wireless network prior to interrogating the secure element.

---

[13] *See* EMVCo, *supra*, at 41–42.
[14] US Payments Forum, *supra* at 41.
[15] Android Developers, *Host-based card emulation overview*, https://developer.android.com/develop/connectivity/nfc/hce (last visited Feb. 17, 2026).

37. Samsung committed the infringing activities without a license from Mobility IP. Samsung's acts of infringement have damaged Mobility IP, as owner of the '345 Patent. Mobility IP is entitled to recover from Samsung the damages it has sustained as a result of Samsung's wrongful acts in an amount subject to proof at trial. The infringement of the '345 Patent by Samsung has damaged and will continue to damage Plaintiff.

38. Samsung's infringement of Mobility IP's '345 Patent is willful as of the date of the service of Mobility IP's Original Complaint.

Count II: Infringement of U.S. Patent No. 8,548,924 ("'924 Patent")

39. All preceding factual allegations above are incorporated as if fully set forth herein.

40. The USPTO duly and legally issued U.S. Patent No. 8,548,924 ("'924 Patent") to C. Douglas Yeager as the named inventor. All right, title, and interest in the '924 Patent have been assigned to Mobility IP.

41. The '924 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

42. Samsung has directly infringed and continues to directly infringe the '924 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '924 Patent. For example, claim 60 of the '924 Patent[16] recites:

> A token for transmitting a communications data package to a host device, the token comprising:
>
> a mounting structure;
>
> a secure element affixed to the mounting structure, the secure element including a data file containing transaction information;

[16] Claim 60 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

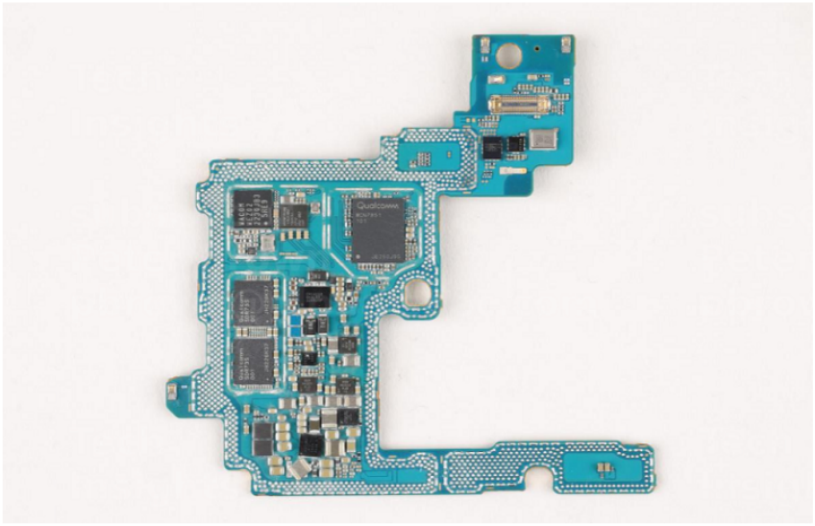
a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator and to generate the communications data package based on the transaction information; and

a communications controller affixed to the mounting structure and configured to receive the communications data package from the secure element interrogator and to transmit the communications data package to the host device.

43. The Accused Instrumentalities meet the recited elements of claim 60.

44. For example, the Accused Instrumentalities include a mounting structure and a secure element affixed to the mounting structure. The teardown of an exemplary Samsung Galaxy S23 Ultra is presented below.[17] The motherboard includes a mounting structure, a secure element, a secure element interrogator, and a communications controller that is configured to interrogate the secure element to acquire transaction information and generate a communications package and further configured to transmit a communications data package to a host device.

[17] TechInsights Teardown, *supra*.



The main board of the Samsung Galaxy S23 Ultra includes the main components that help the phone operate with the cellular connection, Wi-Fi, Bluetooth and more. Source: TechInsights

Main board

The main board includes the heart of the phone with the main applications processor from Qualcomm with an octa-core Snapdragon 8 generation and 8 GB mobile LPDDR5X SDRAM multi-chip memory from Samsung. Other electronic components include:

- 256 GB 3D TLC V-NAND flash and camera power management from Samsung
- NFC and secure element chip, SIM card interface and battery charger from NXP Semiconductors
- Qualcomm 5G RF transceiver and power management IC
- Power management IC from Analog Devices
- Class-D audio amplifier from Cirrus Logic
- Overvoltage protection from ETEK
- OVP load switch from Kinetic Technologies.
- 32-bit ARM Cotex-M0 microcontroller from ST Microelectronics

45. The secure element is used to store electronic payment information.[18] The Accused Instrumentalities follow EMV's standards for processing contactless payments.[19]

[18] Samsung Developer, *supra* (describing the "embedded Secure Element (eSE)" of Samsung devices and how they store "payments."); *How secure is Samsung Pay*, *supra* (describing Samsung Pay's use of tokenization to store credit card (transaction) information).

[19] https://www.uspaymentsforum.org/wp-content/uploads/2019/06/EMV-Payment-Tokenization-Primer-Lessons-Learned-FINAL-June-2019.pdf at 24–25; *see also* EMV Payment Tokenisation, *A Guide to Use Cases* (Jan. 2023) at 42–43, found at https://www.emvco.com/emv-technologies/payment-tokenisation/.

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

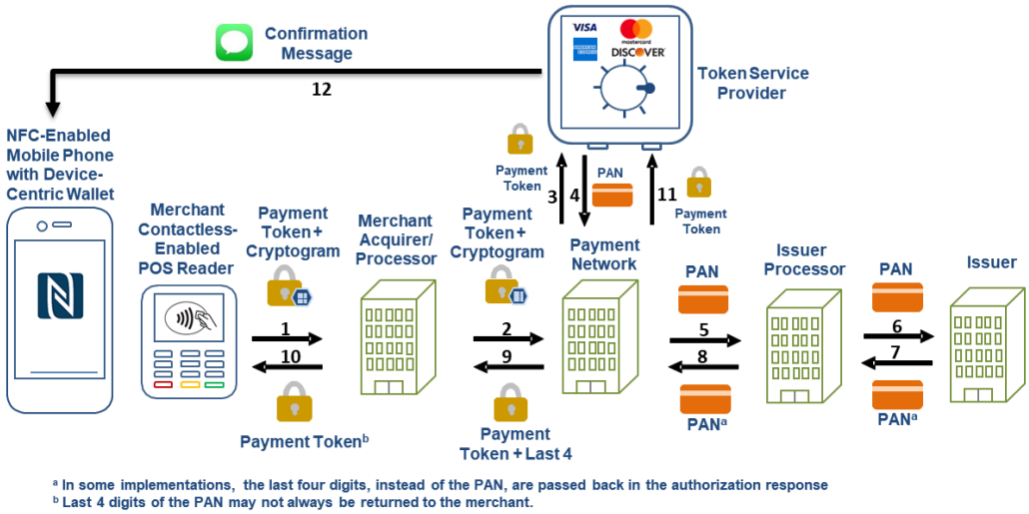


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

46. The cardholder's primary account number (PAN) is sent to a token provider that verifies the card via the card issuer. Once verified, a token known as the Device Account Number is activated and stored in the phone. The Device Account Number is a surrogate that represents the PAN for purposes of payment processing.[20] Thus, the secure element includes a data file containing transaction information.

47. The above-described functionality is initiated by the processor that accessed the transaction information (e.g., the Device Account Number) from the secure element. The information is then combined into a communications data package (the unique cryptogram) based on the transaction information. During a Samsung Pay transaction, the mobile device creates a dynamic cryptogram specific to the transaction. The cryptogram is created using the token (based on the credit card), token key, transaction amount, etc. according to the EMV contactless specification.[21] The dynamic cryptogram, token, and other data is transmitted via NFC from the mobile device to the terminal. Thus, the communications data package is based on the transaction information.

48. The communications data package is created and transmitted to the host device. The processor is used to perform such functionality.

49. Samsung committed the infringing activities without license from Mobility IP. Samsung's acts of infringement have damaged Mobility IP, as owner of the '924 Patent. Mobility IP is entitled to recover from Samsung the damages it has sustained as a result of Samsung's wrongful acts in an amount subject to proof at trial. The infringement of the '924 Patent by Samsung has damaged and will continue to damage Plaintiff.

[20] *See* EMVCo., *supra* at 41–42.
[21] US Payments Forum, *supra* at 41.

50. Samsung's infringement of Mobility IP's '924 Patent is willful as of the date of the service of Mobility IP's Original Complaint.

Count III: Infringement of U.S. Patent No. 8,766,772

51. All preceding factual allegations are incorporated as if fully set forth herein.

52. The USPTO duly and legally issued U.S. Patent No. 8,766,772 ("'772 Patent") to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the '772 Patent have been assigned to Mobility IP.

53. The '772 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

54. Samsung has directly infringed the '772 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '772 Patent. For example, Claim 9 of the '772 Patent[22] recites:

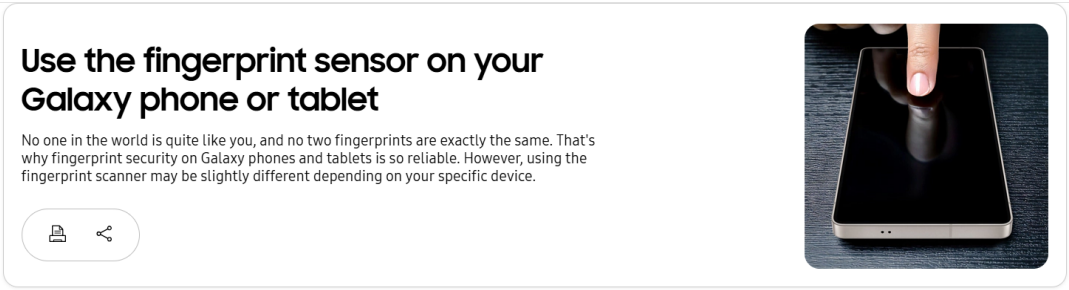
> A mobile device, comprising:
>
> a biometric input device configured to receive biometric data; and
>
> a radio frequency antenna and a chip, the chip comprising:
>
> > a memory, the memory configured to store transaction information and biometric information for identifying an individual associated with the transaction, and
> >
> > a processor coupled with the memory and the biometric input, the processor configured to:
> >
> > > receive a signal via the radio frequency antenna, the signal comprising a request to access the memory and retrieve the transaction information,
> > >
> > > receive biometric information from the biometric input device,
> > >
> > > compare the received biometric information with the biometric information stored in the memory, and

[22] Claim 9 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

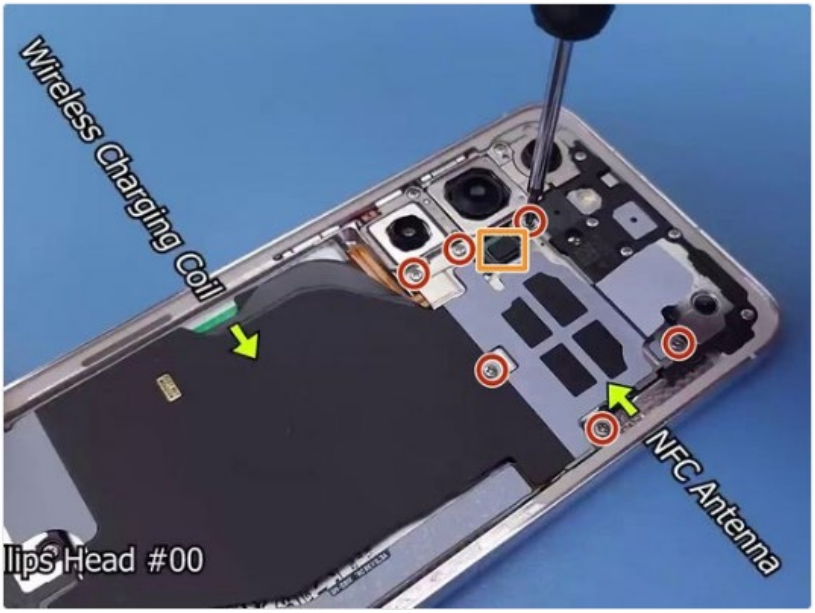
provide the transaction information in response to the access request when the biometric information matches.

The Accused Instrumentalities meet the recited elements of Claim 9.

55. For instance, Samsung's mobile devices include a biometric input device such as a fingerprint sensor:[23]

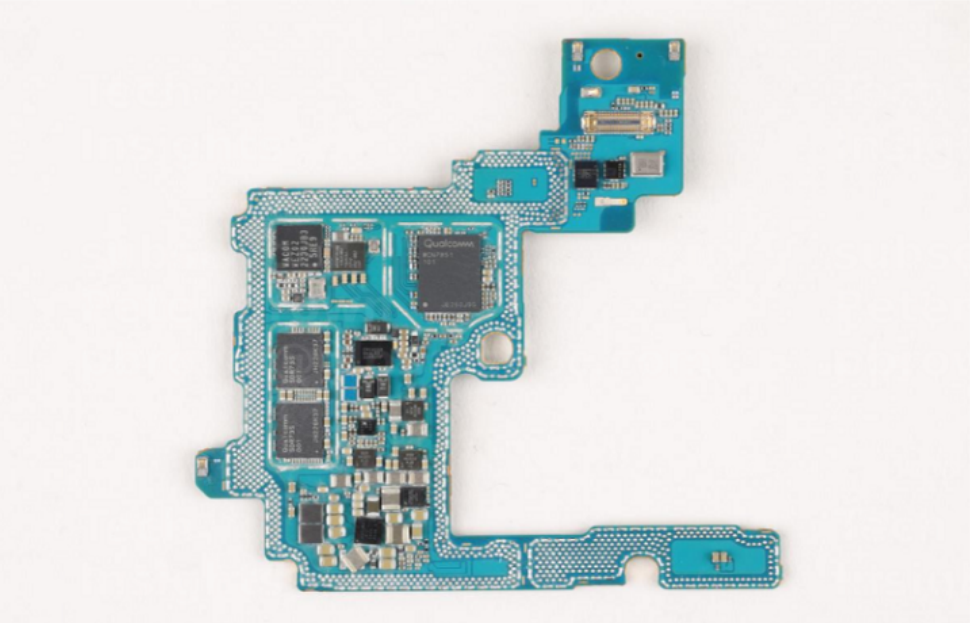


56. The Accused Instrumentalities include a radio frequency antenna. For example, the Accused Instrumentalities include NFC technology that includes an antenna configured to communicate via NFC, which utilizes radio frequency.[24]



[23] Samsung, *Use the fingerprint sensor on your Galaxy phone of tablet*, https://www.samsung.com/us/support/answer/ANS10001613/ (last visited Feb. 17, 2026).
[24] iFixit, *Galaxy S23 Teardown*, https://www.ifixit.com/Teardown/Galaxy+S23+Teardown/158006 (last visited Feb. 17, 2026).

57. The Accused Instrumentalities include a chip. For illustrative purposes, the main board of a Samsung Galaxy S23 Ultra is illustrated below.[25] The main board includes multiple chips.



The main board of the Samsung Galaxy S23 Ultra includes the main components that help the phone operate with the cellular connection, Wi-Fi, Bluetooth and more. Source: TechInsights

Main board

The main board includes the heart of the phone with the main applications processor from Qualcomm with an octa-core Snapdragon 8 generation and 8 GB mobile LPDDR5X SDRAM multi-chip memory from Samsung. Other electronic components include:

- 256 GB 3D TLC V-NAND flash and camera power management from Samsung
- NFC and secure element chip, SIM card interface and battery charger from NXP Semiconductors
- Qualcomm 5G RF transceiver and power management IC
- Power management IC from Analog Devices
- Class-D audio amplifier from Cirrus Logic
- Overvoltage protection from ETEK
- OVP load switch from Kinetic Technologies.
- 32-bit ARM Cotex-M0 microcontroller from ST Microelectronics

58. The Accused Instrumentalities include a memory. The memory is configured to store transaction information and biometric information for identifying an individual associated

[25] TechInsights Teardown, *supra*.

with the transaction. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.[26]

MEMORY	Card slot	No
	Internal	256GB 8GB RAM, 256GB 12GB RAM, 512GB 12GB RAM, 1TB 12GB RAM
		UFS 4.0

59. The memory is used to store fingerprint information and transaction information. The Accused Instrumentalities store sensitive data such as biometric authentication information and transaction information in a variety of different ways. For example, Samsung's Knox Vault can be used to store biometric authentication information.[27] Fingerprint biometrics may be stored in a Trusted Execution Environment (TEE).[28] Such information is "encrypted and stored in a separate part of the smartphone, completely inaccessible to the regular operating system."[29] A secure element may also be used to store card information.[30]

60. The Accused Instrumentalities include a processor coupled with the memory and the biometric input. For example, the Samsung Galaxy S23 Ultra has a Qualcomm Snapdragon 8 Gen 2 CPU:[31]

PLATFORM	OS	Android 13, up to 4 major Android upgrades, One UI 6.1.1
	Chipset	Qualcomm SM8550-AC Snapdragon 8 Gen 2 (4 nm)
	CPU	Octa-core (1x3.36 GHz Cortex-X3 & 2x2.8 GHz Cortex-A715 & 2x2.8 GHz Cortex-A710 & 3x2.0 GHz Cortex-A510)
	GPU	Adreno 740

[26] GSMArena, *Samsung Galaxy S23 Ultra*, https://www.gsmarena.com/samsung_galaxy_s23_ultra-12024.php (last visited Feb. 17, 2026).
[27] Samsung Knox Documentation, *Knox Vault*, https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-mobile-security/system-security/knox-vault/ (last visited Feb. 17, 2026)
[28] Samsung Knox, *Using biometrics for authentication in Android*, (Sep. 18, 2020) https://www.samsungknox.com/en/blog/using-biometrics-for-authentication-in-android
[29] *Id*.
[30] *Samsung eSE SDK*, *supra* (describing the "embedded Secure Element (eSE)" of Samsung devices and how they store "payments."); *How secure is Samsung Pay*, *supra* (describing Samsung Pay's use of tokenization to store credit card (transaction) information).
[31] GSMArena, *supra*.

61. In the Accused Instrumentalities, the processor is configured to receive a signal via the radio frequency antenna, the signal comprising a request to access the memory and retrieve the transaction information. For example, the Accused Instrumentalities follow EMV's standards for processing contactless payments.[32]

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

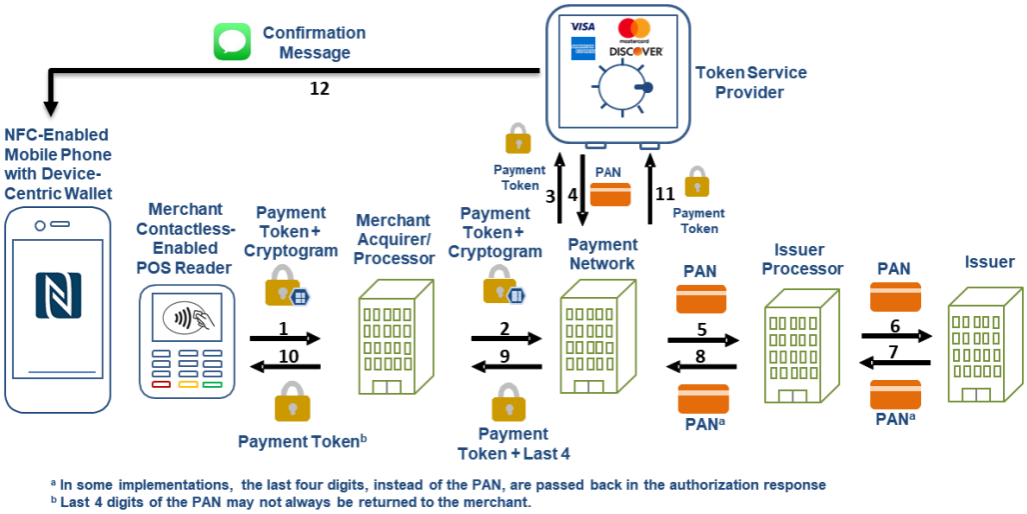


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

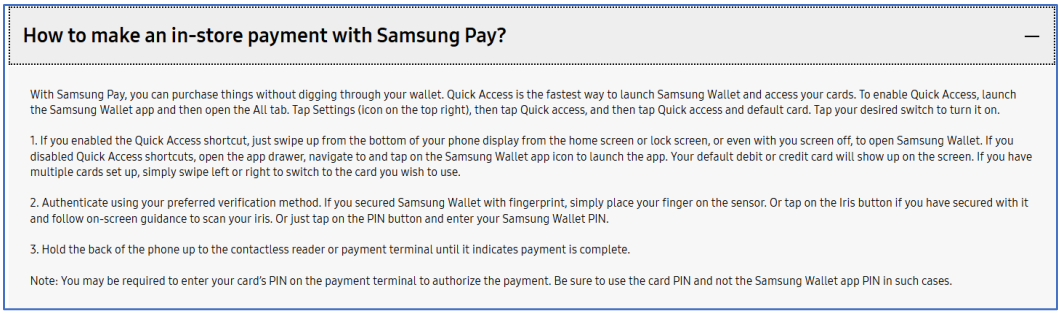
[32] US Payments Forum, *supra* at 24–25; *see also* EMVCo., *supra* at 42–43.

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

62. During a transaction, as exemplarily illustrated above, the user places the cellular phone in proximity to the NFC reader in the POS terminal. As part of the process, the POS terminal sends a signal to the user's cellular phone—"One device (usually the NFC reader) generates an electromagnetic field to establish a connection."[33]

63. In the Accused Instrumentalities, the processor is configured to receive biometric information from the biometric input device. The user authenticates himself/herself using biometric information, such as through the use of a fingerprint sensor.[34]

[33] Katie Nelson, *What is NFC and How Does it Work?*, Lightspeed (Jun. 5, 2025) https://www.lightspeedhq.com/blog/near-field-communication-payments-explained/.
[34] Samsung, *Samsung Wallet FAQ*, https://www.samsung.com/us/apps/samsung-wallet/faq/ (last visited Feb. 17, 2026).



64. In the Accused Instrumentalities, the processor is configured to provide the transaction information in response to the access request when the biometric information matches. For example, after the Accused Instrumentality authenticates the user, the user places the Accused Instrumentality "up to the contactless reader or payment terminal" to provide the transaction information. After the user is authenticated, the process follows the EMV standard for processing contactless payments, illustrated below. This includes providing the transaction information in response to the transaction request when the biometric information matches.[35]

[35] US Payments Forum, *supra* at 24–25.

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

65. Samsung committed the infringing activities without license from Mobility IP. Samsung's acts of infringement have damaged Mobility IP, as owner of the '772 Patent. Mobility IP is entitled to recover from Samsung the damages it has sustained as a result of Samsung's wrongful acts in an amount subject to proof at trial. The infringement of the '772 Patent by Samsung has damaged Plaintiff.

66. Samsung's infringement of Mobility IP's '772 Patent was willful. Samsung was aware of the '772 Patent since at least October 25, 2016, when Samsung filed Patent Application No. US 15/333,343.[36] In its initial Information Disclosure Statement in support of the '343 Application, Samsung cited the '772 Patent as one of only three prior art United States Patents

[36] Filed on October 25, 2016. Issued as U.S. Patent 10,404,695 on September 3, 2019.

disclosed by Samsung. Despite this familiarity with the '772 Patent, Samsung practiced the invention of the '772 Patent through the Accused Instrumentalities.

Count IV: Infringement of U.S. Patent No. 8,933,807

67. All preceding factual allegations are incorporated as if fully set forth herein.

68. The USPTO duly and legally issued U.S. Patent No. 8,933,807 ("'807 Patent") to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the '807 Patent have been assigned to Mobility IP.

69. The '807 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

70. Samsung has directly infringed the '807 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '807 Patent. For example, claim 1 of the '807 Patent[37] recites:

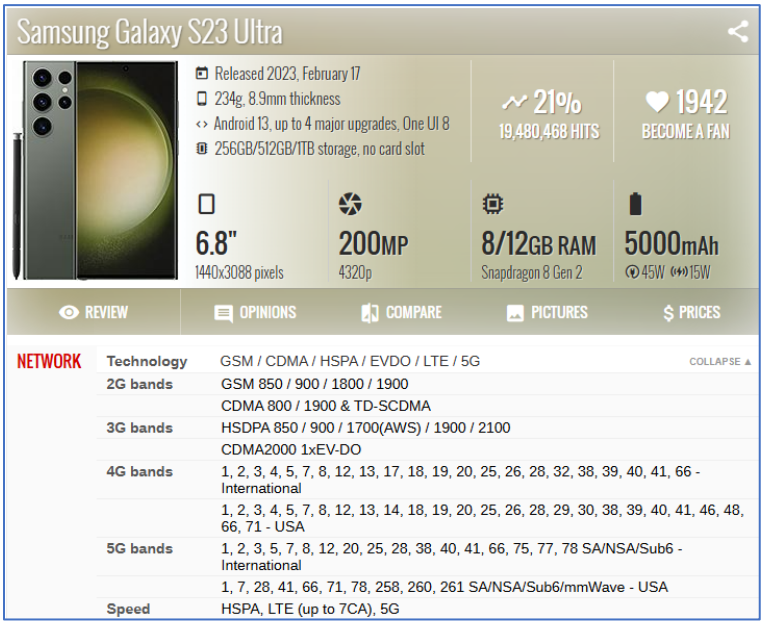
> A mobile device, comprising:
>
> > Radio Frequency (RF) cellular circuitry;
> >
> > short range RF circuitry;
> >
> > memory configured to store biometric authentication information and transaction information, wherein the biometric authentication information has been previously associated with the transaction information;
> >
> > a biometric reading device configured to read biometric information;
> >
> > an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory; and

[37] Claim 1 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

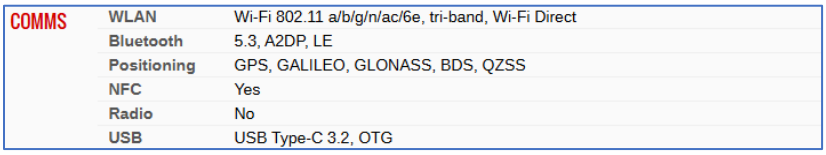
a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication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

71. The Accused Instrumentalities meet the recited elements of the claimed mobile device of claim 1.

72. Samsung's mobile devices include radio frequency cellular circuitry that allows access to various cellular networks. For example, the Galaxy S23 Ultra contains the following cellular radio technology:[38]



73. The Accused Instrumentalities include short-range RF circuitry. For example, the Accused Instrumentalities include NFC technology that includes an antenna configured to communicate via NFC, which is a short-range technology that utilizes radio frequency.[39]



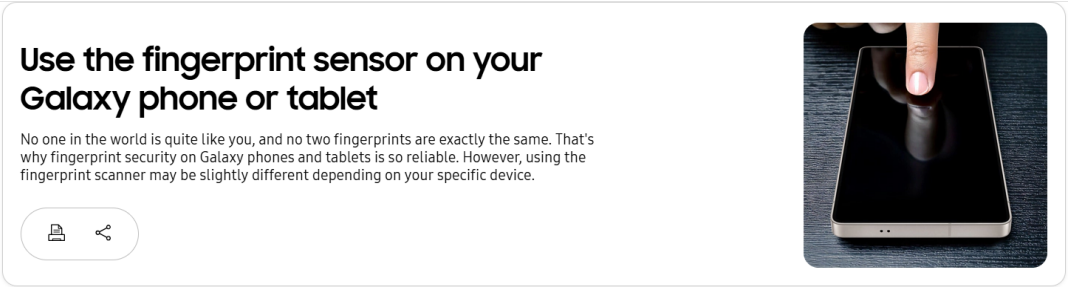
[38] GSMArena, *supra*.
[39] *Id*.

74. The Accused Instrumentalities include a memory. The memory is configured to store transaction information and biometric information. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.[40]

MEMORY	Card slot	No
	Internal	256GB 8GB RAM, 256GB 12GB RAM, 512GB 12GB RAM, 1TB 12GB RAM
		UFS 4.0

75. The memory is used to store fingerprint information and transaction information. The Accused Instrumentalities store sensitive data such as biometric authentication information and transaction information in a variety of different ways. For example, Samsung's Knox Vault can be used to store biometric authentication information.[41] Fingerprint biometrics may be stored in a Trusted Execution Environment (TEE).[42] Such information is "encrypted and stored in a separate part of the smartphone, completely inaccessible to the regular operating system."[43] A secure element may also be used to store card information.[44]

76. Samsung's mobile devices include a biometric reading device such as a fingerprint sensor:



[40] *Id*.
[41] Samsung Knox Documentation, *supra*.
[42] Samsung Knox, *supra*.
[43] *Id*.
[44] *Samsung eSE SDK*, *supra* (describing the "embedded Secure Element (eSE)" of Samsung devices and how they store "payments."); *How secure is Samsung Pay*, *supra* (describing Samsung Pay's use of tokenization to store credit card (transaction) information).

77. The Accused Instrumentalities include an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information based at least in part on the biometric authentication information stored in memory. For example, the devices include one or more processors that can authenticate biometric information. For example, the Samsung Galaxy S23 Ultra has a Qualcomm Snapdragon 8 Gen 2 CPU:

PLATFORM	OS	Android 13, up to 4 major Android upgrades, One UI 6.1.1
	Chipset	Qualcomm SM8550-AC Snapdragon 8 Gen 2 (4 nm)
	CPU	Octa-core (1x3.36 GHz Cortex-X3 & 2x2.8 GHz Cortex-A715 & 2x2.8 GHz Cortex-A710 & 3x2.0 GHz Cortex-A510)
	GPU	Adreno 740

78. The Accused Instrumentalities include a transaction module configured to provide the transaction information via the short-range RF circuitry for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated as being associated with the transaction information by the authentication module. For example, the Accused Instrumentalities follow EMV's standards for processing contactless payments.[45]

[45] US Payments Forum, *supra* at 24–25; *see also* EMVCo., *supra* at 42–43.

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

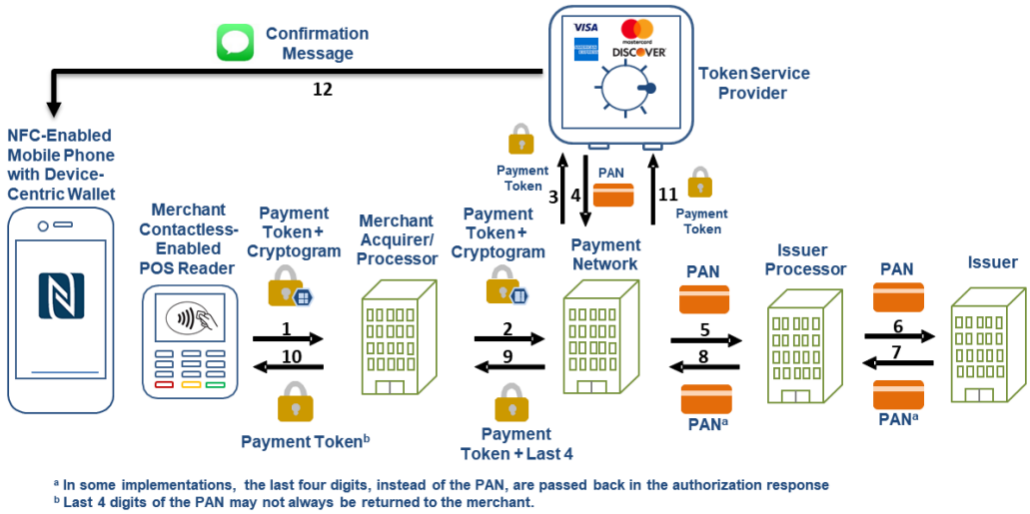


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

79. During a transaction, as illustrated exemplarily above, the user places the cellular phone in proximity to the NFC reader in the POS terminal. As part of the process, the POS terminal sends a signal to the user's cellular phone—"One device (usually the NFC reader) generates an electromagnetic field to establish a connection."[46]

80. Samsung committed the infringing activities without license from Mobility IP. Samsung's acts of infringement have damaged Mobility IP, as owner of the '807 Patent. Mobility IP is entitled to recover from Samsung the damages it has sustained as a result of Samsung's wrongful acts in an amount subject to proof at trial. The infringement of the '807 Patent by Samsung has damaged Plaintiff.

Count V: Infringement of U.S. Patent No. 10,235,513

81. All preceding factual allegations are incorporated as if fully set forth herein.

82. The USPTO duly and legally issued U.S. Patent No. 10,235,513 ("'513 Patent") to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the '513 Patent have been assigned to Mobility IP.

83. The '513 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

84. Samsung has directly infringed the '513 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '513 Patent. For example, Claim 1 of the '513 Patent[47] recites:

A mobile device, comprising:

[46] Nelson, *supra*.

[47] Claim 1 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

a biometric input device configured to receive biometric data;

a short range radio frequency circuit;

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

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

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

receive the biometric data from the biometric input device,

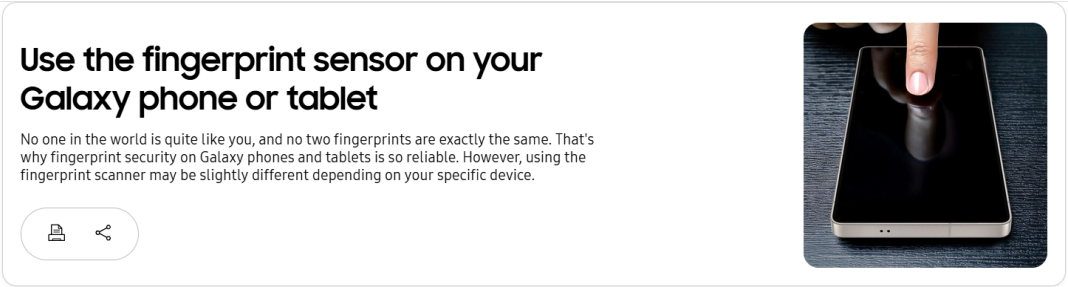
compare the received biometric data with the biometric information stored in the memory, and

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

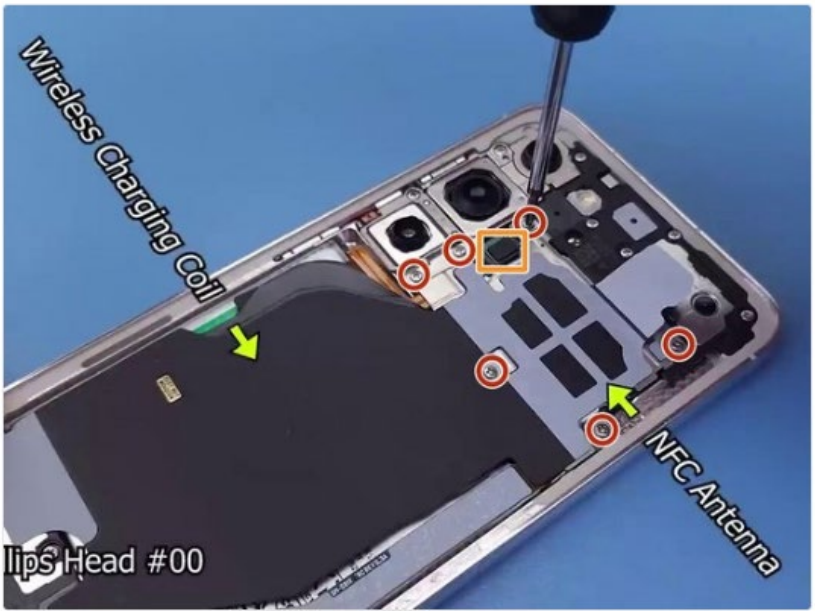
a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor.

85. The Accused Instrumentalities meet the recited elements of Claim 1.

86. Samsung's Accused Instrumentalities include a fingerprint scanner (which qualifies as a biometric reading device) configured to receive biometric data:



87. The Accused Instrumentalities include a short-range radio frequency circuit. For example, the Accused Instrumentalities include NFC technology that includes an antenna configured to communicate via NFC, which utilizes radio frequency.



88. The Accused Instrumentalities include a memory. The memory is configured to store transaction information and fingerprint information. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.

MEMORY	Card slot	No
	Internal	256GB 8GB RAM, 256GB 12GB RAM, 512GB 12GB RAM, 1TB 12GB RAM
		UFS 4.0

89. The memory is used to store biometric information and transaction information. The Accused Instrumentalities store sensitive data such as biometric information and transaction information in a variety of different ways. For example, Samsung's Knox Vault can be used to store biometric information.[48] Fingerprint biometrics may be stored in a Trusted Execution Environment (TEE).[49] Such information is "encrypted and stored in a separate part of the smartphone, completely inaccessible to the regular operating system."[50] A secure element may also be used to store card information.[51]

[48] Samsung Knox Documentation, *supra*
[49] Samsung Knox, *supra*.
[50] *Id*.
[51] *Samsung eSE SDK*, *supra*; *How secure is Samsung Pay*, *supra*.

90. The Accused Instrumentalities include a processor. The processor is coupled with the memory and fingerprint scanner. For example, the devices include one or more processors. For example, the Samsung Galaxy S23 Ultra has a Qualcomm Snapdragon 8 Gen 2 CPU:

PLATFORM	OS	Android 13, up to 4 major Android upgrades, One UI 6.1.1
	Chipset	Qualcomm SM8550-AC Snapdragon 8 Gen 2 (4 nm)
	CPU	Octa-core (1x3.36 GHz Cortex-X3 & 2x2.8 GHz Cortex-A715 & 2x2.8 GHz Cortex-A710 & 3x2.0 GHz Cortex-A510)
	GPU	Adreno 740

91. The processor is configured to receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information. The processor is also configured to receive the fingerprint data from the fingerprint scanner and compare the received fingerprint data with the fingerprint information stored in the memory. The processor is further configured to transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received fingerprint data matches the stored fingerprint information.

92. For example, the Accused Instrumentalities follow EMV's standards for processing contactless payments.[52]

[52] US Payments Forum, *supra* at 24–25; *see also* EMVCo, *supra* at 42–43.

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

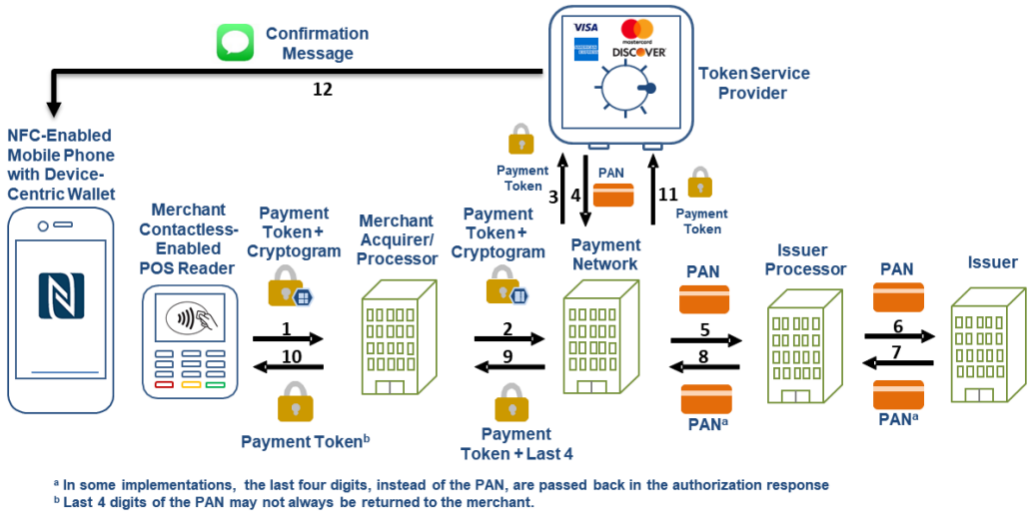
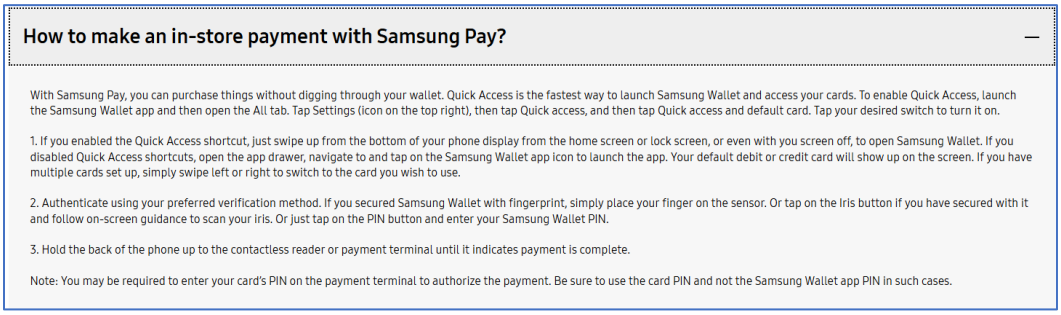


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

93. During a transaction, as exemplarily illustrated above, the user places the cellular phone in proximity to the NFC reader in the POS terminal, the cellular phone transmits transaction information, and as part of the process, the POS terminal sends a signal that is received by the user's cellular phone—"One device (usually the NFC reader) generates an electromagnetic field to establish a connection."[53]

94. In the Accused Instrumentalities, the user authenticates himself/herself using biometric information, such as through the use of a fingerprint sensor.[54]



95. The Accused Instrumentalities include a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor. This can be seen in a teardown of an exemplary Accused Instrumentality, such as the Samsung Galaxy S23 Ultra.[55]

96. Samsung committed the infringing activities without license from Mobility IP. Samsung's acts of infringement have damaged Mobility IP, as owner of the '513 Patent. Mobility IP is entitled to recover from Samsung the damages it has sustained as a result of Samsung's wrongful acts in an amount subject to proof at trial. The infringement of the '513 Patent by Samsung has damaged Plaintiff.

Count VI: Infringement of U.S. Patent No. 10,706,412

[53] Nelson, *supra*.
[54] *Samsung Wallet FAQ*, *supra*.
[55] PBKreviews, *Samsung Galaxy S23 Ultra Teardown Disassembly Repair Video Review*, (Feb. 8, 2023), https://youtu.be/6KV7rQrSJZQ

97. All preceding factual allegations are incorporated as if fully set forth herein.

98. The USPTO duly and legally issued U.S. Patent No. 10,706,412 ("'412 Patent") to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the '412 Patent have been assigned to Mobility IP.

99. The '412 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

100. Samsung has directly infringed the '412 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '412 Patent. For example, Claim 1 of the '412 Patent[56] recites:

> 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:
> >
> > > 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,

[56] Claim 1 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

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,

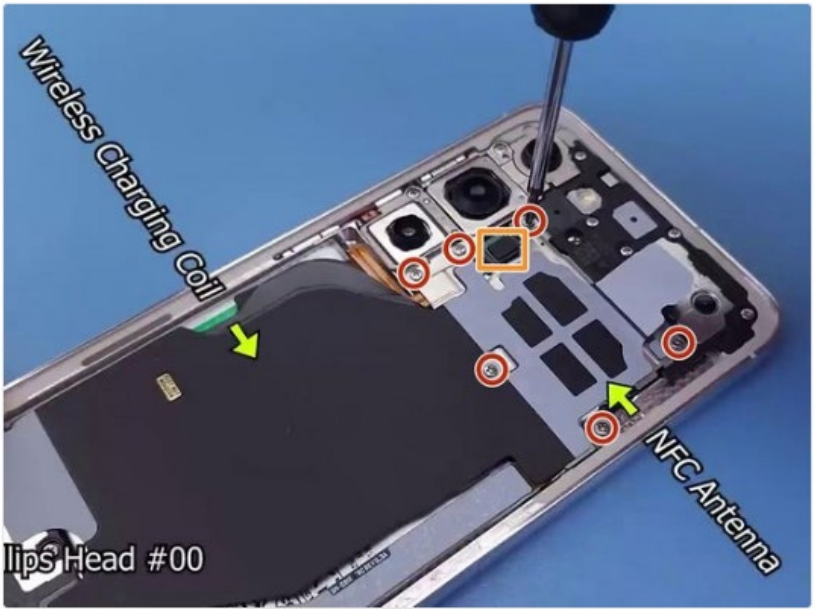
in response to the authentication, generating a key,

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.

101. The Accused Instrumentalities meet the recited elements of Claim 1.

102. The Accused Instrumentalities include a short-range radio frequency circuit. For example, the Accused Instrumentalities include NFC technology that includes an antenna configured to communicate via NFC, which utilizes radio frequency.

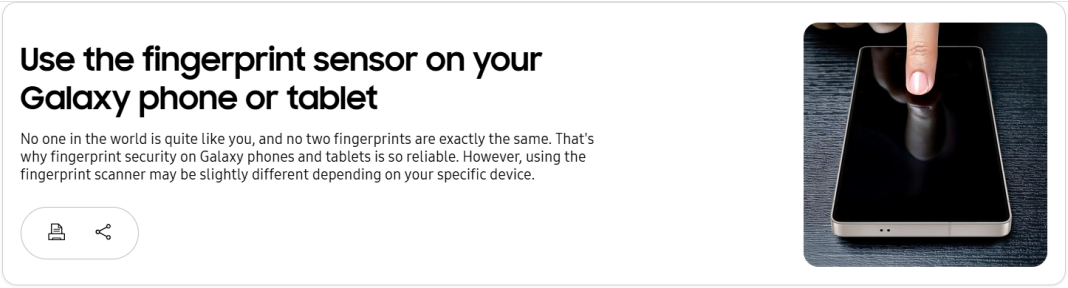


103. The Accused Instrumentalities include a memory. The memory is configured to store transaction information and fingerprint information. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.

MEMORY	Card slot	No
	Internal	256GB 8GB RAM, 256GB 12GB RAM, 512GB 12GB RAM, 1TB 12GB RAM
		UFS 4.0

104. The memory is used to store fingerprint information and transaction information. The Accused Instrumentalities store sensitive data such as biometric authentication information and transaction information in a variety of different ways. For example, Samsung's Knox Vault can be used to store biometric authentication information.[57] Fingerprint biometrics may be stored in a Trusted Execution Environment (TEE).[58] Such information is "encrypted and stored in a separate part of the smartphone, completely inaccessible to the regular operating system."[59] A secure element may also be used to store card information.[60]

105. Samsung's Accused Instrumentalities include a biometric reading device, such as a fingerprint scanner configured to receive fingerprint data:



106. The Accused Instrumentalities include one or more processors that are coupled with the memory, short-range RF circuitry, and the biometric reading device. For example, the Samsung Galaxy S23 Ultra has a Qualcomm Snapdragon 8 Gen 2 CPU:

PLATFORM	OS	Android 13, up to 4 major Android upgrades, One UI 6.1.1
	Chipset	Qualcomm SM8550-AC Snapdragon 8 Gen 2 (4 nm)
	CPU	Octa-core (1x3.36 GHz Cortex-X3 & 2x2.8 GHz Cortex-A715 & 2x2.8 GHz Cortex-A710 & 3x2.0 GHz Cortex-A510)
	GPU	Adreno 740

[57] Samsung Knox Documentation, *supra*.
[58] Samsung Knox, *supra*.
[59] *Id*.
[60] *Samsung eSE SDK*, *supra* (describing the "embedded Secure Element (eSE)" of Samsung devices and how they store "payments."); https://www.samsung.com/uk/support/apps-services/how-secure-is-samsung-pay/ (describing Samsung Pay's use of tokenization to store credit card (transaction) information).

107. The processor is configured to establish a connection with a point of sale (POS) device, via the short-range RF circuitry to conduct a secure transaction between the mobile device and the POS device. For example, the Accused Instrumentalities follow EMV's standards for processing contactless payments.[61]

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

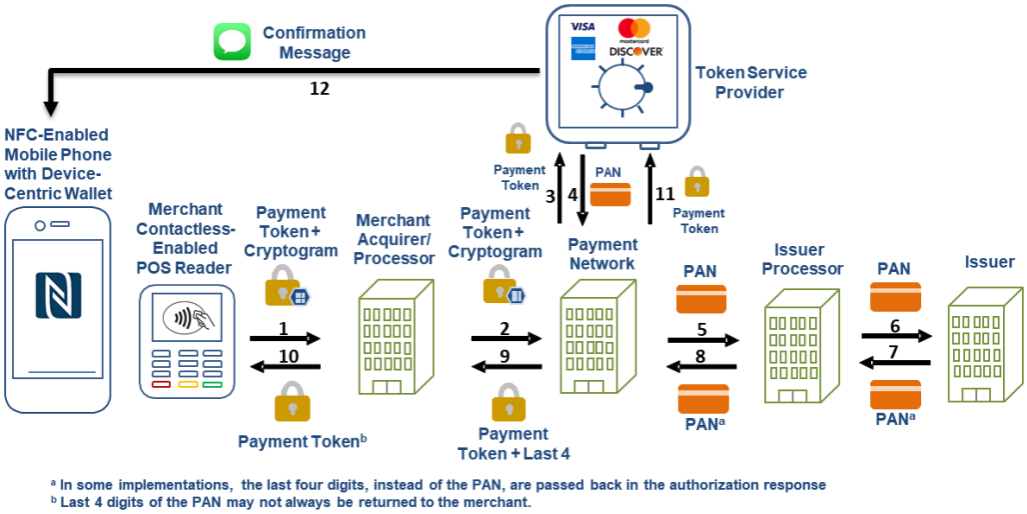


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

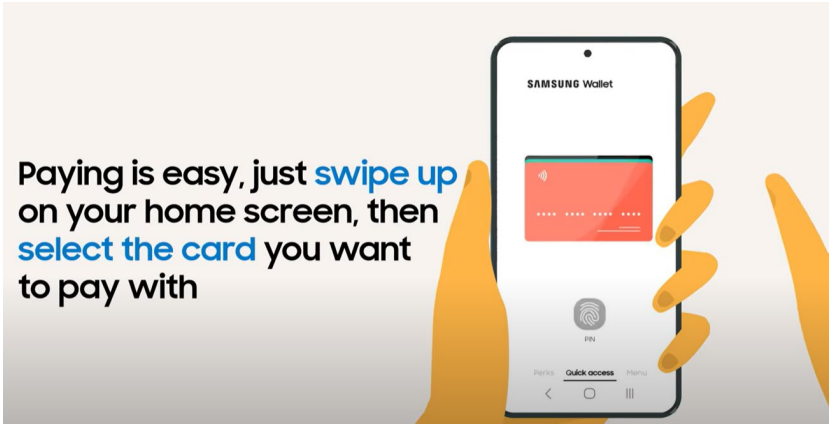
[61] US Payments Forum, *supra* at 24–25; *see also* EMVCo, *supra* at 42–43.

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

108. During a transaction, as illustrated above for example, the user places the cellular phone in proximity to the NFC reader in the POS terminal, the cellular phone transmits transaction information, and as part of the process, the POS terminal sends a signal that is received by the user's cellular phone—"One device (usually the NFC reader) generates an electromagnetic field to establish a connection."[62]

109. The processor is configured to prompt the user to provide biometric information to the biometric reading device.[63]

[62] Nelson, *supra*.
[63] Samsung UK, *How to set-up Samsung Pay on your Galaxy phone*, (Nov. 18, 2022) https://youtu.be/Aw2zbFUIGls?t=28; MK Loves Tech, *How to Use Samsung Wallet– Add Cards and Pay in Store*, (Jul. 3, 2024), https://youtu.be/ZDNh-gBhLvQ?t=154.



110. In the Accused Instrumentalities, the user authenticates himself/herself using biometric information, such as through the use of a fingerprint sensor.[64]

How to make an in-store payment with Samsung Pay?

With Samsung Pay, you can purchase things without digging through your wallet. Quick Access is the fastest way to launch Samsung Wallet and access your cards. To enable Quick Access, launch the Samsung Wallet app and then open the All tab. Tap Settings (icon on the top right), then tap Quick access, and then tap Quick access and default card. Tap your desired switch to turn it on.

1. If you enabled the Quick Access shortcut, just swipe up from the bottom of your phone display from the home screen or lock screen, or even with you screen off, to open Samsung Wallet. If you disabled Quick Access shortcuts, open the app drawer, navigate to and tap on the Samsung Wallet app icon to launch the app. Your default debit or credit card will show up on the screen. If you have multiple cards set up, simply swipe left or right to switch to the card you wish to use.

2. Authenticate using your preferred verification method. If you secured Samsung Wallet with fingerprint, simply place your finger on the sensor. Or tap on the Iris button if you have secured with it and follow on-screen guidance to scan your iris. Or just tap on the PIN button and enter your Samsung Wallet PIN.

3. Hold the back of the phone up to the contactless reader or payment terminal until it indicates payment is complete.

Note: You may be required to enter your card's PIN on the payment terminal to authorize the payment. Be sure to use the card PIN and not the Samsung Wallet app PIN in such cases.

[64] *Samsung Wallet FAQ*, *supra*.

111. In the Accused Instrumentalities, the Accused Instrumentalities generate a key. For example, the EMV standard described above involves the generation of a cryptogram after authentication. A cryptogram (also known as a token cryptogram or a "transaction specific dynamic security code") is a secure code generated during a transaction that verifies the transaction and helps prevent fraud. The payment network validates the cryptogram and de-tokenizes the token to determine the PAN, which is then processed by the payment network. Thus, the cryptogram acts as a key to the transaction.

112. In the Accused Instrumentalities, the processor is configured to secure the payment information stored in the memory. The Accused Instrumentalities use a secure element to store card information.[65]

113. In the Accused Instrumentalities, the processor is configured to transmit to the POS device, via the short-range RF circuitry, the key and the secured payment information for use in the secure transaction. For example, as described above, the EMV standard involves transmitting the cryptogram and the secured payment information from the Accused Instrumentality to the POS device.

114. Samsung committed the infringing activities without license from Mobility IP. Samsung's acts of infringement have damaged Mobility IP, as owner of the '412 Patent. Mobility IP is entitled to recover from Samsung the damages it has sustained as a result of Samsung's wrongful acts in an amount subject to proof at trial. The infringement of the '412 Patent by Samsung has damaged Plaintiff.

Count VII: Infringement of U.S. Patent No. 10,762,187

[65] Samsung Developer, *supra* (describing the "embedded Secure Element (eSE)" of Samsung devices and how they store "payments."); *How secure is Samsung Pay*, *supra* (describing Samsung Pay's use of tokenization to store credit card (transaction) information).

115. All preceding factual allegations are incorporated as if fully set forth herein.

116. The USPTO duly and legally issued U.S. Patent No. 10,762,187 ("'187 Patent") to Mr. Franciso Martinez de Velasco Cortina and Mr. Manfred Rietzler as named inventors. All right, title, and interest in the '187 Patent have been assigned to Mobility IP.

117. The '187 Patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code.

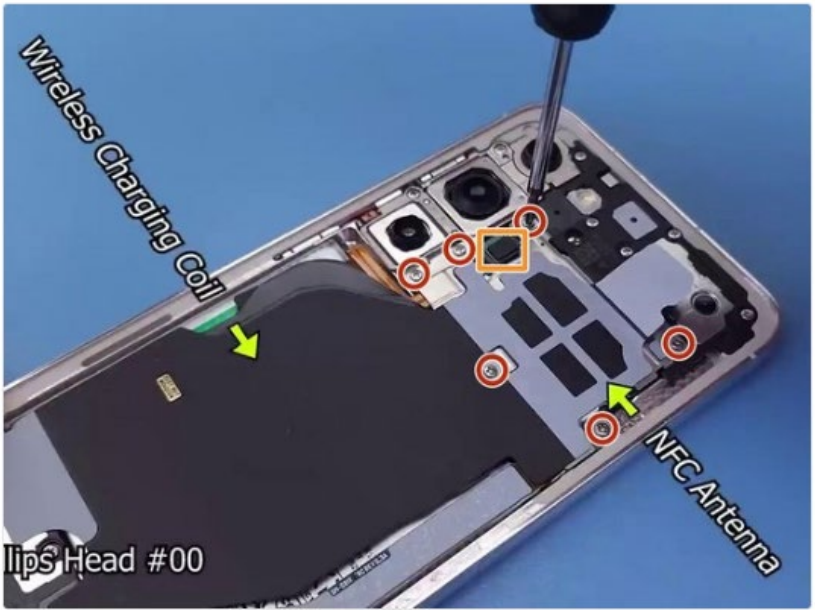
118. Samsung has directly infringed the '187 Patent. The infringing acts include, but are not limited to, the manufacture, use, sale, importation, and/or offer for sale of the Accused Instrumentalities to practice the claimed invention in the '187 Patent. For example, Claim 1 of the '187 Patent[66] recites:

> A mobile device, comprising:
>
> > short range radio frequency (RF) circuitry;
> >
> > memory configured to store biometric authentication information and payment information;
> >
> > a biometric module configured to read biometric information;
> >
> > an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and
> >
> > a secure module configured to:
> >
> > > generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;
> > >
> > > encrypt the key and the payment information stored in memory; and
> > >
> > > provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction.

119. The Accused Instrumentalities meet the recited elements of Claim 1.

[66] Claim 1 is referenced herein for representative purposes. Plaintiff reserves the right to identify additional asserted claims and reserves its right to provide greater detail and scope via its Infringement Contentions at the time required under this Court's scheduling order.

120. The Accused Instrumentalities include short-range radio frequency circuitry. For example, the Accused Instrumentalities include NFC technology that includes an antenna configured to communicate via NFC, which utilizes radio frequency.



121. The Accused Instrumentalities include memory. The memory is configured to store payment information and fingerprint information. For example, the Accused Instrumentalities include random access memory (RAM) which qualifies as memory.

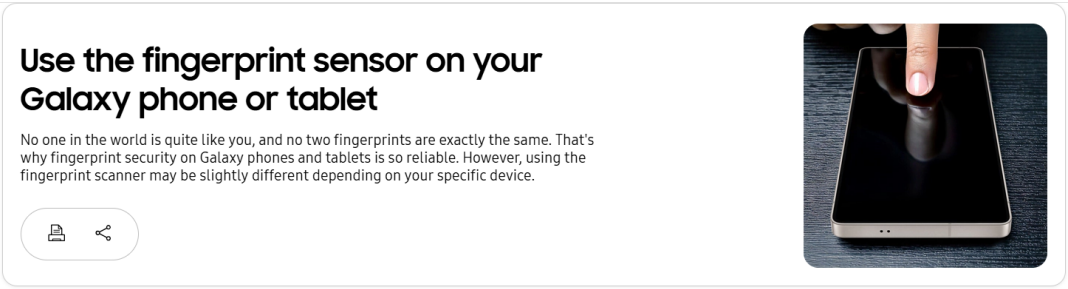
MEMORY	Card slot	No
	Internal	256GB 8GB RAM, 256GB 12GB RAM, 512GB 12GB RAM, 1TB 12GB RAM
		UFS 4.0

122. The memory is used to store fingerprint information and payment information. The Accused Instrumentalities store sensitive data such as biometric authentication information and transaction information in a variety of different ways. For example, Samsung's Knox Vault can be used to store biometric authentication information.[67] Fingerprint biometrics may be stored in a Trusted Execution Environment (TEE).[68] Such information is "encrypted and stored in a separate

[67] Samsung Knox Documentation, *supra*
[68] Samsung Knox, *supra.*

part of the smartphone, completely inaccessible to the regular operating system."[69] A secure element may also be used to store card information.[70]

123. Samsung's Accused Instrumentalities include a biometric module, such as a fingerprint scanner configured to receive fingerprint data:



124. The Accused Instrumentalities include an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory. For example, the Accused Instrumentalities are configured to use biometrics to authenticate users.[71]

How biometrics work

The first step to understanding biometrics is to realize the biometrics are not being saved in the network or passed around between devices and servers. Instead, biometrics are used to lock up and protect other authentication information — usually a digital certificate private key — and it's the "protected" information that is actually being used to authenticate the user.

Android v6 ("Marshmallow") introduced a standardized API for biometrics, focusing on fingerprint readers. Companies looking to leverage biometrics as part of authentication can depend on having a common set of services, a high level of security, and a consistent user experience across platforms.

The key requirement in Android is that fingerprint biometrics have to be stored in the Trusted Execution Environment (TEE). This means that the biometric information is encrypted and stored in a separate part of the smartphone, completely inaccessible to the regular operating system. They can't even be exported. Android can ask the TEE to validate an identity using biometrics, but cannot extract the biometric information. This means that when the user stores their biometric information, such as a fingerprint, they are not sharing that information outside of their own smartphone or tablet. They are just establishing a way to identify themselves to their device.

[69] *Id*.
[70] *Samsung eSE SDK*, *supra* (describing the "embedded Secure Element (eSE)" of Samsung devices and how they store "payments."); *How secure is Samsung Pay*, *supra* (describing Samsung Pay's use of tokenization to store credit card (transaction) information).
[71] Samsung Knox, *supra*.

125. The Accused Instrumentalities include one or more processors that can be configured as a secure module. For example, the Samsung Galaxy S23 Ultra has a Qualcomm Snapdragon 8 Gen 2 CPU:

PLATFORM	OS	Android 13, up to 4 major Android upgrades, One UI 6.1.1
	Chipset	Qualcomm SM8550-AC Snapdragon 8 Gen 2 (4 nm)
	CPU	Octa-core (1x3.36 GHz Cortex-X3 & 2x2.8 GHz Cortex-A715 & 2x2.8 GHz Cortex-A710 & 3x2.0 GHz Cortex-A510)
	GPU	Adreno 740

126. The processor is configured to generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory. For example, the Accused Instrumentalities follow EMV's standards for processing contactless payments.[72]

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

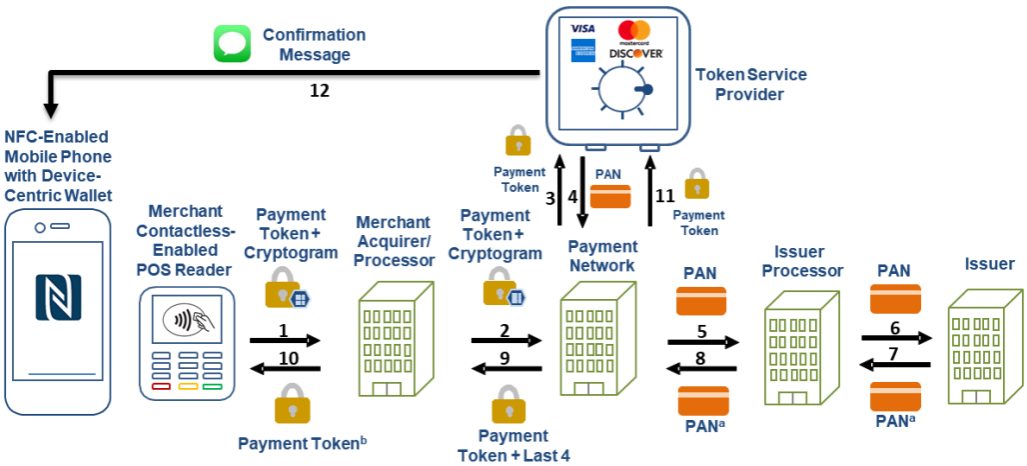
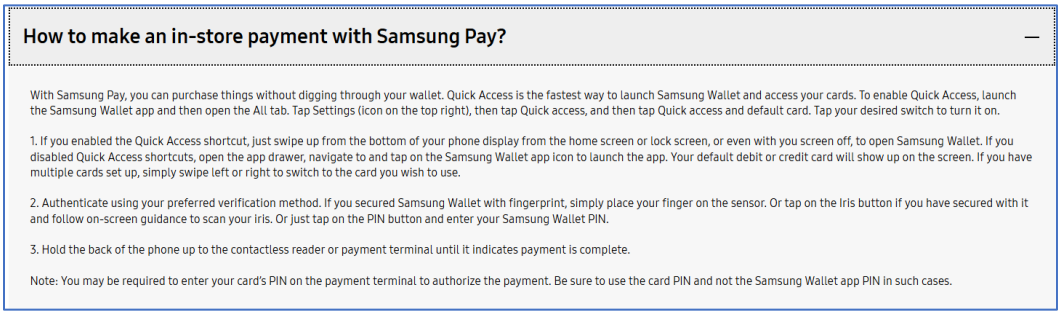


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

[72] US Payments Forum, *supra* at 24–25; *see also* EMVCo., *supra* at 42–43.

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

127. In the Accused Instrumentalities, the user authenticates himself/herself using biometric information, such as through the use of a fingerprint sensor.[73]



128. In the Accused Instrumentalities, the Accused Instrumentalities generate a key. For example, the EMV standard described above involves the generation of a cryptogram after

[73] *Samsung Wallet FAQ*, *supra*.

authentication. A cryptogram (also known as a token cryptogram or a "transaction specific dynamic security code") is a secure code generated during a transaction that verifies the transaction and helps prevent fraud. The payment network validates the cryptogram and de-tokenizes the token to determine the PAN, which is then processed by the payment network. Thus, the cryptogram acts as a key to the transaction. In the Accused Instrumentalities, the processor is configured to encrypt the key and the payment information stored in the memory. The Accused Instrumentalities use a secure element to store card information.[74] The key and payment information are encrypted via the tokenization process. The key is encrypted in that the information used to create the cryptogram are cryptographically combined to create the cryptogram.

129. In the Accused Instrumentalities, the processor is configured to provide, via the short range RF circuitry, the encrypted key and payment information for use in a transaction. For example, as described above, the EMV standard involves transmitting the cryptogram and the secured payment information from the Accused Instrumentality to the POS device.

130. Samsung committed the infringing activities without license from Mobility IP. Samsung's acts of infringement have damaged Mobility IP, as owner of the '187 Patent. Mobility IP is entitled to recover from Samsung the damages it has sustained as a result of Samsung's wrongful acts in an amount subject to proof at trial. The infringement of the '187 Patent by Samsung has damaged Plaintiff.

JURY DEMAND

131. Mobility IP hereby demands a trial by jury on all issues.

[74] *Samsung eSE SDK*, *supra* (describing the "embedded Secure Element (eSE)" of Samsung devices and how they store "payments."); *How secure is Samsung Pay*, *supra* (describing Samsung Pay's use of tokenization to store credit card (transaction) information).

PRAYER

Wherefore, Mobility IP prays for entry of judgment as follows:

132. A judgment in favor of Mobility IP that Samsung has infringed and is infringing, either literally and/or under the doctrine of equivalents, the Asserted Patents;

133. A judgment in favor of Mobility IP that Samsung's infringement of the '772 patent has been willful and a judgment in favor of Mobility IP that Samsung's infringement of the '345 patent and the '924 patent is willful and continues to be willful as of the date Samsung received notice of its infringement through this lawsuit;

134. An award of damages in favor of Mobility IP adequate to compensate Mobility IP for Samsung's infringement of the Asserted Patents which shall in no event be less than a reasonable royalty, together with interest and cost as fixed by the court pursuant to 35 U.S.C. § 284;

135. An award of enhanced damages in favor of Mobility IP against Samsung for up to three times the award of actual damages for Samsung's willful infringement of the '772 patent, '345 patent, and '924 patent, pursuant to 35 U.S.C. § 284;

136. A permanent injunction in favor of Mobility IP against Samsung enjoining Samsung, its officers, agents, employees, and others acting in privity, from further infringement of the '345 and '924 Patents;

137. An award of an ongoing royalty for Samsung's post-judgment infringement in the event a permanent injunction is not granted;

138. An award of attorneys' fees pursuant to 35 U.S.C. § 285 or as otherwise permitted by law in an amount deemed just and appropriate by the Court;

139. An award of costs and expenses as deemed appropriate by the Court; and

Any other legal or equitable relief to which Mobility IP is justly entitled.

Dated: February 27, 2026

Respectfully submitted,

/s/ Jason S. McManis

Jason S. McManis
State Bar No.: 24088032
Weining Bai
State Bar No.: 24101477
Thomas Delrosario
State Bar No.: 24110645
Justin Kenney
State Bar No.: 24126702
Ab Henry
State Bar No.: 24131987
Zach Grinovich
State Bar No.: 24149804
AHMAD, ZAVITSANOS & MENSING, PLLC
1221 McKinney Street, Suite 2500
Houston, Texas 77010
(713) 655-1101
jmcmanis@azalaw.com
wbai@azalaw.com
tdelrosario@azalaw.com
jkenney@azalaw.com
ahenry@azalaw.com
zgrinovich@azalaw.com

Of Counsel:

Howard Wisnia
Wisnia PC
California Bar No. 184626
howard@wisnialaw.com
12636 High Bluff Dr., Suite 400
San Diego CA 92130
Tel: +1 858 461 0989

Andrea L. Fair
State Bar No. 24078488
andrea@millerfairhenry.com
Miller Fair Henry, PLLC
1507 Bill Owens Parkway
Longview, Texas 75604
Tel: 903-757-6400
Fax: 903-757-2323

COUNSEL FOR PLAINTIFF

EXHIBIT 1

US008151345B1

(12) **United States Patent**
Yeager

(10) **Patent No.: US 8,151,345 B1**
(45) **Date of Patent: Apr. 3, 2012**

(54) **SELF-AUTHORIZING DEVICES**

(76) Inventor: **C. Douglas Yeager**, Knoxville, TN (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1058 days.

(21) Appl. No.: **12/019,318**

(22) Filed: **Jan. 24, 2008**

Related U.S. Application Data

(60) Provisional application No. 60/897,110, filed on Jan. 25, 2007, provisional application No. 60/932,704, filed on Jun. 1, 2007.

(51) **Int. Cl.**
G06F 7/04 (2006.01)

(52) **U.S. Cl.** **726/20**; 726/9; 235/380; 235/375; 235/439; 235/492; 713/165; 710/313

(58) **Field of Classification Search** 726/9, 20; 235/380, 375, 439, 492; 710/313; 713/165
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,439,464	B1	8/2002	Fruhauf et al.	
6,763,399	B2 *	7/2004	Margalit et al.	710/13
6,883,715	B1	4/2005	Fruhauf et al.	
6,991,173	B2	1/2006	Fruhauf	
7,011,247	B2 *	3/2006	Drabczuk et al.	235/451
7,150,397	B2	12/2006	Morrow et al.	
7,213,766	B2 *	5/2007	Ryan et al.	235/492
7,249,266	B2	7/2007	Margalit et al.	
2006/0143326	A1 *	6/2006	Hauck	710/18
2006/0255158	A1	11/2006	Margalit et al.	
2007/0208949	A1 *	9/2007	Lu et al.	713/186
2007/0262138	A1 *	11/2007	Somers et al.	235/380
2008/0128513	A1 *	6/2008	Hammad et al.	235/492
2009/0039156	A1 *	2/2009	Brandli et al.	235/382
2009/0187687	A1 *	7/2009	Hulbert et al.	710/73

FOREIGN PATENT DOCUMENTS

EP	1843277	10/2007

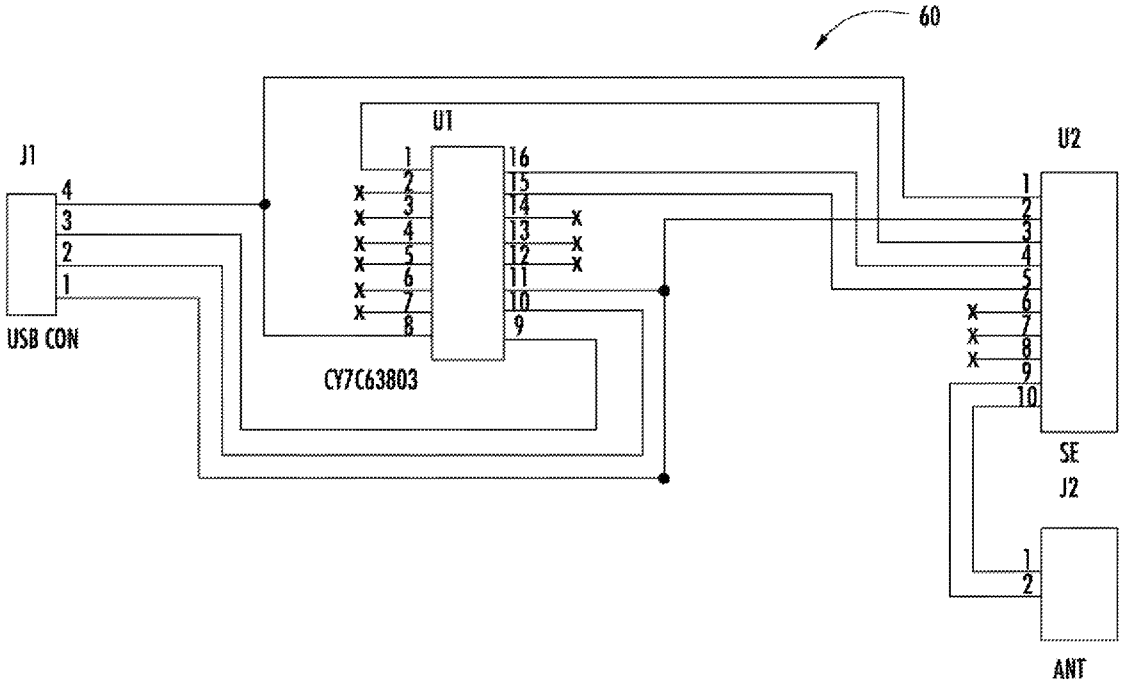
* cited by examiner

Primary Examiner — Vivek Srivastava
Assistant Examiner — Hee Song
(74) *Attorney, Agent, or Firm* — Luedeka Neely Group, P.C.

(57) **ABSTRACT**

Self-authorizing cards and cellular network adapters for authorization of financially payments and other secure transactions. In some embodiments a smart card is provided with a connector for a USB port on a computer terminal such as a personal computer (PC). Embodiments are also provided for mobile phones, personal digital assistants (PDAs), and similar devices. The self-authorizing devices typically include a secure element that has been previously provisioned with information about a particular card holder account. A secure element reader interrogates the smart element and derives information needed to authorize the transaction. A communications controller transmits the information to a host device, such as a PC, PDA, or a mobile phone.

25 Claims, 19 Drawing Sheets



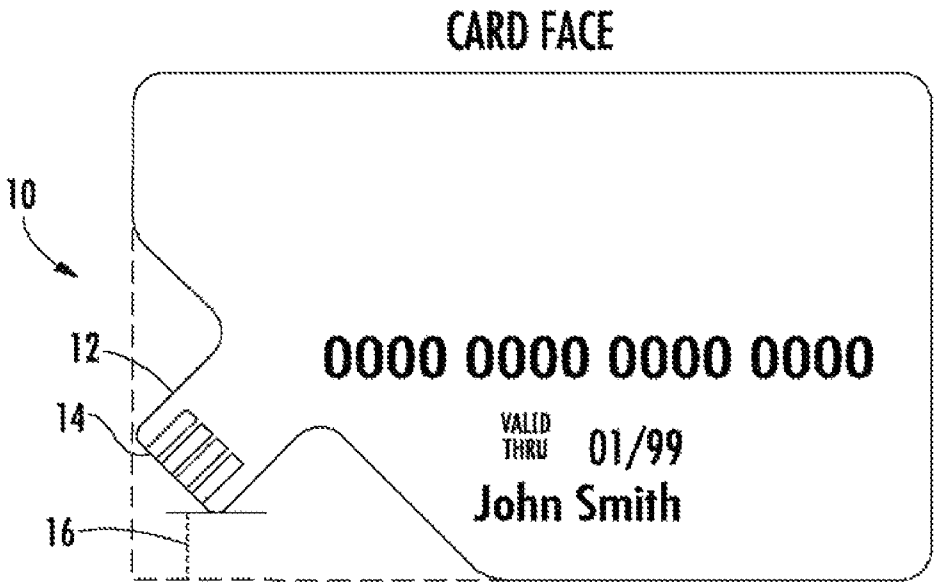

CARD FACE
10
12
14
16
0000 0000 0000 0000
VALID THRU 01/99
John Smith

FIG. 1

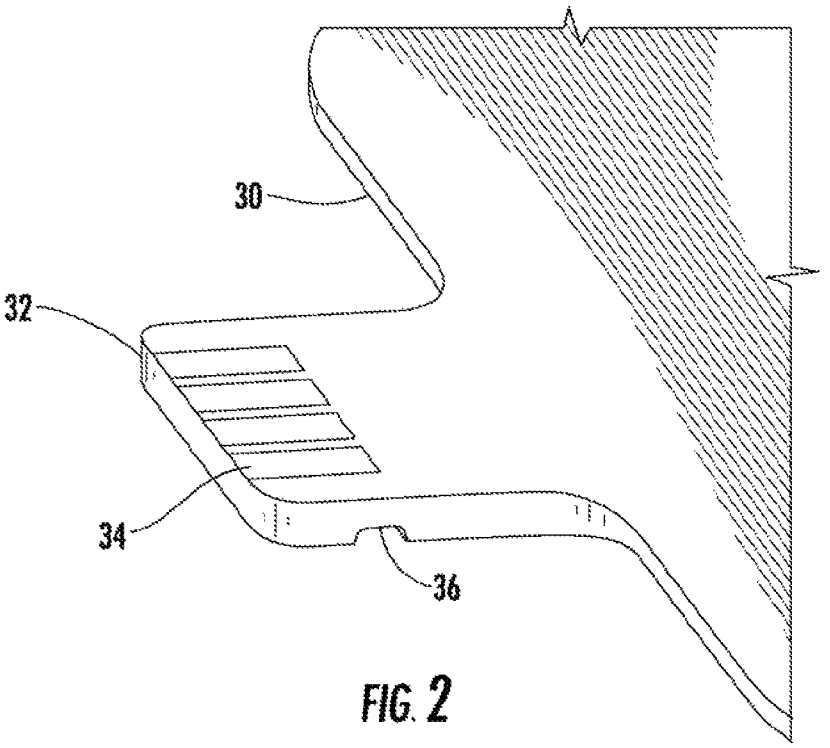


FIG. 2

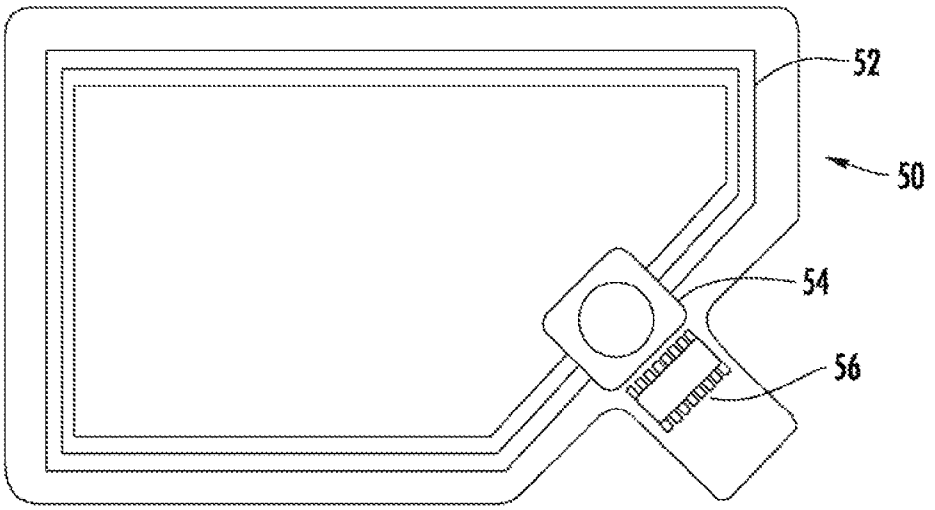


FIG. 3

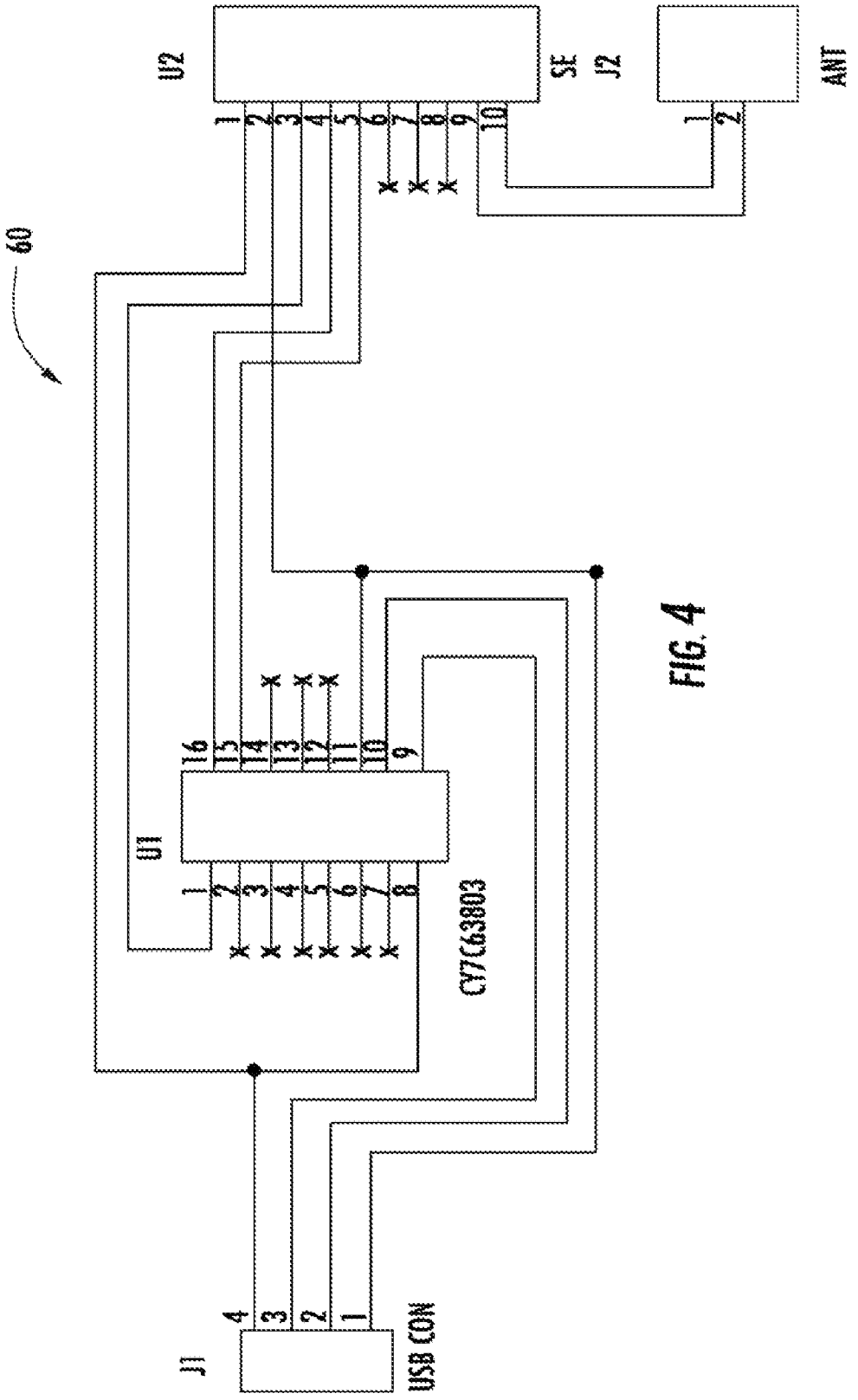


FIG. 4

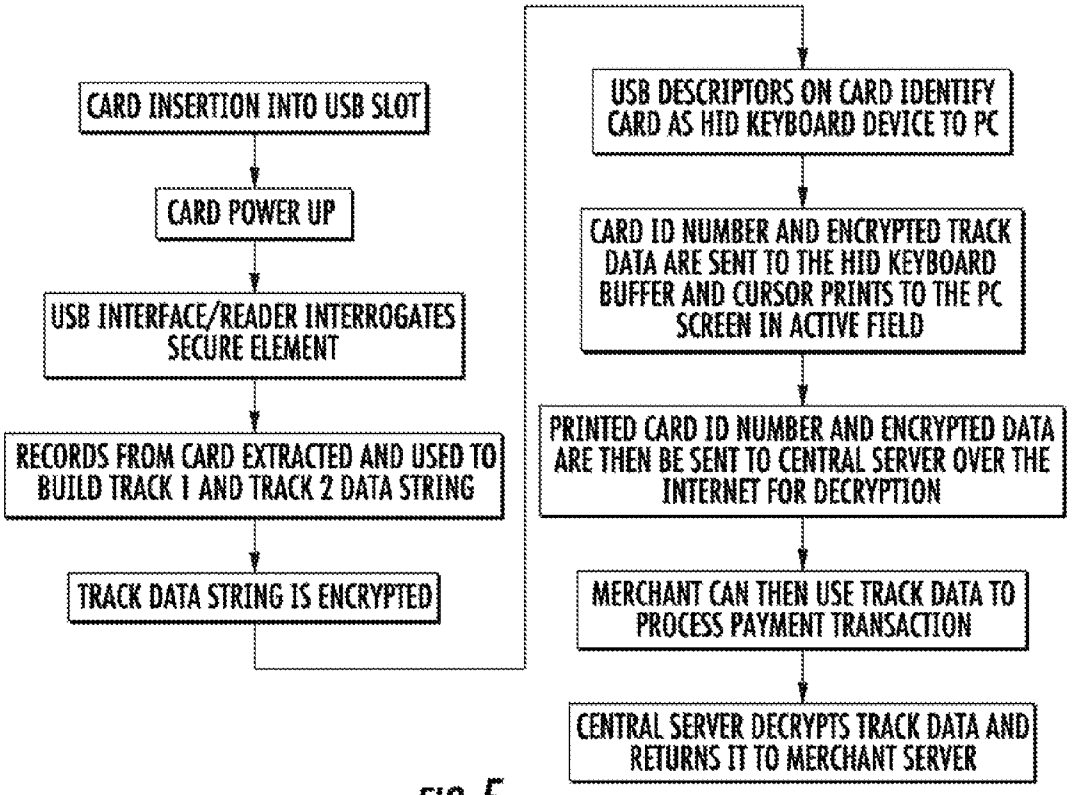

CARD INSERTION INTO USB SLOT
CARD POWER UP
USB INTERFACE/READER INTERROGATES SECURE ELEMENT
RECORDS FROM CARD EXTRACTED AND USED TO BUILD TRACK 1 AND TRACK 2 DATA STRING
TRACK DATA STRING IS ENCRYPTED
USB DESCRIPTORS ON CARD IDENTIFY CARD AS HID KEYBOARD DEVICE TO PC
CARD ID NUMBER AND ENCRYPTED TRACK DATA ARE SENT TO THE HID KEYBOARD BUFFER AND CURSOR PRINTS TO THE PC SCREEN IN ACTIVE FIELD
PRINTED CARD ID NUMBER AND ENCRYPTED DATA ARE THEN BE SENT TO CENTRAL SERVER OVER THE INTERNET FOR DECRYPTION
MERCHANT CAN THEN USE TRACK DATA TO PROCESS PAYMENT TRANSACTION
CENTRAL SERVER DECRYPTS TRACK DATA AND RETURNS IT TO MERCHANT SERVER

FIG. 5

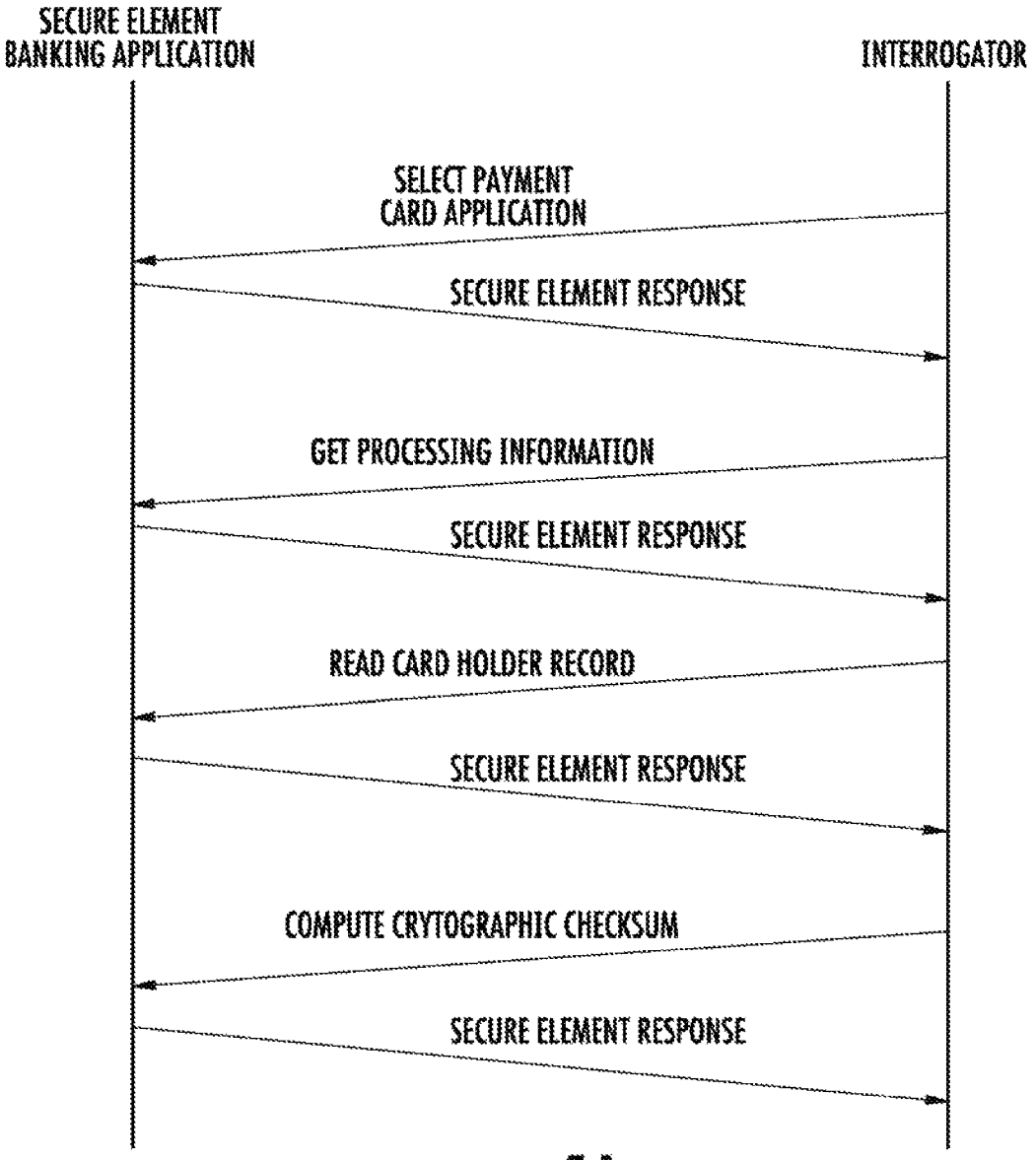

SECURE ELEMENT
BANKING APPLICATION
INTERROGATOR
SELECT PAYMENT
CARD APPLICATION
SECURE ELEMENT RESPONSE
GET PROCESSING INFORMATION
SECURE ELEMENT RESPONSE
READ CARD HOLDER RECORD
SECURE ELEMENT RESPONSE
COMPUTE CRYTOGRAPHIC CHECKSUM
SECURE ELEMENT RESPONSE

FIG. 5.1

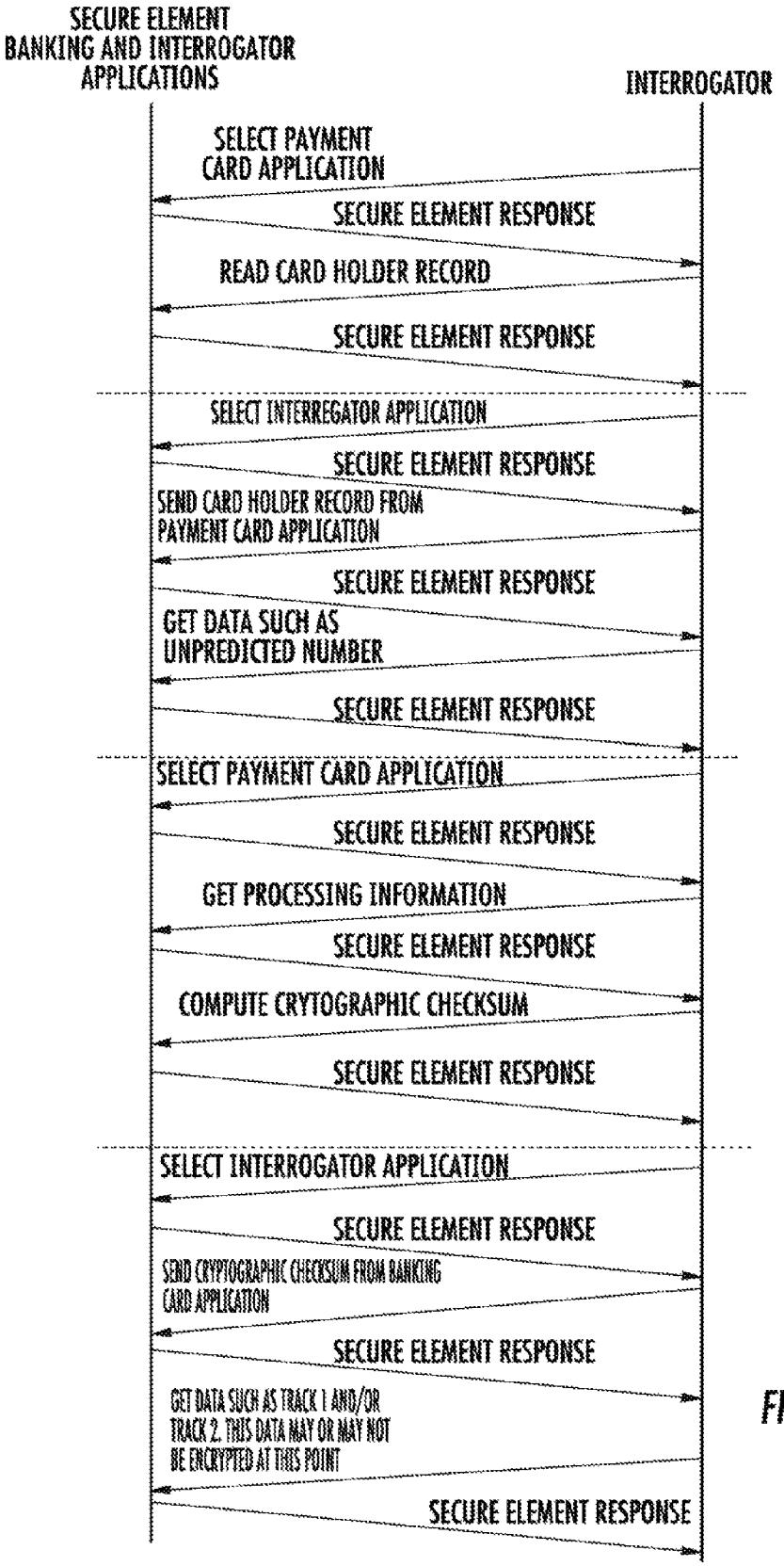

SECURE ELEMENT
BANKING AND INTERROGATOR
APPLICATIONS
INTERROGATOR
SELECT PAYMENT
CARD APPLICATION
SECURE ELEMENT RESPONSE
READ CARD HOLDER RECORD
SECURE ELEMENT RESPONSE
SELECT INTERREGATOR APPLICATION
SECURE ELEMENT RESPONSE
SEND CARD HOLDER RECORD FROM
PAYMENT CARD APPLICATION
SECURE ELEMENT RESPONSE
GET DATA SUCH AS
UNPREDICTED NUMBER
SECURE ELEMENT RESPONSE
SELECT PAYMENT CARD APPLICATION
SECURE ELEMENT RESPONSE
GET PROCESSING INFORMATION
SECURE ELEMENT RESPONSE
COMPUTE CRYTOGRAPHIC CHECKSUM
SECURE ELEMENT RESPONSE
SELECT INTERROGATOR APPLICATION
SECURE ELEMENT RESPONSE
SEND CRYPTOGRAPHIC CHECKSUM FROM BANKING
CARD APPLICATION
SECURE ELEMENT RESPONSE
GET DATA SUCH AS TRACK 1 AND/OR
TRACK 2. THIS DATA MAY OR MAY NOT
BE ENCRYPTED AT THIS POINT
SECURE ELEMENT RESPONSE

FIG. 5.2

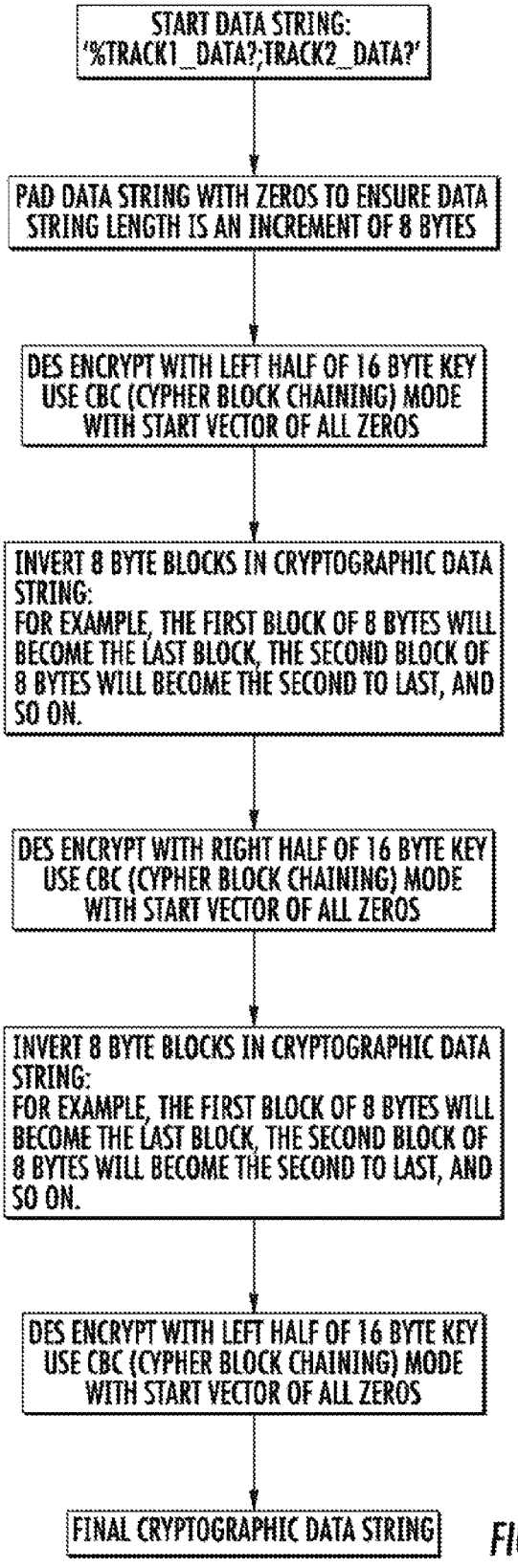

START DATA STRING:
'%TRACK1_DATA?;TRACK2_DATA?'
PAD DATA STRING WITH ZEROS TO ENSURE DATA STRING LENGTH IS AN INCREMENT OF 8 BYTES
DES ENCRYPT WITH LEFT HALF OF 16 BYTE KEY USE CBC (CYPHER BLOCK CHAINING) MODE WITH START VECTOR OF ALL ZEROS
INVERT 8 BYTE BLOCKS IN CRYPTOGRAPHIC DATA STRING:
FOR EXAMPLE, THE FIRST BLOCK OF 8 BYTES WILL BECOME THE LAST BLOCK, THE SECOND BLOCK OF 8 BYTES WILL BECOME THE SECOND TO LAST, AND SO ON.
DES ENCRYPT WITH RIGHT HALF OF 16 BYTE KEY USE CBC (CYPHER BLOCK CHAINING) MODE WITH START VECTOR OF ALL ZEROS
INVERT 8 BYTE BLOCKS IN CRYPTOGRAPHIC DATA STRING:
FOR EXAMPLE, THE FIRST BLOCK OF 8 BYTES WILL BECOME THE LAST BLOCK, THE SECOND BLOCK OF 8 BYTES WILL BECOME THE SECOND TO LAST, AND SO ON.
DES ENCRYPT WITH LEFT HALF OF 16 BYTE KEY USE CBC (CYPHER BLOCK CHAINING) MODE WITH START VECTOR OF ALL ZEROS
FINAL CRYPTOGRAPHIC DATA STRING

FIG. 5.3

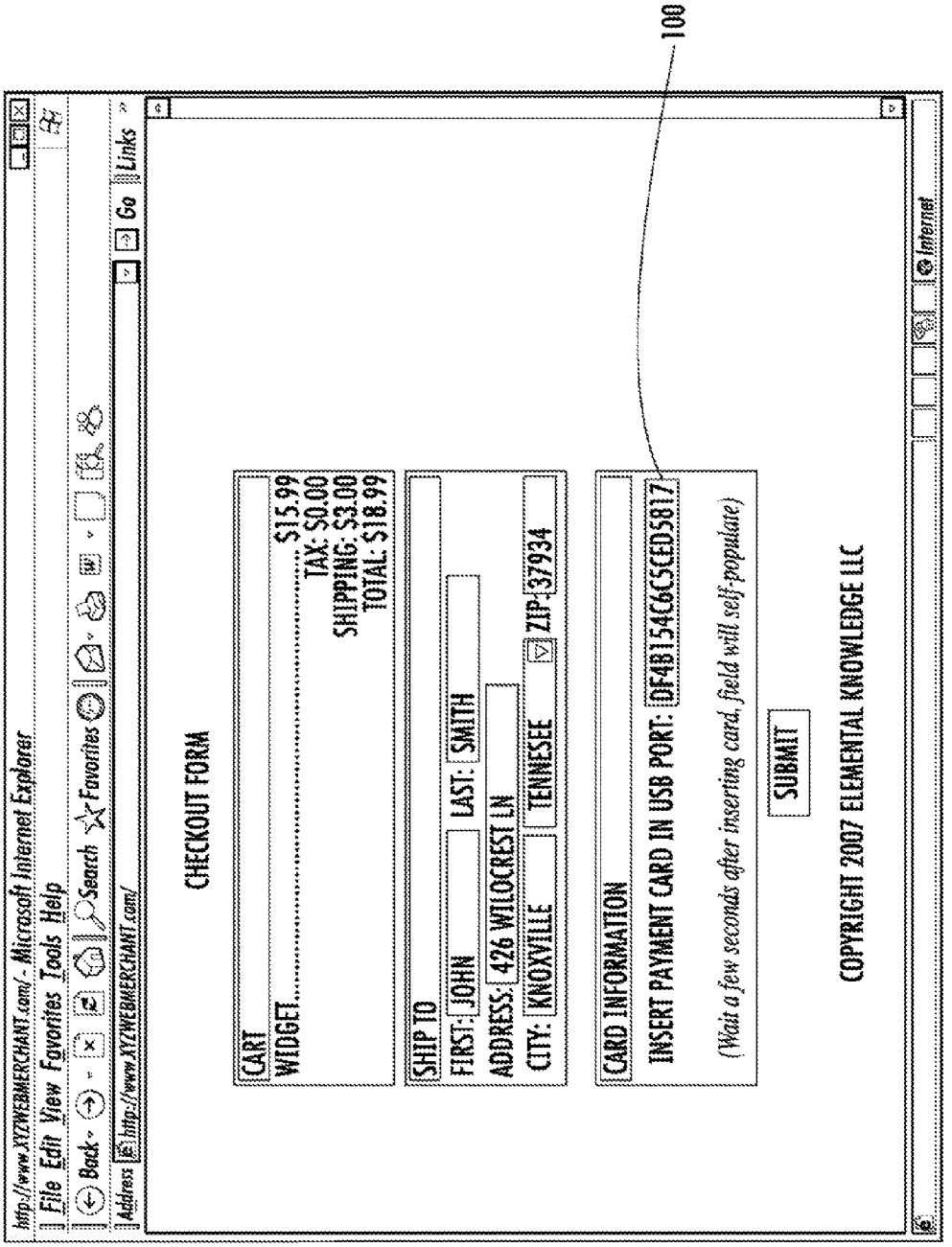

100
http://www.XYZWEBMERCHANT.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.XYZWEBMERCHANT.com/
Go Links
CHECKOUT FORM
CART
WIDGET..... $15.99
TAX: $0.00
SHIPPING: $3.00
TOTAL: $18.99
SHIP TO
FIRST: JOHN LAST: SMITH
ADDRESS: 426 WILDCREST LN
CITY: KNOXVILLE TENNESSEE ZIP: 37934
CARD INFORMATION
INSERT PAYMENT CARD IN USB PORT: DF4B154C6C5CED5817
(Wait a few seconds after inserting card, field will self-populate)
SUBMIT
COPYRIGHT 2007 ELEMENTAL KNOWLEDGE LLC
Internet

FIG. 6

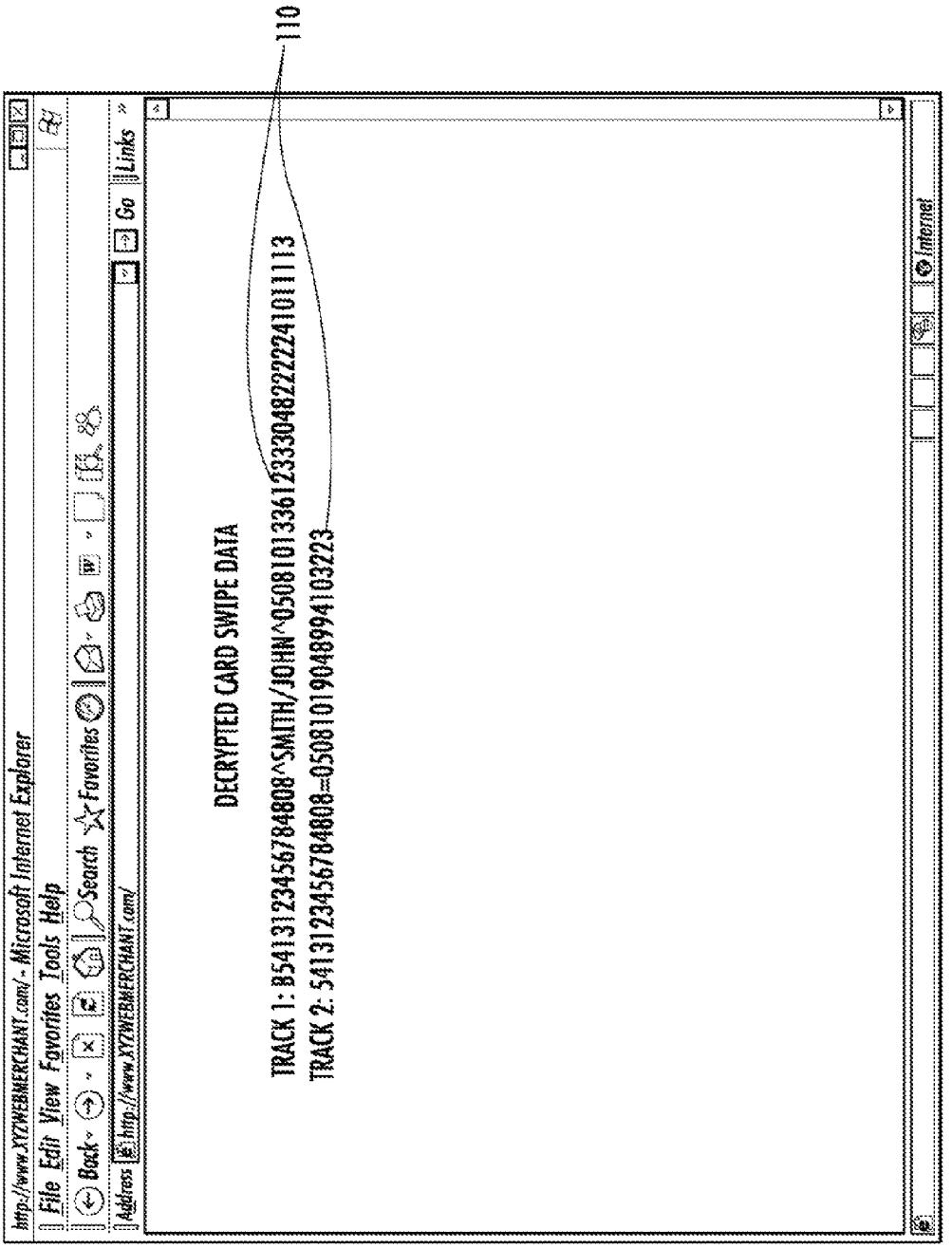

110
http://www.XYZWEBMERCHANT.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.XYZWEBMERCHANT.com/
Go Links
DECRYPTED CARD SWIPE DATA
TRACK 1: B5413123456784808^SMITH/JOHN^05081013361233304822222410111113
TRACK 2: 5413123456784808=05081019048994103223
Internet

FIG. 7

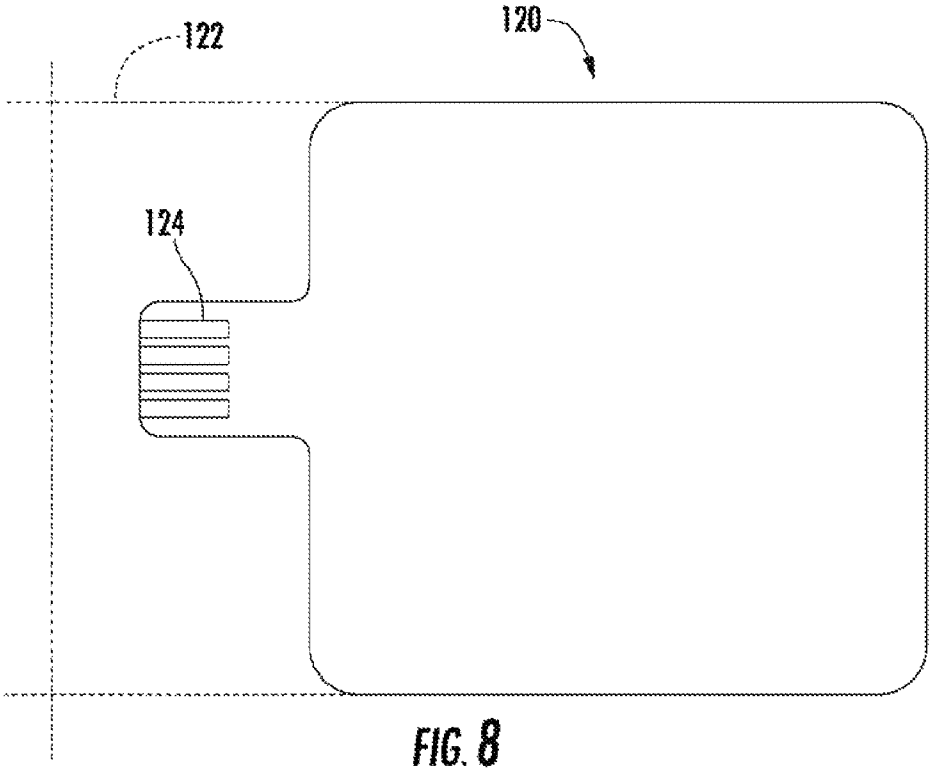


FIG. 8

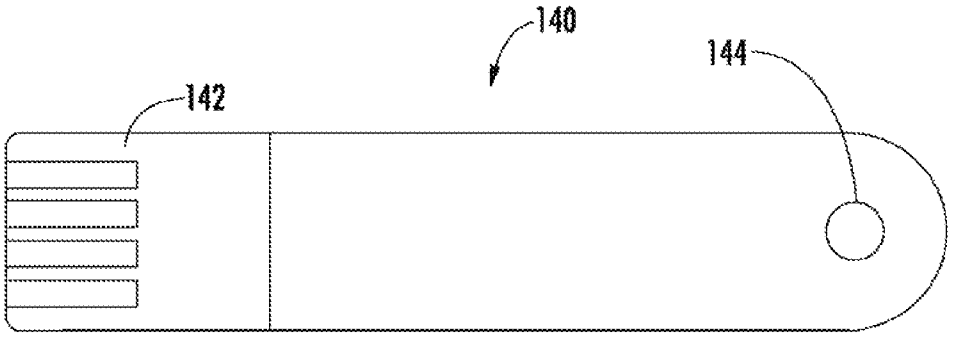


FIG. 9

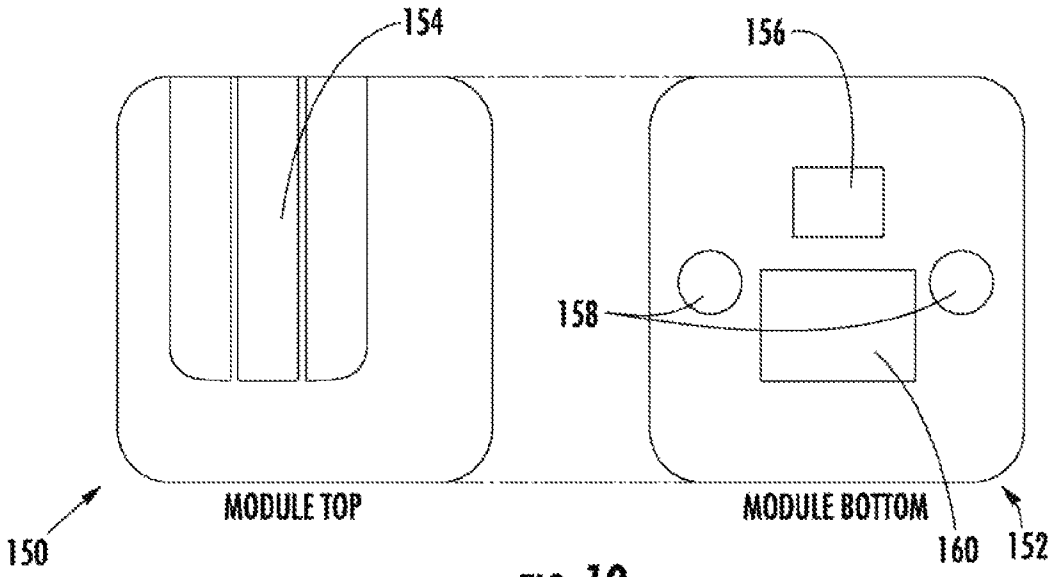


FIG. 10

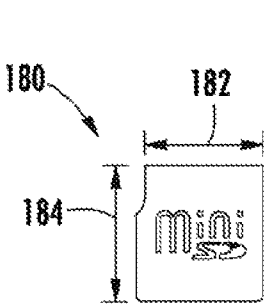


FIG. 11A

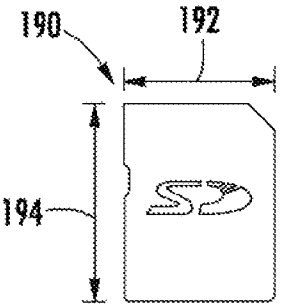


FIG. 11B

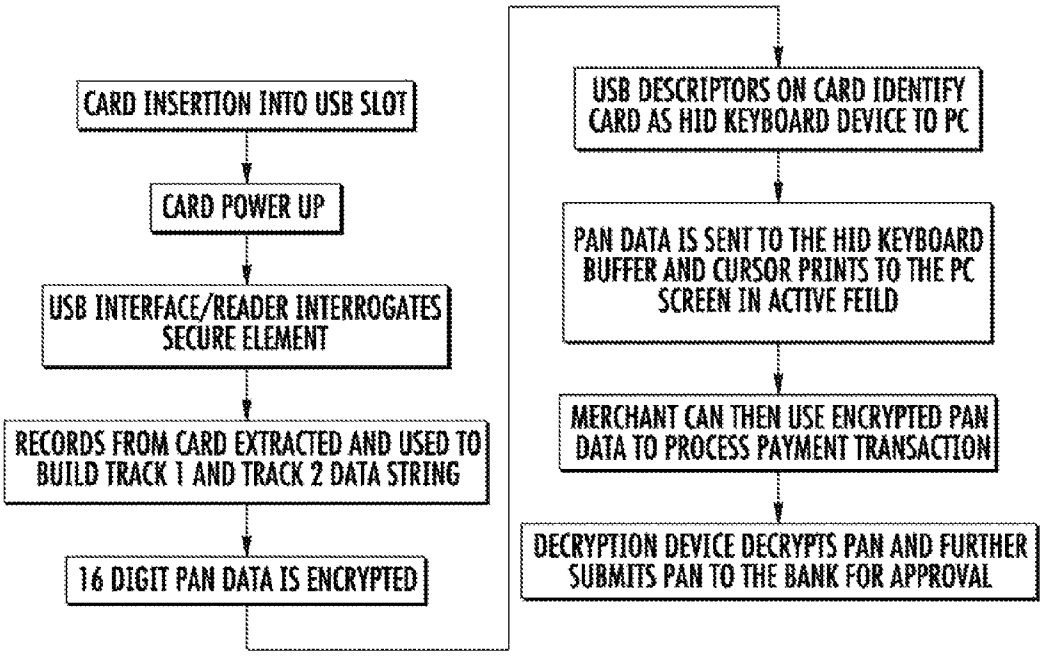

CARD INSERTION INTO USB SLOT
CARD POWER UP
USB INTERFACE/READER INTERROGATES SECURE ELEMENT
RECORDS FROM CARD EXTRACTED AND USED TO BUILD TRACK 1 AND TRACK 2 DATA STRING
16 DIGIT PAN DATA IS ENCRYPTED
USB DESCRIPTORS ON CARD IDENTIFY CARD AS HID KEYBOARD DEVICE TO PC
PAN DATA IS SENT TO THE HID KEYBOARD BUFFER AND CURSOR PRINTS TO THE PC SCREEN IN ACTIVE FEILD
MERCHANT CAN THEN USE ENCRYPTED PAN DATA TO PROCESS PAYMENT TRANSACTION
DECRYPTION DEVICE DECRYPTS PAN AND FURTHER SUBMITS PAN TO THE BANK FOR APPROVAL

FIG. 12

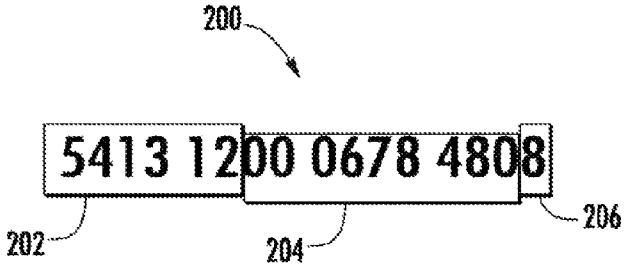

200
5413 1200 0678 4808
202
204
206

FIG. 13

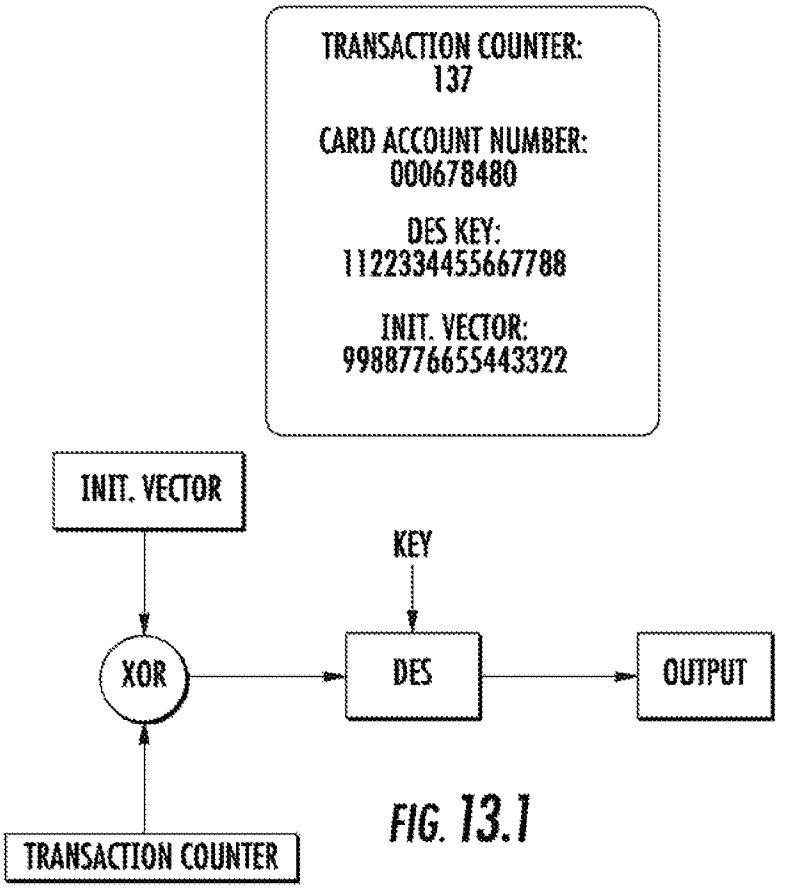


FIG. 13.1

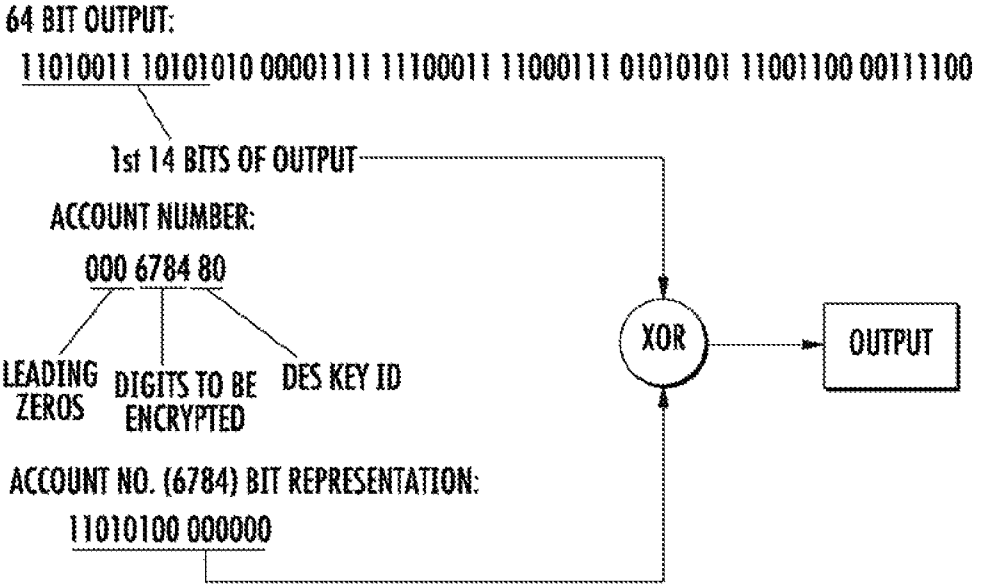


FIG. 13.2

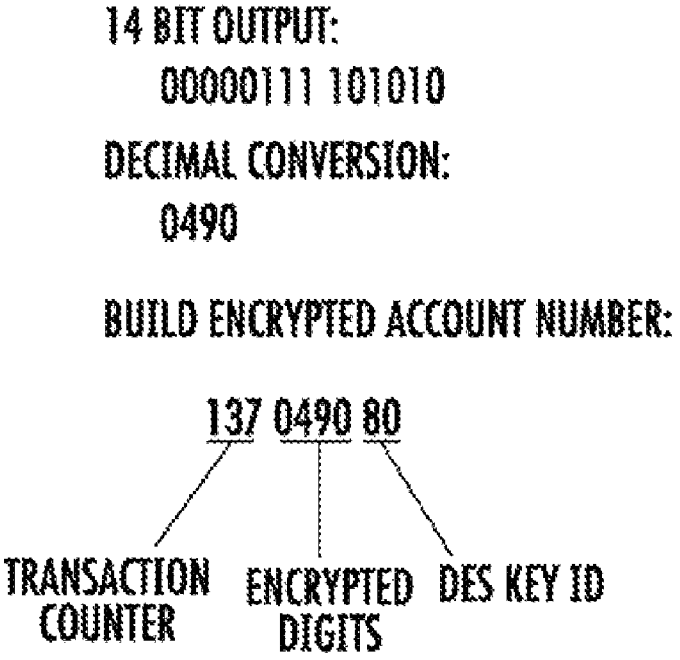


FIG. 13.3

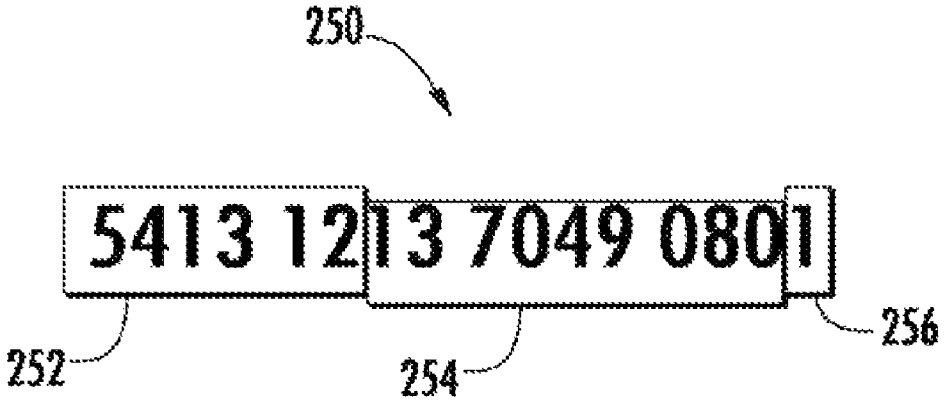


FIG. 13.4

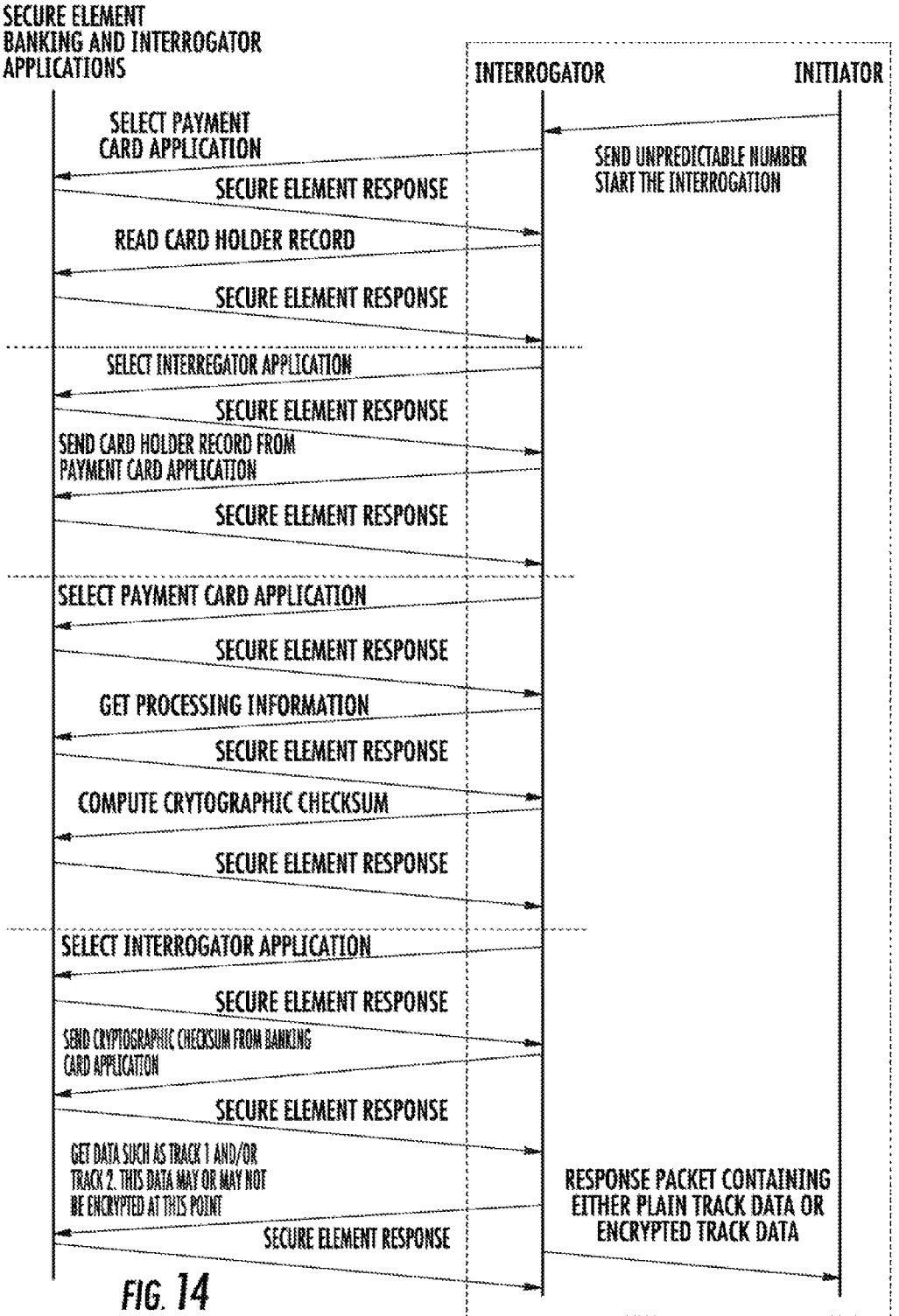

SECURE ELEMENT
BANKING AND INTERROGATOR
APPLICATIONS
INTERROGATOR
INITIATOR
SELECT PAYMENT
CARD APPLICATION
SEND UNPREDICTABLE NUMBER
START THE INTERROGATION
SECURE ELEMENT RESPONSE
READ CARD HOLDER RECORD
SECURE ELEMENT RESPONSE
SELECT INTERREGATOR APPLICATION
SECURE ELEMENT RESPONSE
SEND CARD HOLDER RECORD FROM
PAYMENT CARD APPLICATION
SECURE ELEMENT RESPONSE
SELECT PAYMENT CARD APPLICATION
SECURE ELEMENT RESPONSE
GET PROCESSING INFORMATION
SECURE ELEMENT RESPONSE
COMPUTE CRYTOGRAPHIC CHECKSUM
SECURE ELEMENT RESPONSE
SELECT INTERROGATOR APPLICATION
SECURE ELEMENT RESPONSE
SEND CRYPTOGRAPHIC CHECKSUM FROM BANKING
CARD APPLICATION
SECURE ELEMENT RESPONSE
GET DATA SUCH AS TRACK 1 AND/OR
TRACK 2. THIS DATA MAY OR MAY NOT
BE ENCRYPTED AT THIS POINT
RESPONSE PACKET CONTAINING
EITHER PLAIN TRACK DATA OR
ENCRYPTED TRACK DATA
SECURE ELEMENT RESPONSE

FIG. 14

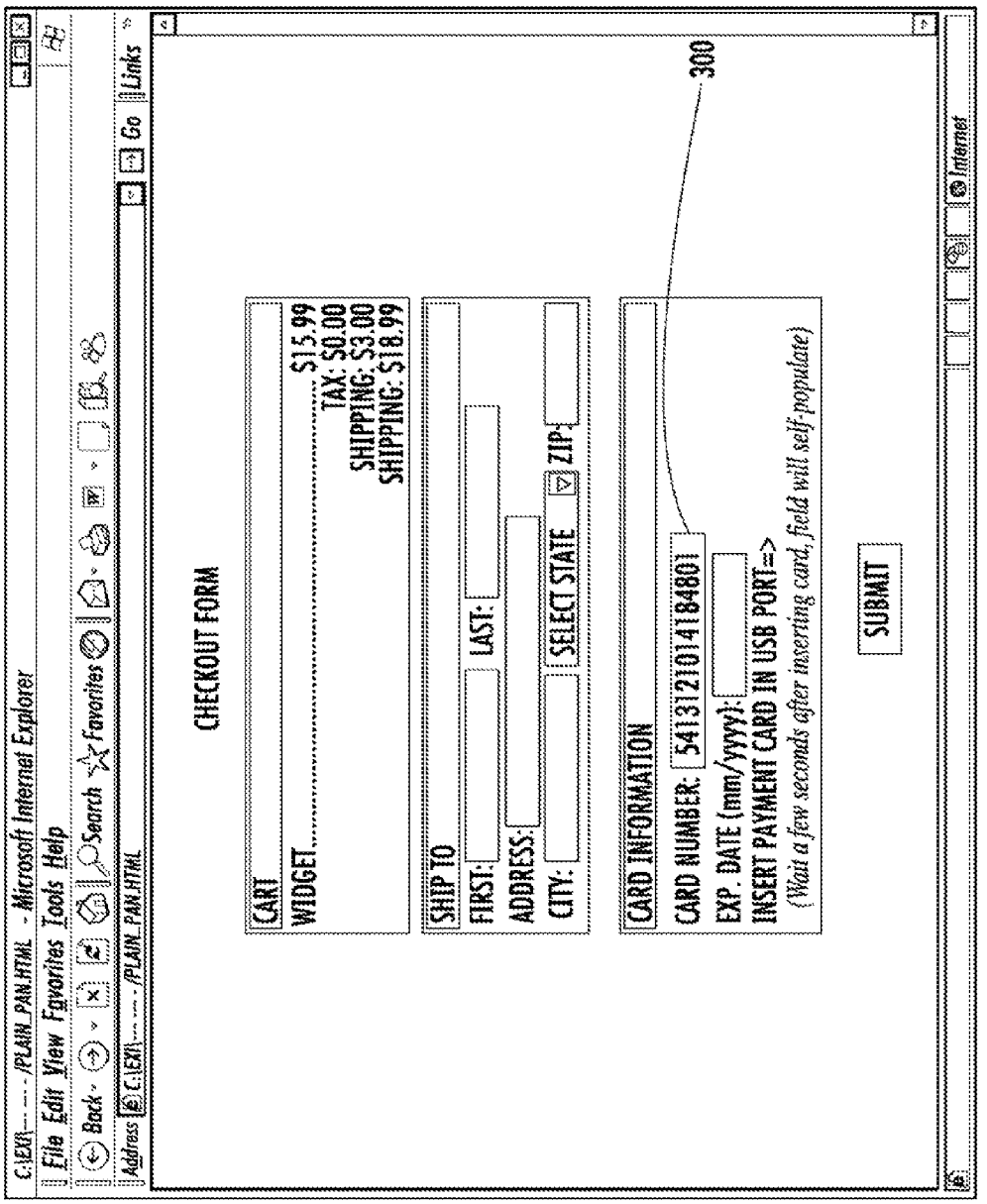

C:\EXP\---- ---/PLAIN_PAN.HTML - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\EXP\---- ---/PLAIN_PAN.HTML
Go Links
CHECKOUT FORM
CART
WIDGET..... $15.99
TAX: $0.00
SHIPPING: $3.00
SHIPPING: $18.99
SHIP TO
FIRST: LAST:
ADDRESS:
CITY: SELECT STATE ZIP:
CARD INFORMATION
CARD NUMBER: 5413121014184801
EXP. DATE (mm/yyyy):
INSERT PAYMENT CARD IN USB PORT=>
(Wait a few seconds after inserting card, field will self-populate)
SUBMIT
300
Internet

FIG. 15

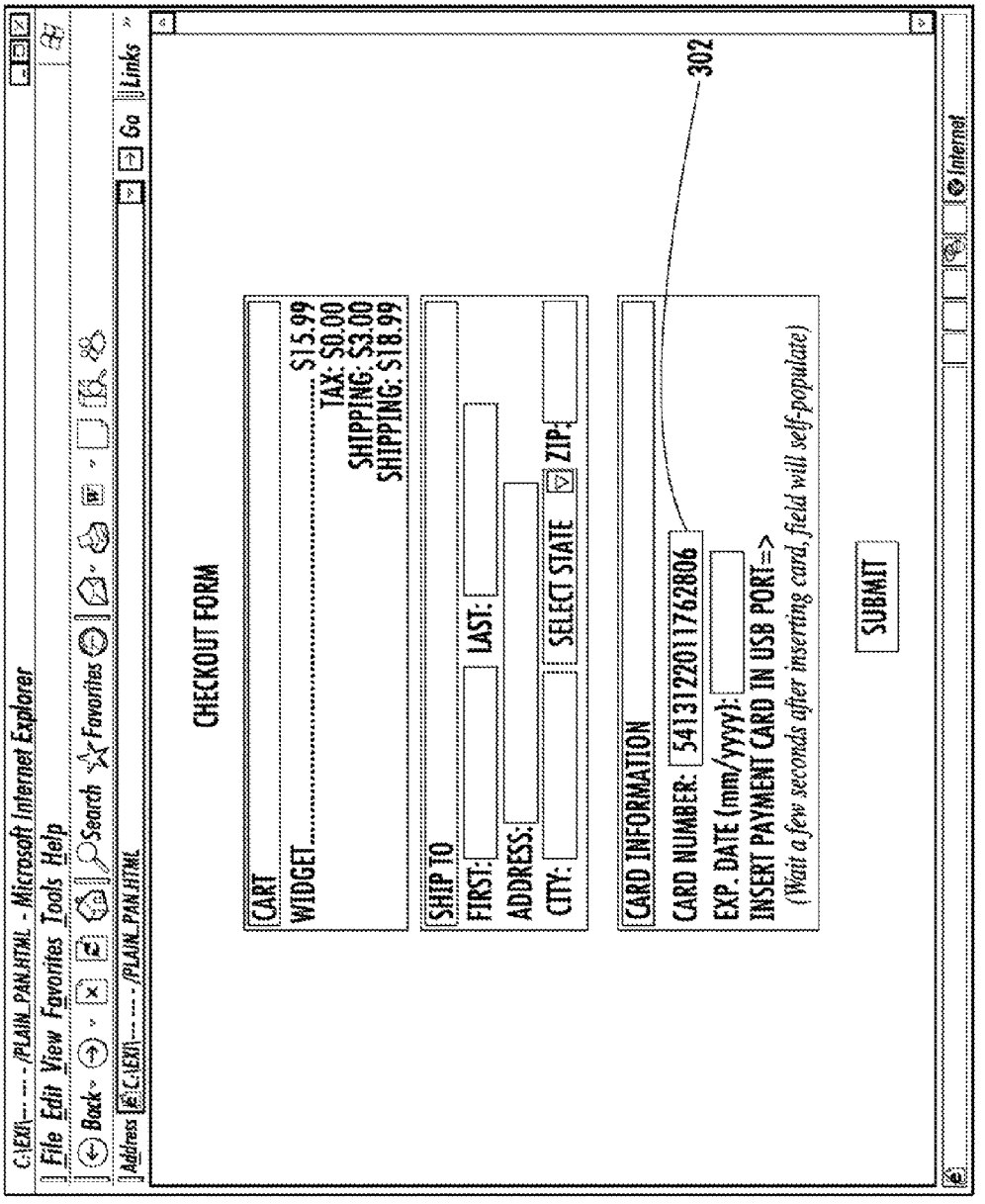

C:\EXE\---- ---- /PLAIN_PAN.HTML - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\EXE\---- ---- /PLAIN_PAN.HTML
Go Links
CHECKOUT FORM
CART
WIDGET..... $15.99
TAX: $0.00
SHIPPING: $3.00
SHIPPING: $18.99
SHIP TO
FIRST: LAST:
ADDRESS:
CITY: SELECT STATE ZIP:
CARD INFORMATION
CARD NUMBER: 5413122011762806
EXP. DATE (mm/yyyy):
INSERT PAYMENT CARD IN USB PORT=>
(Wait a few seconds after inserting card, field will self-populate)
SUBMIT
302
Internet

FIG. 15.1

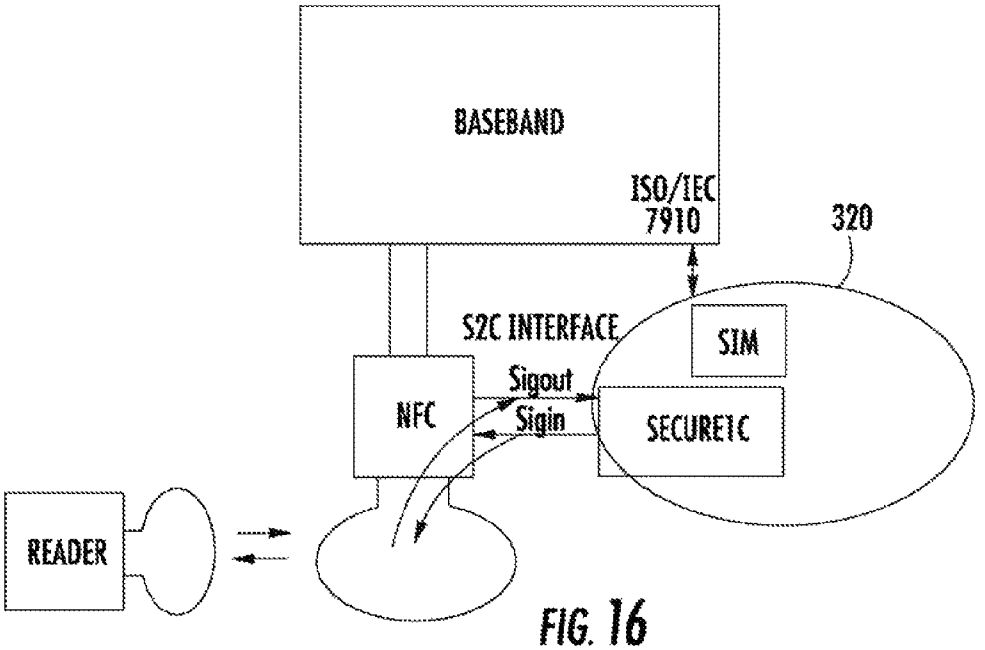


FIG. 16

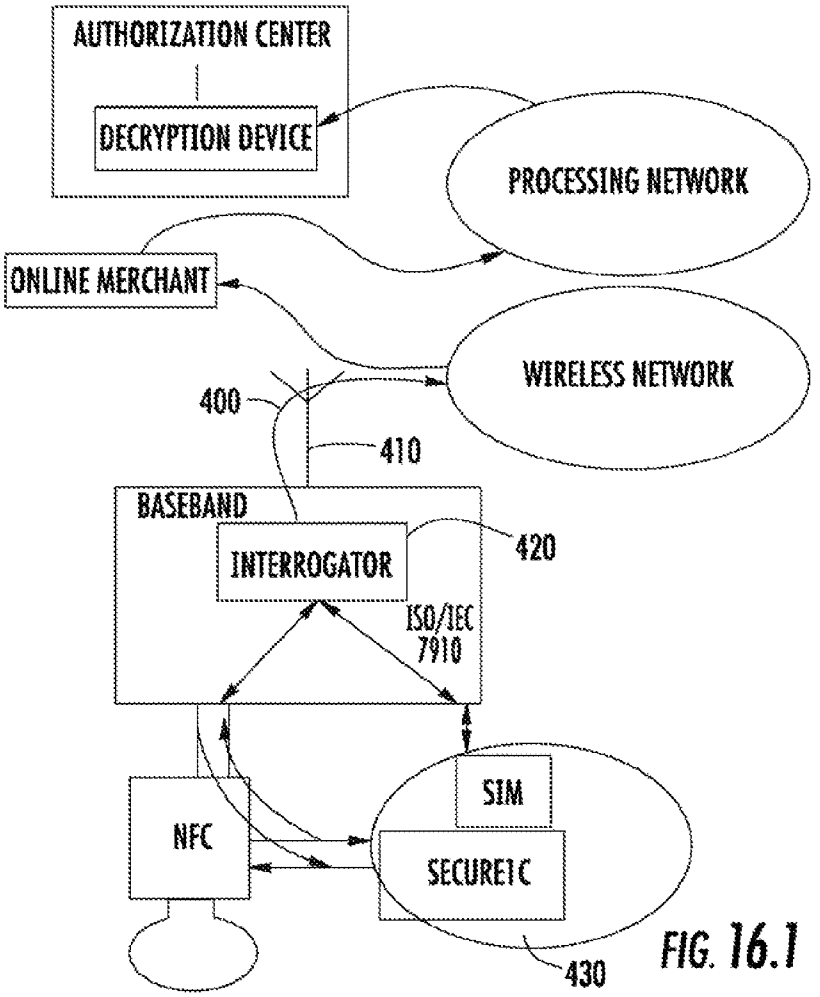


FIG. 16.1

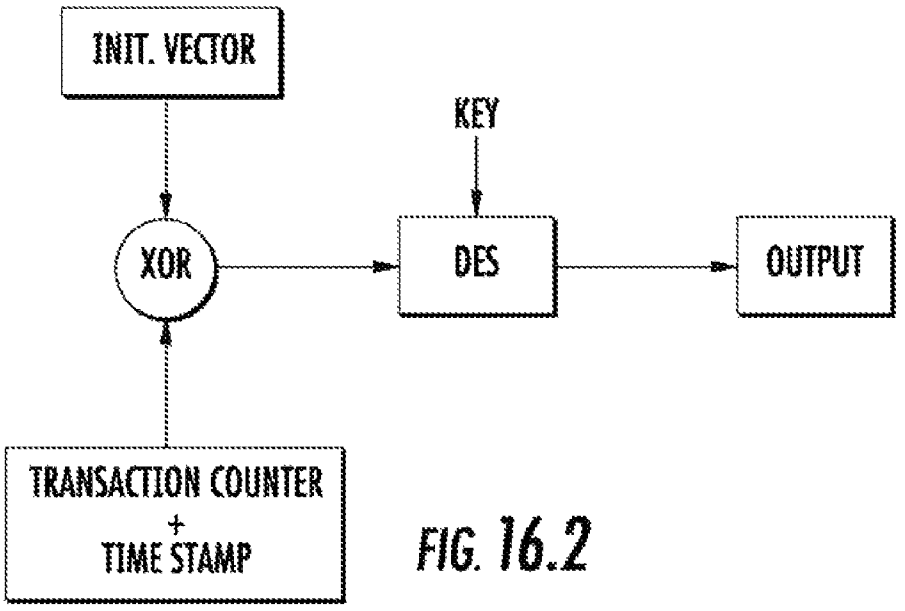

INIT. VECTOR
KEY
XOR
DES
OUTPUT
TRANSACTION COUNTER
+
TIME STAMP

FIG. 16.2

SELF-AUTHORIZING DEVICES

CROSS REFERENCES TO RELATED APPLICATIONS

This patent application claims priority from and is related to U.S. Provisional Patent Application Ser. No. 60/897,110 filed Jan. 25, 2007, entitled: Method and Apparatus for Self-swiping Smartcard Payments and this patent application claims priority from and is related to U.S. Provisional Patent Application Ser. No. 60/932,704 filed Jun. 1, 2007, entitled: Method and Apparatus for a Self-swiping Smartcard. Provisional Patent Application Ser. Nos. 60/897,110 and 60/932,704 are incorporated by reference in their entirety herein.

FIELD

This invention relates to the field of devices configured to authorize transactions using secure element microchips. More particularly, this invention relates to tokens or cellular network devices that contain secure element microchips and are configured to authorize financial transactions over the internet.

BACKGROUND

In some payment technologies such as smartcards, a microchip referred to as a "Secure Element" (SE) is embedded into the payment card, the payment fob, or another other device that may be used for making payments. In order to extract information from the SE, an interrogator, also referred to herein as a "reader", is required to interact electrically with the SE. The reader typically follows standards set forth by the International Organization for Standardization (ISO) or proprietary standards established by financial institutions or other application providers. In addition to making payments such devices may be used for other purposes such as controlling access to networks and databases and verifying identity. Such devices typically employ sophisticated technologies for enhancing the security of these transactions and preventing fraud. However, the use of the internet is becoming more popular for such purposes. What are needed therefore are devices and methods that adapt the enhanced security and fraud prevention techniques used in smartcard systems for use in internet-based transactions.

SUMMARY

The present disclosure provides, in one embodiment, a self-authorizing smart token that includes a mounting structure having an integral communication connector configured to connect to a computer terminal. This embodiment also includes a secure element that is affixed to the mounting structure and the secure element has a data file. There is also a secure element reader that is affixed to the mounting structure and configured to interrogate the secure element by executing file system functions according to ISO 7816-4 and to generate file information from the secure element data file. The self-authorizing smart token also has a communications controller that is affixed to the mounting structure and that is configured to receive the file information from the secure element reader and that is configured to convert at least a portion of the file information into transaction information and to transmit the transaction information to the computer terminal through the communications connector.

Another embodiment provides a self-authorizing smart token that has a mounting structure that includes an integral Universal Serial Bus (USB) connector configured to connect to a computer terminal. There is also a secure element that is affixed to the mounting structure and the secure element has a data file. This embodiment also includes a communications controller that is affixed to the mounting structure and that is configured as a Human Interface Device (HID) class USB-device and that is configured to extract information from the secure element data file and that is configured to convert at least a portion of the data file into transaction information and to transmit the transaction information to the computer terminal through the USB connector.

In another embodiment, a self-authorizing smart token has a mounting structure that has an integral communication connector that is configured to connect to a computer terminal. There is a secure element that is affixed to the mounting structure, and the secure element comprising a data file comprising financial authorization data. There is a communications controller that is affixed to the mounting structure and configured to extract at least a portion of the financial authorization data from the secure element data file and configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data as transaction information to the computer terminal using the communication connector.

A further embodiment provides a self-authorizing cellular network adapter for a cellular network device configured with a cellular network application interface. The self-authorizing cellular network adapter includes a secure element that has a data file. There is a secure element reader that is configured to interrogate the secure element by executing file system functions according to ISO 7816-4 and to generate file information from the secure element data file. Further, there is a communications controller that is configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction authorization information and to transmit the transaction authorization information to the cellular network device through the cellular network application interface.

BRIEF DESCRIPTION OF THE DRAWINGS

Various advantages are apparent by reference to the detailed description in conjunction with the figures, wherein elements are not to scale so as to more clearly show the details, wherein like reference numbers indicate like elements throughout the several views, and wherein:

FIG. **1** is a drawing of one embodiment of a self-swiping card with a USB interface.

FIG. **2** is a drawing of a close up view of the USB interface connector on one embodiment of a self-swiping card.

FIG. **3** is a drawing of the internals of one embodiment of a self-swiping card.

FIG. **4** illustrates a circuit board schematic according to one embodiment.

FIG. **5** illustrates a system where a self-swiping card is used to deliver track 1 and track 2 data to a merchant remotely via the internet.

FIGS. **5.1** and **5.2** illustrate interaction and data exchange between an interrogator chip and an SE.

FIG. **5.3** illustrates a method of encrypting data.

FIG. **6** illustrates one embodiment of an online web form with an auto-populating field for a self-swiping card.

FIG. **7** illustrates the decrypted track data that was encoded within the information that came from the auto-populating field from FIG. **6**.

FIG. **8** illustrates an embodiment of a self-swiping card with a USB interface.

FIG. **9** illustrates a further embodiment of a self-swiping card with a USB interface.

FIG. **10** illustrates an embodiment of the smart card module embedded in the card.

FIGS. **11**A and **11**B illustrates embodiments of a self-swiping card in a mini-SD and an SD form factor.

FIG. **12** illustrates a system where track 1 and track 2 data with an encrypted PAN (Personal Account Number) data are delivered via the world-wide web.

FIG. **13** illustrates a method of encrypting PAN digits that maintains the original bank routing code.

FIGS. **13.1**-**13.4** illustrate elements of an encryption algorithm.

FIG. **14** illustrates a system where a reader on card is queried as an alternative to keyboard input.

FIGS. **15** and **15.1** illustrate an embodiment of an online web form with an auto-populating field.

FIGS. **16** and **16.1** illustrate a mobile phone embodiment.

FIG. **16.2** illustrates and encryption technique.

DETAILED DESCRIPTION

In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings, which form a part hereof, and within which are shown by way of illustration the practice of specific embodiments of self-authorizing smart tokens and embodiments of self-authorizing cellular network adapters. It is to be understood that other embodiments may be utilized, and that structural changes may be made and processes may vary in other embodiments.

For the purpose of simplifying language and providing a convenient example, the device that houses a secure element (SE) microchip is typically referred to herein as a "card" or "card device." It is important to note that the "card" or "card device" may not physically resemble the shape or size of a typical payment card and may come in various alternate form factors such as fobs, cartridges, or dongles, or form factors that resemble removable digital memory media such as secure digital (SD) chips. The term "token" is used to encompass all of these form factors and the term "smart token" refers to a token that includes an SE. Each token has a mounting structure such as substrate (for card devices) or a packaging case (for fobs, cartridges, and dongles or SD chips).

In many embodiments described herein a card is configured to interact with a computer terminal. As used herein a computer terminal refers to a personal computer or a special-purpose terminal provided at a point of sale or public kiosk. For the purpose of simplifying language and providing a convenient example the term "PC" (referring to a personal computer) will be used as an example of a computer terminal. Typically the PC has access to an internet. As used herein the term internet includes the world-wide web as well as any other public or proprietary network that may be used for authorizing transactions.

In addition to applications involving computer terminals, embodiments are provided for mobile phones and personal digital assistants (PDAs) that communicate over a cellular network. Such mobile phones and PDAs are referred to herein as cellular network devices. The term "cellular network adapter" is used herein to describe a system that includes in a secure element (SE) microchip for use in a cellular network device. Of particular interest are cellular network devices that are configured for authorization of financial transactions over a network. Typically the cellular network device includes a web browser that is configured for authorization of a financial transaction over the world-wide-web. However in some embodiments the browser may connect to a different public network or to a proprietary network. In some embodiments the cellular network device may connect to a dialup voice network and the cellular network device may be configured for authorization of a financial transaction over the voice network, such as by transmission of DTMF tones or by other encoding.

As previously indicated, in order to extract information from an SE, an interrogator or "reader" is used to interact electrically with the SE. Because readers are not typically part of most PCs, it is very beneficial to place the reader functionality on the card device and translate information from the SE into a data stream format such as a USB (Universal Serial Bus) that PCs are generally capable of processing. Other convenient translated formats include software application output, text messaging (e.g., short message service (SMS)), and email messaging. It is particularly advantageous to configure the card devices for HID (Human Interface Device) keyboard emulation for inputting a form field or fields on an application running on the PC. It is also very beneficial to place the reader functionality in the cellular network adapter and translate information into a data stream that may be sent over the cellular network by the cellular network device.

As used herein the term "host device" is used to refer to either (a) the computer terminal that receives the information from a card device or (b) the cellular network device that receives the information from the cellular network adapter.

A significant advantage of extracting and delivering the data within a card device or cellular network adapter is the ability to know beyond reasonable doubt that the data string being delivered over the internet indeed came from a particular SE. This knowledge creates a more secure transaction with lower risk to the merchant, card issuing bank, and card associations.

Heretofore the most secure methods for assuring the validity of an electronic transaction has involved extracting information from a banking card by of swiping the magnetic stripe through a magnetic stripe reader, or extracting the information from a smartcard with a separate contact or contactless reader connected to a point of sale terminal (POS). These methods are known as "card-present transactions." Because of their enhanced level of confidence in validity these methods allow a merchant to receive a discounted transaction fee for that particular transaction. An example of a less secure transaction is reading or entering account numbers, expiration dates, and card verification codes from a card in a phone call or with on-line internet ordering. These transactions are known as "card not present transactions" and incur a full transaction fee.

Preferred embodiments provided herein provide for incorporating a reader on a card device or within a cellular network adapter to extract and deliver banking track data that were generally not previously possible because of the inability to extract information from the SE or from a magnetic stripe at a computer terminal without a reader or to extract information from an SE in a cellular network adapter without a reader. Such embodiments add value in a mobile commerce or e-commerce environment by enabling more secure transactions over a voice network or an internet.

To prevent fraud, electronic transaction systems typically attempt to verify one or more of the following characteristics of a requestor:

1) Something the requestor knows (a password, answer to a question, etc.)
2) Something the requestor has (a physical token, such may be confirmed by embodiments herein)

3) Something the requestor is (such as a physical trait established by a fingerprint or other biometric identifier)

"2-factor authentication" is defined as an authentication where the requestor (the entity to be authenticated) successfully provides two of the above three different types of verifications. If two of these verifications have been provided the authentication is considered "strong." One important advantage of many embodiments described herein is the ability to confirm that a card is present and authentic. This by itself provides a basis for 2-factor authentication over a public or private network using currently ubiquitous access hardware such as a computer terminal or a cellular network device.

Described herein are configurations of a "Reader On Card" (ROC) or "self-swiping" card, or "self-authorizing" card. The terms "ROC," "self-swiping" and "self-authorizing" are synonymous and refer a configuration wherein the card device or cellular network adapter contains both an SE and SE reader functionality. Configurations for a dynamic or encrypted PAN (Personal Account Number) are also described. This refers to configurations where the "Reader On Card" further encrypts the track data in order to securely transport the data packet over a public network. Neither of these concepts is limited to one particular form factor or embodiment. Some examples of devices that may employ these elements include a USB device or a token or a mobile phone that is enabled with contactless (13.56 MHz radio frequency) or NFC (Near Field Communication) RFID technology.

An SE typically contains a microprocessor, random access memory (RAM) that stores a data file, read-only memory (ROM), flash memory (EEPROM), encryption engine(s), and one or more methods of interfacing the SE. Executable applications such as the MasterCard, PayPass, VISA, Contactless, and AMEX Express Pay may be compiled and placed on an SE. Personalization information that is unique to the specific card holder is generally also placed on an SE. The applications for an SE are typically specified by application providers such as MasterCard, VISA, or AMEX among others. The applications may be created using any number of software development tools and then compiled to run on any number of SE architectures.

The applications running on the SE are typically provisioned with card holder specific information prior to being delivered to the card holder. The provisioning entities such as First Data Corp. must follow strict guidelines set forth by card associations such as VISA, MasterCard, AMEX, and others that keep the provisioning process secure and ensure that customer data is protected inside the SE and that only the card issuing banks or their agents are able to verify the information that is extracted from the SE. It is important that this process is not disrupted and abided by while including the advantages of the present invention.

In order to extract information from the application(s) on an SE, an interrogator, also referred to as a "reader", is required to interact electrically with an SE. The interrogator software may be provided in many different forms such as a software module or a pre-programmed microchip. The hardware that the interrogator runs on may also come in different forms such as an ARM processor, or a small M8 processor. The hardware that encompasses a SE and or an interrogator may be referred to as a chip or die. A die is the raw silicon that is packaged during the chip manufacturing process.

The applications on an SE are accessed by a reader with specific query/response calls defined by the application provider as mentioned above. These applications are generally designed to protect the data on a SE via encryption engines in the SE. The protocols used by a reader to pass data to and from a SE are typically defined in the ISO 7816 or ISO 14443 specifications. These protocols are referred to as query/response protocols. An interrogator sends a query and a SE sends a response.

In many embodiments the physical interface between a reader and an SE conforms to standards defined in the ISO 7816 and ISO 14443 specifications. The ISO 7816 specification defines a "Contact" interface to a SE in which the SE is powered by DC voltage and ground electrical connections from an interrogator. The data transfer during the interrogation is managed by an interrogator providing a clock signal connection and data line connection to an SE. The ISO 14433 specification defines a "Contactless" interface to an SE in which the SE is powered by an inductive field produced by an interrogator during the interrogation. The data transfer during the interrogation is managed over a 13.56 MHz carrier signal provided by an interrogator. The physical interface that the interrogator uses to connect to the SE may also be provided in different forms such as UART, or an NXP proprietary S2C interface. It is also possible that the interrogator shares the same silicon chip as the SE and the interface between them is provided by internal memory or physical traces in the silicon.

The "Universal Serial Bus" USB interface is a standard interface to laptop computers and personal computers or other form of computer terminal as a means of expanding the capabilities of the computer terminal or transferring information between the computer terminal and another device. More information about the USB interface may be obtained at www.usb.org.

The "Human Interface Device" HID interface is a class of USB interface which is a universal standard for a USB host to connect to USB client device. Within the HID class, there are several defined types of devices, including a "keyboard" type. By the USB device interfacing the USB host with the "keyboard" type of HID class interface, the standards require that the USB host recognize the device as a standard device (e.g., a keyboard) and accept input as such without requiring that the computer have any special drivers or operating system updates installed. By configuring a card device as an HID keyboard the card device emulates a keyboard attached to the computer terminal. The computer terminal will recognize and accept the card device as a keyboard input device. This is a very useful feature in many applications for enabling a more user friendly "self-swiping" functionality in the card device.

Included in most embodiments is a "communications controller." The communications controller provides the interface for data exchange between the reader and a communications connector (in the case of a card device) or the interface for data exchange between the interrogator and a cellular network application interface (in the case of a cellular network adapter). The communications connector may be provided in different forms such as USB, USB connection with HID class keyboard type or USB connection with mass storage class, among many others. The interface may be established using other hardware interface standards as well such as SDIO, mini-SD. In many card device embodiments the communications connector is an integral part of the card device, meaning that the communications connector is formed on an edge portion of the card. The cellular network application interface may, for example, be provided as a baseband input/output port for a web browser running on the cellular network device. The physical connection may be provided by a communication bus or by micro-circuitry in common processor and memory areas in the baseband portion of the cellular network device.

In either card device embodiments or in cellular network adapter embodiments, the communications controller may be physically incorporated into the reader or may be physically

incorporated into the secure element or the communications controller may be a physically separate electronic element. In some embodiments the capabilities defined herein for the communications controller may physically be performed in the chip that is primarily the SE and/or the interrogator, or the capabilities of the interrogator may physically be performed in the chip that is primarily the SE and/or the communications controller, or the capabilities of the SE may be physically performed in the chip that is primarily the communications controller and/or the interrogator, or the capabilities of the interrogator and the SE and the communications controller may all be performed in a single chip. In any case, the capabilities of the communications controller, the SE and the interrogator are still considered to be performed by the "communications controller," the "SE" and the "interrogator" respectfully. Furthermore, in some embodiments the PDA or phone processor may be connected directly to the SE. In such embodiments the phone processor interrogates the SE to achieve valid transaction data from the SE. The PDA or phone processor may deliver this data to a form field or directly over the cellular network. In such embodiments the communications controller and the interrogator of the SE are now a portion of the PDA or phone processor itself instead of either of communications controller or the interrogator being a separate hardware chip.

In some embodiments of a self-swiping "Reader On Card" (ROC) device the interrogator and SE are integrated together on the same medium, device or circuit. It is important to note that in contactless implementations the interrogator portion of the ROC device may not be able to function from power harvested from the contactless inductive antenna, and therefore may require power from an external source, such as the communication connector to the computer terminal (in the case of a card device) or the cellular network device battery (in the case of a cellular network adapter).

The data that are automatically delivered to the host device may represent bank account information in the form of "Track 1" and/or "Track 2" data. Track 1 and Track 2 data are commonly-used representations of bank account information that is specific to a card holder. These data generally have a very specific industry standard format in order to be properly processed through transaction processing systems. The Track 1 data format was developed by International Air Transportation Association (IATA). The Track 2 data format was developed by the American Banker Association (ABA). In some embodiments the Track 1 data that are generated as file information from the SE data file and converted into transaction information by the communication controller and transmitted to the host device may comprise only a portion of the Track 1 data content specified in a standard published by the IATA. In some embodiments the transaction information may be the entire Track 1 data content specified in an IATA standard. In some embodiments the Track 2 data that are generated as file information from the SE data file and converted into transaction information by the communication controller and transmitted to the host device may comprise only a portion of the Track 2 data content specified in a standard published by the ABA. In some embodiments the transaction information may be the entire Track 2 data content specified in an ABA standard. However, it is important to note that in some embodiments the transaction data delivered to the host device may not be standard Track 1 or Track 2 data. It is possible that this data may be in another standard or proprietary format. In any case, the transaction data may or may not be an encrypted cipher text in whole or part upon delivery to the host device.

Typically a card device transaction authorization process begins when a user is instructed by a web browser-based application program on a computer terminal to insert a self-authorizing smartcard into a USB port on a computer terminal. When the smartcard is inserted, if the self-authorizing smart card is a USB HID keyboard class card device, the smartcard typically self-initializes with the operating system of the PC and begins to automatically input the relative card data into the appropriate field in the browser form. Many embodiments automate the input of card information such as PAN, expiration date, and security code. The USB HID keyboard class card device may use access keys or "hot keys" to navigate the form that has the current focus for input in the computing device. The card device may also automatically remove any information that may have been inadvertently typed prior to card device insertion. The card device may also automatically "submit" the online form using access keys or "hot keys".

An example where the HID keyboard device of the card automatically inputs a sequence of key presses of the device using "hot keys" is as follows.

a. [alt]+',' (This makes the cursor take focus on form element that has a designated access key of ',' —the comma key)
b. [ctrl]+'a' (This makes the cursor select all the text that is existing in the current field of focus)
c. [Backspace] (This makes the cursor erase all the currently selected text)
d. [alt]+'.' (This makes the cursor take focus on the form element that has a designed access key of '.' —the period key . . . this could be set to a "submit" button for example)

A benefit of many embodiments is delivery of the information on the SE to the form that has the current focus for input in the host device. A self-authorizing smart token or a self-authorizing cellular network adapter the may deliver this information in a manner of emulating keystrokes from a keyboard device to the host device. For security reasons the application program that has the current focus on the host device (and is collecting this input) may take precaution inside its programming logic to require that the keystrokes being input into a particular form field are keystrokes and not simply a "paste" keystroke from an electronic "clipboard." Alternately, the application program may require that the keystrokes being input into the form field are fast keystrokes resembling the pattern that only an automated keystroke emulation input device could provide, and not a slower pattern of input that would resemble a manual input of keystrokes. Knowing these requirements, the communications controller element of the card device or the cellular network adapter may be programmed to provide the transaction information to the host device in a prescribed cadence for an application running on the host device.

For security reasons the form that has the current focus on the host device and is collecting this input may take precaution inside the programming logic that various pattern of "hot key" presses ([alt]+'some key') may be used to identify the input device as a secure input device. It is important to note the "hot key" keystrokes cannot be duplicated with the traditional "copy", "cut", or "paste" to the clipboard that some operating environments provide. However, such hot key keystrokes may be provided by various embodiments of communication controllers in self-authorizing devices defined herein.

Many embodiments deliver Track 1 and/or Track 2 data to a merchant from the SE of a payment card using the USB interface of a remote customer's PC in a simple, customer

friendly manner. The consumer typically only has to insert the card device into a USB port on his/her computing device and the keystroke data will automatically input into the form that has the current focus on the computing device via keyboard emulation from the card device.

Many embodiments deliver Track 1 and/or Track 2 data that contain a dynamic card verification number from the SE of a payment card device, using the USB interface on a PC of a remote customer.

Many embodiments deliver Track 1 and/or Track 2 data that contain an incrementing transaction counter from the SE of a payment card device, using the USB interface on a PC of a remote customer.

Many embodiments use a "unique number" that is stored in the SE and delivered from the card device as further access control security that must be provided to in order to protected content such as recorded music, recorded video, live media, photos, documents and other similar media. An example of this is that the data file of sensitive or licensed content may be encrypted with a key or a diversified key based on the key within the SE. This would allow only the card holder of the SE to successfully "unlock" and view or listen to the protected content.

Many embodiments use a transaction counter that is stored and updated in the SE to uniquely identify a card holder as well as uniquely identify each given transaction or "swipe" from the card device. Remote transaction approval software may check that the Track 1 and Track 2 data from an SE is what is expected for the current transaction, and may update the transaction counter for the next transaction.

In many embodiments the card device is configured to resemble the physical form factor of typical payment cards as closely as possible with the exception of adding a region of the card that is meant to be inserted into the USB port of a computing device. This facilitates carrying the card device in an ordinary wallet or purse.

In many embodiments the smart token is configured to resemble the physical form factor of a "fob" that may be placed on a consumer key ring.

In many embodiments the card device is configured to limit the height of the USB connector so that the device is thin enough to still be carried in an ordinary wallet or purse.

In many embodiments the self-authorizing smart token or the self-authorizing cellular network adapter is designed to minimize part count and assembly costs so that it can be manufactured at a very low price for high volume, low cost uses.

Referring now to FIG. **1**, the face and back of the self-swiping card medium **10** are shown. The dimensions of this embodiment are roughly 2⅛×3⅛ inches, with a preferred maximum thickness of 0.09 in. The nominal thickness of the card is a maximum of 1/32 in. Looking at the left side of the figure, there is a diagonal protrusion **12** that contains the connector **14** for a USB connection of a mating PC. The four contacts visible in the figure are the power, ground, D+, and D− signals that are defined in the USB specification at www.usb.org. The diagonal of the USB connector protrusion **12** is approximately 45 degrees and allows the protrusion approximately ⅝ in. clearance for insertion into a USB connector on a PC. The boundary of the card has been adjusted from its typical rectangular shape to account for this connection area. The diagonal protrusion has a clearance gap **16** between itself and the lower boundary of the card as seen in the figure. This gap **16** is for the purpose of allowing clearance of the "thicker" USB connection protrusion into some forms of "insertion" type magnetic stripe card readers. The face of the card also shows the PAN (portrayed as 0000 0000 0000 0000), expiration date, and card holder name in similar location to a typical rectangular banking card. The back of the card includes a magnetic stripe **18** that is disposed in a location similar to that of a typical rectangular banking card.

Referring to FIG. **2**, the close view of the USB connection protrusion of the self-swiping card medium as shown. Note the change in this thickness of the card from region **30**, where the card is approximately 1/32 inch thick to zone **32** where the maximum thickness of the protrusion is approximately 0.09 in. where the USB contracts **34** are located. The protrusion of the male USB connection is approximately 15/32 in. wide in order to fit into the standard USB female connection on a PC as defined at www.usb.org. Approximately 3/16 in. in back of the leading edge of the protrusion there is a notch **36** that changes the thickness of the protrusion. This thickness change is for accommodating the "snap fit" of the USB female connector on the PC as defined at www.usb.org. The clearance between the leading edge of the protrusion and the bulk of the card medium is approximately ⅝ in. The style of this particular type of USB connection is not a standard mail USB connection. It has been altered to be much thinner than the typical male connection. As a result, it is susceptible to "upside down" insertion into the female USB connection.

Referring to FIG. **3**, the profile of a self-swiping card **50** with inside components exposed is shown. An antenna **52** is a printed or wire wound antenna that creates an inductive coil that provides power and transmits data to and from a secure element **54**. The number of turns in the antenna **52** is dependant on the properties of the SE as well as the size of surface area the perimeter of the antenna covers. The antenna **52** is embedded inside the card medium and may or may not be congruent with the card medium perimeter. In some embodiments it may be desirable to shrink the area of the antenna **52** for manufacturing reasons such as card embossing. The secure element **54** shown in FIG. **3** is a microchip die that is wire bound to the module face plate through manufacturing methods. The secure element microchip die is typically then coated with epoxy for protection. In the embodiment of FIG. **3** the secure element **54** is a dual interface device that is accessible through the contactless antenna interface or through the contact **7816** style interface. When not plugged into the USB connection on a PC, the antenna serves as the sole power supply, data transmitter, and data receiver for the SE **54**. When plugged into the USB connection on a PC, the antenna **52** is not intended to be used as a power supply or to transmit or receive data. Instead a combined interrogator/communications controller reads information from the SE **54** and transmits information to the PC through a USB connector on the protrusion of self-swiping card **50**.

The protocols that define the communication to the SE are defined in ISO 14443 (contactless) and ISO 7816 (contact). The commands to communicate to the applications that are running on the SE are typically designed to interrogate the secure element and execute file system functions according to ISO 7816-4 in order to generate file information from SE data file. However, in some embodiments the commands to communicate to the applications that are running on the SE are provide by the application providers. In any case, the commands are generally the same regardless of the interface method (contact or contactless).

The SE is generally a secure microchip that has built in encryption engines, RAM, micro-processor, EEPROM, and communication interfaces. The interrogator and the communication controller (USB interface) chip shown in FIG. **3** is a chip that contains a microprocessor, RAM, EEPROM, and built in USB interface engine. The chip is programmed to describe itself to the host PC as a HID class "keyboard"

device upon connection to the PC. The chip then communicates to the SE via ISO 7816 (contact) interface protocols to acquire and build Track 1 and Track 2 data. After track data are acquired from a successful "read" of the SE, the data is then delivered to the PC's USB bus through the communications connector protrusion shown in the FIG. **3**. It is important to note that it is possible for both the SE and the interrogator/USB interface chip die to be mounted and wire bound together on the same module medium. It is also important to note that these two chips could also be contained in one piece of silicon sharing the same RAM and/or EEPROM memory space.

FIG. **4** illustrates a circuit board schematic **60** according to one embodiment. This shows a more detailed layout of the components described in FIG. **3** as well as the supporting components of typical embodiments. In this particular embodiment, the interrogator/USB bridge chip/die is a chip made by cypress semiconductor with a part number of CY7C3. The SE used in this particular embodiment is a chip/die with a standard ISO 7816 contact type interface in combination with a standard ISO 14443 contactless interface.

FIG. **5** illustrates a flow diagram that describes one method embodiment. After the card device is plugged into the USB connector on the customer computing device, the card device powers up and begins to interrogate the SE on the card device. The interaction and data exchange between the interrogator chip and the on the SE could look something like the diagram in FIG. **5.1**. In preferred embodiments the interrogation process conforms to application level protocols (APIs) established by ISO 7816-4. ISO 7816-4 defines two such application-level protocols:

(a) File system API providing a set of functions to manipulate files (e.g. read, write, select etc.)

(b) Security service API allowing the smart card and the reader to mutually authenticate themselves and also to encrypt data to be exchanged between the card and the reader.

In preferred embodiments the interrogation process conforms to protocol message structures also defined in 7816-4 to support the APIs. This message structure consists of application protocol data units (APDUs) which are exchanged between the reader application and the smart card application by the link level protocol. There are two types of messages used to support the ISO 7816-4 application protocols: the command Application Protocol Data Units APDU (sent from the reader to the card) and the response APDU (sent from the card to the reader).

After the interrogator has received the all the data from the interrogation of the banking application on the SE, the interrogator can then build the data string that is to be sent to the computing device as keystrokes. It is important to know that the SE can run multiple applications from different application providers. It is possible, and is one embodiment of this invention, for the interrogator to deliver the information that was acquired during interrogation of the banking application on the SE to a second application that resides on the same SE so that the second application can process, build, and possibly encrypt the data that will be delivered to the computing device as keystrokes.

An example of this embodiment that contains the interrogation of two applications on the SE may look something like the diagram in FIG. **5.2**. The dotted lines in the figure represent the times during the entire interrogation of the SE that the interrogator selects different applications to use. The interrogator or the interrogator application on the SE may or may not encrypt the final Track 1 and/or Track 2 data.

FIG. **5.3** shows one embodiment of a method of encrypting this data. After the interrogator has acquired or built the data to be sent to the computing device as keystrokes, the USB interface enumeration begins. During the enumeration process, the card device, which is the client device, exchanges information with the USB host device. The information exchange is defined in the USB specifications and can be obtained at www.usb.org. As part of the exchange, the card device will send "descriptors" that tell the host device about the drivers that are required to run the client card device. The descriptors that the card device sends to the host include a HID (Human Interface Device) descriptor. The card device sends another descriptor that further defines the type of HID device to be a "keyboard" type of device. The USB host will now recognize the card device as a keyboard and expect that the card device will deliver "key codes" that represent keystrokes as input data. After enumeration has occurred and the host USB device recognizes the card device as a keyboard, the card device begins to deliver data to the current form that has the focus on the computing device. The data that are delivered may consist of:

a. Identification of the entity to which the data must be passed to for further processing.

b. Identification number of the particular card device that is delivering the data.

c. Identification number of the cryptographic key to be used for decrypting the data that is delivered from the card device.

The application, such as an internet browser, that is running on the computing device that has collected this information is then responsible for passing the information to the entity identified by the data above for processing. One embodiment of this invention involves passing this information in an online setting by one internet server passing this information string to another internet server. In this embodiment, the entity that controls the internet server that receives this information can then process the information along with the identity of the owner of the requesting internet server as they see fit. The entity that received the data can then return resultant data back to the requesting party. Also, in this embodiment, the information that is passed back to the requesting party is Track 1 and/or Track 2 data that is used to process typical card payment transactions by merchants.

Referring to FIG. **6** the internet browser form that receives the information from the card device as shown. This form represents one example of how a card device may be used. In this example an application running on a PC includes one specific field **100** on a form that is designated as the field that the card device will automatically populate when the card device is plugged into the PC that is displaying this form. In this example, the application has been programmed so that the form field **100** can be addressed using an access key or "hotkey" of ',' (the comma key). That is, when the card device issues this "hot key" keystroke (by use of keyboard emulation), the cursor will automatically move its focus to the field **100**. The HTML (hypertext markup language) code that is used to create the self populating field may have this syntax:

<input type="text" name="data" size=""access key=","/>

The card device then populates the form field **100** with data. Then the auto-populating field **100** may be further checked by the application program for the authenticity of the keystrokes by the internet browser using "Java-Script" code that may be embedded into the HTML code. Also, the internet browser may check that each key was actually typed into the field by keystrokes rather than the use of "copy", "cut", and "paste" commands that may be provided some operating environments. The internet browser may also check that each key-

stroke was typed very fast resembling an automated input rather than a slower manner that would resemble manual input. The internet browser may check other aspects of the input data for its validity as it sees fit.

Referring to FIG. **7**, an internet browser screen displays decrypted data **110** that may be provided to a merchant transaction authorization system. The track information shown here is acquired using a Reader On Card (ROC) system. After the card reader extracts information from the SE and builds the track data containing the DVCC from the SE on the card, the track data are then delivered to the appropriate field in the transaction requester's browser as encrypted data via a USB HID keyboard interface. The information that is auto-populated on the requester's screen is not the Track data that is depicted in FIG. **7** because the ROC system encrypts the track data on the card device before the field on the requestor's browser is populated and the encrypted data are transmitted. The data on FIG. **7** is a decryption of the data that appears on the requester's screen. If the process is repeated by the requester the DVCC data and the transaction counter will change, in accordance with specifications for secure transaction encryption. In a typical application a merchant that is processing the information would not expose the clear text track information portrayed on the browser screen of FIG. **7**. This figure is merely showing it as an example of the decrypted data. It should also be noted that in many embodiments the SE on the requester's card device may be used to make contactless transactions at in-store POS terminals by holding the card device up to a contactless reader.

Referring to FIG. **8**, the face of one embodiment of a self-swiping card **120** is depicted. The placement of the protrusion that exposes the USB connection, relative to the card boundary **122**, is important. The USB connector **124** may be manufactured in a similar fashion to a typical ISO 7816 smart card module. The typical ISO 7816 module is then seated into the card medium during an assembly process. The exact placement of the module relative to the card boundary is defined in the ISO 7816 specification and many of the assembly machines used to place this module inside the card medium is set to place the module in a specific location as shown in the figure.

Referring to FIG. **9**, one embodiment of an alternate form-factor self-swiping card **140** is shown. This embodiment includes a USB connector **142** but has a form factor that lends itself to placing the card device on a key ring through a hole **144**. The purpose of this figure is to illustrate some of the wide variations that can encompass various potential embodiments.

Referring to FIG. **10**, components of a smartcard module **150** are depicted. On the left is the connector plate (module top) and on the right is the module bottom of the smartcard module **150**. Looking at the right side of the figure, the bottom of the module exposes how the die from both the SE **160** and the interrogator **156** may be mounted. Also shown in the right portion of this figure, are the mounting pads **158** that may be connected to the inductive coil antenna for the contactless interface of the SE. The inductive coil antenna is typically assembled into the card medium prior to placement of the smart card module. The mounting pads are designed to make contact with the exposed ends of the inductive coil antenna. Looking at the left side of the figure, the connector plate is carved or scored in such a way that the connection pads **154** align themselves with the standard female USB connections of DC voltage, ground, D+, and D− that are defined in the USB specification at www.usb.org.

Two embodiments of a self-swiping card medium are shown in FIGS. **11**A and **11**B. FIG. **11**A depicts a standard "miniSD" **180** that is a common form factors for expansion memory or IO functionality. The miniSD **180** has a width **184** that is approximately 20 mm and a height **184** that is approximately 21.5 mm. FIG. **11**B depicts a standard secured device ("SD") **190**. The standard SD has a width **192** that is approximately 24 mm and a height **194** that is approximately 32 mm. These form factors **180** and **182** are fairly ubiquitous in mobile phones and personal digital assistants (PDAs) and therefore are convenient for use in various embodiments of a cellular network adapter. The SE and other electronics to interrogate the SE may be contained within these form factors. Additional features may be added such as additional expansion memory for the mobile device or PDA to access. Further detailed specifications for the SD **190** and the miniSD **180** form factor may be obtained at www.sdcard.org.

FIG. **12** illustrates a flow diagram that describes one method and use embodiment. After the card device is plugged into the USB connector on the customer computing device, the card device powers up and begins to interrogate the SE on the card device. The interaction and data exchange between the interrogator chip and the on the SE could look something like the diagram in FIG. **5**.**1**. After the interrogator has received the all the data from the interrogation of the banking application on the SE, the interrogator can then build the data string that is to be sent to the computing device as keystrokes. It is important to know that the SE can run multiple applications from different application providers. In some embodiments the interrogator delivers the information that was acquired during interrogation of the banking application on the SE to a second application that resides on the same SE so that the second application can process, build, and possibly encrypt the data that will be delivered to the computing device as keystrokes.

An example of an embodiment that contains the interrogation of two applications on the SE typically looks something like the diagram in FIG. **5**.**2**. The dotted lines in the figure represent the times during the entire interrogation of the SE that the interrogator selects different applications to use. The interrogator or the interrogator application on the SE may or may not encrypt the final Track 1 and/or Track 2 data. Specifically, in the embodiment reflected in FIG. **12** the PAN or Personal Account Number is encrypted within the final Track 1 and/or Track 2 data, or possibly by itself only. The encryption is handled in such a way as to not disturb the bank routing code within the PAN. This is typically the first 6 digits of the PAN. The final digit of the PAN is also adjusted as to equal the proper check digit for the new PAN. Once the new PAN is created from encrypting the original PAN, it is substituted in the place of the original PAN. Using this method, the merchant is able to receive the PAN and verify that it is a valid credit card number by checking the digits and calculating the proper check digit. After the PAN is submitted to the merchant for processing via HID keyboard buffer which prints the PAN and possibly other data into a "web form," the information is submitted by the user for processing. The merchant would be able to authorize the transaction as it would any other credit card transaction over the internet. When the encrypted PAN is submitted to the processor for authorization, the processor is able to send the encrypted PAN to a decryption device that will properly decrypt the PAN and build the original PAN to check for authorization. The advantage of using a method like this is that valid Personal Account Numbers are never transmitted from the user's computer over the internet.

To add further protection to the encrypted PAN, there is a transaction counter that can be factored into the encryption algorithm. This allows for a unique card number for each

transaction that is processed. The encryption algorithm, encryption key, and transaction counter may be contained within the SE of the card. The encryption of the PAN may take place with every transaction and to take place within the SE. This type of encryption of the PAN may used with several embodiments of the present invention including mobile phones containing a SE. In the case of the mobile phone, the interrogation of the secure element is very similar to the interrogation depicted in FIG. **5.2**. The mobile phone may not deliver the final data to a "web form", however, by auto populating a field, but instead it may receive the encrypted PAN and other data within its own memory structure and then pass the data to the merchant for processing either via internet or its own phone connection. In any case, this method of PAN encryption helps to protect the original PAN data that is needed to authorize a transaction. Because the PAN data is encrypted on the card itself, it may be considered safe to transmit over a network in clear text to the decryption device.

FIG. **13** presents a representation of a Personal Account Number or PAN **200** that is found on the face of a credit card and within the Track 1 and Track 2 data that is stored on the magnetic stripe or SE of a credit card. The first set of digits **202**, usually ranging from the first 3 to the first 6 digits, is referred to as the Bank Code. This code is designated as a routing number for the many card association networks that describes which bank or "issuer" the PAN belongs to. The second set of digits **204** shown in FIG. **13** indicates the personal account number of the card holder at the issuer. The last digit **206** of the PAN is usually considered a "check byte" that is used to calculate if the complete PAN is indeed a valid PAN number. The algorithm normally used for the "check byte" is called the Luhn algorithm. The algorithm uses the digits in the PAN itself to make the proper calculation of the check byte. For this reason, if any digit in the PAN is changed, it is likely that the check byte will also need to be adjusted in order to make the new PAN considered valid. When encrypting the PAN, it is important not to change the bank code. The bank code may remain the original bank code in order for the encrypted PAN data to be routed to the appropriate bank and then to the decryption device that will replace the encrypted PAN digits with the original PAN digits.

In FIG. **13.1**, and FIG. **13.2**, one embodiment of an encryption algorithm is shown. This embodiment used DES in OFB mode as described in FIPS **81** as defined by NIST. A known initialization vector is XOR with a transaction counter that is maintained by the reader-on-card. Every transaction that is committed to, the counter increases. This will effectively change the initialization vector for encrypting the PAN digits. In a separate embodiment, it is also possible to incorporate a timestamp into the randomization processes of the initialization vector. This may not be possible in embodiments that do not have access to an accurate clock. After the initialization vector is XORed with the transaction counter, or other information, DES encryption is performed on the 64 bit, value using the DES key that is has been previously loaded into the interrogator application that is stored on the SE. This produces a 64 bit output value.

FIG. **13.2** shows the 64 bit output value from FIG. **13.1**. The original account number from the PAN is also shown. The digits that will be changed within this account number are typically the middle **5** digits '6784'. The leading three digits '0' are generally reserved as placeholders for passing the transaction counter to the decryption device. The final two digits '80' are generally used to mark a DES key ID for the decryption device. The DES key ID may or may not be included is some embodiments. The purpose is to allow many different DES keys to be used by many different interrogators. Further on this subject, it is possible to create greater randomization of DES key by including a diversification process of the DES key in the interrogator application. A diversification process takes a master key and applies an algorithm to the key based on known data to produce a further randomized key to be used in the actual transaction. The two-digit key ID may actually be used to diversify a master DES key instead of identify a separate key.

The middle **4** digits to be encrypted may be represented in 14 bits. The 14 bits to be encrypted of the original account number are also shown at the bottom of FIG. **13.2**. According to FIPS **81**, using DES in OFB mode, the number of bits to encrypt can range from one to sixty-four during each iteration of the algorithm.

In this particular embodiment one iteration is shown, resulting in fourteen bits of encrypted cipher text. In order achieve the final cipher text; the first fourteen bits of the DES encrypted output text are XORed with the fourteen account bits that are to be encrypted. The resultant output is the fourteen bit cipher text to be placed back into the PAN, creating an encrypted PAN. FIG. **13.3** shows the conversion of the fourteen bit output from FIG. **13.2** into a four digit decimal. The four digit number is then placed into the issuer account number along with the transaction counter as shown in FIG. **13.3**.

FIG. **13.4** shows the total encrypted PAN **250** with the bank code **252**, the account number **254** and the updated check digit **256** that reflects the new PAN digits. Now, it is possible for this number to be processed in the exact same manner as a legitimate card PAN. The decryption device must be used to replace the encrypted PAN with the original PAN, but it is important to note that all the information for how to do so, including the transaction counter and DES key ID are included in the encrypted PAN.

The number of digits used for the DES key ID, transaction counter, and encrypted digits may vary depending on implementation of this method and the particular embodiment. It is also possible to share a single digit to represent parts of two different data elements. One example of this would be to divide a digit by 2 and discard the remainder to represent 0-4 for one data element (transaction counter, DES key ID, or encrypted digits), and then to divide the same digit by 2 and only use the remainder to represent 0-1 for separate data element (transaction counter, DES key ID, or encrypted digits).

Referring to FIG. **15**, the internet browser form that receives the information from the card device as shown. This form is shown after the field **300** has been self-populated. The content in the form that is shown is an example of an encrypted PAN which is digits in this case and has a bank routing code of '541312'. The transaction counter is populated backwards over the next 3 digits '101'. The third digit, in this example, is used to share with the encrypted digits data element as described in the previous paragraph. So, the transaction counter is actually showing '001' when reversed. Including the shared digit, the next 5 digits represent the encrypted digits of the account number'14194'. The following two digits, '80', represent the DES key ID. And the final digit of'1' represents the check byte.

Looking at FIG. **15.1**, the same "web form" as shown in FIG. **15** is shown with a field **302** auto populated with a second transaction from the same card device. When comparing the encrypted PAN's from FIG. **15** and FIG. **15.1**, the differences are seen here:

1st Transaction—FIG. **15**: 5413 1210 1419 4801 (encrypted PAN)

2nd Transaction—FIG. **15.1**: 5413 1220 1176 280 (encrypted PAN)

When these transactions are received by the decryption device the original PAN may be decrypted and created. In this particular example shown in these figures, the original or valid PAN is:

Original PAN: 5413 1200 0763 2801 (valid PAN)

FIG. **14** illustrates a flow diagram that describes one method embodiment. This particular embodiment is generally not appropriate for use with the HID keyboard emulation class of a USB device. This embodiment shows a 2-way form of communication from the base band device or host PC to the card device. The HID keyboard emulation class of a USB device is typically a 1-way device upon which the HID keyboard USB device communicates to the host PC via an "in" endpoint only. This allows data to move from the keyboard emulation device to the PC only. In such a case the interrogation most likely starts at the time the USB device is plugged into the computer and cannot be initialized by the PC.

The 2-way device as shown in FIG. **14**, offers some added features to the system. In a case like this, the interrogation of the SE may be controlled by the base band device or by the host PC. Data such as an unpredictable number (UN), a timestamp, or some other type of deterministic data may be used during the interrogation of the SE, or may be sent to the card device to initiate an interrogation. An unpredictable number refers a number that may be used in algorithms of certain financial transaction authorization systems, such as VISA® or MASTERCARD®, in the encryption phase of a dynamic card verification code (DCVC). A DCVC is a 3 digit encrypted number that changes for each transaction (the dynamic aspect of the track data). The algorithm to create a DCVC typically uses a UN, a transaction counter, and DES key to derive a DCVC for each transaction. In some embodiments the financial transaction authorization system instructs a reader to create an unpredictable number. In some embodiments the communications controller may be configured to create a random UN and send it to the secure element during a transaction. The UN may be constructed as a hash of a timestamp, for example, and such a UN would ensure the authorization system that the SE made and returned its encrypted DCVC and that it was constructed at a certain (recent) time. This also adds another layer of security by establishing a basis for a precise expiration time for a particular transaction.

After the interrogation is complete, the resultant data string may be sent back to the base band device or host PC. There are many ways this system can be implemented. One example of an implementation would be using a generic HID class that allows both an "in" endpoint and an "out" endpoint to the USB card device. Both the "in" and "out" endpoints of a USB device are described by documentation that may be obtained at the www.usb.org website. The HID class driver is packaged and available on most host PC's. In order to use this HID class driver on a host PC, a client application must be resident and running on the host PC that identifies the proper HID device when it is connected to the host PC. The client application that is using the HID class driver may then issue command packets to the USB card device using the HID class interface and receive response packets from the USB card device using the HID class interface. Although using the HID class interface is not quite as ubiquitous to the system as using the HID keyboard class interface, it is still more ubiquitous then communicating to the USB device using a custom driver implantation. The HID class interface is possible to implement in PC side applications without creating a hardware driver **5** that runs on the host PC. The HID class interface can be created and used as a plug-in to internet web browsers and other PC applications. The HID class interface can also be built into simple executable programs that are allowed to communicate directly to a USB card.

In a similar embodiment it is possible to create a dual-purpose USB device that has both a HID class driver that allows an "out" endpoint to communicate to the USB card device from the host PC, and also uses the HID keyboard class interface with an "in" endpoint to send data back to the host PC via keyboard emulation. Another implementation of this system could be entirely contained inside a mobile phone. A 2-way data channel is used to initiate an interrogation with a secure element as well as receive the resultant data string after the interrogation is completed. It is important to note that there is a dashed line that encompasses a rectangle on FIG. **14** that contains both the "initiator" and the "interrogator" entities. These two entities may be handled and running within the same base band processor in the mobile phone. In this case they may exchange information within libraries or memory space only. The mobile phone may receive the resultant data via a keyboard buffer that can then auto-populate a form field, for example, in a mobile web browser. In any case, the 2-way data channel can be used to give more control as well as possibly more security to the system. By passing the unpredictable number, that is used in the dynamic Card Validation Code (CVC) generation within the SE, timestamp, or some other type of deterministic information, the baseband portion of the mobile phone or the host PC may validate and timestamp any transaction that it requests by linking a timestamp to a particular unpredictable number.

Also, the 2-way data channel represented in FIG. **14** allows for the entire transaction to be triggered by the base band device or host PC. The act of sending data to the card device can signal a start to the interrogation process.

Referring to FIG. **16**, a diagram of a mobile phone with contactless or NFC functionality is displayed. One purpose of a mobile phone or like device with NFC technology is to enable the mobile phone itself to act as a payment card in order to make payments at a contactless terminal that may be located at a retailer location. In this embodiment the SE is embedded in a Secure IC within the phone. The SE on the phone may contain multiple bank accounts and may be controlled by the user interface of the phone. The diagram depicts the phone itself (baseband portion), the cellular network adapter **320** that includes a reader, the SE, and a processor in one of potentially multiple form factors (here either within the SIM or a Secure IC), the NFC bridge chip that is used to convert an electronic data signal to an RF data signal for an external reader, and the external reader that may also be used to interact with the SE in order to retrieve banking information. The reader in the cellular network adapter **320** may communicate to the using a number of different methods. For example, the reader in the cellular network adapter may communicate directly to the SE using ISO 7816-3 and 7816-4 protocols. An external reader may also communicate to the SE through an NFC bridge controller. The NFC controller controls the data paths to the RF interface as well as the data path to the SE. It is important to note that the interrogation of the SE can be initiated and carried out by either the reader in the cellular network adapter **320** or an external reader as shown in the diagram in FIG. **16**.

FIG. **16.1** shows the same hardware device depicted in FIG. **16** being used for a different application. The application in FIG. **16.1** relates to using the same banking information stored on the SE for making a mobile payment transaction over the wireless network. A transaction like this is usually performed using a mobile phone connecting to a remote merchant over a wireless network (such as a cellular network) that

may also be using the public internet and a mobile web browser on the phone itself. In order to deliver the transaction data from the SE to the web browser by the interrogator, keyboard emulation or software plug-in may be used to populate the web browser with the appropriate data. In the case where the transaction is not performed using a mobile web browser, the transaction information may pass to the merchant using other methods such as email, SMS, or other proprietary or standardized communication methods. The cellular network adapter **430** (the interrogator and the communications controller and the secure element), in this case, may be contained as an element **420** inside the mobile phone and exist as a software module running on the baseband of the phone. The interrogator essentially serves the same purpose as the contactless reader shown in FIG. **16**. Its job is to interrogate the SE inside the phone and build a communication data package **400** that typically includes an encrypted pan and optionally Track 1 and/or Track 2 data. In order to do this, a "Reader On Card" mechanism may be used in order to further encrypt the PAN or full Track 1 and Track 2 data for transportation over a public network using the antenna **410** of a mobile phone.

After the interrogator has completed an interrogation process that is typically similar to the interrogation routine in FIG. **14** or FIG. **5**.**2**, the data packet to be issued for authorization is sent to the "online merchant" over a wireless network. This data packet may contain full Track 1 and/or Track 2 information that has been encrypted or may contain only an encrypted PAN with an expiration date. The encrypted PAN is encrypted using the same method as described in FIG. **13**, FIG. **13**.**1**, FIG. **13**.**2**, FIG. **13**.**3**, and FIG. **13**.**4**. After the encrypted data is passed to the "online merchant" the merchant may further submit the data just as it would a traditional card transaction to the processing network for authorization. The processing network then routes the data to the appropriate bank for authorization as shown in FIG. **16**.**1**. Prior to the authorization of the data packet a "Decryption Device" interprets the data packet, decrypts the PAN or full track data, and replaces it with the original and legitimate PAN or track data. The decryption device may also perform other statistical checks on the PAN or track data such as verifying the transaction counter or timestamp is not repeated.

FIG. **16**.**2** shows a similar encryption technique for encrypting the card PAN. In this case, it is possible to add a timestamp factor into the encryption of the PAN. Because a mobile phone is an electronic device that can keep accurate time, the interrogator would be able to use a timestamp to further randomize the initialization vector that is used to encrypt the PAN data. When this transaction data reaches the decryption device on the other side of the network, the decryption device can then use a timestamp in a similar manner to decrypt the PAN data. It may not be possible to use a timestamp in all embodiments if the interrogator does not have access to an accurate clock.

As previously indicated, various embodiments may include embedding the SE within a mobile phone or PDA. Such embodiments may use portions of the baseband processor of the mobile phone or PDA as a communications controller and an interrogator. The combination of the SE, the communications controller and the interrogator then provide the principal components of a typical cellular network adapter. Software within the mobile phone may run the interrogation routines while interacting with the SE. The software may then perform communication controller functions by inserting the data extracted from the SE into appropriate areas such as SMS or email message, or form field. The insertion into these areas may include the keyboard emulation tactics previously described herein. The insertion into these areas may include automatic SMS or email message building and sending by software running on the mobile phone. The automatically built SMS or email message typically includes the extracted data from the interrogator.

In summary, embodiments disclosed herein describe various systems and methods for providing self-authorizing tokens and self-authorizing cellular network adapters. The foregoing descriptions of embodiments have been presented for purposes of illustration and exposition. They are not intended to be exhaustive or to limit the embodiments to the precise forms disclosed. Obvious modifications or variations are possible in light of the above teachings. The embodiments are chosen and described in an effort to provide the best illustrations of principles and practical applications, and to thereby enable one of ordinary skill in the art to utilize the various embodiments as described and with various modifications as are suited to the particular use contemplated. All such modifications and variations are within the scope of the appended claims when interpreted in accordance with the breadth to which they are fairly, legally, and equitably entitled.

What is claimed is:

1. A token comprising:

a mounting structure having a communication connector configured to connect to a computer terminal;

a secure element affixed to the mounting structure, the secure element comprising a data file,

a secure element reader affixed to the mounting structure and configured to interrogate the secure element by executing file system functions comprising a command to select a payment card application according to ISO 7816-4 and to generate file information from the secure element data file; and

a communications controller affixed to the mounting structure and configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction information and to transmit the transaction information to the computer terminal through the communications connector, wherein the communication connector is a Universal Serial Bus (USB) connector and the communications controller is configured as a Human Interface Device (HID) class USB-device and the communications controller is configured to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal.

2. The token of claim **1** wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.

3. The token of claim **1** wherein the secure element data file comprises financial authorization data and the communications controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal through the communications connector.

4. The token of claim **1** wherein:

the secure element data file comprises financial authorization data and the controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal using the USB connector.

5. The token of claim 4 wherein:
the communications controller is configured to provide the transaction information in a prescribed cadence for the application running on the computer terminal.

6. The token of claim 1 wherein the transaction information comprises an encrypted unpredictable number constructed as a hash of a timestamp.

7. The token of claim 1 wherein the transaction information comprises an encryption constructed from a timestamp and a transaction counter.

8. The token of claim 1 wherein the secure element reader is configured to await a startup instruction comprising an unpredictable number originating from the computer terminal prior to interrogating the secure element.

9. A token comprising:
a mounting structure having a communication connector configured to connect to a computer terminal;
a secure element affixed to the mounting structure, the secure element comprising a data file,
a secure element reader affixed to the mounting structure and configured to interrogate the secure element by executing file system functions comprising a command to select a payment card application according to ISO 7816-4 and to generate file information from the secure element data file; and
a communications controller affixed to the mounting structure and configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction information and to transmit the transaction information to the computer terminal through the communications connector; wherein
the secure element data file comprises financial authorization data and the communications controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal through the communications connector, and wherein
the communications controller is configured to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal.

10. The token of claim 9 wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.

11. A token comprising:
a mounting structure having a Universal Serial Bus (USB) connector configured to connect to a computer terminal;
a secure element affixed to the mounting structure, the secure element comprising a data file,
a communications controller affixed to the mounting structure and configured as a Human Interface Device (HID) class USB-device and configured to extract information from the secure element data file and to convert at least a portion of the data file into transaction information and to transmit the transaction information to the computer terminal through the USB connector as keyboard emulation and wherein the communications controller is configured to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal.

12. The token of claim 11 wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.

13. The token of claim 11 wherein the secure element data file comprises financial authorization data and the communications controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal through the USB connector.

14. The token of claim 11 wherein the transaction information comprises an encrypted unpredictable number constructed as a hash of a timestamp.

15. The token of claim 11 wherein the transaction information comprises an encryption constructed from a timestamp and a transaction counter.

16. The token of claim 11 wherein the secure element reader is configured to await a startup instruction comprising an unpredictable number originating from the computer terminal prior to interrogating the secure element.

17. A token comprising:
a mounting structure having a Universal Serial Bus (USB) connector configured to connect to a computer terminal;
a secure element affixed to the mounting structure, the secure element comprising a data file; and
a communications controller affixed to the mounting structure and configured as a Human Interface Device (HID) class USB-device and configured to extract information from the secure element data file and to convert at least a portion of the data file into transaction information and to transmit the transaction information to the computer terminal through the USB connector as keyboard emulation; wherein
the secure element data file comprises financial authorization data and the communications controller is configured to extract at least a portion of the financial authorization data and is configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data for transmission as transaction information to the computer terminal through the USB connector; and wherein
the communications controller is configured to provide the transaction information in a format that auto-populates a form field defined by an application running on the computer terminal.

18. The token of claim 17 wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.

19. A token comprising:
a mounting structure having a communication connector configured to connect to a computer terminal;
a secure element affixed to the mounting structure, the secure element comprising a data file comprising financial authorization data,
a communications controller affixed to the mounting structure and configured to extract at least a portion of the financial authorization data from the secure element data file and configured to encrypt the at least a portion of the financial data and to transmit the encrypted financial authorization data as transaction information comprising an encrypted unpredictable number constructed as a hash of a timestamp to the computer terminal using the communication connector, wherein the communications controller is configured to provide the transaction

information in a format that auto-populates a form field defined by an application running on the computer terminal.

20. The token of claim **19** wherein the communications controller is configured to provide the transaction information in a prescribed cadence for an application running on the computer terminal.

21. The token of claim **19** wherein the transaction information comprises an encryption constructed from the hash of the timestamp and a transaction counter.

22. The token of claim **19** wherein the secure element reader is configured to await a startup instruction comprising an unpredictable number originating from the computer terminal prior to interrogating the secure element.

23. A cellular network adapter for a cellular network device configured with a cellular network application interface comprising;

a secure element comprising a data file;

a secure element reader in the cellular network adapter configured to interrogate the secure element by executing file system functions according to ISO 7816-4 and to generate file information from the secure element data file;

a near field communications controller bridge chip to convert the file information to an RF data signal for an external reader; and

a communications controller configured to receive the file information from the secure element reader and to convert at least a portion of the file information into transaction authorization information and to transmit the transaction authorization information from the cellular network device over a wireless network through the cellular network application interface, wherein the wireless network comprises a cellular network and the secure element reader in the cellular network adapter is configured to await a startup instruction comprising an unpredictable number originating over the cellular wireless network prior to interrogating the secure element.

24. The cellular network adapter of claim **23** wherein the transaction authorization information comprises an encrypted unpredictable number constructed as a hash of a timestamp.

25. The cellular network adapter of claim **23** wherein the transaction authorization information comprises an encryption constructed from a timestamp and a transaction counter.

* * * * *

EXHIBIT 2

US008548924B2

(12) **United States Patent**
Yeager

(10) **Patent No.: US 8,548,924 B2**
(45) **Date of Patent: *Oct. 1, 2013**

(54) **SELF-AUTHORIZING TOKEN**

(76) Inventor: **C. Douglas Yeager**, Austin, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/403,141**

(22) Filed: **Feb. 23, 2012**

(65) **Prior Publication Data**

US 2012/0173432 A1 Jul. 5, 2012

Related U.S. Application Data

(63) Continuation of application No. 12/019,318, filed on Jan. 24, 2008, now Pat. No. 8,151,345.

(60) Provisional application No. 60/897,110, filed on Jan. 25, 2007, provisional application No. 60/932,704, filed on Jun. 1, 2007.

(51) **Int. Cl.**
G06Q 20/00 (2012.01)

(52) **U.S. Cl.**
USPC **705/65**; 726/9; 726/20; 235/375; 235/380; 235/435; 235/492; 713/165; 710/313

(58) **Field of Classification Search**
USPC 726/9, 20; 235/380, 375, 439, 492; 713/165; 710/313; 705/65
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,439,464	B1	8/2002	Fruhauf et al.	
6,763,399	B2	7/2004	Margalit et al.	
6,883,715	B1	4/2005	Fruhauf et al.	
6,991,173	B2	1/2006	Fruhauf	
7,011,247	B2	3/2006	Drabczuk et al.	
7,150,397	B2	12/2006	Morrow et al.	
7,213,766	B2 *	5/2007	Ryan et al.	235/492
7,249,266	B2	7/2007	Margalit et al.	
8,081,060	B1 *	12/2011	Saarisalo et al.	340/10.1
2005/0165695	A1 *	7/2005	Berardi et al.	705/64
2005/0231467	A1 *	10/2005	Gold	345/156
2006/0255158	A1	11/2006	Margalit et al.	
2007/0023503	A1 *	2/2007	Kang	235/380
2007/0084925	A1 *	4/2007	Palmade	235/451
2007/0152070	A1 *	7/2007	D'Albore	235/492
2007/0170266	A1 *	7/2007	Krygier et al.	235/492
2007/0262138	A1 *	11/2007	Somers et al.	235/380
2010/0207742	A1 *	8/2010	Buhot et al.	340/10.51

FOREIGN PATENT DOCUMENTS

EP	1843277	10/2007

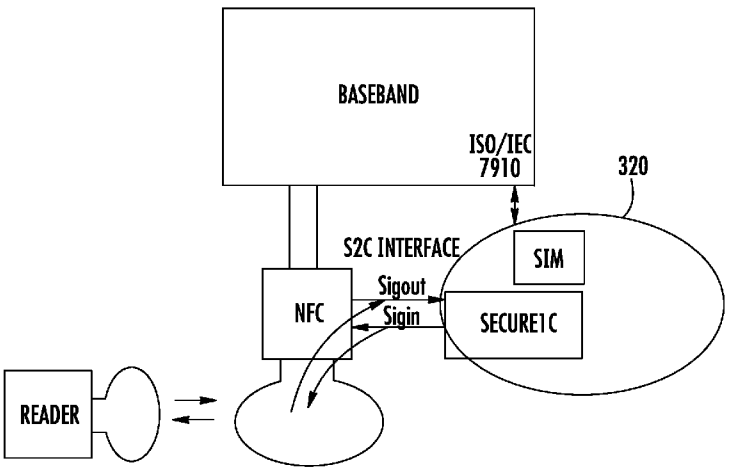
* cited by examiner

Primary Examiner — Brandon Hoffman
Assistant Examiner — Hee Song
(74) *Attorney, Agent, or Firm* — Luedeka Neely Group, P.C.

(57) **ABSTRACT**

Self-authorizing tokens are disclosed. Typical embodiments employ a secure element and a secure element interrogator. Such tokens may be used for authorization of financial payments and other secure transactions. In some embodiments the secure element is provisioned with information about a particular payment card holder account. A secure element reader interrogates the smart element and derives information needed to authorize a transaction. In some embodiments the secure element and the secure element interrogator communicate using communications formatted according to ISO 7816-4.

87 Claims, 19 Drawing Sheets



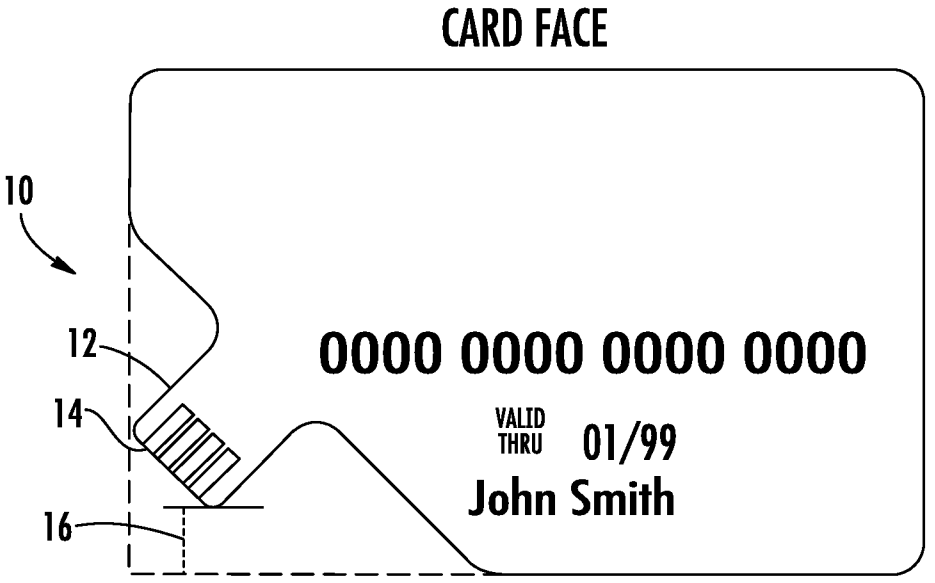

CARD FACE
10
12
14
16
0000 0000 0000 0000
VALID
THRU
01/99
John Smith

FIG. 1

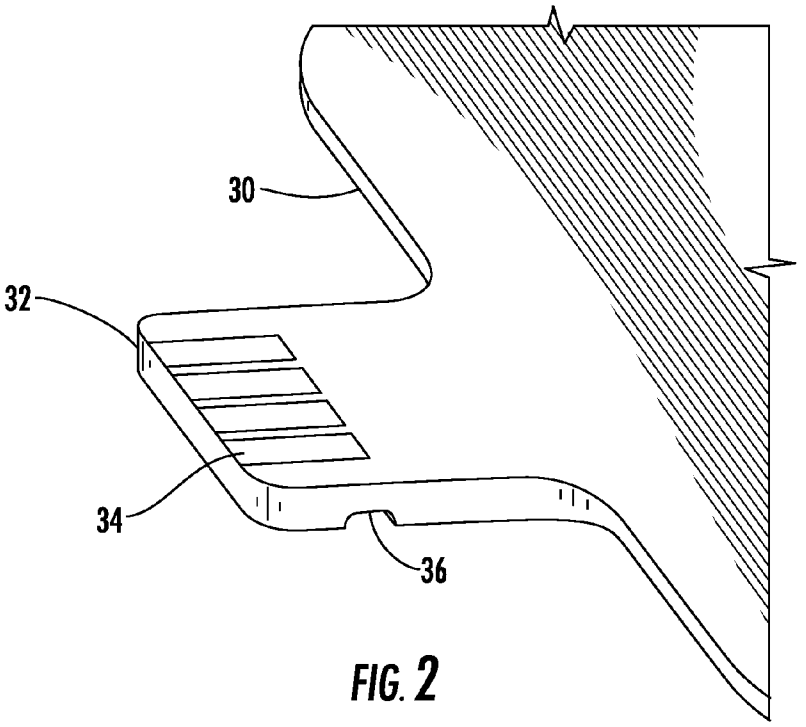


FIG. 2

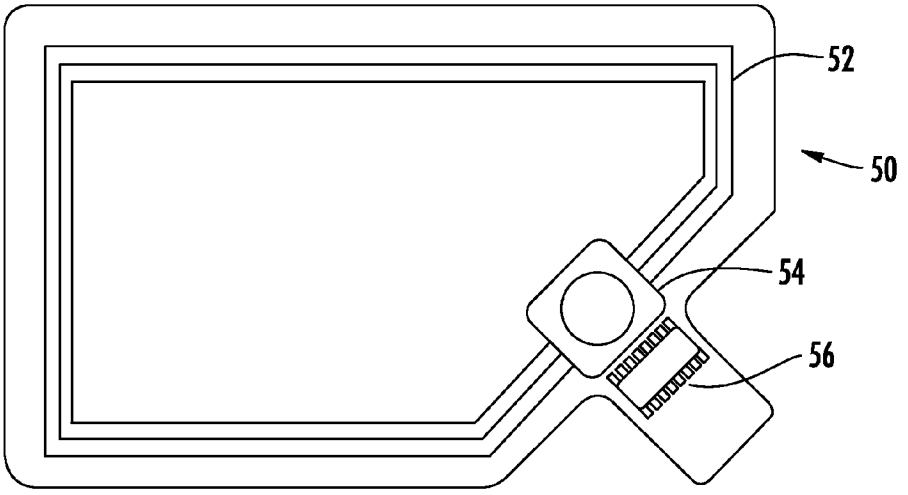


FIG. 3

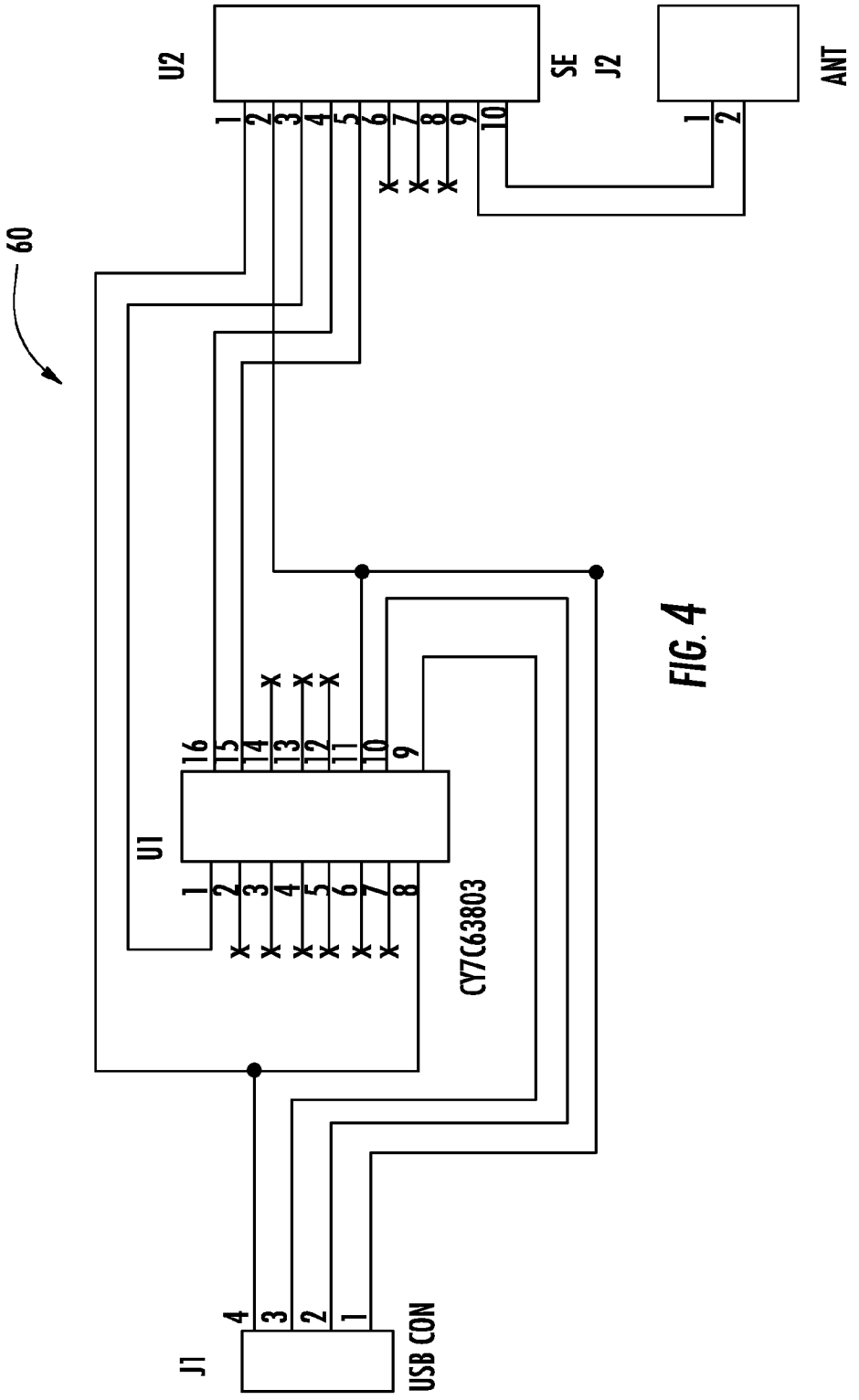

60
U2
SE
J2
ANT
1
2
3
4
5
6
7
8
9
10
1
2
U1
16
15
14
13
12
11
10
9
1
2
3
4
5
6
7
8
CY7C63803
J1
USB CON
4
3
2
1

FIG. 4

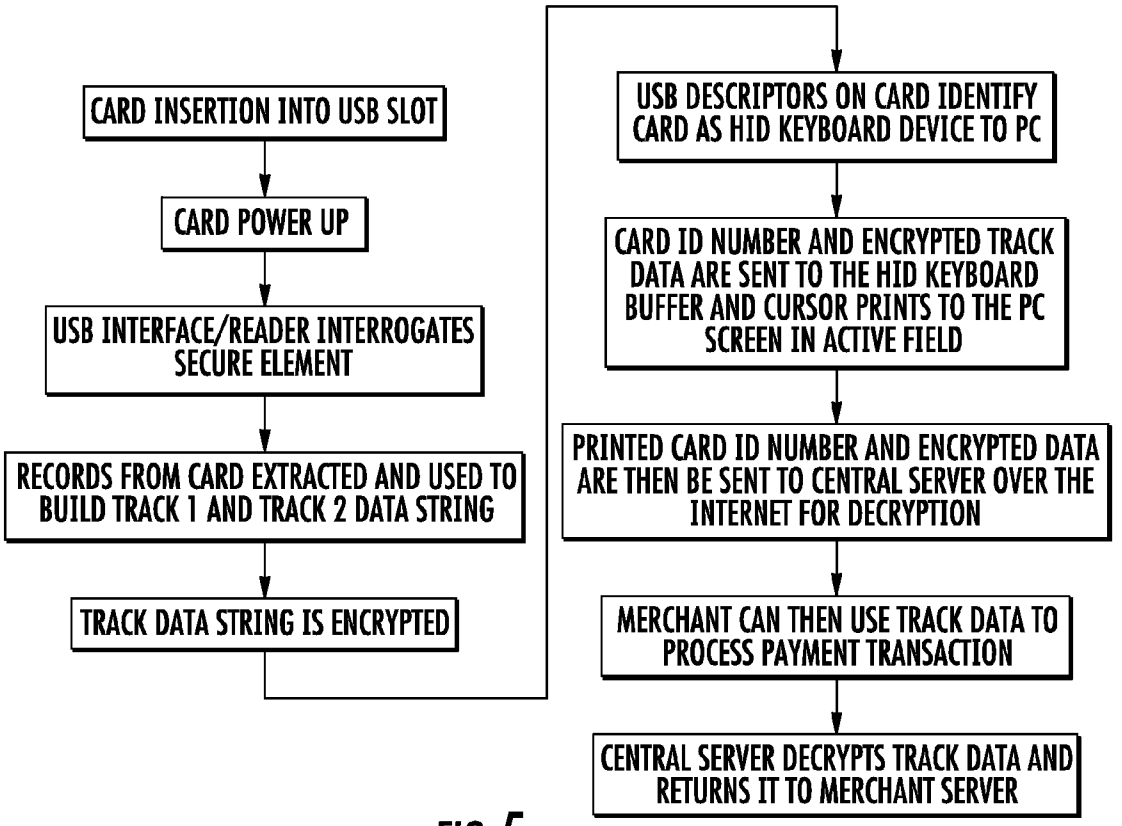

CARD INSERTION INTO USB SLOT
CARD POWER UP
USB INTERFACE/READER INTERROGATES SECURE ELEMENT
RECORDS FROM CARD EXTRACTED AND USED TO BUILD TRACK 1 AND TRACK 2 DATA STRING
TRACK DATA STRING IS ENCRYPTED
USB DESCRIPTORS ON CARD IDENTIFY CARD AS HID KEYBOARD DEVICE TO PC
CARD ID NUMBER AND ENCRYPTED TRACK DATA ARE SENT TO THE HID KEYBOARD BUFFER AND CURSOR PRINTS TO THE PC SCREEN IN ACTIVE FIELD
PRINTED CARD ID NUMBER AND ENCRYPTED DATA ARE THEN BE SENT TO CENTRAL SERVER OVER THE INTERNET FOR DECRYPTION
MERCHANT CAN THEN USE TRACK DATA TO PROCESS PAYMENT TRANSACTION
CENTRAL SERVER DECRYPTS TRACK DATA AND RETURNS IT TO MERCHANT SERVER

FIG. 5

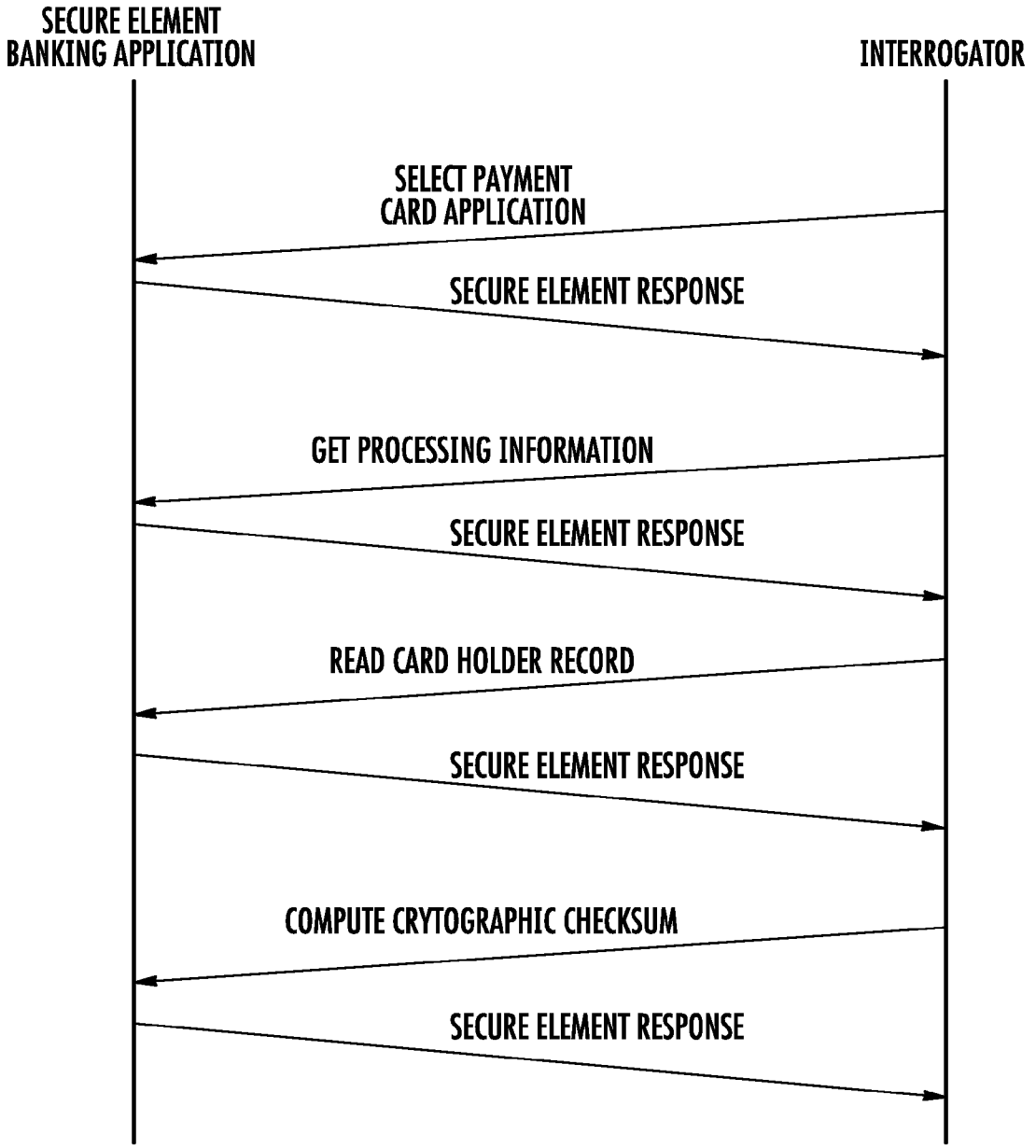

SECURE ELEMENT
BANKING APPLICATION
INTERROGATOR
SELECT PAYMENT
CARD APPLICATION
SECURE ELEMENT RESPONSE
GET PROCESSING INFORMATION
SECURE ELEMENT RESPONSE
READ CARD HOLDER RECORD
SECURE ELEMENT RESPONSE
COMPUTE CRYTOGRAPHIC CHECKSUM
SECURE ELEMENT RESPONSE

FIG. 5.1

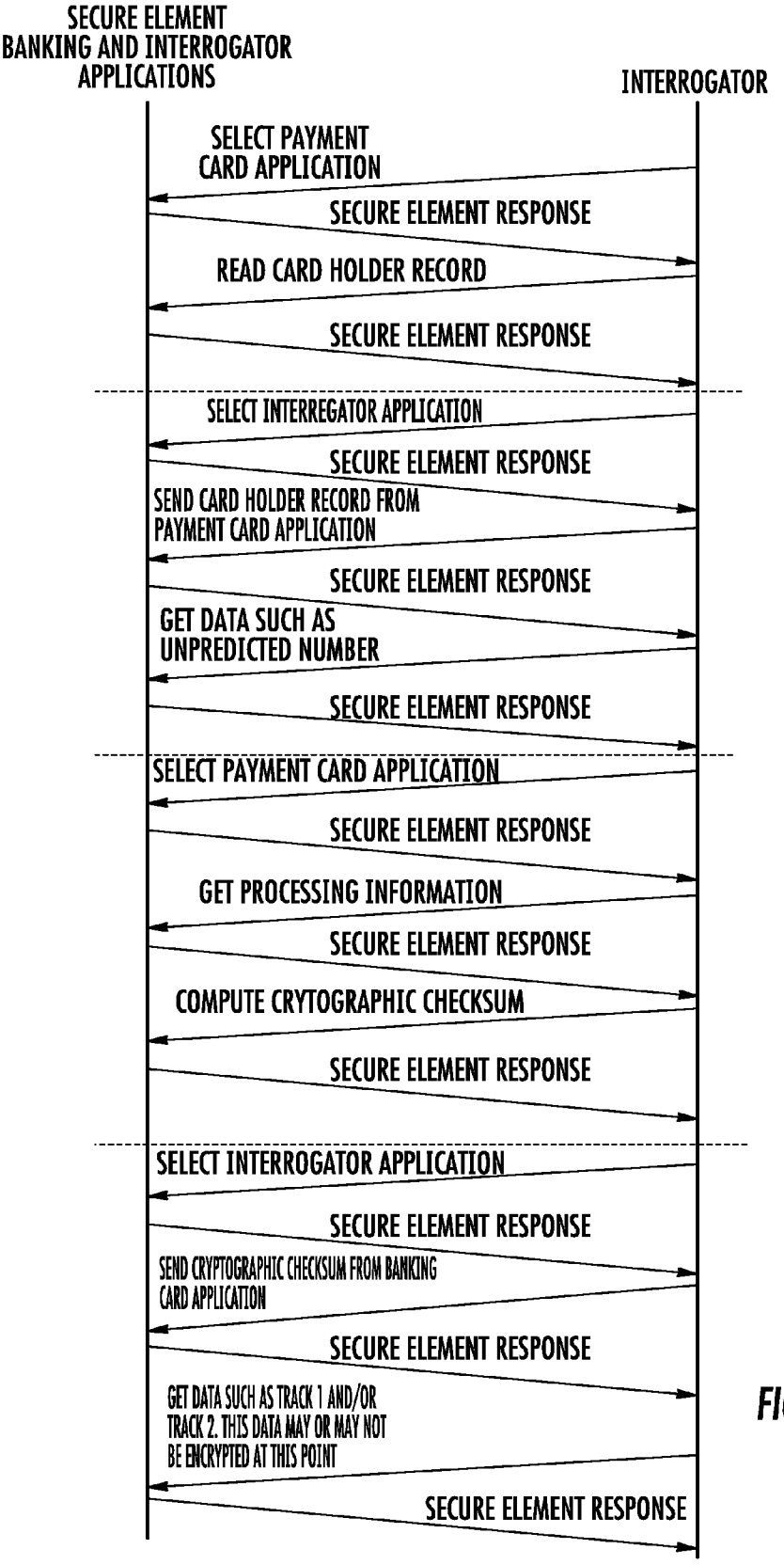

SECURE ELEMENT BANKING AND INTERROGATOR APPLICATIONS
INTERROGATOR
SELECT PAYMENT CARD APPLICATION
SECURE ELEMENT RESPONSE
READ CARD HOLDER RECORD
SECURE ELEMENT RESPONSE
SELECT INTERREGATOR APPLICATION
SECURE ELEMENT RESPONSE
SEND CARD HOLDER RECORD FROM PAYMENT CARD APPLICATION
SECURE ELEMENT RESPONSE
GET DATA SUCH AS UNPREDICTED NUMBER
SECURE ELEMENT RESPONSE
SELECT PAYMENT CARD APPLICATION
SECURE ELEMENT RESPONSE
GET PROCESSING INFORMATION
SECURE ELEMENT RESPONSE
COMPUTE CRYTOGRAPHIC CHECKSUM
SECURE ELEMENT RESPONSE
SELECT INTERROGATOR APPLICATION
SECURE ELEMENT RESPONSE
SEND CRYPTOGRAPHIC CHECKSUM FROM BANKING CARD APPLICATION
SECURE ELEMENT RESPONSE
GET DATA SUCH AS TRACK 1 AND/OR TRACK 2. THIS DATA MAY OR MAY NOT BE ENCRYPTED AT THIS POINT
SECURE ELEMENT RESPONSE

FIG. 5.2

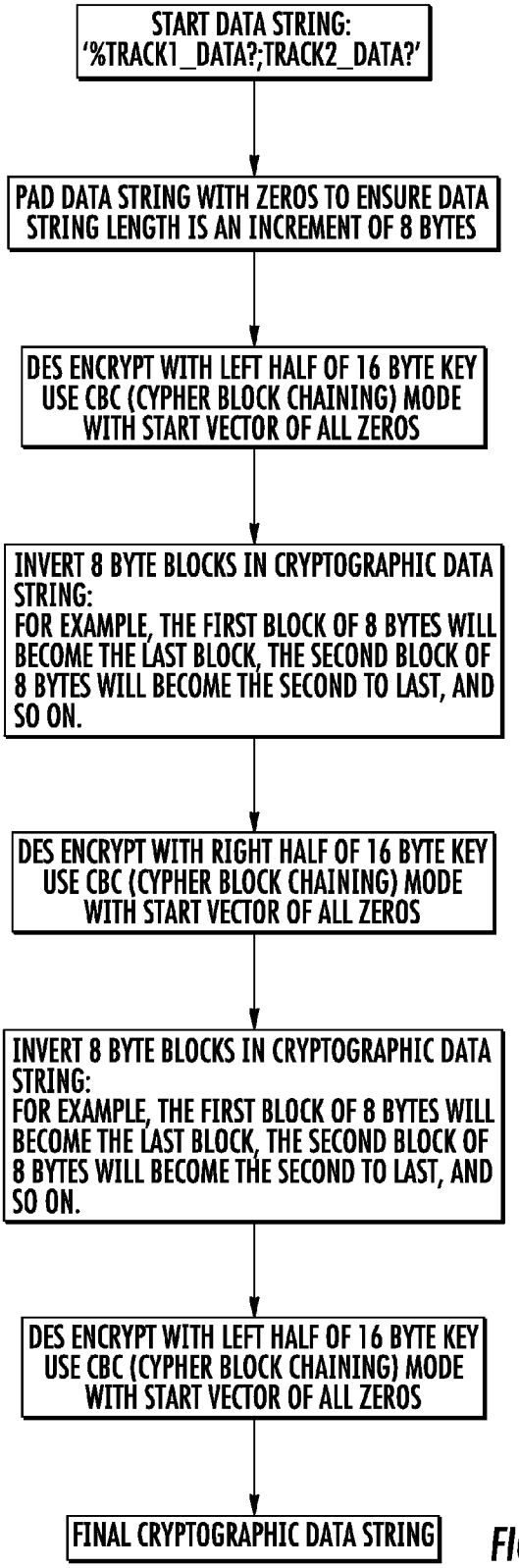

START DATA STRING:
'%TRACK1_DATA?;TRACK2_DATA?'
PAD DATA STRING WITH ZEROS TO ENSURE DATA STRING LENGTH IS AN INCREMENT OF 8 BYTES
DES ENCRYPT WITH LEFT HALF OF 16 BYTE KEY USE CBC (CYPHER BLOCK CHAINING) MODE WITH START VECTOR OF ALL ZEROS
INVERT 8 BYTE BLOCKS IN CRYPTOGRAPHIC DATA STRING:
FOR EXAMPLE, THE FIRST BLOCK OF 8 BYTES WILL BECOME THE LAST BLOCK, THE SECOND BLOCK OF 8 BYTES WILL BECOME THE SECOND TO LAST, AND SO ON.
DES ENCRYPT WITH RIGHT HALF OF 16 BYTE KEY USE CBC (CYPHER BLOCK CHAINING) MODE WITH START VECTOR OF ALL ZEROS
INVERT 8 BYTE BLOCKS IN CRYPTOGRAPHIC DATA STRING:
FOR EXAMPLE, THE FIRST BLOCK OF 8 BYTES WILL BECOME THE LAST BLOCK, THE SECOND BLOCK OF 8 BYTES WILL BECOME THE SECOND TO LAST, AND SO ON.
DES ENCRYPT WITH LEFT HALF OF 16 BYTE KEY USE CBC (CYPHER BLOCK CHAINING) MODE WITH START VECTOR OF ALL ZEROS
FINAL CRYPTOGRAPHIC DATA STRING

FIG. 5.3

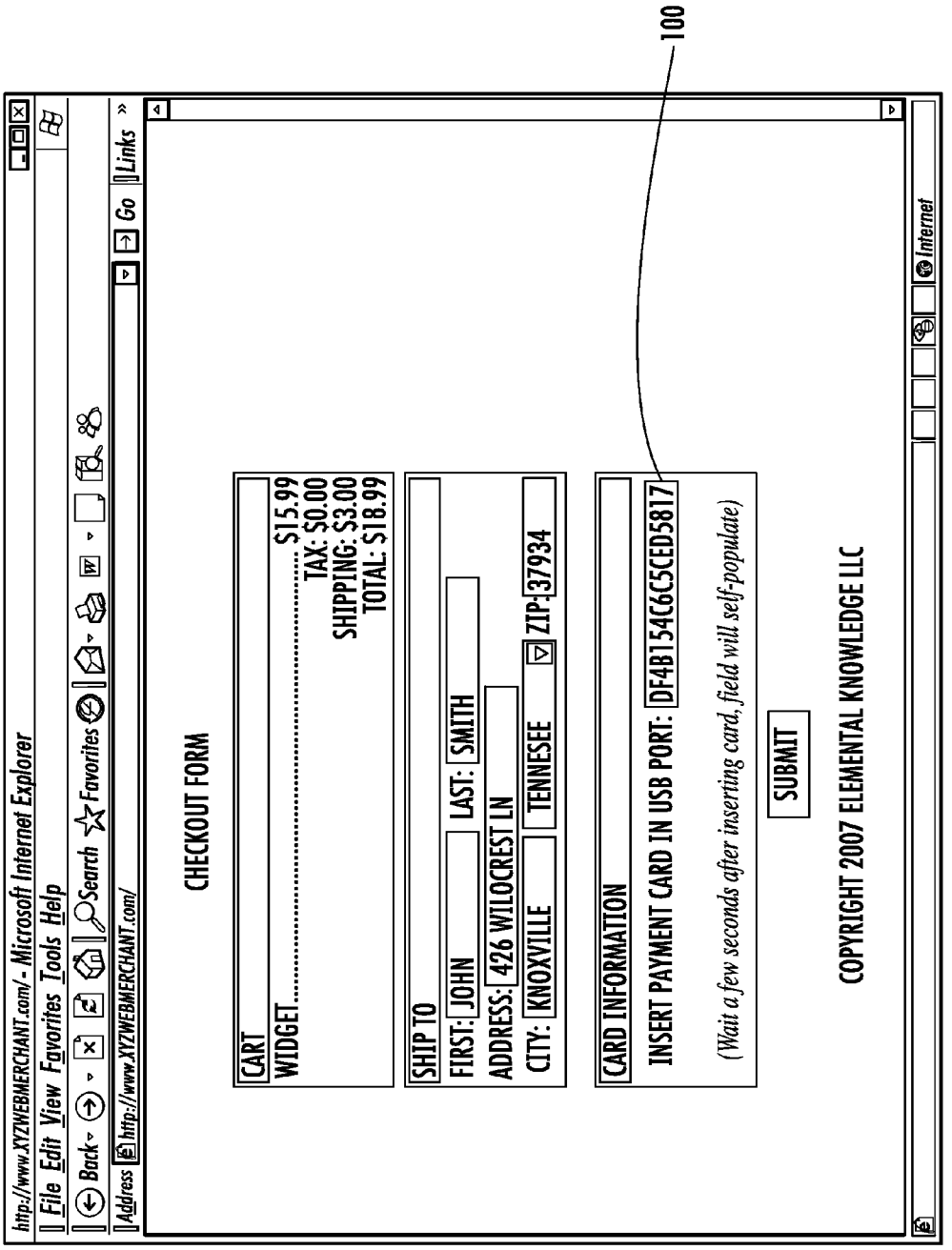

http://www.XYZWEBMERCHANT.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.XYZWEBMERCHANT.com/
Go Links
CHECKOUT FORM
CART
WIDGET $15.99
TAX: $0.00
SHIPPING: $3.00
TOTAL: $18.99
SHIP TO
FIRST: JOHN LAST: SMITH
ADDRESS: 426 WILOCREST LN
CITY: KNOXVILLE TENNESEE ZIP: 37934
CARD INFORMATION
INSERT PAYMENT CARD IN USB PORT: DF4B154C6C5CED5817
(Wait a few seconds after inserting card, field will self-populate)
SUBMIT
COPYRIGHT 2007 ELEMENTAL KNOWLEDGE LLC
Internet
100

FIG. 6

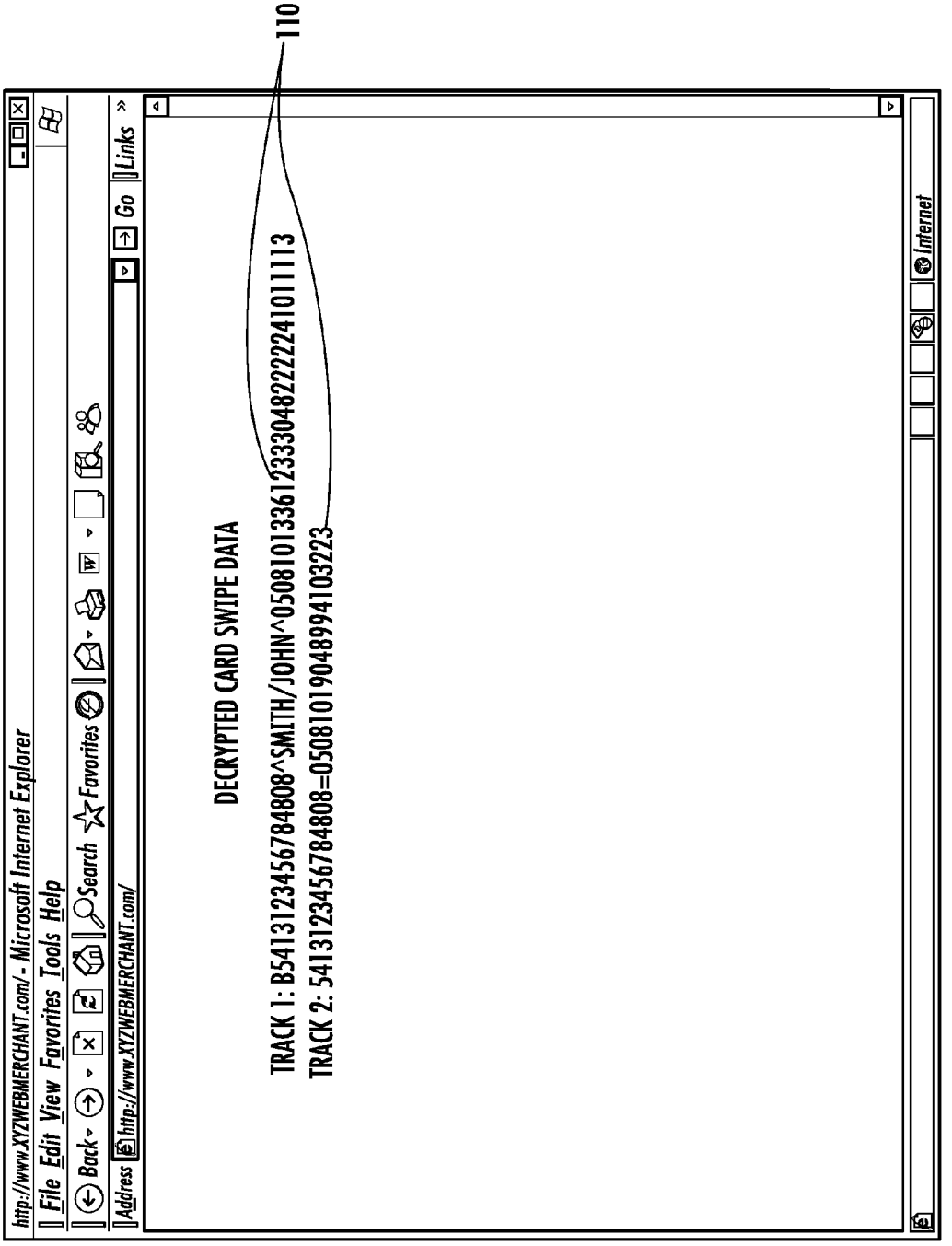

110
http://www.XYZWEBMERCHANT.com/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.XYZWEBMERCHANT.com/
Go
Links
DECRYPTED CARD SWIPE DATA
TRACK 1: B5413123456784808^SMITH/JOHN^05081013361233304822222241011113
TRACK 2: 5413123456784808=05081019048994103223
Internet

FIG. 7

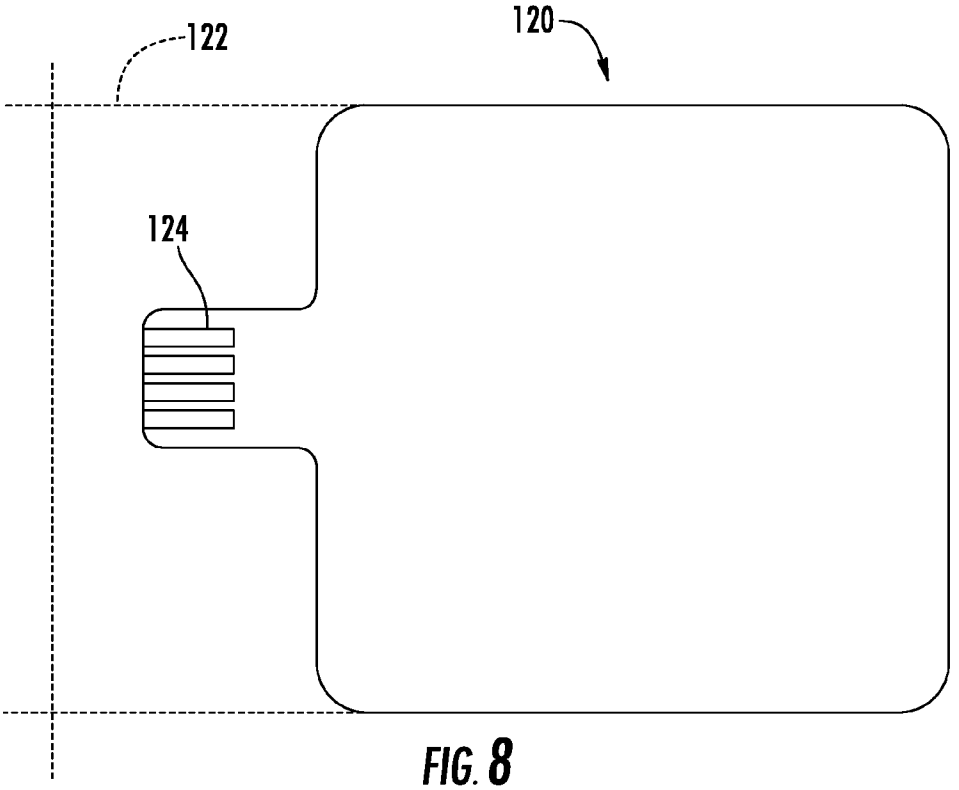


FIG. 8

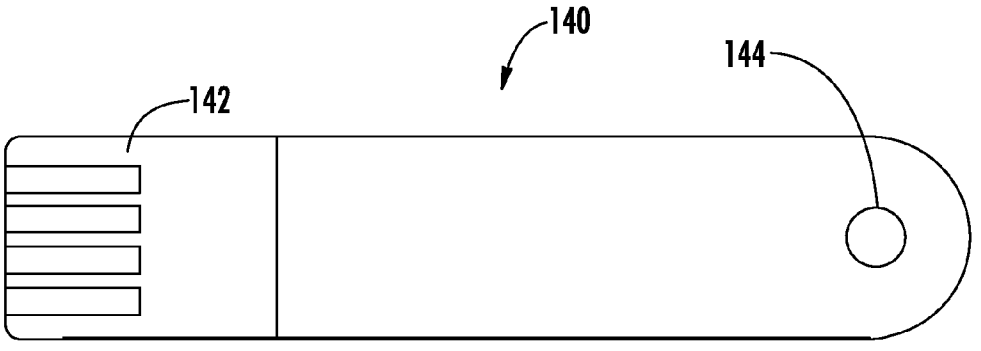


FIG. 9

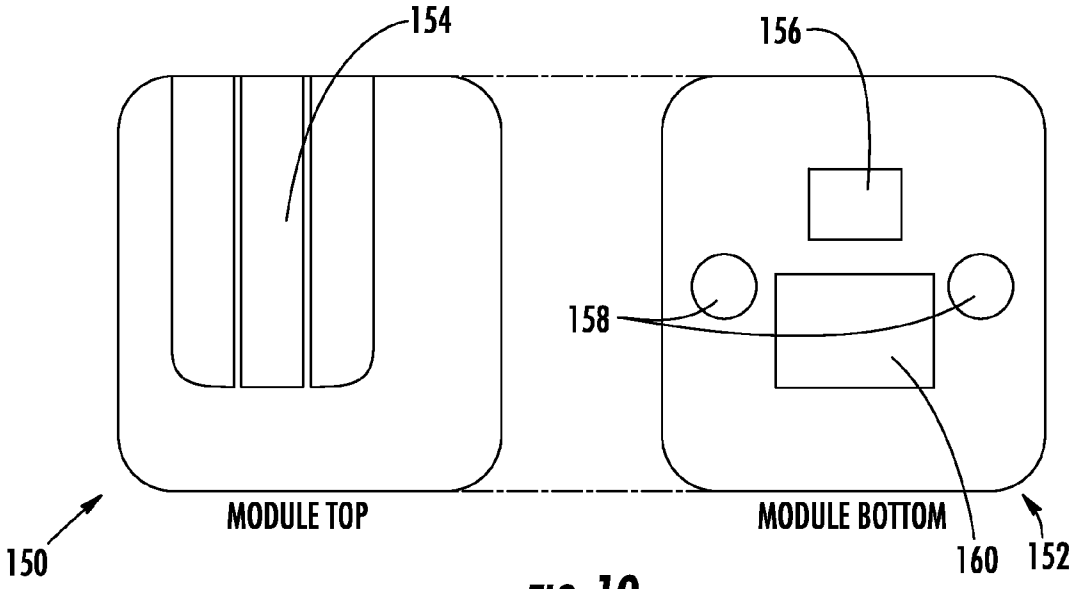


FIG. 10

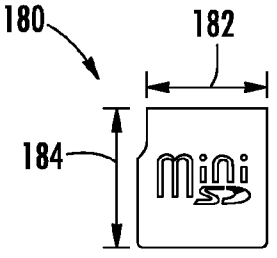


FIG. 11A

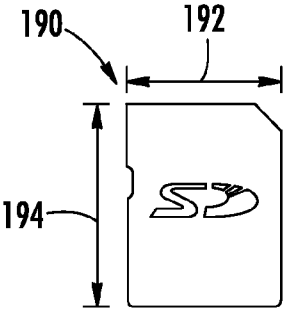


FIG. 11B

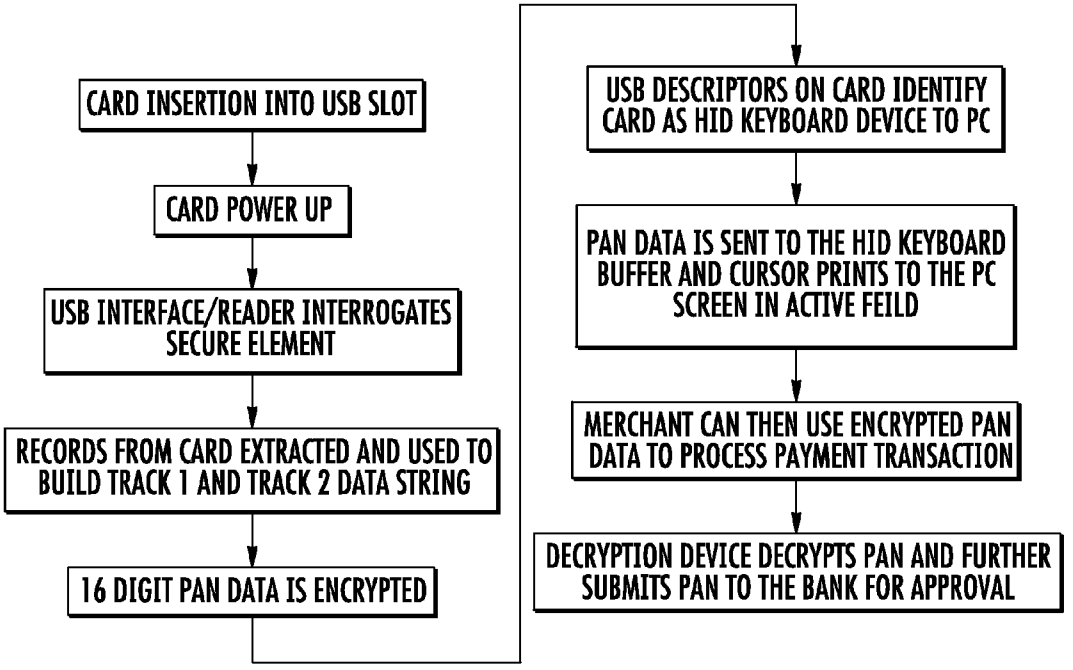

CARD INSERTION INTO USB SLOT
CARD POWER UP
USB INTERFACE/READER INTERROGATES SECURE ELEMENT
RECORDS FROM CARD EXTRACTED AND USED TO BUILD TRACK 1 AND TRACK 2 DATA STRING
16 DIGIT PAN DATA IS ENCRYPTED
USB DESCRIPTORS ON CARD IDENTIFY CARD AS HID KEYBOARD DEVICE TO PC
PAN DATA IS SENT TO THE HID KEYBOARD BUFFER AND CURSOR PRINTS TO THE PC SCREEN IN ACTIVE FEILD
MERCHANT CAN THEN USE ENCRYPTED PAN DATA TO PROCESS PAYMENT TRANSACTION
DECRYPTION DEVICE DECRYPTS PAN AND FURTHER SUBMITS PAN TO THE BANK FOR APPROVAL

FIG. 12

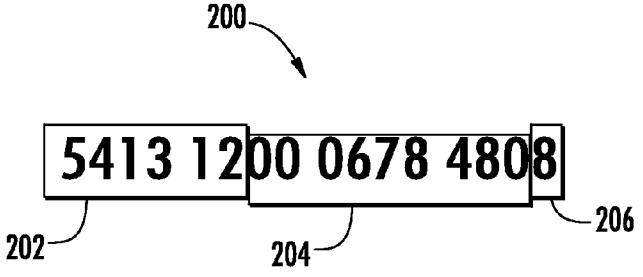

200
5413 1200 0678 4808
202
204
206

FIG. 13

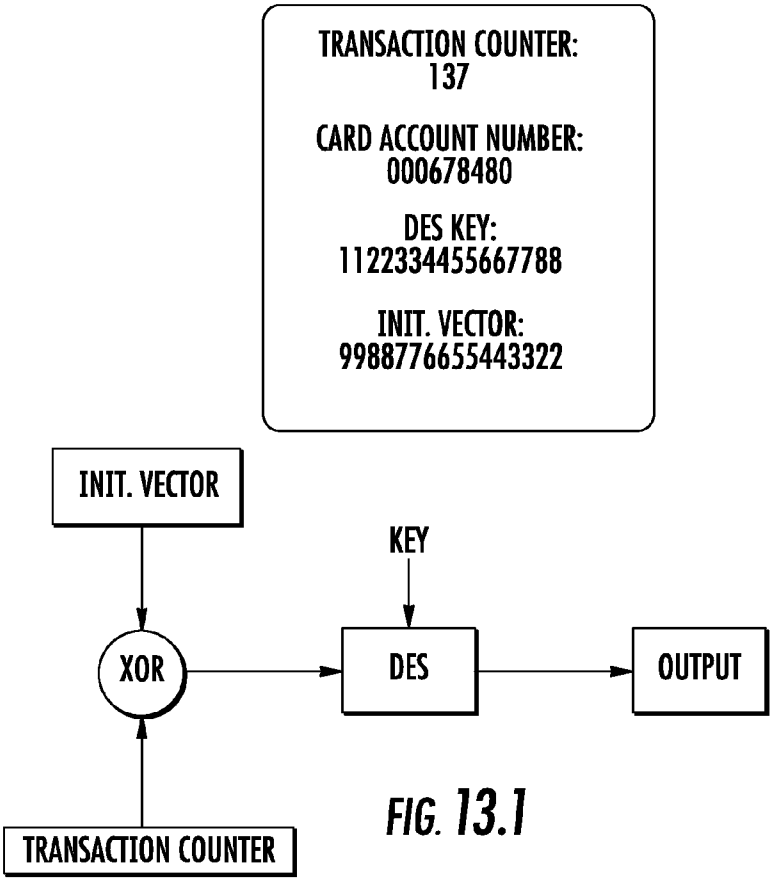


FIG. 13.1

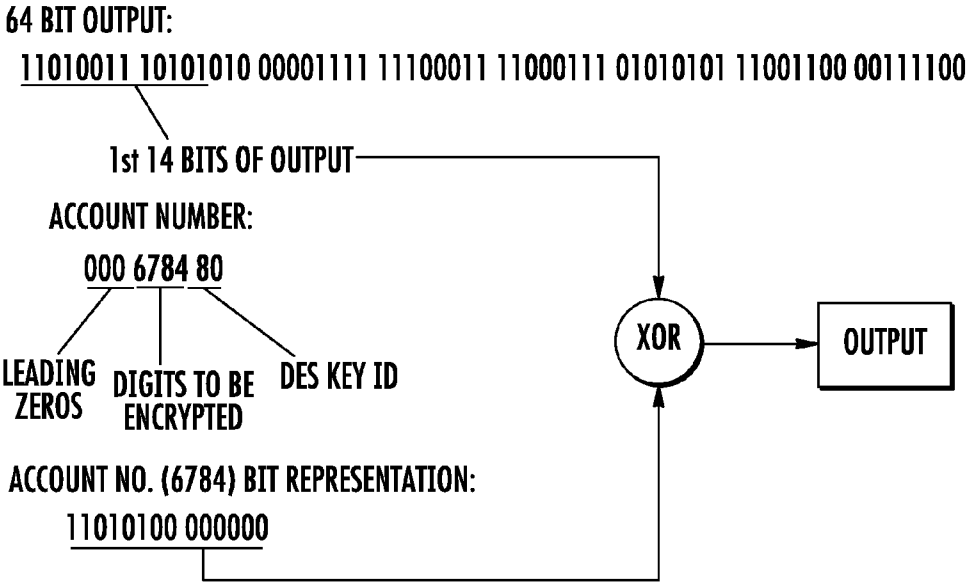


FIG. 13.2

14 BIT OUTPUT:
00000111 101010

DECIMAL CONVERSION:
0490

BUILD ENCRYPTED ACCOUNT NUMBER:

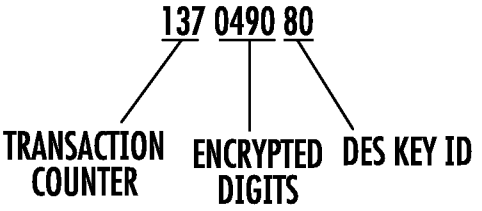


FIG. 13.3

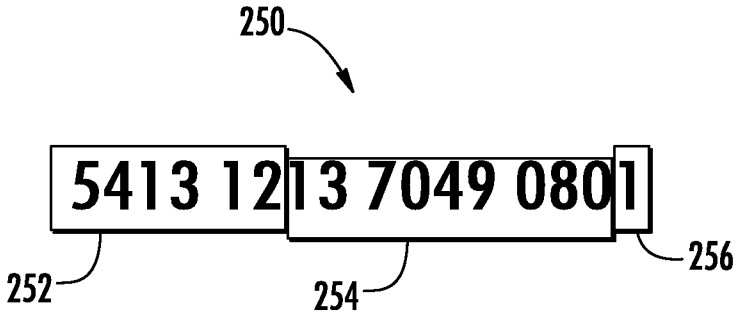


FIG. 13.4

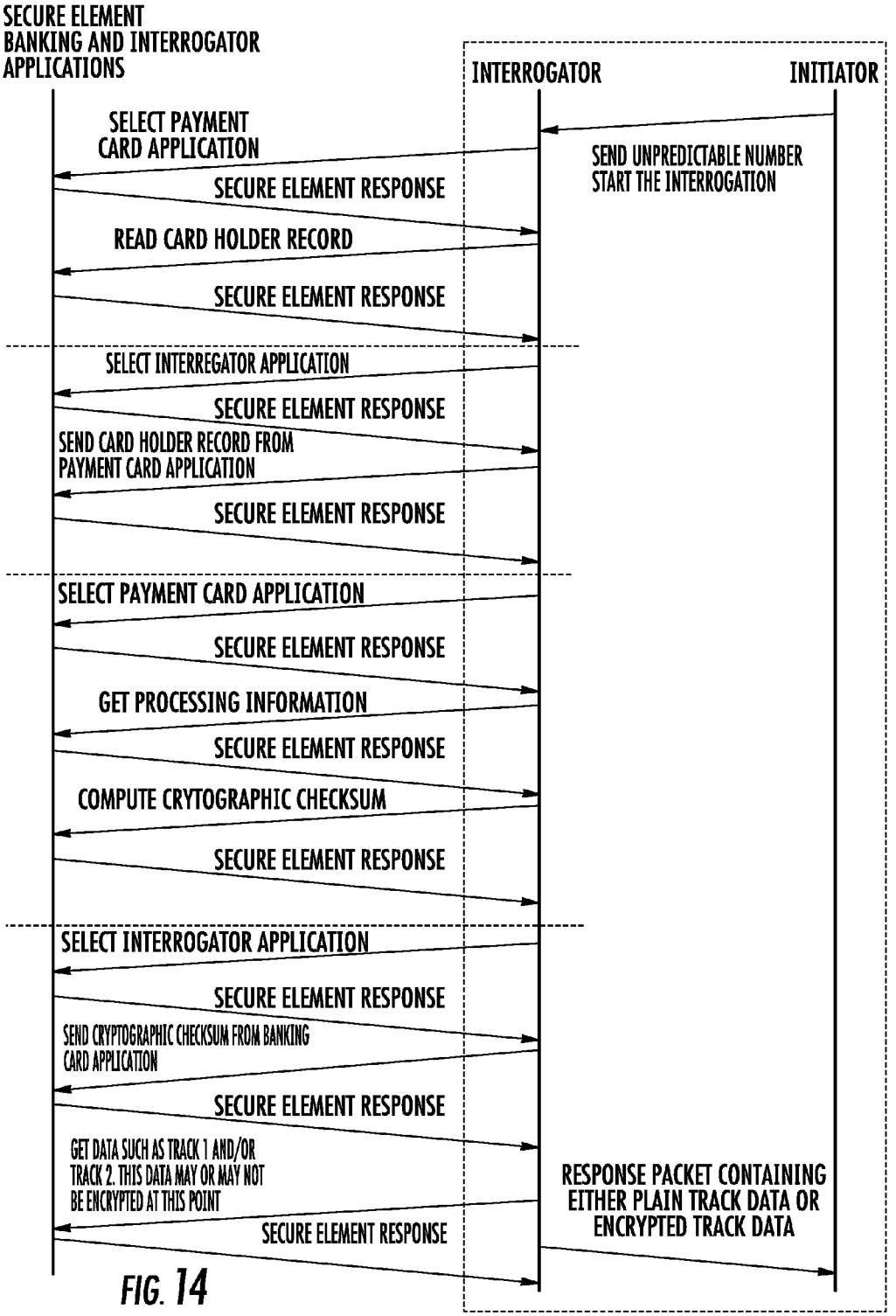

SECURE ELEMENT
BANKING AND INTERROGATOR
APPLICATIONS
INTERROGATOR
INITIATOR
SELECT PAYMENT
CARD APPLICATION
SEND UNPREDICTABLE NUMBER
START THE INTERROGATION
SECURE ELEMENT RESPONSE
READ CARD HOLDER RECORD
SECURE ELEMENT RESPONSE
SELECT INTERREGATOR APPLICATION
SECURE ELEMENT RESPONSE
SEND CARD HOLDER RECORD FROM
PAYMENT CARD APPLICATION
SECURE ELEMENT RESPONSE
SELECT PAYMENT CARD APPLICATION
SECURE ELEMENT RESPONSE
GET PROCESSING INFORMATION
SECURE ELEMENT RESPONSE
COMPUTE CRYTOGRAPHIC CHECKSUM
SECURE ELEMENT RESPONSE
SELECT INTERROGATOR APPLICATION
SECURE ELEMENT RESPONSE
SEND CRYPTOGRAPHIC CHECKSUM FROM BANKING
CARD APPLICATION
SECURE ELEMENT RESPONSE
GET DATA SUCH AS TRACK 1 AND/OR
TRACK 2. THIS DATA MAY OR MAY NOT
BE ENCRYPTED AT THIS POINT
RESPONSE PACKET CONTAINING
EITHER PLAIN TRACK DATA OR
ENCRYPTED TRACK DATA
SECURE ELEMENT RESPONSE

FIG. 14

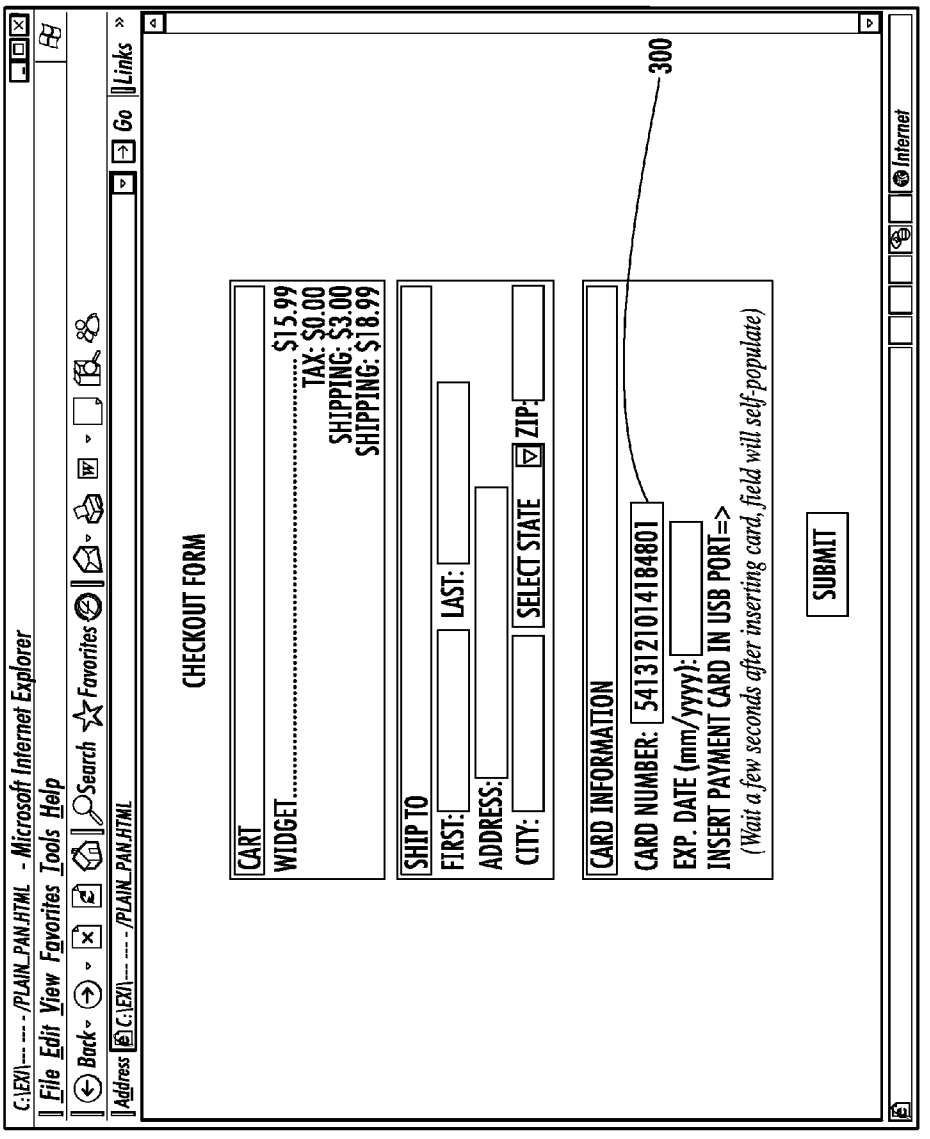

C:\EXI\---- ---- /PLAIN_PAN.HTML - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\EXI\---- ---- /PLAIN_PAN.HTML
Go Links
CHECKOUT FORM
CART
WIDGET..... $15.99
TAX: $0.00
SHIPPING: $3.00
SHIPPING: $18.99
SHIP TO
FIRST: LAST:
ADDRESS:
CITY: SELECT STATE ZIP:
CARD INFORMATION
CARD NUMBER: 5413121014184801
EXP. DATE (mm/yyyy):
INSERT PAYMENT CARD IN USB PORT=>
(Wait a few seconds after inserting card, field will self-populate)
SUBMIT
300
Internet

FIG. 15

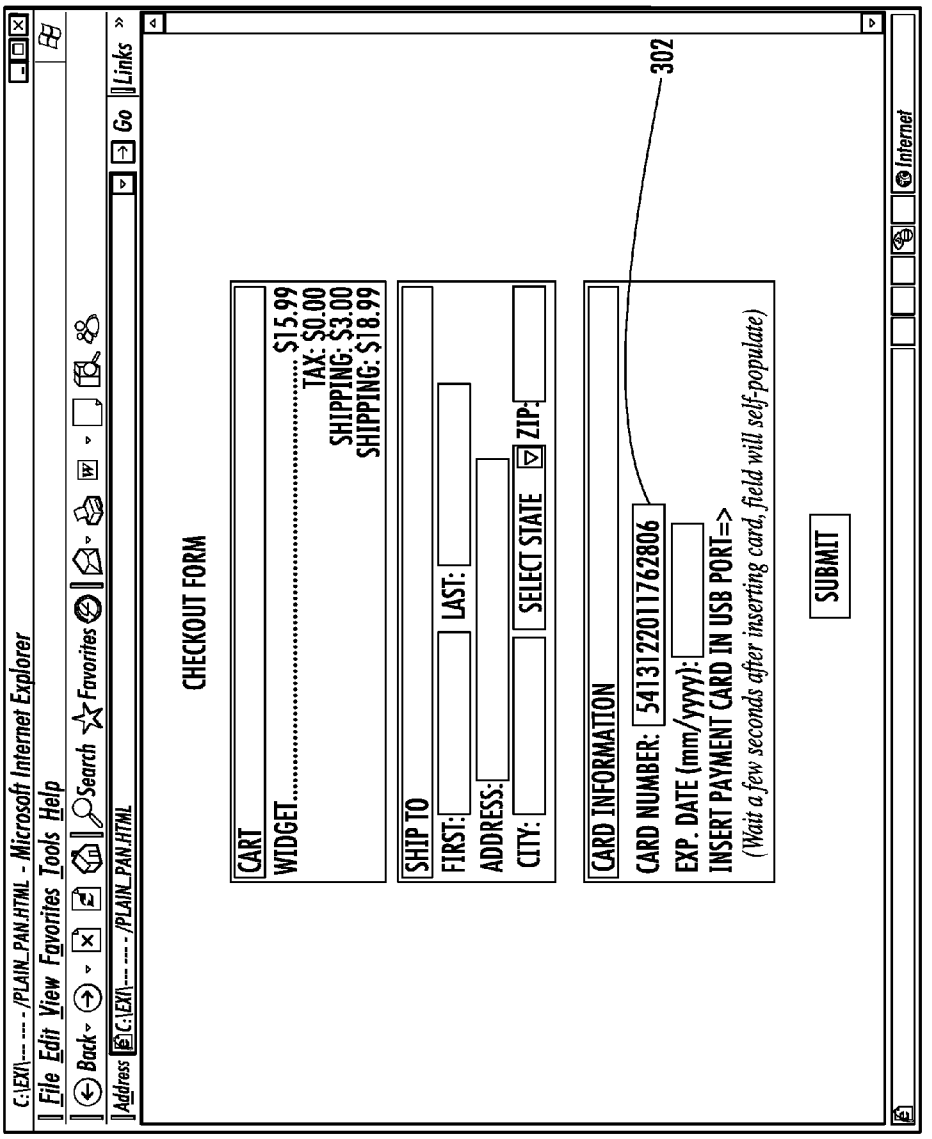

C:\EX1\--- ---- -/PLAIN_PAN.HTML - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\EX1\--- ---- -/PLAIN_PAN.HTML
Go Links
CHECKOUT FORM
CART
WIDGET..... $15.99
TAX: $0.00
SHIPPING: $3.00
SHIPPING: $18.99
SHIP TO
FIRST: LAST:
ADDRESS:
CITY: SELECT STATE ZIP:
CARD INFORMATION
CARD NUMBER: 5413122011762806
EXP. DATE (mm/yyyy):
INSERT PAYMENT CARD IN USB PORT=>
(Wait a few seconds after inserting card, field will self-populate)
SUBMIT
302
Internet

FIG. 15.1

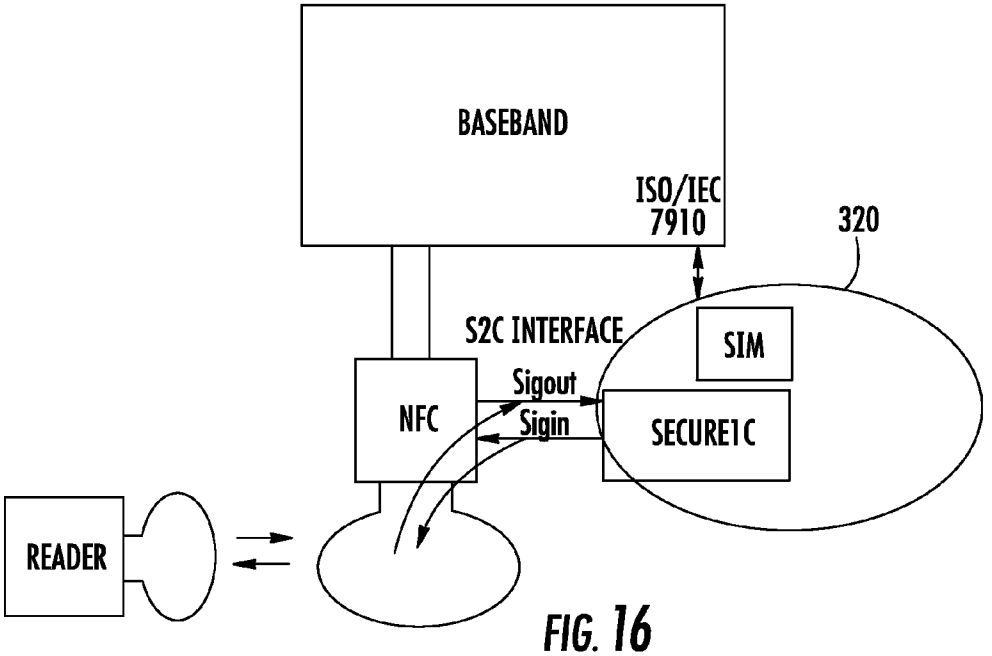


FIG. 16

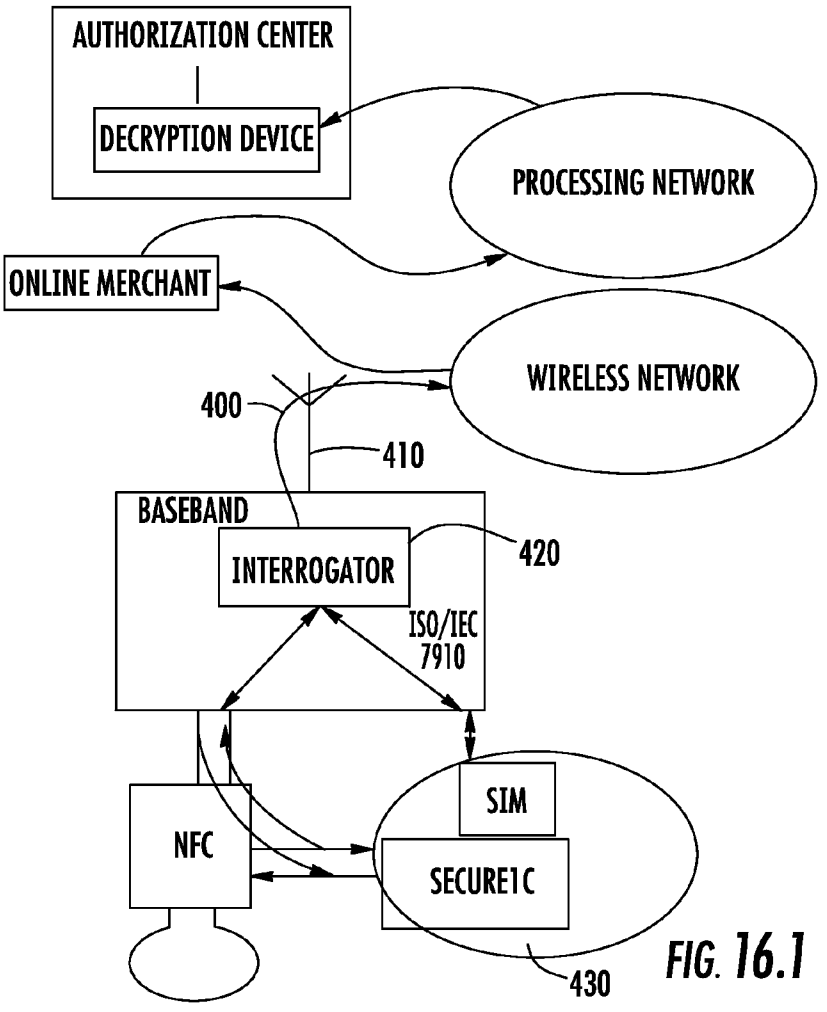


FIG. 16.1

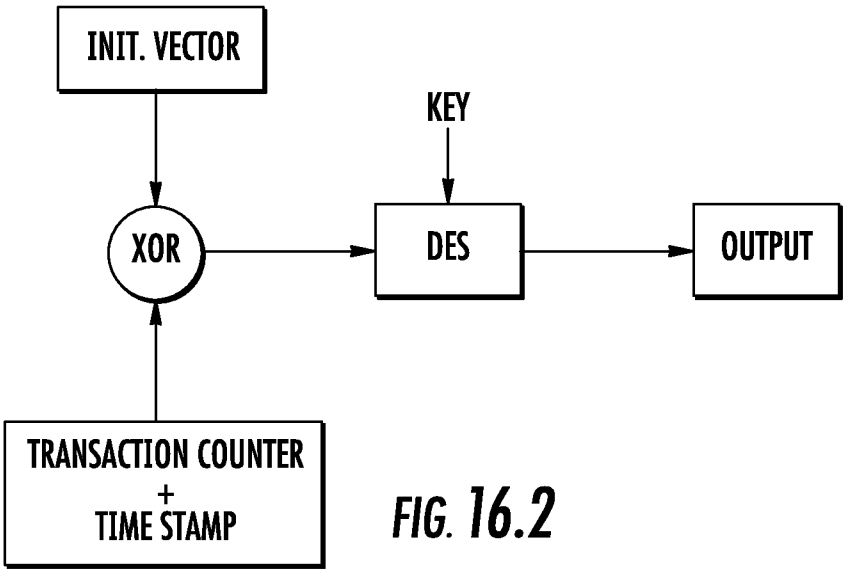

INIT. VECTOR
KEY
XOR
DES
OUTPUT
TRANSACTION COUNTER
+
TIME STAMP

FIG. 16.2

SELF-AUTHORIZING TOKEN

CROSS REFERENCES TO RELATED APPLICATIONS

This application is a Continuation of currently pending and allowed U.S. patent application Ser. No. 12/019,318 filed Jan. 24, 2008, entitled "Self-Authorizing Devices." This Application and U.S. patent application Ser. No. 12/019,318 claim priority from and are related to U.S. Provisional Patent Application Ser. No. 60/897,110 filed Jan. 25, 2007, entitled: "Method and Apparatus for Self-swiping Smartcard Payments," and this patent application and U.S. patent application Ser. No. 12/019,318 claim priority from and are related to U.S. Provisional Patent Application Ser. No. 60/932,704 filed Jun. 1, 2007, entitled: "Method and Apparatus for a Self-swiping Smartcard." Provisional Patent Application Ser. Nos. 60/897,110 and 60/932,704 are incorporated by reference in their entirety herein.

FIELD

This invention relates to the field of devices configured to authorize transactions using secure element microchips. More particularly, this invention relates to tokens that contain secure element microchips and are configured to authorize financial transactions over the internet.

BACKGROUND

In some payment technologies such as smartcards, a microchip referred to as a "Secure Element" (SE) is embedded into the payment card, the payment fob, or another other device that may be used for making payments. In order to extract information from the SE, an interrogator, also referred to herein as a "reader", is required to interact electrically with the SE. The reader typically follows standards set forth by the International Organization for Standardization (ISO) or proprietary standards established by financial institutions or other application providers. In addition to making payments such devices may be used for other purposes such as controlling access to networks and databases and verifying identity. Such devices typically employ sophisticated technologies for enhancing the security of these transactions and preventing fraud. However, the use of the internet is becoming more popular for such purposes. What are needed therefore are devices and methods that adapt the enhanced security and fraud prevention techniques used in smartcard systems for use in internet-based transactions.

SUMMARY

The present disclosure provides, in one embodiment, a token that has a mounting structure having a communication connector configured to connect to a computer terminal. In this embodiment a secure element is affixed to the mounting structure, and the secure element includes a data file. This embodiment further includes a secure element interrogator that is affixed to the mounting structure and that is configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator. This embodiment further includes a communications controller that is affixed to the mounting structure and that is configured to receive the data from the secure element interrogator and to transmit the transaction information as a single data communication to the computer terminal through the communications connector.

Another embodiment provides a token that has a mounting structure having a communication connector configured to connect to a computer terminal. This embodiment further includes a secure element that is affixed to the mounting structure, and the secure element has a payment card application and a data file. Further, this embodiment includes a secure element interrogator that is affixed to the mounting structure and that is configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator. The embodiment also includes a communications controller that is affixed to the mounting structure and that is configured to receive the data from the secure element interrogator and to transmit the transaction information as track data to the computer terminal through the communications connector.

A further embodiment provides a token that has a mounting structure having a communication connector configured to connect to a computer terminal. There is a secure element that is affixed to the mounting structure, and the secure element has a data file. In this embodiment a secure element interrogator is affixed to the mounting structure and the secure element interrogator is configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator. This embodiment further provides a communications controller that is affixed to the mounting structure and that is configured to receive the data from the secure element interrogator and that is configured to transmit the transaction information to the computer terminal through the communications connector.

A further embodiment provides a token that has a mounting structure having a communication connector configured to connect to a computer terminal. This embodiment includes a secure element that is affixed to the mounting structure, and the secure element has a data file. There is a secure element interrogator that is affixed to the mounting structure and that is configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communication only between the secure element and the secure element interrogator. Further included in this embodiment is a communications controller that is affixed to the mounting structure and that is configured to receive the data from the secure element interrogator and to transmit the transaction information as a single data communication to the computer terminal through the communications connector.

In another embodiment a token has a mounting structure that has a communication connector configured to connect to a computer terminal. There is a secure element that is affixed to the mounting structure, and the secure element includes a payment card application and a data file. There is a secure element interrogator that is affixed to the mounting structure and that is configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communication only between the secure element and the secure element interrogator. Further provided in this embodiment is a communications controller that is affixed to the mounting structure and that is configured to receive the data from the secure element interrogator and to transmit the transaction information as track data to the computer terminal through the communications connector.

Another embodiment provides a token that has a mounting structure having a communication connector configured to connect to a computer terminal. There is a secure element affixed to the mounting structure, and the secure element includes a data file. There is a secure element interrogator affixed to the mounting structure and the secure element interrogator is configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communications only between the secure element and the secure element interrogator. Further provided is a communications controller that is affixed to the mounting structure and that is configured to receive the data from the secure element interrogator and that is configured to transmit the transaction information to the computer terminal through the communications connector.

BRIEF DESCRIPTION OF THE DRAWINGS

Various advantages are apparent by reference to the detailed description in conjunction with the figures, wherein elements are not to scale so as to more clearly show the details, wherein like reference numbers indicate like elements throughout the several views, and wherein:

FIG. **1** is a drawing of one embodiment of a self-swiping card with a USB interface.

FIG. **2** is a drawing of a close up view of the USB interface connector on one embodiment of a self-swiping card.

FIG. **3** is a drawing of the internals of one embodiment of a self-swiping card.

FIG. **4** illustrates a circuit board schematic according to one embodiment.

FIG. **5** illustrates a system where a self-swiping card is used to deliver track 1 and track 2 data to a merchant remotely via the internet.

FIGS. **5.1** and **5.2** illustrate interaction and data exchange between an interrogator chip and an SE.

FIG. **5.3** illustrates a method of encrypting data.

FIG. **6** illustrates one embodiment of an online web form with an auto-populating field for a self-swiping card.

FIG. **7** illustrates the decrypted track data that was encoded within the information that came from the auto-populating field from FIG. **6**.

FIG. **8** illustrates an embodiment of a self-swiping card with a USB interface.

FIG. **9** illustrates a further embodiment of a self-swiping card with a USB interface.

FIG. **10** illustrates an embodiment of the smart card module embedded in the card.

FIGS. **11**A and **11**B illustrates embodiments of a self-swiping card in a mini-SD and an SD form factor.

FIG. **12** illustrates a system where track 1 and track 2 data with an encrypted PAN (Personal Account Number) data are delivered via the world-wide web.

FIG. **13** illustrates a method of encrypting PAN digits that maintains the original bank routing code.

FIGS. **13.1**-**13.4** illustrate elements of an encryption algorithm.

FIG. **14** illustrates a system where a reader on card is queried as an alternative to keyboard input.

FIGS. **15** and **15.1** illustrate an embodiment of an online web form with an auto-populating field.

FIGS. **16** and **16.1** illustrate a mobile phone embodiment.

FIG. **16.2** illustrates and encryption technique.

DETAILED DESCRIPTION

In the following detailed description of the preferred embodiments, reference is made to the accompanying drawings, which form a part hereof, and within which are shown by way of illustration the practice of specific embodiments of self-authorizing smart tokens and embodiments of self-authorizing cellular network adapters. It is to be understood that other embodiments may be utilized, and that structural changes may be made and processes may vary in other embodiments.

For the purpose of simplifying language and providing a convenient example, the device that houses a secure element (SE) microchip is typically referred to herein as a "card" or "card device." It is important to note that the "card" or "card device" may not physically resemble the shape or size of a typical payment card and may come in various alternate form factors such as fobs, cartridges, or dongles, or form factors that resemble removable digital memory media such as secure digital (SD) chips. The term "token" is used to encompass all of these form factors and the term "smart token" refers to a token that includes an SE. Each token has a mounting structure such as substrate (for card devices) or a packaging case (for fobs, cartridges, and dongles or SD chips).

In many embodiments described herein a card is configured to interact with a computer terminal. As used herein a computer terminal refers to a personal computer or a special-purpose terminal provided at a point of sale or public kiosk. For the purpose of simplifying language and providing a convenient example the term "PC" (referring to a personal computer) will be used as an example of a computer terminal. Typically the PC has access to an internet. As used herein the term internet includes the world-wide web as well as any other public or proprietary network that may be used for authorizing transactions.

In addition to applications involving computer terminals, embodiments are provided for mobile phones and personal digital assistants (PDAs) that communicate over a cellular network. Such mobile phones and PDAs are referred to herein as cellular network devices. The term "cellular network adapter" is used herein to describe a system that includes in a secure element (SE) microchip for use in a cellular network device. Of particular interest are cellular network devices that are configured for authorization of financial transactions over a network. Typically the cellular network device includes a web browser that is configured for authorization of a financial transaction over the world-wide-web. However in some embodiments the browser may connect to a different public network or to a proprietary network. In some embodiments the cellular network device may connect to a dialup voice network and the cellular network device may be configured for authorization of a financial transaction over the voice network, such as by transmission of DTMF tones or by other encoding.

As previously indicated, in order to extract information from an SE, an interrogator or "reader" is used to interact electrically with the SE. Because readers are not typically part of most PCs, it is very beneficial to place the reader functionality on the card device and translate information from the SE into a data stream format such as a USB (Universal Serial Bus) that PCs are generally capable of processing. Other convenient translated formats include software application output, text messaging (e.g., short message service (SMS)), and email messaging. It is particularly advantageous to configure the card devices for HID (Human Interface Device) keyboard emulation for inputting a form field or fields on an application running on the PC. It is also very beneficial to place the reader functionality in the cellular network adapter and translate information into a data stream that may be sent over the cellular network by the cellular network device.

As used herein the term "host device" is used to refer to either (a) the computer terminal that receives the information from a card device or (b) the cellular network device that receives the information from the cellular network adapter.

A significant advantage of extracting and delivering the data within a card device or cellular network adapter is the ability to know beyond reasonable doubt that the data string being delivered over the internet indeed came from a particular SE. This knowledge creates a more secure transaction with lower risk to the merchant, card issuing bank, and card associations.

Heretofore the most secure methods for assuring the validity of an electronic transaction has involved extracting information from a banking card by of swiping the magnetic stripe through a magnetic stripe reader, or extracting the information from a smartcard with a separate contact or contactless reader connected to a point of sale terminal (POS). These methods are known as "card-present transactions." Because of their enhanced level of confidence in validity these methods allow a merchant to receive a discounted transaction fee for that particular transaction. An example of a less secure transaction is reading or entering account numbers, expiration dates, and card verification codes from a card in a phone call or with on-line internet ordering. These transactions are known as "card not present transactions" and incur a full transaction fee.

Preferred embodiments provided herein provide for incorporating a reader on a card device or within a cellular network adapter to extract and deliver banking track data that were generally not previously possible because of the inability to extract information from the SE or from a magnetic stripe at a computer terminal without a reader or to extract information from an SE in a cellular network adapter without a reader. Such embodiments add value in a mobile commerce or e-commerce environment by enabling more secure transactions over a voice network or an internet.

To prevent fraud, electronic transaction systems typically attempt to verify one or more of the following characteristics of a requestor:

1) Something the requestor knows (a password, answer to a question, etc.)
2) Something the requestor has (a physical token, such may be confirmed by embodiments herein)
3) Something the requestor is (such as a physical trait established by a fingerprint or other biometric identifier)

"2-factor authentication" is defined as an authentication where the requestor (the entity to be authenticated) successfully provides two of the above three different types of verifications. If two of these verifications have been provided the authentication is considered "strong." One important advantage of many embodiments described herein is the ability to confirm that a card is present and authentic. This by itself provides a basis for 2-factor authentication over a public or private network using currently ubiquitous access hardware such as a computer terminal or a cellular network device.

Described herein are configurations of a "Reader On Card" (ROC) or "self-swiping" card, or "self-authorizing" card. The terms "ROC," "self-swiping" and "self-authorizing" are synonymous and refer a configuration wherein the card device or cellular network adapter contains both an SE and SE reader functionality. Configurations for a dynamic or encrypted PAN (Personal Account Number) are also described. This refers to configurations where the "Reader On Card" further encrypts the track data in order to securely transport the data packet over a public network. Neither of these concepts is limited to one particular form factor or embodiment. Some examples of devices that may employ these elements include a USB device or a token or a mobile phone that is enabled with contactless (13.56 MHz radio frequency) or NFC (Near Field Communication) RFID technology.

An SE typically contains a microprocessor, random access memory (RAM) that stores a data file, read-only memory (ROM), flash memory (EEPROM), encryption engine(s), and one or more methods of interfacing the SE. Executable applications such as the MasterCard, PayPass, VISA, Contactless, and AMEX Express Pay may be compiled and placed on an SE. Personalization information that is unique to the specific card holder is generally also placed on an SE. The applications for an SE are typically specified by application providers such as MasterCard, VISA, or AMEX among others. The applications may be created using any number of software development tools and then compiled to run on any number of SE architectures.

The applications running on the SE are typically provisioned with card holder specific information prior to being delivered to the card holder. The provisioning entities such as First Data Corp. must follow strict guidelines set forth by card associations such as VISA, MasterCard, AMEX, and others that keep the provisioning process secure and ensure that customer data is protected inside the SE and that only the card issuing banks or their agents are able to verify the information that is extracted from the SE. It is important that this process is not disrupted and abided by while including the advantages of the present invention.

In order to extract information from the application(s) on an SE, an interrogator, also referred to as a "reader", is required to interact electrically with an SE. The interrogator software may be provided in many different forms such as a software module or a pre-programmed microchip. The hardware that the interrogator runs on may also come in different forms such as an ARM processor, or a small M8 processor. The hardware that encompasses a SE and or an interrogator may be referred to as a chip or die. A die is the raw silicon that is packaged during the chip manufacturing process.

The applications on an SE are accessed by a reader with specific query/response calls defined by the application provider as mentioned above. These applications are generally designed to protect the data on a SE via encryption engines in the SE. The protocols used by a reader to pass data to and from a SE are typically defined in the ISO 7816 or ISO 14443 specifications. These protocols are referred to as query/response protocols. An interrogator sends a query and a SE sends a response.

In many embodiments the physical interface between a reader and an SE conforms to standards defined in the ISO 7816 and ISO 14443 specifications. The ISO 7816 specification defines a "Contact" interface to a SE in which the SE is powered by DC voltage and ground electrical connections from an interrogator. The data transfer during the interrogation is managed by an interrogator providing a clock signal connection and data line connection to an SE. The ISO 14433 specification defines a "Contactless" interface to an SE in which the SE is powered by an inductive field produced by an interrogator during the interrogation. The data transfer during the interrogation is managed over a 13.56 MHz carrier signal provided by an interrogator. The physical interface that the interrogator uses to connect to the SE may also be provided in different forms such as UART, or an NXP proprietary S2C interface. It is also possible that the interrogator shares the same silicon chip as the SE and the interface between them is provided by internal memory or physical traces in the silicon.

The "Universal Serial Bus" USB interface is a standard interface to laptop computers and personal computers or other form of computer terminal as a means of expanding the

capabilities of the computer terminal or transferring information between the computer terminal and another device. More information about the USB interface may be obtained at www.usb.org.

The "Human Interface Device" HID interface is a class of USB interface which is a universal standard for a USB host to connect to USB client device. Within the HID class, there are several defined types of devices, including a "keyboard" type. By the USB device interfacing the USB host with the "keyboard" type of HID class interface, the standards require that the USB host recognize the device as a standard device (e.g., a keyboard) and accept input as such without requiring that the computer have any special drivers or operating system updates installed. By configuring a card device as an HID keyboard the card device emulates a keyboard attached to the computer terminal. The computer terminal will recognize and accept the card device as a keyboard input device. This is a very useful feature in many applications for enabling a more user friendly "self-swiping" functionality in the card device.

Included in most embodiments is a "communications controller." The communications controller provides the interface for data exchange between the reader and a communications connector (in the case of a card device) or the interface for data exchange between the interrogator and a cellular network application interface (in the case of a cellular network adapter). The communications connector may be provided in different forms such as USB, USB connection with HID class keyboard type or USB connection with mass storage class, among many others. The interface may be established using other hardware interface standards as well such as SDIO, mini-SD. In many card device embodiments the communications connector is an integral part of the card device, meaning that the communications connector is formed on an edge portion of the card. The cellular network application interface may, for example, be provided as a baseband input/output port for a web browser running on the cellular network device. The physical connection may be provided by a communication bus or by micro-circuitry in common processor and memory areas in the baseband portion of the cellular network device.

In either card device embodiments or in cellular network adapter embodiments, the communications controller may be physically incorporated into the reader or may be physically incorporated into the secure element or the communications controller may be a physically separate electronic element. In some embodiments the capabilities defined herein for the communications controller may physically be performed in the chip that is primarily the SE and/or the interrogator, or the capabilities of the interrogator may physically be performed in the chip that is primarily the SE and/or the communications controller, or the capabilities of the SE may be physically performed in the chip that is primarily the communications controller and/or the interrogator, or the capabilities of the interrogator and the SE and the communications controller may all be performed in a single chip. In any case, the capabilities of the communications controller, the SE and the interrogator are still considered to be performed by the "communications controller," the "SE" and the "interrogator" respectfully. Furthermore, in some embodiments the PDA or phone processor may be connected directly to the SE. In such embodiments the phone processor interrogates the SE to achieve valid transaction data from the SE. The PDA or phone processor may deliver this data to a form field or directly over the cellular network. In such embodiments the communications controller and the interrogator of the SE are now a portion of the PDA or phone processor itself instead of either of communications controller or the interrogator being a separate hardware chip.

In some embodiments of a self-swiping "Reader On Card" (ROC) device the interrogator and SE are integrated together on the same medium, device or circuit. It is important to note that in contactless implementations the interrogator portion of the ROC device may not be able to function from power harvested from the contactless inductive antenna, and therefore may require power from an external source, such as the communication connector to the computer terminal (in the case of a card device) or the cellular network device battery (in the case of a cellular network adapter).

The data that are automatically delivered to the host device may represent bank account information in the form of "Track 1" and/or "Track 2" data. Track 1 and Track 2 data are commonly-used representations of bank account information that is specific to a card holder. These data generally have a very specific industry standard format in order to be properly processed through transaction processing systems. The Track 1 data format was developed by International Air Transportation Association (IATA). The Track 2 data format was developed by the American Banker Association (ABA). In some embodiments the Track 1 data that are generated as file information from the SE data file and converted into transaction information by the communication controller and transmitted to the host device may comprise only a portion of the Track 1 data content specified in a standard published by the IATA. In some embodiments the transaction information may be the entire Track 1 data content specified in an IATA standard. In some embodiments the Track 2 data that are generated as file information from the SE data file and converted into transaction information by the communication controller and transmitted to the host device may comprise only a portion of the Track 2 data content specified in a standard published by the ABA. In some embodiments the transaction information may be the entire Track 2 data content specified in an ABA standard. However, it is important to note that in some embodiments the transaction data delivered to the host device may not be standard Track 1 or Track 2 data. It is possible that this data may be in another standard or proprietary format. In any case, the transaction data may or may not be an encrypted cipher text in whole or part upon delivery to the host device.

Typically a card device transaction authorization process begins when a user is instructed by a web browser-based application program on a computer terminal to insert a self-authorizing smartcard into a USB port on a computer terminal. When the smartcard is inserted, if the self-authorizing smart card is a USB HID keyboard class card device, the smartcard typically self-initializes with the operating system of the PC and begins to automatically input the relative card data into the appropriate field in the browser form. Many embodiments automate the input of card information such as PAN, expiration date, and security code. The USB HID keyboard class card device may use access keys or "hot keys" to navigate the form that has the current focus for input in the computing device. The card device may also automatically remove any information that may have been inadvertently typed prior to card device insertion. The card device may also automatically "submit" the online form using access keys or "hot keys".

An example where the HID keyboard device of the card automatically inputs a sequence of key presses of the device using "hot keys" is as follows.

a. [alt]+',' (This makes the cursor take focus on form element that has a designated access key of ','—the comma key)
b. [ctrl]+'a' (This makes the cursor select all the text that is existing in the current field of focus)
c. [Backspace] (This makes the cursor erase all the currently selected text)
d. [alt]+'.' (This makes the cursor take focus on the form element that has a designed access key of '.'—the period key . . . this could be set to a "submit" button for example)

A benefit of many embodiments is delivery of the information on the SE to the form that has the current focus for input in the host device. A self-authorizing smart token or a self-authorizing cellular network adapter the may deliver this information in a manner of emulating keystrokes from a keyboard device to the host device. For security reasons the application program that has the current focus on the host device (and is collecting this input) may take precaution inside its programming logic to require that the keystrokes being input into a particular form field are keystrokes and not simply a "paste" keystroke from an electronic "clipboard." Alternately, the application program may require that the keystrokes being input into the form field are fast keystrokes resembling the pattern that only an automated keystroke emulation input device could provide, and not a slower pattern of input that would resemble a manual input of keystrokes. Knowing these requirements, the communications controller element of the card device or the cellular network adapter may be programmed to provide the transaction information to the host device in a prescribed cadence for an application running on the host device.

For security reasons the form that has the current focus on the host device and is collecting this input may take precaution inside the programming logic that various pattern of "hot key" presses ([alt]+'some key') may be used to identify the input device as a secure input device. It is important to note the "hot key" keystrokes cannot be duplicated with the traditional "copy", "cut", or "paste" to the clipboard that some operating environments provide. However, such hot key keystrokes may be provided by various embodiments of communication controllers in self-authorizing devices defined herein.

Many embodiments deliver Track 1 and/or Track 2 data to a merchant from the SE of a payment card using the USB interface of a remote customer's PC in a simple, customer friendly manner. The consumer typically only has to insert the card device into a USB port on his/her computing device and the keystroke data will automatically input into the form that has the current focus on the computing device via keyboard emulation from the card device.

Many embodiments deliver Track 1 and/or Track 2 data that contain a dynamic card verification number from the SE of a payment card device, using the USB interface on a PC of a remote customer.

Many embodiments deliver Track 1 and/or Track 2 data that contain an incrementing transaction counter from the SE of a payment card device, using the USB interface on a PC of a remote customer.

Many embodiments use a "unique number" that is stored in the SE and delivered from the card device as further access control security that must be provided to in order to protected content such as recorded music, recorded video, live media, photos, documents and other similar media. An example of this is that the data file of sensitive or licensed content may be encrypted with a key or a diversified key based on the key within the SE. This would allow only the card holder of the SE to successfully "unlock" and view or listen to the protected content.

Many embodiments use a transaction counter that is stored and updated in the SE to uniquely identify a card holder as well as uniquely identify each given transaction or "swipe" from the card device. Remote transaction approval software may check that the Track 1 and Track 2 data from an SE is what is expected for the current transaction, and may update the transaction counter for the next transaction.

In many embodiments the card device is configured to resemble the physical form factor of typical payment cards as closely as possible with the exception of adding a region of the card that is meant to be inserted into the USB port of a computing device. This facilitates carrying the card device in an ordinary wallet or purse.

In many embodiments the smart token is configured to resemble the physical form factor of a "fob" that may be placed on a consumer key ring.

In many embodiments the card device is configured to limit the height of the USB connector so that the device is thin enough to still be carried in an ordinary wallet or purse.

In many embodiments the self-authorizing smart token or the self-authorizing cellular network adapter is designed to minimize part count and assembly costs so that it can be manufactured at a very low price for high volume, low cost uses.

Referring now to FIG. **1**, the face and back of the self-swiping card medium **10** are shown. The dimensions of this embodiment are roughly 2⅛×3⅛ inches, with a preferred maximum thickness of 0.09 in. The nominal thickness of the card is a maximum of 1/32 in. Looking at the left side of the figure, there is a diagonal protrusion **12** that contains the connector **14** for a USB connection of a mating PC. The four contacts visible in the figure are the power, ground, D+, and D− signals that are defined in the USB specification at www.usb.org. The diagonal of the USB connector protrusion **12** is approximately 45 degrees and allows the protrusion approximately ⅝ in. clearance for insertion into a USB connector on a PC. The boundary of the card has been adjusted from its typical rectangular shape to account for this connection area. The diagonal protrusion has a clearance gap **16** between itself and the lower boundary of the card as seen in the figure. This gap **16** is for the purpose of allowing clearance of the "thicker" USB connection protrusion into some forms of "insertion" type magnetic stripe card readers. The face of the card also shows the PAN (portrayed as 0000 0000 0000 0000), expiration date, and card holder name in similar location to a typical rectangular banking card. The back of the card includes a magnetic stripe **18** that is disposed in a location similar to that of a typical rectangular banking card.

Referring to FIG. **2**, the close view of the USB connection protrusion of the self-swiping card medium as shown. Note the change in this thickness of the card from region **30**, where the card is approximately 1/32 inch thick to zone **32** where the maximum thickness of the protrusion is approximately 0.09 in. where the USB contracts **34** are located. The protrusion of the male USB connection is approximately 15/32 in. wide in order to fit into the standard USB female connection on a PC as defined at www.usb.org. Approximately 3/16 in. in back of the leading edge of the protrusion there is a notch **36** that changes the thickness of the protrusion. This thickness change is for accommodating the "snap fit" of the USB female connector on the PC as defined at www.usb.org. The clearance between the leading edge of the protrusion and the bulk of the card medium is approximately ⅝ in. The style of this particular type of USB connection is not a standard mail

USB connection. It has been altered to be much thinner than the typical male connection. As a result, it is susceptible to "upside down" insertion into the female USB connection.

Referring to FIG. **3**, the profile of a self-swiping card **50** with inside components exposed is shown. An antenna **52** is a printed or wire wound antenna that creates an inductive coil that provides power and transmits data to and from a secure element **54**. The number of turns in the antenna **52** is dependant on the properties of the SE as well as the size of surface area the perimeter of the antenna covers. The antenna **52** is embedded inside the card medium and may or may not be congruent with the card medium perimeter. In some embodiments it may be desirable to shrink the area of the antenna **52** for manufacturing reasons such as card embossing. The secure element **54** shown in FIG. **3** is a microchip die that is wire bound to the module face plate through manufacturing methods. The secure element microchip die is typically then coated with epoxy for protection. In the embodiment of FIG. **3** the secure element **54** is a dual interface device that is accessible through the contactless antenna interface or through the contact 7816 style interface. When not plugged into the USB connection on a PC, the antenna serves as the sole power supply, data transmitter, and data receiver for the SE **54**. When plugged into the USB connection on a PC, the antenna **52** is not intended to be used as a power supply or to transmit or receive data. Instead a combined interrogator/communications controller reads information from the SE **54** and transmits information to the PC through a USB connector on the protrusion of self-swiping card **50**.

The protocols that define the communication to the SE are defined in ISO 14443 (contactless) and ISO 7816 (contact). The commands to communicate to the applications that are running on the SE are typically designed to interrogate the secure element and execute file system functions according to ISO 7816-4 in order to generate file information from SE data file. However, in some embodiments the commands to communicate to the applications that are running on the SE are provide by the application providers. In any case, the commands are generally the same regardless of the interface method (contact or contactless).

The SE is generally a secure microchip that has built in encryption engines, RAM, micro-processor, EEPROM, and communication interfaces. The interrogator and the communication controller (USB interface) chip shown in FIG. **3** is a chip that contains a microprocessor, RAM, EEPROM, and built in USB interface engine. The chip is programmed to describe itself to the host PC as a HID class "keyboard" device upon connection to the PC. The chip then communicates to the SE via ISO 7816 (contact) interface protocols to acquire and build Track 1 and Track 2 data. After track data are acquired from a successful "read" of the SE, the data is then delivered to the PC's USB bus through the communications connector protrusion shown in the FIG. **3**. It is important to note that it is possible for both the SE and the interrogator/USB interface chip die to be mounted and wire bound together on the same module medium. It is also important to note that these two chips could also be contained in one piece of silicon sharing the same RAM and/or EEPROM memory space.

FIG. **4** illustrates a circuit board schematic **60** according to one embodiment. This shows a more detailed layout of the components described in FIG. **3** as well as the supporting components of typical embodiments. In this particular embodiment, the interrogator/USB bridge chip/die is a chip made by cypress semiconductor with a part number of CY7C3. The SE used in this particular embodiment is a chip/die with a standard ISO 7816 contact type interface in combination with a standard ISO 14443 contactless interface.

FIG. **5** illustrates a flow diagram that describes one method embodiment. After the card device is plugged into the USB connector on the customer computing device, the card device powers up and begins to interrogate the SE on the card device. The interaction and data exchange between the interrogator chip and the on the SE could look something like the diagram in FIG. **5.1**. In preferred embodiments the interrogation process conforms to application level protocols (APIs) established by ISO 7816-4. ISO 7816-4 defines two such application-level protocols:

(a) File system API providing a set of functions to manipulate files (e.g. read, write, select etc.)

(b) Security service API allowing the smart card and the reader to mutually authenticate themselves and also to encrypt data to be exchanged between the card and the reader.

In preferred embodiments the interrogation process conforms to protocol message structures also defined in 7816-4 to support the APIs. This message structure consists of application protocol data units (APDUs) which are exchanged between the reader application and the smart card application by the link level protocol. There are two types of messages used to support the ISO 7816-4 application protocols: the command Application Protocol Data Units APDU (sent from the reader to the card) and the response APDU (sent from the card to the reader).

After the interrogator has received the all the data from the interrogation of the banking application on the SE, the interrogator can then build the data string that is to be sent to the computing device as keystrokes. It is important to know that the SE can run multiple applications from different application providers. It is possible, and is one embodiment of this invention, for the interrogator to deliver the information that was acquired during interrogation of the banking application on the SE to a second application that resides on the same SE so that the second application can process, build, and possibly encrypt the data that will be delivered to the computing device as keystrokes.

An example of this embodiment that contains the interrogation of two applications on the SE may look something like the diagram in FIG. **5.2**. The dotted lines in the figure represent the times during the entire interrogation of the SE that the interrogator selects different applications to use. The interrogator or the interrogator application on the SE may or may not encrypt the final Track 1 and/or Track 2 data.

FIG. **5.3** shows one embodiment of a method of encrypting this data. After the interrogator has acquired or built the data to be sent to the computing device as keystrokes, the USB interface enumeration begins. During the enumeration process, the card device, which is the client device, exchanges information with the USB host device. The information exchange is defined in the USB specifications and can be obtained at www.usb.org. As part of the exchange, the card device will send "descriptors" that tell the host device about the drivers that are required to run the client card device. The descriptors that the card device sends to the host include a HID (Human Interface Device) descriptor. The card device sends another descriptor that further defines the type of HID device to be a "keyboard" type of device. The USB host will now recognize the card device as a keyboard and expect that the card device will deliver "key codes" that represent keystrokes as input data. After enumeration has occurred and the host USB device recognizes the card device as a keyboard, the

card device begins to deliver data to the current form that has the focus on the computing device. The data that are delivered may consist of:

a. Identification of the entity to which the data must be passed to for further processing.
b. Identification number of the particular card device that is delivering the data.
c. Identification number of the cryptographic key to be used for decrypting the data that is delivered from the card device.

The application, such as an internet browser, that is running on the computing device that has collected this information is then responsible for passing the information to the entity identified by the data above for processing. One embodiment of this invention involves passing this information in an online setting by one internet server passing this information string to another internet server. In this embodiment, the entity that controls the internet server that receives this information can then process the information along with the identity of the owner of the requesting internet server as they see fit. The entity that received the data can then return resultant data back to the requesting party. Also, in this embodiment, the information that is passed back to the requesting party is Track 1 and/or Track 2 data that is used to process typical card payment transactions by merchants.

Referring to FIG. **6** the internet browser form that receives the information from the card device as shown. This form represents one example of how a card device may be used. In this example an application running on a PC includes one specific field **100** on a form that is designated as the field that the card device will automatically populate when the card device is plugged into the PC that is displaying this form. In this example, the application has been programmed so that the form field **100** can be addressed using an access key or "hotkey" of ',' (the comma key). That is, when the card device issues this "hot key" keystroke (by use of keyboard emulation), the cursor will automatically move its focus to the field **100**. The HTML (hypertext markup language) code that is used to create the self populating field may have this syntax:

```
<input type="text" name="data" size="" access
    key=","/>
```

The card device then populates the form field **100** with data. Then the auto-populating field **100** may be further checked by the application program for the authenticity of the keystrokes by the internet browser using "Java-Script" code that may be embedded into the HTML code. Also, the internet browser may check that each key was actually typed into the field by keystrokes rather than the use of "copy", "cut", and "paste" commands that may be provided some operating environments. The internet browser may also check that each keystroke was typed very fast resembling an automated input rather than a slower manner that would resemble manual input. The internet browser may check other aspects of the input data for its validity as it sees fit.

Referring to FIG. **7**, an internet browser screen displays decrypted data **110** that may be provided to a merchant transaction authorization system. The track information shown here is acquired using a Reader On Card (ROC) system. After the card reader extracts information from the SE and builds the track data containing the DVCC from the SE on the card, the track data are then delivered to the appropriate field in the transaction requester's browser as encrypted data via a USB HID keyboard interface. The information that is auto-populated on the requester's screen is not the Track data that is depicted in FIG. **7** because the ROC system encrypts the track data on the card device before the field on the requestor's browser is populated and the encrypted data are transmitted. The data on FIG. **7** is a decryption of the data that appears on the requester's screen. If the process is repeated by the requester the DVCC data and the transaction counter will change, in accordance with specifications for secure transaction encryption. In a typical application a merchant that is processing the information would not expose the clear text track information portrayed on the browser screen of FIG. **7**. This figure is merely showing it as an example of the decrypted data. It should also be noted that in many embodiments the SE on the requester's card device may be used to make contactless transactions at in-store POS terminals by holding the card device up to a contactless reader.

Referring to FIG. **8**, the face of one embodiment of a self-swiping card **120** is depicted. The placement of the protrusion that exposes the USB connection, relative to the card boundary **122**, is important. The USB connector **124** may be manufactured in a similar fashion to a typical ISO 7816 smart card module. The typical ISO 7816 module is then seated into the card medium during an assembly process. The exact placement of the module relative to the card boundary is defined in the ISO 7816 specification and many of the assembly machines used to place this module inside the card medium is set to place the module in a specific location as shown in the figure.

Referring to FIG. **9**, one embodiment of an alternate form-factor self-swiping card **140** is shown. This embodiment includes a USB connector **142** but has a form factor that lends itself to placing the card device on a key ring through a hole **144**. The purpose of this figure is to illustrate some of the wide variations that can encompass various potential embodiments.

Referring to FIG. **10**, components of a smartcard module **150** are depicted. On the left is the connector plate (module top) and on the right is the module bottom of the smartcard module **150**. Looking at the right side of the figure, the bottom of the module exposes how the die from both the SE **160** and the interrogator **156** may be mounted. Also shown in the right portion of this figure, are the mounting pads **158** that may be connected to the inductive coil antenna for the contactless interface of the SE. The inductive coil antenna is typically assembled into the card medium prior to placement of the smart card module. The mounting pads are designed to make contact with the exposed ends of the inductive coil antenna. Looking at the left side of the figure, the connector plate is carved or scored in such a way that the connection pads **154** align themselves with the standard female USB connections of DC voltage, ground, D+, and D− that are defined in the USB specification at www.usb.org.

Two embodiments of a self-swiping card medium are shown in FIGS. **11**A and **11**B. FIG. **11**A depicts a standard "miniSD" **180** that is a common form factors for expansion memory or IO functionality. The miniSD **180** has a width **184** that is approximately 20 mm and a height **184** that is approximately 21.5 mm. FIG. **11**B depicts a standard secured device ("SD") **190**. The standard SD has a width **192** that is approximately 24 mm and a height **194** that is approximately 32 mm. These form factors **180** and **182** are fairly ubiquitous in mobile phones and personal digital assistants (PDAs) and therefore are convenient for use in various embodiments of a cellular network adapter. The SE and other electronics to interrogate the SE may be contained within these form factors. Additional features may be added such as additional expansion memory for the mobile device or PDA to access. Further detailed specifications for the SD **190** and the miniSD **180** form factor may be obtained at www.sdcard.org.

FIG. **12** illustrates a flow diagram that describes one method and use embodiment. After the card device is plugged into the USB connector on the customer computing device, the card device powers up and begins to interrogate the SE on the card device. The interaction and data exchange between the interrogator chip and the on the SE could look something like the diagram in FIG. **5.1**. After the interrogator has received the all the data from the interrogation of the banking application on the SE, the interrogator can then build the data string that is to be sent to the computing device as keystrokes. It is important to know that the SE can run multiple applications from different application providers. In some embodiments the interrogator delivers the information that was acquired during interrogation of the banking application on the SE to a second application that resides on the same SE so that the second application can process, build, and possibly encrypt the data that will be delivered to the computing device as keystrokes.

An example of an embodiment that contains the interrogation of two applications on the SE typically looks something like the diagram in FIG. **5.2**. The dotted lines in the figure represent the times during the entire interrogation of the SE that the interrogator selects different applications to use. The interrogator or the interrogator application on the SE may or may not encrypt the final Track 1 and/or Track 2 data. Specifically, in the embodiment reflected in FIG. **12** the PAN or Personal Account Number is encrypted within the final Track 1 and/or Track 2 data, or possibly by itself only. The encryption is handled in such a way as to not disturb the bank routing code within the PAN. This is typically the first 6 digits of the PAN. The final digit of the PAN is also adjusted as to equal the proper check digit for the new PAN. Once the new PAN is created from encrypting the original PAN, it is substituted in the place of the original PAN. Using this method, the merchant is able to receive the PAN and verify that it is a valid credit card number by checking the digits and calculating the proper check digit. After the PAN is submitted to the merchant for processing via HID keyboard buffer which prints the PAN and possibly other data into a "web form," the information is submitted by the user for processing. The merchant would be able to authorize the transaction as it would any other credit card transaction over the internet. When the encrypted PAN is submitted to the processor for authorization, the processor is able to send the encrypted PAN to a decryption device that will properly decrypt the PAN and build the original PAN to check for authorization. The advantage of using a method like this is that valid Personal Account Numbers are never transmitted from the user's computer over the internet.

To add further protection to the encrypted PAN, there is a transaction counter that can be factored into the encryption algorithm. This allows for a unique card number for each transaction that is processed. The encryption algorithm, encryption key, and transaction counter may be contained within the SE of the card. The encryption of the PAN may take place with every transaction and to take place within the SE. This type of encryption of the PAN may used with several embodiments of the present invention including mobile phones containing a SE. In the case of the mobile phone, the interrogation of the secure element is very similar to the interrogation depicted in FIG. **5.2**. The mobile phone may not deliver the final data to a "web form", however, by auto populating a field, but instead it may receive the encrypted PAN and other data within its own memory structure and then pass the data to the merchant for processing either via internet or its own phone connection. In any case, this method of PAN encryption helps to protect the original PAN data that is needed to authorize a transaction. Because the PAN data is encrypted on the card itself, it may be considered safe to transmit over a network in clear text to the decryption device.

FIG. **13** presents a representation of a Personal Account Number or PAN **200** that is found on the face of a credit card and within the Track 1 and Track 2 data that is stored on the magnetic stripe or SE of a credit card. The first set of digits **202**, usually ranging from the first 3 to the first 6 digits, is referred to as the Bank Code. This code is designated as a routing number for the many card association networks that describes which bank or "issuer" the PAN belongs to. The second set of digits **204** shown in FIG. **13** indicates the personal account number of the card holder at the issuer. The last digit **206** of the PAN is usually considered a "check byte" that is used to calculate if the complete PAN is indeed a valid PAN number. The algorithm normally used for the "check byte" is called the Luhn algorithm. The algorithm uses the digits in the PAN itself to make the proper calculation of the check byte. For this reason, if any digit in the PAN is changed, it is likely that the check byte will also need to be adjusted in order to make the new PAN considered valid. When encrypting the PAN, it is important not to change the bank code. The bank code may remain the original bank code in order for the encrypted PAN data to be routed to the appropriate bank and then to the decryption device that will replace the encrypted PAN digits with the original PAN digits.

In FIG. **13.1**, and FIG. **13.2**, one embodiment of an encryption algorithm is shown. This embodiment used DES in OFB mode as described in FIPS 81 as defined by NIST. A known initialization vector is XOR with a transaction counter that is maintained by the reader-on-card. Every transaction that is committed to, the counter increases. This will effectively change the initialization vector for encrypting the PAN digits. In a separate embodiment, it is also possible to incorporate a timestamp into the randomization processes of the initialization vector. This may not be possible in embodiments that do not have access to an accurate clock. After the initialization vector is XORed with the transaction counter, or other information, DES encryption is performed on the 64 bit, value using the DES key that is has been previously loaded into the interrogator application that is stored on the SE. This produces a 64 bit output value.

FIG. **13.2** shows the 64 bit output value from FIG. **13.1**. The original account number from the PAN is also shown. The digits that will be changed within this account number are typically the middle 5 digits '6784'. The leading three digits '0' are generally reserved as placeholders for passing the transaction counter to the decryption device. The final two digits '80' are generally used to mark a DES key ID for the decryption device. The DES key ID may or may not be included is some embodiments. The purpose is to allow many different DES keys to be used by many different interrogators. Further on this subject, it is possible to create greater randomization of DES key by including a diversification process of the DES key in the interrogator application. A diversification process takes a master key and applies an algorithm to the key based on known data to produce a further randomized key to be used in the actual transaction. The two-digit key ID may actually be used to diversify a master DES key instead of identify a separate key.

The middle 4 digits to be encrypted may be represented in 14 bits. The 14 bits to be encrypted of the original account number are also shown at the bottom of FIG. **13.2**. According to FIPS 81, using DES in OFB mode, the number of bits to encrypt can range from one to sixty-four during each iteration of the algorithm.

In this particular embodiment one iteration is shown, resulting in fourteen bits of encrypted cipher text. In order achieve the final cipher text; the first fourteen bits of the DES encrypted output text are XORed with the fourteen account bits that are to be encrypted. The resultant output is the fourteen bit cipher text to be placed back into the PAN, creating an encrypted PAN. FIG. **13.3** shows the conversion of the fourteen bit output from FIG. **13.2** into a four digit decimal. The four digit number is then placed into the issuer account number along with the transaction counter as shown in FIG. **13.3**.

FIG. **13.4** shows the total encrypted PAN **250** with the bank code **252**, the account number **254** and the updated check digit **256** that reflects the new PAN digits. Now, it is possible for this number to be processed in the exact same manner as a legitimate card PAN. The decryption device must be used to replace the encrypted PAN with the original PAN, but it is important to note that all the information for how to do so, including the transaction counter and DES key ID are included in the encrypted PAN.

The number of digits used for the DES key ID, transaction counter, and encrypted digits may vary depending on implementation of this method and the particular embodiment. It is also possible to share a single digit to represent parts of two different data elements. One example of this would be to divide a digit by 2 and discard the remainder to represent 0-4 for one data element (transaction counter, DES key ID, or encrypted digits), and then to divide the same digit by 2 and only use the remainder to represent 0-1 for separate data element (transaction counter, DES key ID, or encrypted digits).

Referring to FIG. **15**, the internet browser form that receives the information from the card device as shown. This form is shown after the field **300** has been self-populated. The content in the form that is shown is an example of an encrypted PAN which is digits in this case and has a bank routing code of '541312'. The transaction counter is populated backwards over the next 3 digits '101'. The third digit, in this example, is used to share with the encrypted digits data element as described in the previous paragraph. So, the transaction counter is actually showing '001' when reversed. Including the shared digit, the next 5 digits represent the encrypted digits of the account number '14194'. The following two digits, '80', represent the DES key ID. And the final digit of '1' represents the check byte.

Looking at FIG. **15.1**, the same "web form" as shown in FIG. **15** is shown with a field **302** auto populated with a second transaction from the same card device. When comparing the encrypted PAN's from FIG. **15** and FIG. **15.1**, the differences are seen here:

1st Transaction—FIG. **15**: 5413 1210 1419 4801 (encrypted PAN)

2nd Transaction—FIG. **15.1**: 5413 1220 1176 280 (encrypted PAN)

When these transactions are received by the decryption device the original PAN may be decrypted and created. In this particular example shown in these figures, the original or valid PAN is:

Original PAN: 5413 1200 0763 2801 (valid PAN)

FIG. **14** illustrates a flow diagram that describes one method embodiment. This particular embodiment is generally not appropriate for use with the HID keyboard emulation class of a USB device. This embodiment shows a 2-way form of communication from the base band device or host PC to the card device. The HID keyboard emulation class of a USB device is typically a 1-way device upon which the HID keyboard USB device communicates to the host PC via an "in" endpoint only. This allows data to move from the keyboard emulation device to the PC only. In such a case the interrogation most likely starts at the time the USB device is plugged into the computer and cannot be initialized by the PC.

The 2-way device as shown in FIG. **14**, offers some added features to the system. In a case like this, the interrogation of the SE may be controlled by the base band device or by the host PC. Data such as an unpredictable number (UN), a timestamp, or some other type of deterministic data may be used during the interrogation of the SE, or may be sent to the card device to initiate an interrogation. An unpredictable number refers a number that may be used in algorithms of certain financial transaction authorization systems, such as VISA® or MASTERCARD®, in the encryption phase of a dynamic card verification code (DCVC). A DCVC is a 3 digit encrypted number that changes for each transaction (the dynamic aspect of the track data). The algorithm to create a DCVC typically uses a UN, a transaction counter, and DES key to derive a DCVC for each transaction. In some embodiments the financial transaction authorization system instructs a reader to create an unpredictable number. In some embodiments the communications controller may be configured to create a random UN and send it to the secure element during a transaction. The UN may be constructed as a hash of a timestamp, for example, and such a UN would ensure the authorization system that the SE made and returned its encrypted DCVC and that it was constructed at a certain (recent) time. This also adds another layer of security by establishing a basis for a precise expiration time for a particular transaction.

After the interrogation is complete, the resultant data string may be sent back to the base band device or host PC. There are many ways this system can be implemented. One example of an implementation would be using a generic HID class that allows both an "in" endpoint and an "out" endpoint to the USB card device. Both the "in" and "out" endpoints of a USB device are described by documentation that may be obtained at the www.usb.org website. The HID class driver is packaged and available on most host PC's. In order to use this HID class driver on a host PC, a client application must be resident and running on the host PC that identifies the proper HID device when it is connected to the host PC. The client application that is using the HID class driver may then issue command packets to the USB card device using the HID class interface and receive response packets from the USB card device using the HID class interface. Although using the HID class interface is not quite as ubiquitous to the system as using the HID keyboard class interface, it is still more ubiquitous then communicating to the USB device using a custom driver implantation. The HID class interface is possible to implement in PC side applications without creating a hardware driver **5** that runs on the host PC. The HID class interface can be created and used as a plug-in to internet web browsers and other PC applications. The HID class interface can also be built into simple executable programs that are allowed to communicate directly to a USB card.

In a similar embodiment it is possible to create a dual-purpose USB device that has both a HID class driver that allows an "out" endpoint to communicate to the USB card device from the host PC, and also uses the HID keyboard class interface with an "in" endpoint to send data back to the host PC via keyboard emulation. Another implementation of this system could be entirely contained inside a mobile phone. A 2-way data channel is used to initiate an interrogation with a secure element as well as receive the resultant data string after the interrogation is completed. It is important to note that there is a dashed line that encompasses a rectangle on FIG. **14** that contains both the "initiator" and the "interrogator" enti-

ties. These two entities may be handled and running within the same base band processor in the mobile phone. In this case they may exchange information within libraries or memory space only. The mobile phone may receive the resultant data via a keyboard buffer that can then auto-populate a form field, for example, in a mobile web browser. In any case, the 2-way data channel can be used to give more control as well as possibly more security to the system. By passing the unpredictable number, that is used in the dynamic Card Validation Code (CVC) generation within the SE, timestamp, or some other type of deterministic information, the baseband portion of the mobile phone or the host PC may validate and timestamp any transaction that it requests by linking a timestamp to a particular unpredictable number.

Also, the 2-way data channel represented in FIG. **14** allows for the entire transaction to be triggered by the base band device or host PC. The act of sending data to the card device can signal a start to the interrogation process.

Referring to FIG. **16**, a diagram of a mobile phone with contactless or NFC functionality is displayed. One purpose of a mobile phone or like device with NFC technology is to enable the mobile phone itself to act as a payment card in order to make payments at a contactless terminal that may be located at a retailer location. In this embodiment the SE is embedded in a Secure IC within the phone. The SE on the phone may contain multiple bank accounts and may be controlled by the user interface of the phone. The diagram depicts the phone itself (baseband portion), the cellular network adapter **320** that includes a reader, the SE, and a processor in one of potentially multiple form factors (here either within the SIM or a Secure IC), the NFC bridge chip that is used to convert an electronic data signal to an RF data signal for an external reader, and the external reader that may also be used to interact with the SE in order to retrieve banking information. The reader in the cellular network adapter **320** may communicate to the using a number of different methods. For example, the reader in the cellular network adapter may communicate directly to the SE using ISO 7816-3 and 7816-4 protocols. An external reader may also communicate to the SE through an NFC bridge controller. The NFC controller controls the data paths to the RF interface as well as the data path to the SE. It is important to note that the interrogation of the SE can be initiated and carried out by either the reader in the cellular network adapter **320** or an external reader as shown in the diagram in FIG. **16**.

FIG. **16.1** shows the same hardware device depicted in FIG. **16** being used for a different application. The application in FIG. **16.1** relates to using the same banking information stored on the SE for making a mobile payment transaction over the wireless network. A transaction like this is usually performed using a mobile phone connecting to a remote merchant over a wireless network (such as a cellular network) that may also be using the public internet and a mobile web browser on the phone itself. In order to deliver the transaction data from the SE to the web browser by the interrogator, keyboard emulation or software plug-in may be used to populate the web browser with the appropriate data. In the case where the transaction is not performed using a mobile web browser, the transaction information may pass to the merchant using other methods such as email, SMS, or other proprietary or standardized communication methods. The cellular network adapter **430** (the interrogator and the communications controller and the secure element), in this case, may be contained as an element **420** inside the mobile phone and exist as a software module running on the baseband of the phone. The interrogator essentially serves the same purpose as the contactless reader shown in FIG. **16**. Its job is to interrogate the SE inside the phone and build a communication data package **400** that typically includes an encrypted pan and optionally Track 1 and/or Track 2 data. In order to do this, a "Reader On Card" mechanism may be used in order to further encrypt the PAN or full Track 1 and Track 2 data for transportation over a public network using the antenna **410** of a mobile phone.

After the interrogator has completed an interrogation process that is typically similar to the interrogation routine in FIG. **14** or FIG. **5.2**, the data packet to be issued for authorization is sent to the "online merchant" over a wireless network. This data packet may contain full Track 1 and/or Track 2 information that has been encrypted or may contain only an encrypted PAN with an expiration date. The encrypted PAN is encrypted using the same method as described in FIG. **13**, FIG. **13.1**, FIG. **13.2**, FIG. **13.3**, and FIG. **13.4**. After the encrypted data is passed to the "online merchant" the merchant may further submit the data just as it would a traditional card transaction to the processing network for authorization. The processing network then routes the data to the appropriate bank for authorization as shown in FIG. **16.1**. Prior to the authorization of the data packet a "Decryption Device" interprets the data packet, decrypts the PAN or full track data, and replaces it with the original and legitimate PAN or track data. The decryption device may also perform other statistical checks on the PAN or track data such as verifying the transaction counter or timestamp is not repeated.

FIG. **16.2** shows a similar encryption technique for encrypting the card PAN. In this case, it is possible to add a timestamp factor into the encryption of the PAN. Because a mobile phone is an electronic device that can keep accurate time, the interrogator would be able to use a timestamp to further randomize the initialization vector that is used to encrypt the PAN data. When this transaction data reaches the decryption device on the other side of the network, the decryption device can then use a timestamp in a similar manner to decrypt the PAN data. It may not be possible to use a timestamp in all embodiments if the interrogator does not have access to an accurate clock.

As previously indicated, various embodiments may include embedding the SE within a mobile phone or PDA. Such embodiments may use portions of the baseband processor of the mobile phone or PDA as a communications controller and an interrogator. The combination of the SE, the communications controller and the interrogator then provide the principal components of a typical cellular network adapter. Software within the mobile phone may run the interrogation routines while interacting with the SE. The software may then perform communication controller functions by inserting the data extracted from the SE into appropriate areas such as SMS or email message, or form field. The insertion into these areas may include the keyboard emulation tactics previously described herein. The insertion into these areas may include automatic SMS or email message building and sending by software running on the mobile phone. The automatically built SMS or email message typically includes the extracted data from the interrogator.

In summary, embodiments disclosed herein describe various systems and methods for providing self-authorizing tokens and self-authorizing cellular network adapters. The foregoing descriptions of embodiments have been presented for purposes of illustration and exposition. They are not intended to be exhaustive or to limit the embodiments to the precise forms disclosed. Obvious modifications or variations are possible in light of the above teachings. The embodiments are chosen and described in an effort to provide the best illustrations of principles and practical applications, and to

thereby enable one of ordinary skill in the art to utilize the various embodiments as described and with various modifications as are suited to the particular use contemplated. All such modifications and variations are within the scope of the appended claims when interpreted in accordance with the breadth to which they are fairly, legally, and equitably entitled.

What is claimed is:

1. A token comprising:

a mounting structure having a communication connector configured to connect to a computer terminal;

a secure element affixed to the mounting structure, the secure element comprising a data file,

a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator; and

a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as a single data communication to the computer terminal through the communications connector.

2. The token of claim **1** wherein the plurality of transaction data communications comprises communications formatted according to ISO 7816-4.

3. The token of claim **1** wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

4. The token of claim **1** wherein the secure element interrogator exchanges the plurality of transaction data communications with the secure element only within libraries or memory space residing on the mounting structure.

5. The token of claim **1** wherein the secure element comprises a payment card application and the single data communication to the computer terminal comprises track data.

6. The token of claim **1** wherein communications to and from the secure element consist of communications from and to a secure element reader.

7. The token of claim **1** further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

8. The token of claim **1** wherein:

the secure element comprises an executable application; and

the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.

9. The token of claim **1** wherein:

the secure element comprises a payment card application;

the secure element interrogator is configured to interrogate the payment card application; and

the transaction information comprises card-present data.

10. A token comprising:

a mounting structure having a communication connector configured to connect to a computer terminal;

a secure element affixed to the mounting structure, the secure element comprising a payment card application and a data file;

a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator; and

a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as track data to the computer terminal through the communications connector.

11. The token of claim **10** wherein the plurality of transaction data communications comprises communications formatted according to ISO 7816-4.

12. The token of claim **10** wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

13. The token of claim **10** wherein the secure element interrogator exchanges the plurality of transaction data communications with the secure element only within libraries or memory space residing on the mounting structure.

14. The token of claim **10** wherein the communications controller creates a random unpredictable number and sends it to the secure element.

15. The token of claim **10** wherein the transaction information comprises a dynamic card verification code.

16. The token of claim **10** wherein communications to and from the secure element consist of communications from and to a secure element reader.

17. The token of claim **10** further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

18. The token of claim **10** wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.

19. The token of claim **10** wherein:

the payment card application comprises an executable payment card application; and

the secure element interrogator is configured to interrogate the executable payment card application to acquire the transaction information from the data file.

20. The token of claim **19** wherein the executable payment card application includes an application level protocol for authentication of the secure element.

21. The token of claim **10** wherein the transaction information comprises card-present data.

22. A token comprising:

a mounting structure having a communication connector configured to connect to a computer terminal;

a secure element affixed to the mounting structure, the secure element comprising a data file,

a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging a plurality of transaction data communications only between the secure element and the secure element interrogator; and

a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information to the computer terminal through the communications connector.

23. The token of claim **22** wherein the plurality of transaction data communications comprises communications formatted according to ISO 7816-4.

24. The token of claim **22** wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

25. The token of claim **22** wherein the secure element interrogator exchanges the plurality of transaction data communications with the secure element only within libraries or memory space residing on the mounting structure.

26. The token of claim 22 wherein the secure element comprises a payment card application and the transaction information comprises track data.

27. The token of claim 22 wherein communications to and from the secure element consist of communications from and to a secure element reader.

28. The token of claim 22 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

29. The token of claim 22 wherein:

the secure element comprises an executable application; and

the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.

30. The token of claim 22 wherein:

the secure element comprises a payment card application;

the secure element interrogator is configured to interrogate the payment card application; and

the transaction information comprises card-present data.

31. A token comprising:

a mounting structure having a communication connector configured to connect to a computer terminal;

a secure element affixed to the mounting structure, the secure element comprising a data file,

a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communication only between the secure element and the secure element interrogator; and

a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as a single data communication to the computer terminal through the communications connector.

32. The token of claim 31 wherein the at least one transaction data communication comprises communications formatted according to ISO 7816-4.

33. The token of claim 31 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

34. The token of claim 31 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.

35. The token of claim 31 wherein the secure element comprises a payment card application and the single data communication to the computer terminal comprises track data.

36. The token of claim 31 wherein communications to and from the secure element consist of communications from and to a secure element reader.

37. The token of claim 31 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

38. The token of claim 31 wherein:

the secure element comprises an executable application; and

the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.

39. The token of claim 31 wherein:

the secure element comprises a payment card application;

the secure element interrogator is configured to interrogate the payment card application; and

the transaction information comprises card-present data.

40. A token comprising:

a mounting structure having a communication connector configured to connect to a computer terminal;

a secure element affixed to the mounting structure, the secure element comprising a payment card application and a data file;

a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communication only between the secure element and the secure element interrogator; and

a communications controller affixed to the mounting structure and configured to receive the data from the secure element interrogator and to transmit the transaction information as track data to the computer terminal through the communications connector.

41. The token of claim 40 wherein the at least one transaction data communication comprises communications formatted according to ISO 7816-4.

42. The token of claim 40 wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

43. The token of claim 40 wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.

44. The token of claim 40 wherein the communications controller creates a random unpredictable number and sends it to the secure element.

45. The token of claim 40 wherein the transaction information comprises a dynamic card verification code.

46. The token of claim 40 wherein communications to and from the secure element consist of communications from and to a secure element reader.

47. The token of claim 40 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

48. The token of claim 40 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.

49. The token of claim 40 wherein:

the payment card application comprises an executable payment card application; and

the secure element interrogator is configured to interrogate the executable payment card application to acquire the transaction information from the data file.

50. The token of claim 49 wherein the executable payment card application includes an application level protocol for authentication of the secure element.

51. The token of claim 40 wherein the transaction information comprises card-present data.

52. A token comprising:

a mounting structure having a communication connector configured to connect to a computer terminal;

a secure element affixed to the mounting structure, the secure element comprising a data file,

a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire transaction information from the data file by exchanging at least one transaction data communications only between the secure element and the secure element interrogator; and

a communications controller affixed to the mounting structure and configured to receive the data from the secure

element interrogator and to transmit the transaction information to the computer terminal through the communications connector.

53. The token of claim **52** wherein the at least one transaction data communication comprises communications formatted according to ISO 7816-4.

54. The token of claim **52** wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

55. The token of claim **52** wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.

56. The token of claim **52** wherein communications to and from the secure element consist of communications from and to a secure element reader.

57. The token of claim **52** further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

58. The token of claim **52** wherein:

the secure element comprises an executable application; and

the secure element interrogator is configured to interrogate the executable application to acquire the transaction information from the data file.

59. The token of claim **52** wherein:

the secure element comprises a payment card application;

the secure element interrogator is configured to interrogate the payment card application; and

the transaction information comprises card-present data.

60. A token for transmitting a communications data package to a host device, the token comprising:

a mounting structure;

a secure element affixed to the mounting structure, the secure element including a data file containing transaction information;

a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator and to generate the communications data package based on the transaction information; and

a communications controller affixed to the mounting structure and configured to receive the communications data package from the secure element interrogator and to transmit the communications data package to the host device.

61. The token of claim **60** wherein the at least one transaction data communication comprises a plurality of transaction data communications between the secure element and the secure element interrogator, the plurality of transaction data communications being formatted according to ISO 7816-4.

62. The token of claim **60** wherein the secure element comprises an encryption algorithm, an encryption key, and a transaction counter.

63. The token of claim **60** wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element occurs only within libraries or memory space residing on the mounting structure.

64. The token of claim **60** wherein all communications to and from the secure element consist of communications from and to a secure element reader.

65. The token of claim **60** wherein the secure element comprises a microprocessor and the transaction information comprises a dynamic card verification code calculated from an unpredictable number by the microprocessor.

66. The token of claim **60** further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

67. The token of claim **60** wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.

68. The token of claim **60** wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller.

69. The token of claim **60** wherein the host device comprises a cellular network device and the cellular network device comprises the secure element, the interrogator and the communications controller and the host device has the physical form of a mobile phone or a PDA.

70. The token of claim **60** wherein the mounting structure comprises a substrate.

71. The token of claim **60** wherein the mounting structure comprises a packaging case.

72. The token of claim **60** wherein the token has the physical form of a payment card.

73. The token of claim **60** wherein the token has the physical form of a fob.

74. The token of claim **60** wherein the token has the physical form of a cartridge.

75. The token of claim **60** wherein the token has the physical form of a dongle.

76. The token of claim **60** wherein the token has the physical form of a secure digital (SD) chip.

77. The token of claim **60** wherein the host device comprises a cellular network device and the cellular network device is configured to transmit the data communications package over a wireless network.

78. The token of claim **60** wherein:

the secure element comprises a payment card application;

the secure element interrogator is configured to interrogate the payment card application; and

the transaction information comprises card-present data.

79. A cellular network device comprising:

a mounting structure;

a secure element affixed to the mounting structure, the secure element including a data file containing transaction information; and

a secure element interrogator affixed to the mounting structure and configured to interrogate the secure element to acquire the transaction information from the data file by exchanging at least one transaction data communication between the secure element and the secure element interrogator and to generate a communications data package based on the transaction information.

80. The token of claim **79** wherein the at least one transaction data communication comprises a plurality of transaction data communications between the secure element and the secure element interrogator, the plurality of transaction data communications being formatted according to ISO 7816-4.

81. The token of claim **79** wherein the secure element interrogator exchanges the at least one transaction data communication with the secure element only within libraries or memory space residing on the mounting structure.

82. The token of claim **79** wherein all communications to and from the secure element consist of communications from and to a secure element reader.

83. The token of claim **79** wherein the secure element comprises a microprocessor and the transaction information comprises a dynamic card verification code calculated from an unpredictable number by the microprocessor.

84. The token of claim 79 further comprising an antenna that transmits data to and from the secure element, wherein the secure element is interrogated by an external reader.

85. The token of claim 79 wherein the secure element comprises a plurality of payment card applications from different card associations and the secure element interrogator interrogates one of the payment card applications.

86. The cellular network device of claim 79 further comprising a communications controller affixed to the mounting structure and configured for receiving the communications data package for transmission by the cellular network device over a wireless network.

87. The cellular network device of claim 79 wherein:

the secure element comprises a payment card application;

the secure element interrogator is configured to interrogate the payment card application; and

the communications data package comprises card-present data.

* * * * *

EXHIBIT 3

US008766772B2

(12) **United States Patent**
Martinez de Velasco Cortina et al.

(10) **Patent No.: US 8,766,772 B2**
(45) **Date of Patent: Jul. 1, 2014**

(54) **SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS**

(71) Applicants: **Francisco Martinez de Velasco Cortina**, La Jolla, CA (US); **Manfred Rietzler**, Marktoberdorf (DE)

(72) Inventors: **Francisco Martinez de Velasco Cortina**, La Jolla, CA (US); **Manfred Rietzler**, Marktoberdorf (DE)

(73) Assignee: **Neology, Inc.**, Poway, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/022,135**

(22) Filed: **Sep. 9, 2013**

(65) **Prior Publication Data**

US 2014/0022056 A1 Jan. 23, 2014

Related U.S. Application Data

(63) Continuation of application No. 13/350,665, filed on Jan. 13, 2012, now Pat. No. 8,587,436, which is a continuation of application No. 13/175,768, filed on Jul. 1, 2011, now Pat. No. 8,237,568, which is a continuation of application No. 12/688,666, filed on Jan. 15, 2010, now Pat. No. 8,004,410, which is a continuation of application No. 11/279,912, filed on Apr. 17, 2006, now Pat. No. 7,671,746, which is a continuation of application No. 10/615,026, filed on Jul. 9, 2003, now Pat. No. 7,081,819.

(60) Provisional application No. 60/394,241, filed on Jul. 9, 2002.

(51) **Int. Cl.**
G06F 19/10 (2011.01)
G08B 13/14 (2006.01)

(52) **U.S. Cl.**
USPC **340/5.8**; 340/5.82; 340/539.11; 340/572.4

(58) **Field of Classification Search**
CPC G06F 1/00; G06F 19/10; G06B 13/14
USPC 340/539.1, 539.11, 539.13, 568.1, 340/568.7, 572.1, 572.4, 572.8, 5.52, 5.53, 340/5.8, 5.82, 5.83, 5.86; 235/380, 381, 235/382, 494; 194/217; 713/175, 189, 176, 713/186; 705/35, 44, 64
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,529,870 A * 7/1985 Chaum 235/380
5,552,789 A 9/1996 Schuermann

(Continued)

FOREIGN PATENT DOCUMENTS

DE 19608757 A1 9/1997
DE 10042805 A1 3/2002

(Continued)

OTHER PUBLICATIONS

Atmel Corporation, Solution Making Smart Cards Smarter, 2000, 12 pages.

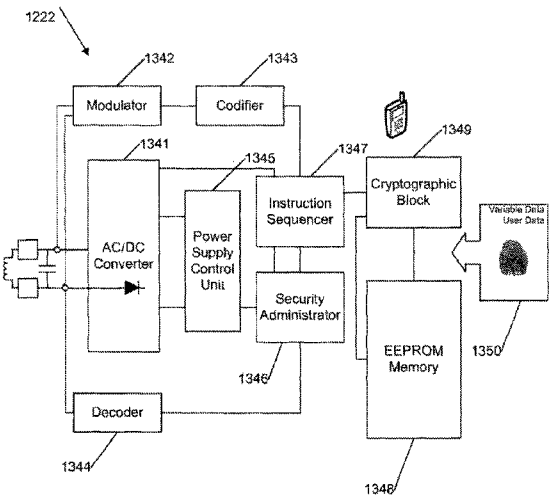
(Continued)

Primary Examiner — Van T. Trieu
(74) *Attorney, Agent, or Firm* — Procopio, Cory, Hargreaves & Savitch LLP; Noel C. Gillespie

(57) **ABSTRACT**

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

18 Claims, 24 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

5,657,008	A	8/1997	Bantli	
5,742,618	A	4/1998	Lowe	
5,787,174	A	7/1998	Tuttle	
5,864,580	A	1/1999	Lowe et al.	
5,874,896	A	2/1999	Small et al.	
5,974,500	A	10/1999	Maletsky et al.	
6,025,780	A	2/2000	Bowers et al.	
6,025,784	A	2/2000	Mish	
6,052,068	A	4/2000	Price et al.	
6,073,840	A	6/2000	Marion et al.	
6,098,879	A	8/2000	Terranova et al.	
6,104,281	A	8/2000	Heinrich et al.	
6,111,506	A	8/2000	Yap et al.	
6,140,941	A	10/2000	Dwyer et al.	
6,157,333	A	12/2000	Louagie et al.	
6,167,333	A	12/2000	Gehlot et al.	
6,175,922	B1	1/2001	Wang	
6,182,894	B1 *	2/2001	Hackett et al.	235/380
6,203,952	B1	3/2001	O'Brien et al.	
6,211,790	B1	4/2001	Radomsky et al.	
6,268,796	B1	7/2001	Gnadinger et al.	
6,269,292	B1	7/2001	Kokubu et al.	
6,275,157	B1	8/2001	Mays et al.	
6,276,607	B1	8/2001	Sato	
6,334,059	B1	12/2001	Stilp et al.	
6,340,116	B1	1/2002	Cecil et al.	
6,360,208	B1	3/2002	Ohanian et al.	
6,388,579	B1	5/2002	Adcox et al.	
6,427,504	B1	8/2002	Janssen et al.	
6,570,487	B1	5/2003	Steeves	
6,617,961	B1	9/2003	Janssen et al.	
6,698,653	B1	3/2004	Diamond et al.	
6,753,759	B2	6/2004	Stegmaier et al.	
6,758,405	B2	7/2004	Look	
6,793,134	B2 *	9/2004	Clark	235/379
6,850,147	B2 *	2/2005	Prokoski et al.	340/5.53
6,894,615	B2	5/2005	Look	
6,950,013	B2	9/2005	Scaman et al.	
6,975,834	B1	12/2005	Forster	
7,031,946	B1	4/2006	Tamai et al.	
7,080,819	B2	7/2006	Tojo	
7,225,337	B2 *	5/2007	Baessler	713/175
7,310,734	B2 *	12/2007	Boate et al.	713/186
7,487,538	B2	2/2009	Mok	
7,533,809	B1	5/2009	Robinson et al.	
7,671,746	B2 *	3/2010	Martinez de Velasco Cortina et al.	340/572.4
7,844,505	B1	11/2010	Arneson et al.	
7,980,378	B2 *	7/2011	Jones et al.	194/217
8,004,410	B2 *	8/2011	Martinez De Velasco Cortina et al.	340/572.4
8,041,815	B2	10/2011	Bahl et al.	
8,126,449	B2 *	2/2012	Beenau et al.	455/419
8,401,539	B2 *	3/2013	Beenau et al.	455/419
2002/0089434	A1	7/2002	Ghazarian	
2002/0109580	A1 *	8/2002	Shreve et al.	340/5.61
2003/0074317	A1 *	4/2003	Hofi	705/44
2003/0200227	A1	10/2003	Ressler	
2005/0149764	A1	7/2005	Bahl et al.	
2010/0094754	A1 *	4/2010	Bertran et al.	705/44
2010/0095130	A1 *	4/2010	Bertran et al.	713/189

FOREIGN PATENT DOCUMENTS

EP	977145	A2	2/2000
EP	993999	A2	4/2000
JP	2002042076	A	2/2002
WO	9843104	A2	10/1998
WO	2004006165	A1	1/2004

OTHER PUBLICATIONS

Extended European Search Report issued by the European Patent Office in related European Application No. 10182033.0 dated Jan. 13, 2012 (7 pages).

Fancher, Carol Hovenga, In Your Pocket Smartcards, IEEE Spectrum, Feb. 2007, 7 pages.

Rakers, Patrick, et al., Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal of Solid-State Circuits, vol. 36, No. 3, Mar. 2001, 7 pages.

Official Action in Japanese Patent Application No. 2004-519130 dated May 12, 2009, 10 pages.

Anonymous, Read Write RFID Offers Standalone Advantages, Security, Aug. 1996, 1 page.

21 C.C.R. §1700.

21 C.C.R. § 1701(r).

21 C.C.R. § 1702.1.

21 C.C.R. § 1703(c).

21 C.C.R. § 1703(e-i).

21 C.C.R. § 1704.1.

21 C.C.R. § 17042.

21 C.C.R. § 1704.3.

21 C.C.R. § 1704.5(e)(1).

21 C.C.R. § 1704.6.

21 C.C.R. § 1705.1.

21 C.C.R. § 1705.2.

21 C.C.R. § 1705.3.

21 C.C.R. § 1705.4.

21 C.C.R. § 1705.5.

21 C.C.R. § 1705.5(d) and (e)(1).

21 C.C.R. 1705.8.

* cited by examiner

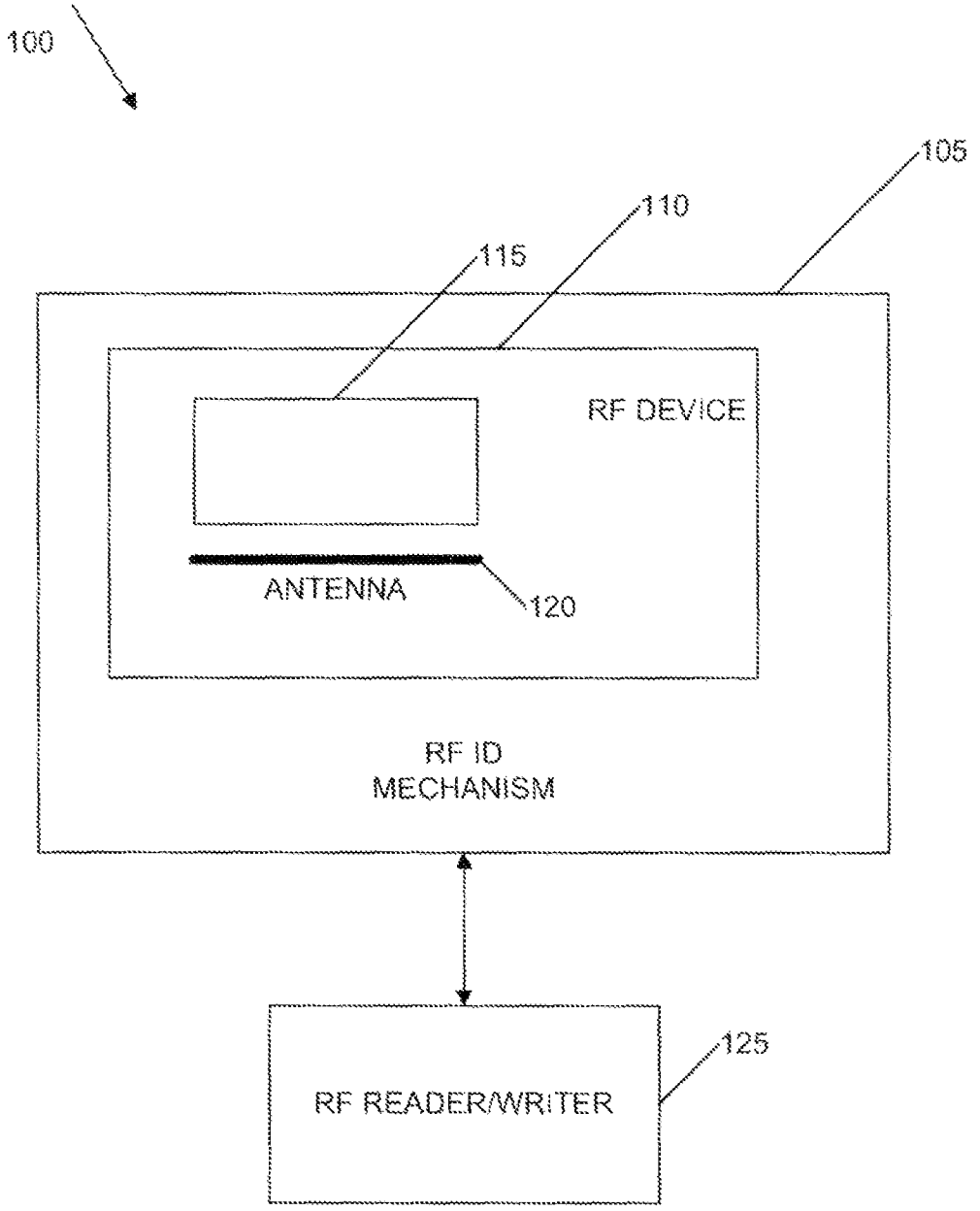

100
105
110
115
RF DEVICE
ANTENNA
120
RF ID
MECHANISM
125
RF READER/WRITER

FIG. 1

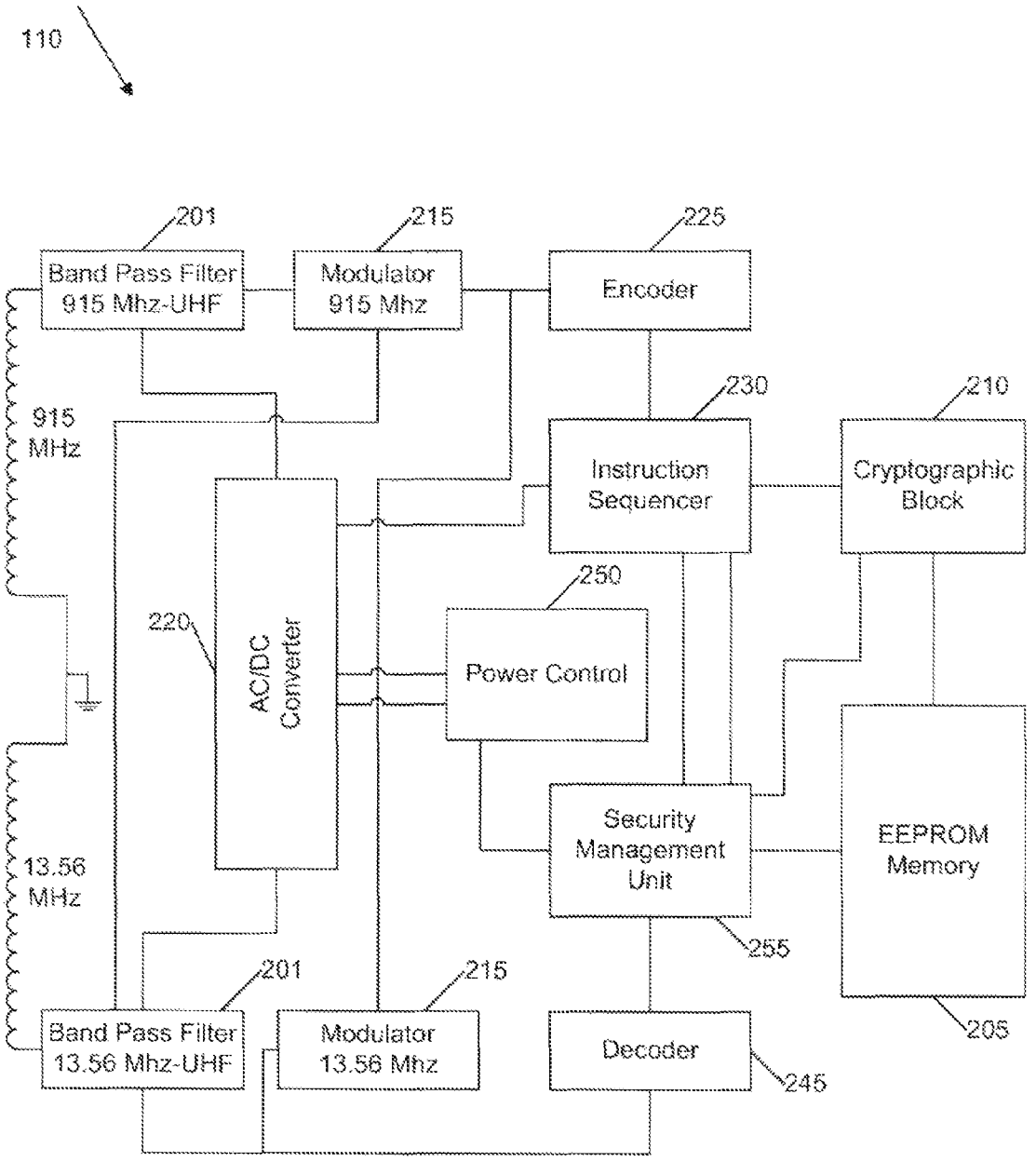

110
201
Band Pass Filter
915 Mhz-UHF
215
Modulator
915 Mhz
225
Encoder
915
MHz
230
Instruction
Sequencer
210
Cryptographic
Block
250
220
AC/DC
Converter
Power Control
Security
Management
Unit
EEPROM
Memory
13.56
MHz
255
201
215
Band Pass Filter
13.56 Mhz-UHF
Modulator
13.56 Mhz
Decoder
205
245

FIG. 2

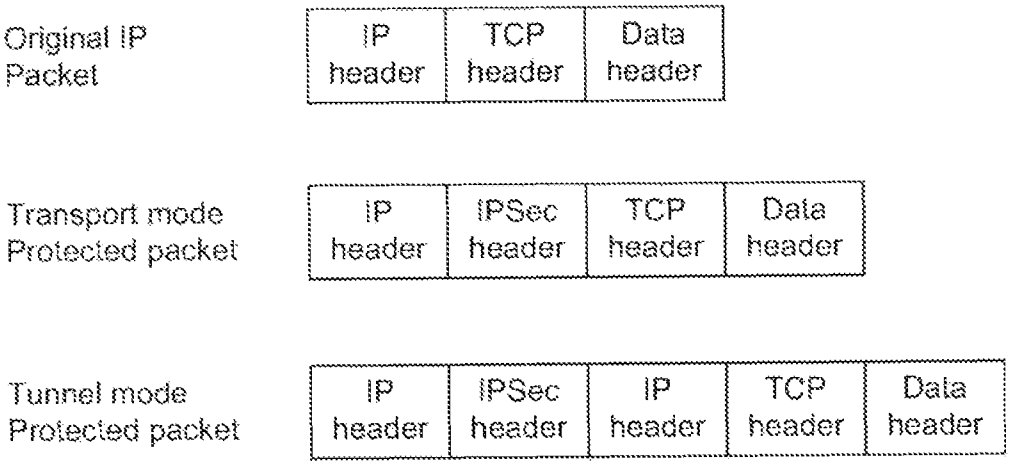

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIG. 3A

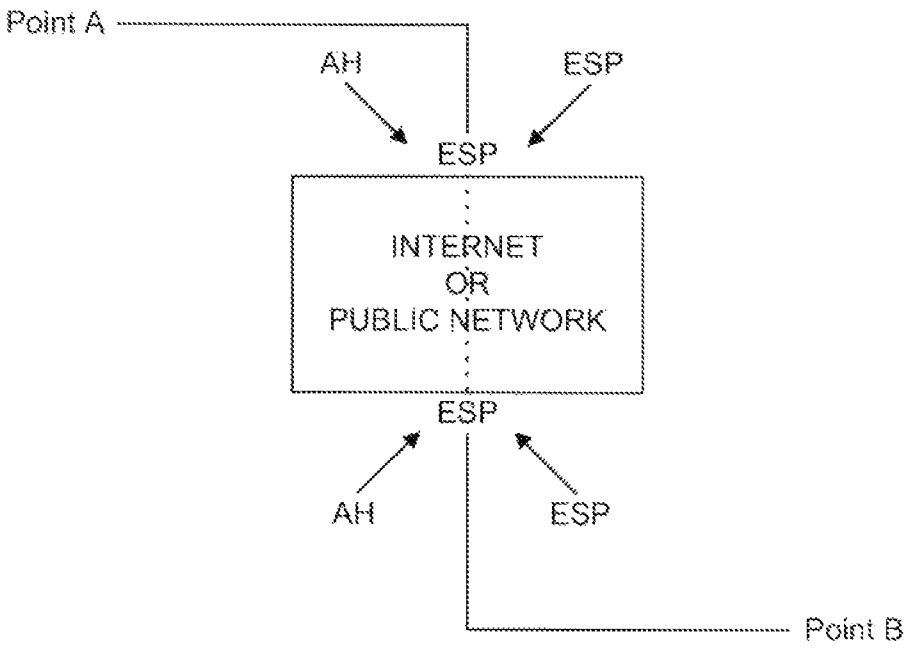

Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORK
ESP
AH
ESP
Point B

FIG. 3B

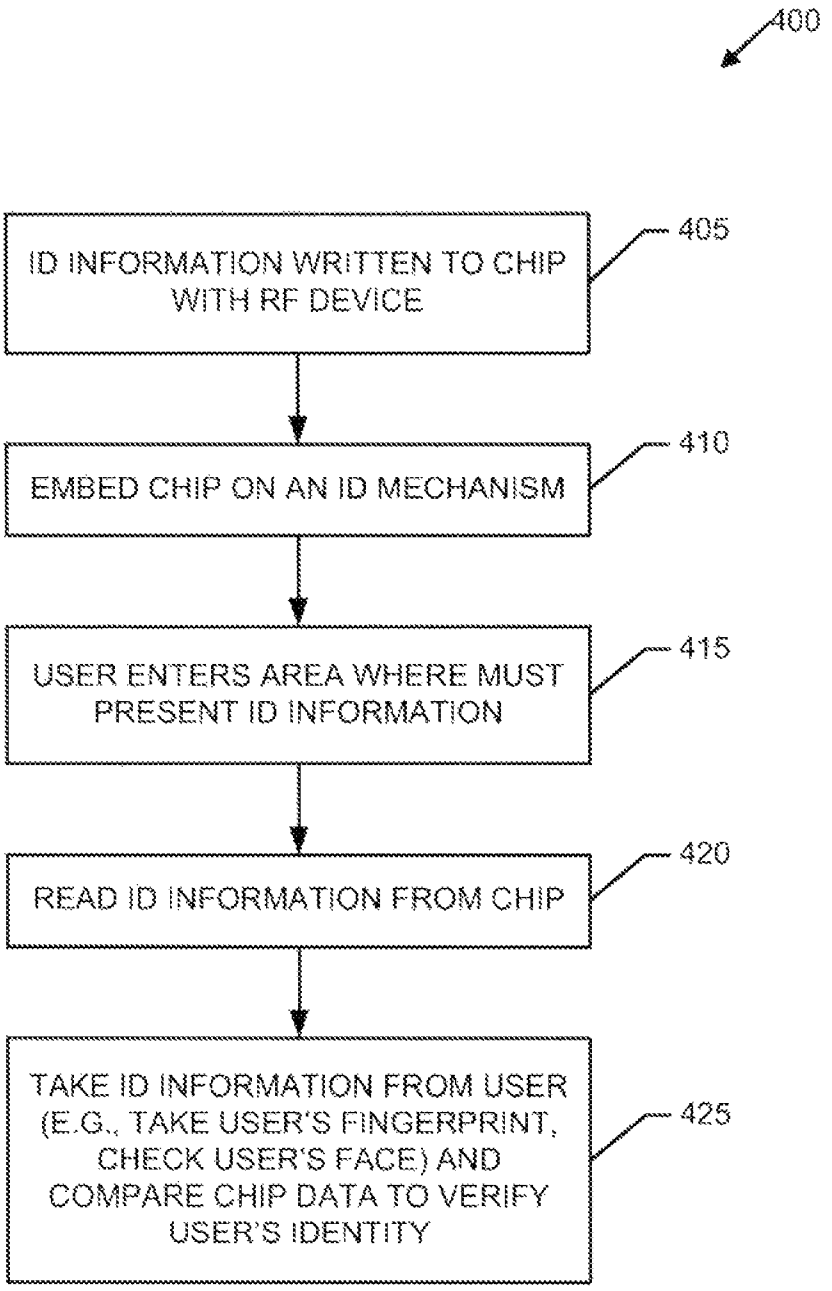

400
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
405
EMBED CHIP ON AN ID MECHANISM
410
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
415
READ ID INFORMATION FROM CHIP
420
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE CHIP DATA TO VERIFY USER'S IDENTITY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

FIG. 4

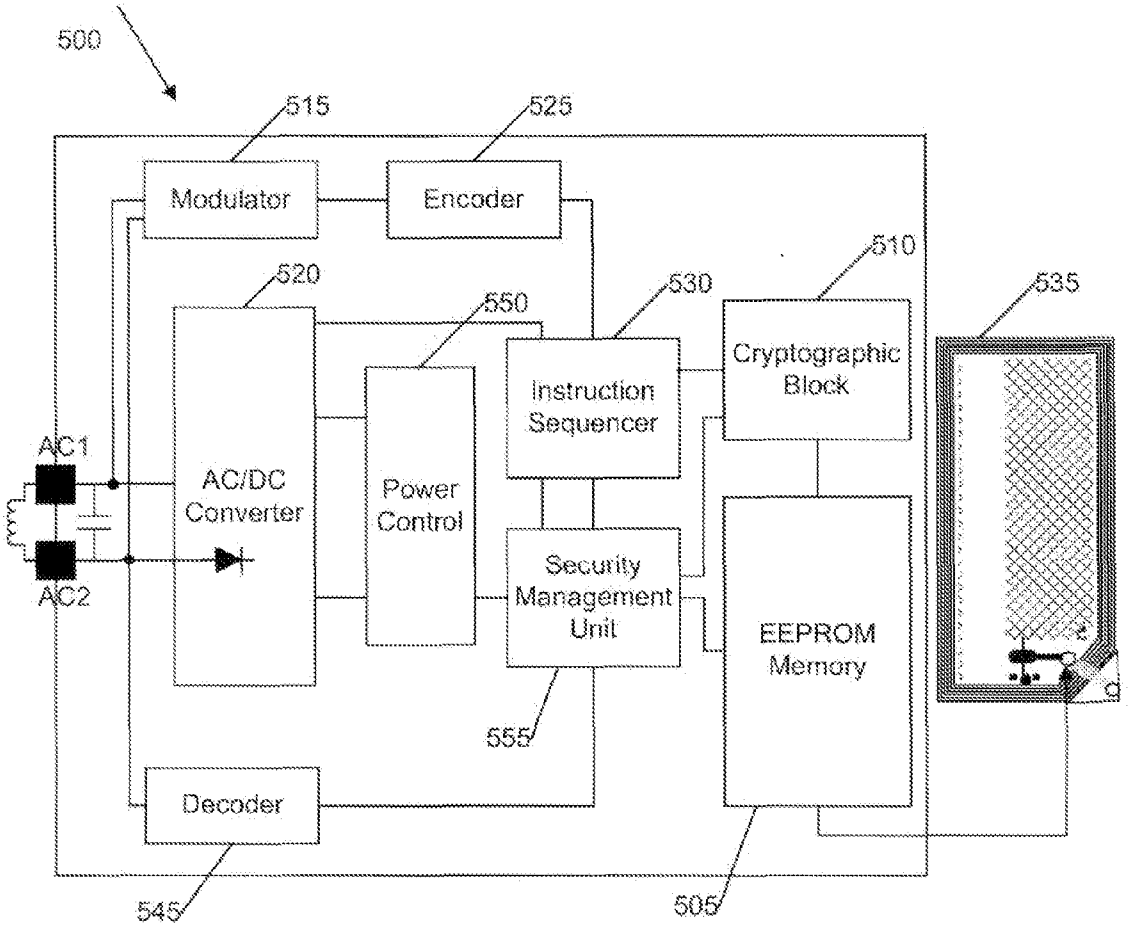

500
515
525
Modulator
Encoder
510
520
550
530
535
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
555
Decoder
545
505

FIG. 5

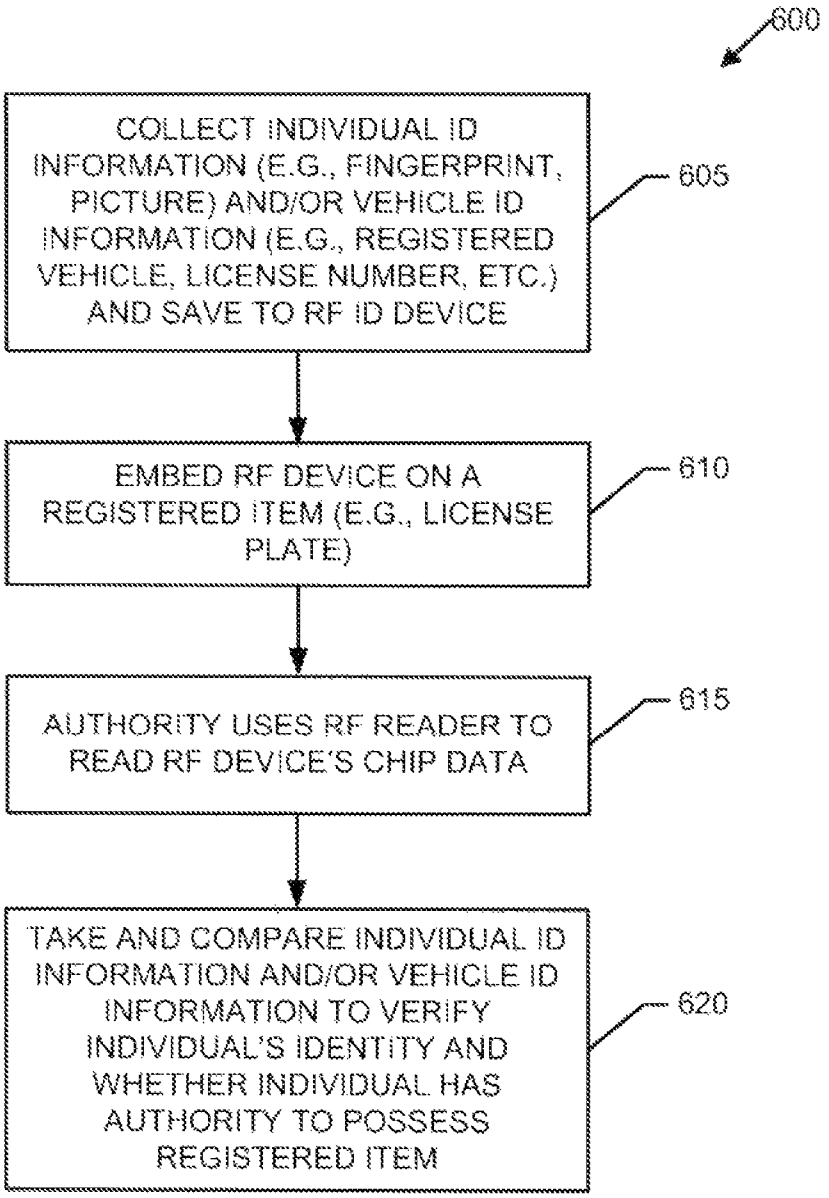

600
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
605
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
610
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
615
TAKE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

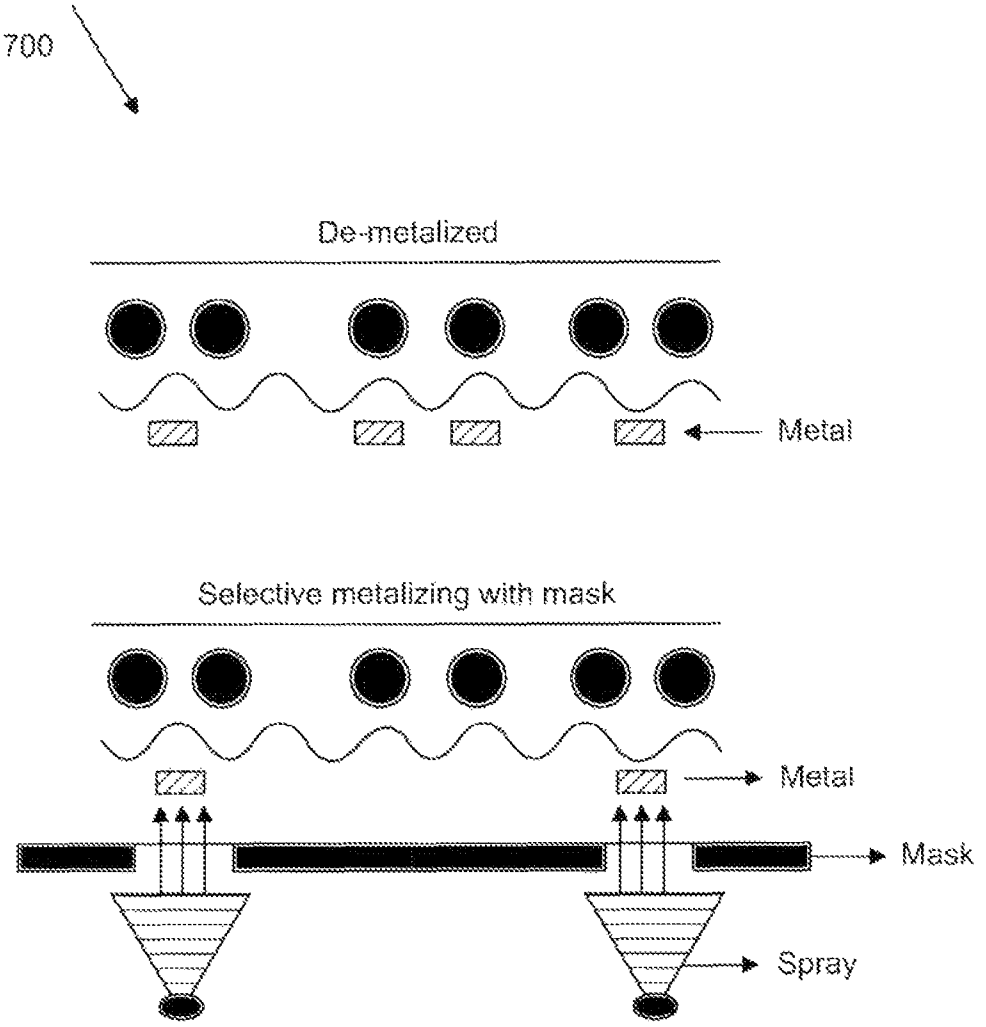

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIG. 7

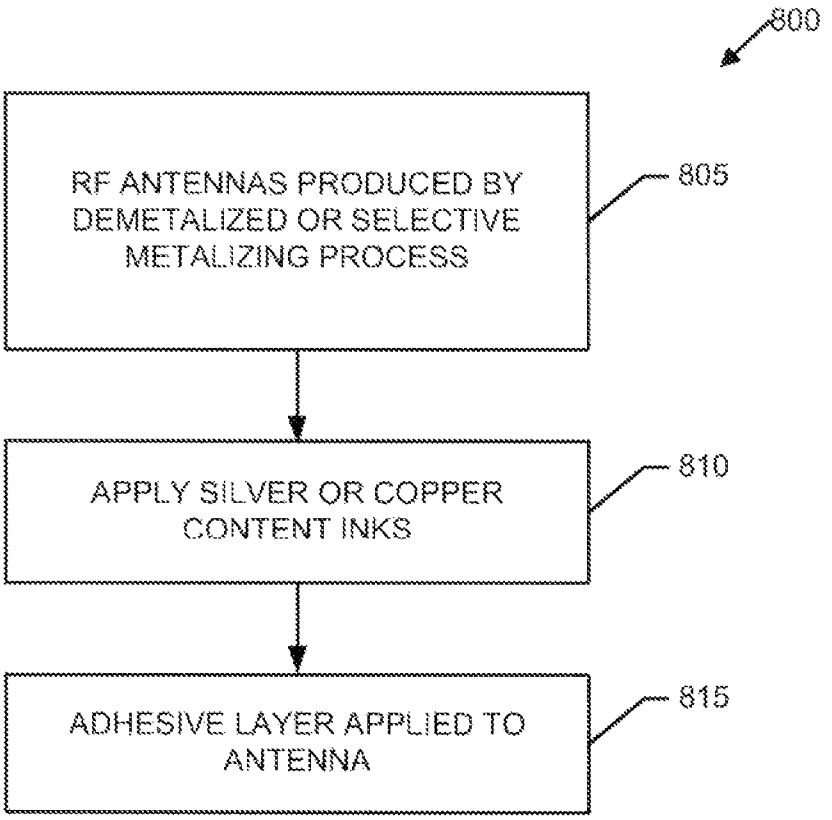

800
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
805
APPLY SILVER OR COPPER CONTENT INKS
810
ADHESIVE LAYER APPLIED TO ANTENNA
815

FIG. 8

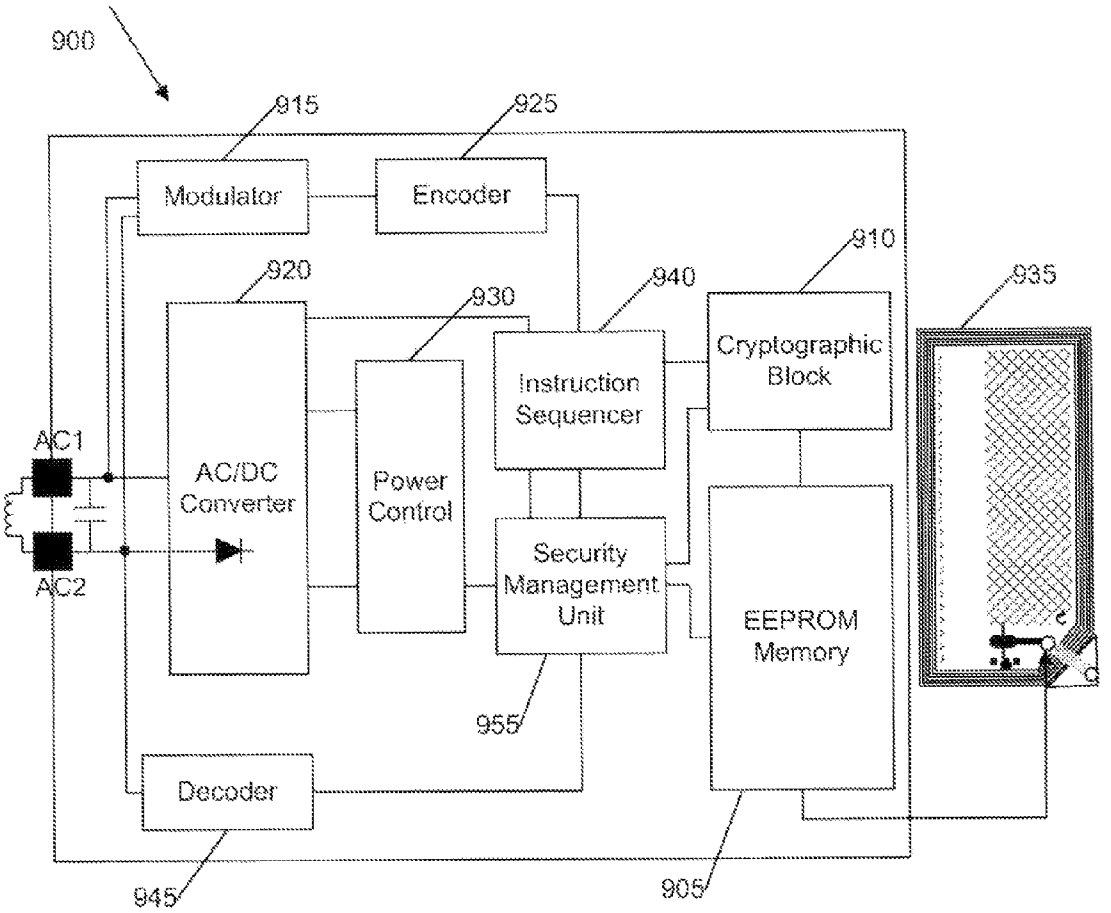

900
915
925
Modulator
Encoder
910
920
930
940
935
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
955
Decoder
945
905

FIG. 9

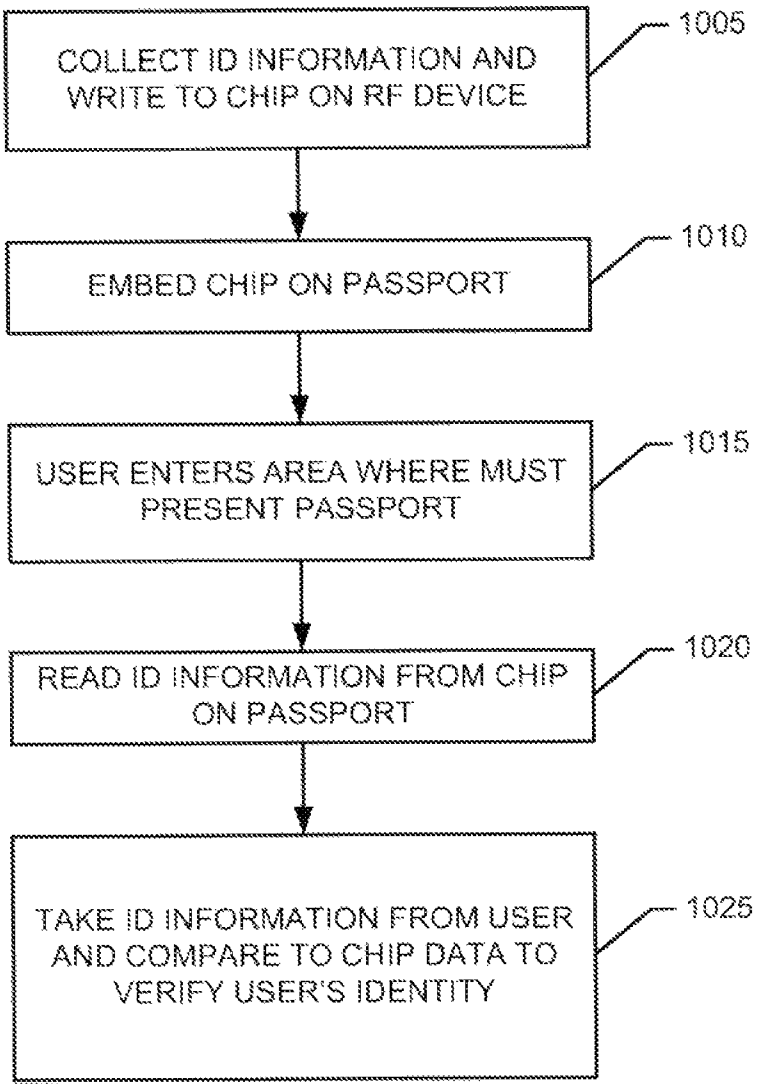

COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1005
EMBED CHIP ON PASSPORT
1010
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1015
READ ID INFORMATION FROM CHIP ON PASSPORT
1020
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY
1025

FIG. 10

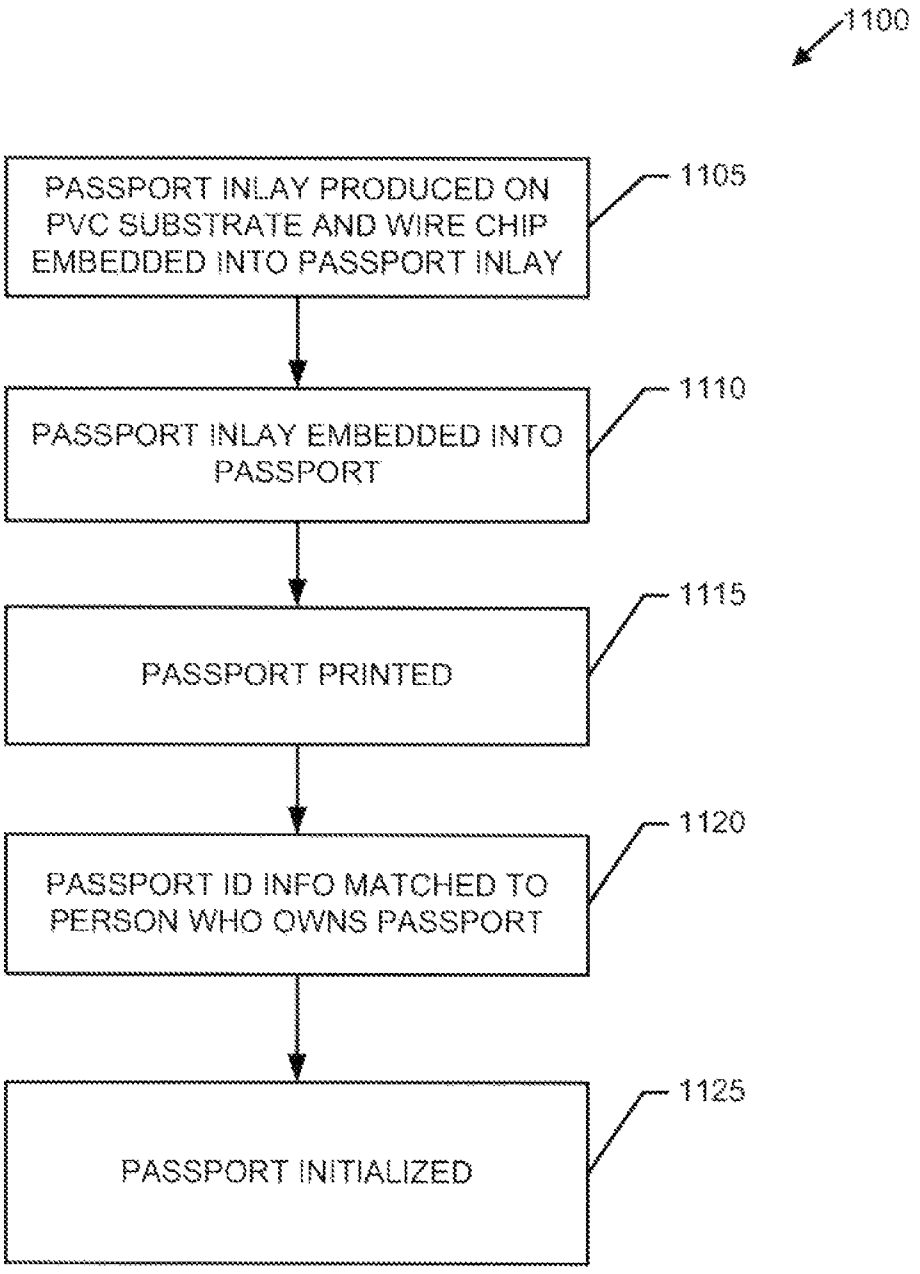

1100
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1105
PASSPORT INLAY EMBEDDED INTO PASSPORT
1110
PASSPORT PRINTED
1115
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1120
PASSPORT INITIALIZED
1125

FIG. 11

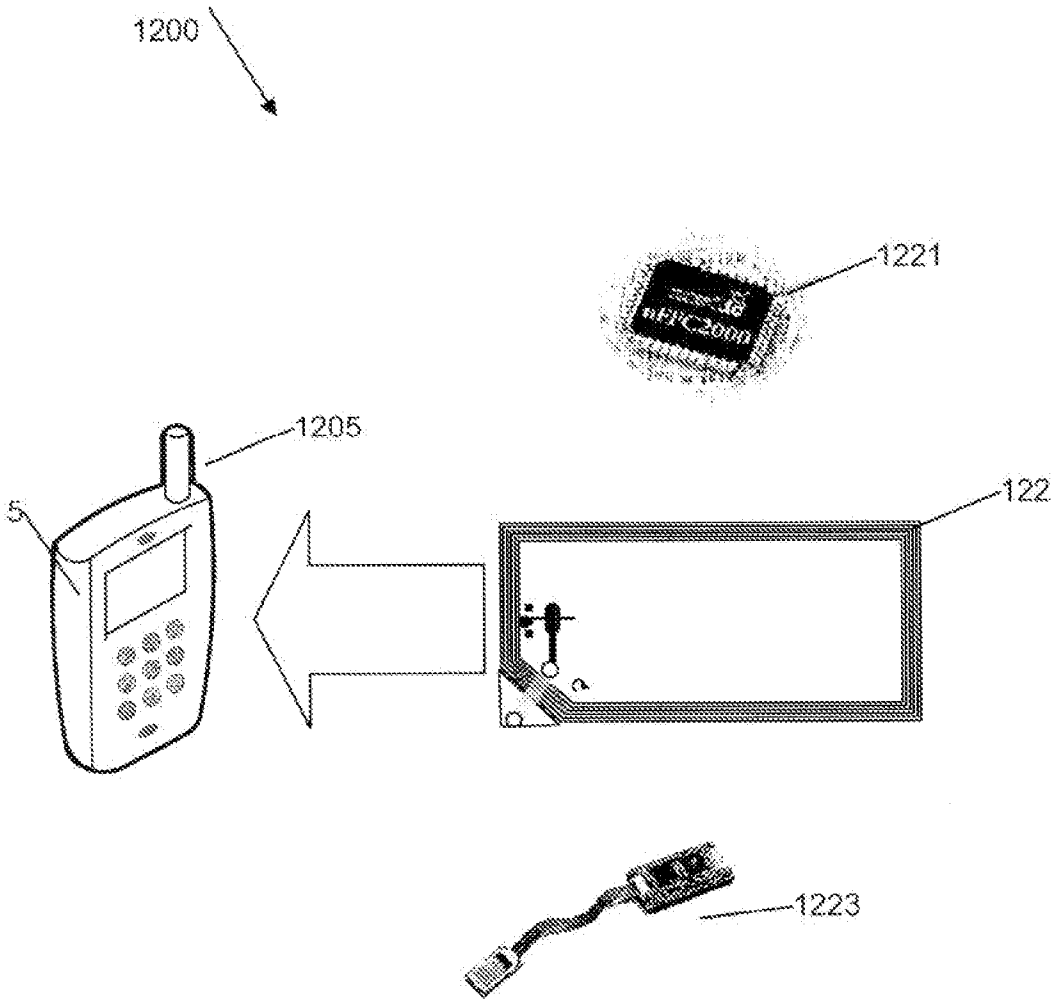


FIG. 12

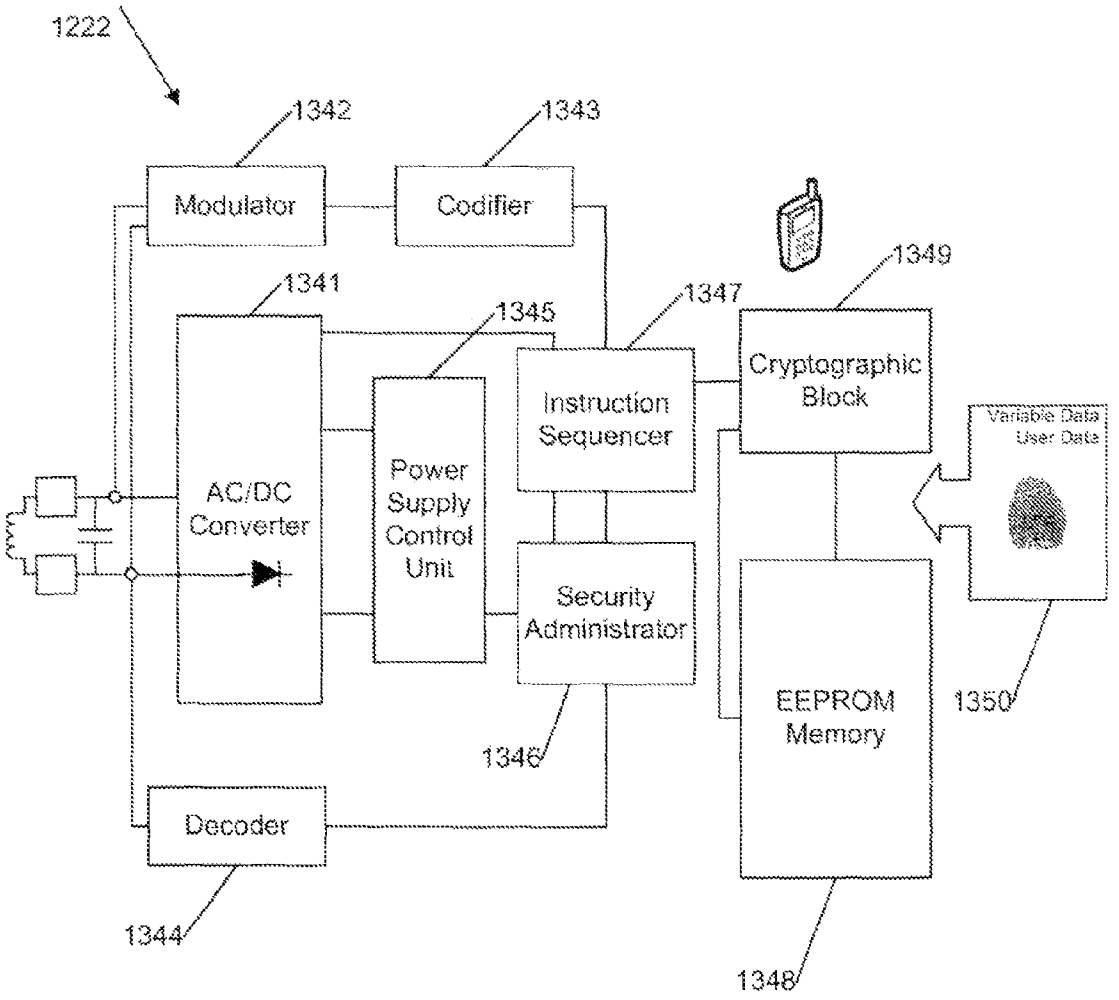

1222
1342
1343
Modulator
Codifier
1349
1341
1345
1347
Cryptographic Block
Instruction Sequencer
Variable Data
User Data
AC/DC Converter
Power Supply Control Unit
Security Administrator
EEPROM Memory
1350
1346
Decoder
1344
1348

FIG. 13

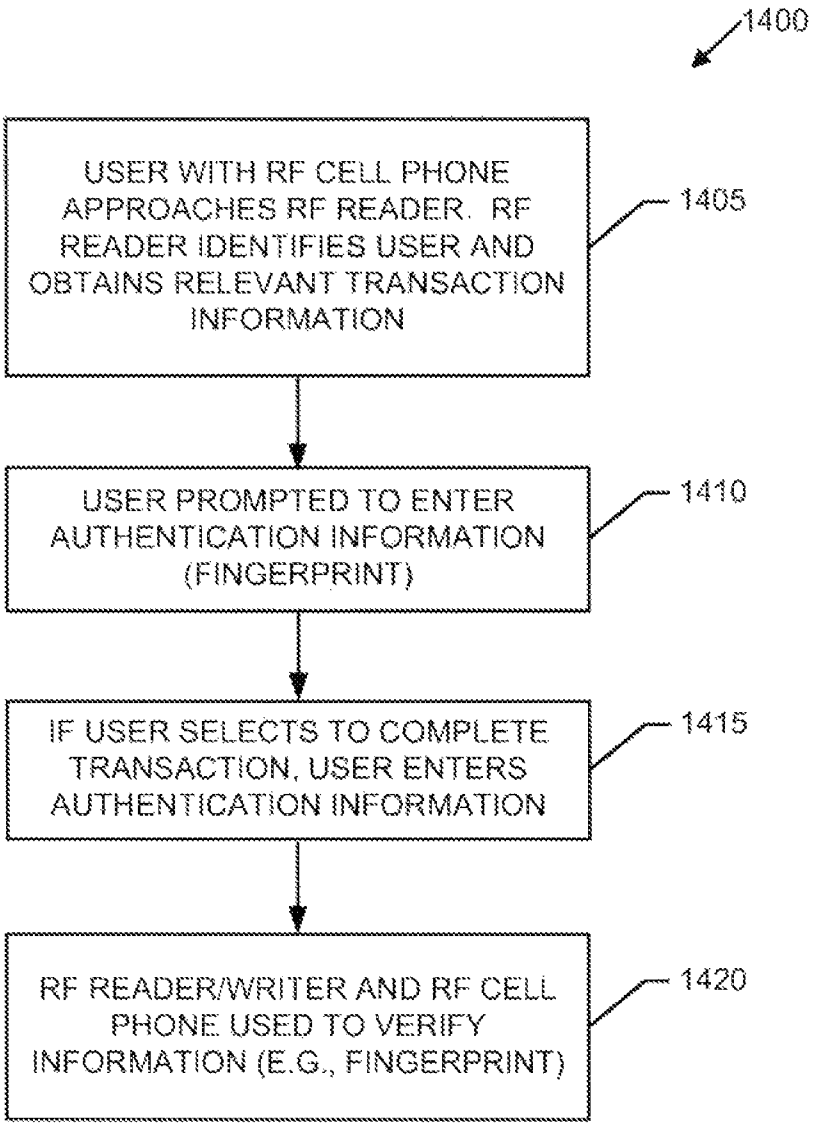

1400
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION
1405
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT)
1410
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION
1415
RF READER/WRITER AND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

FIG. 14

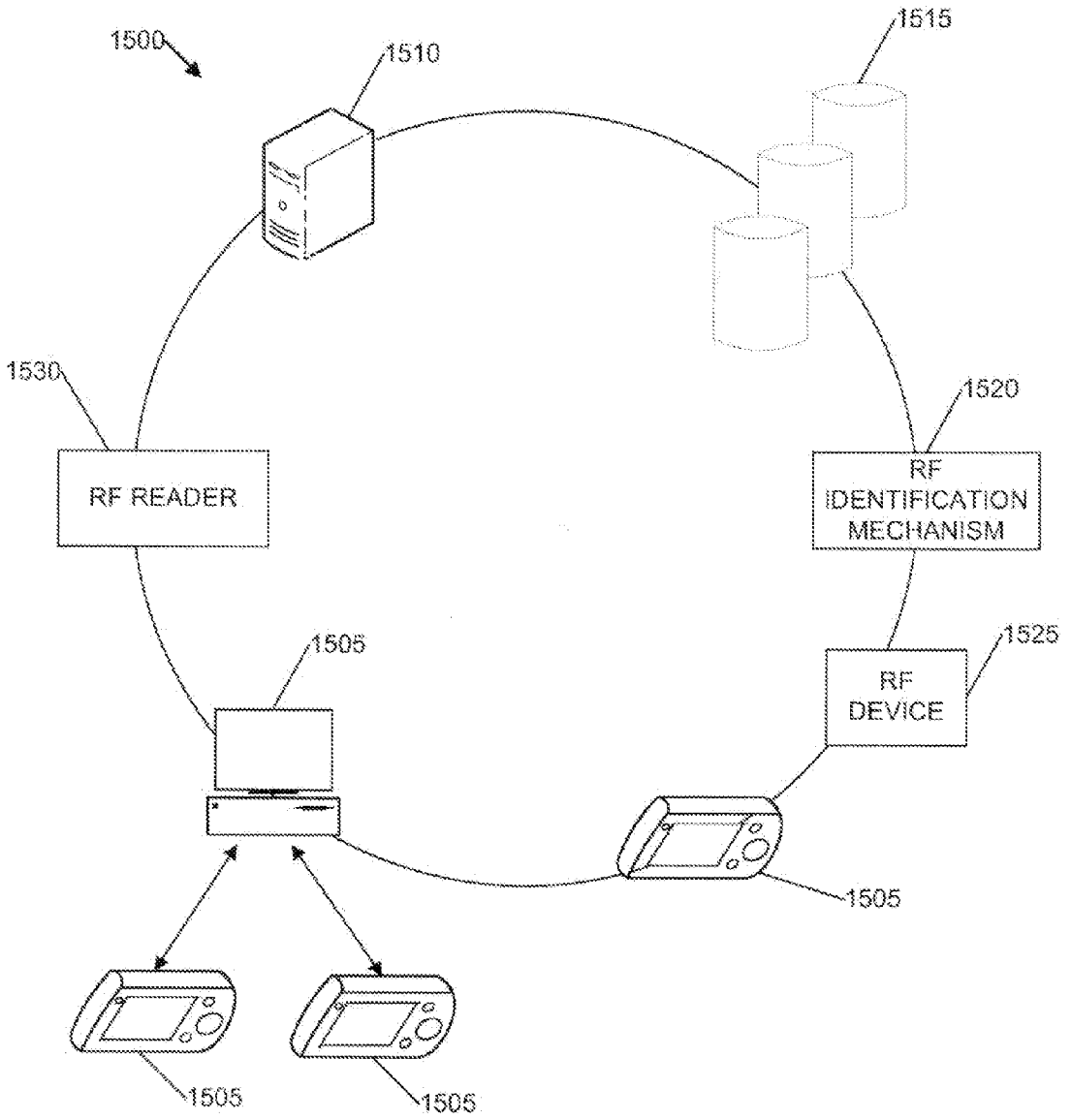

1500
1510
1515
1530
1520
RF READER
RF IDENTIFICATION MECHANISM
1505
1525
RF DEVICE
1505
1505
1505

FIG. 15

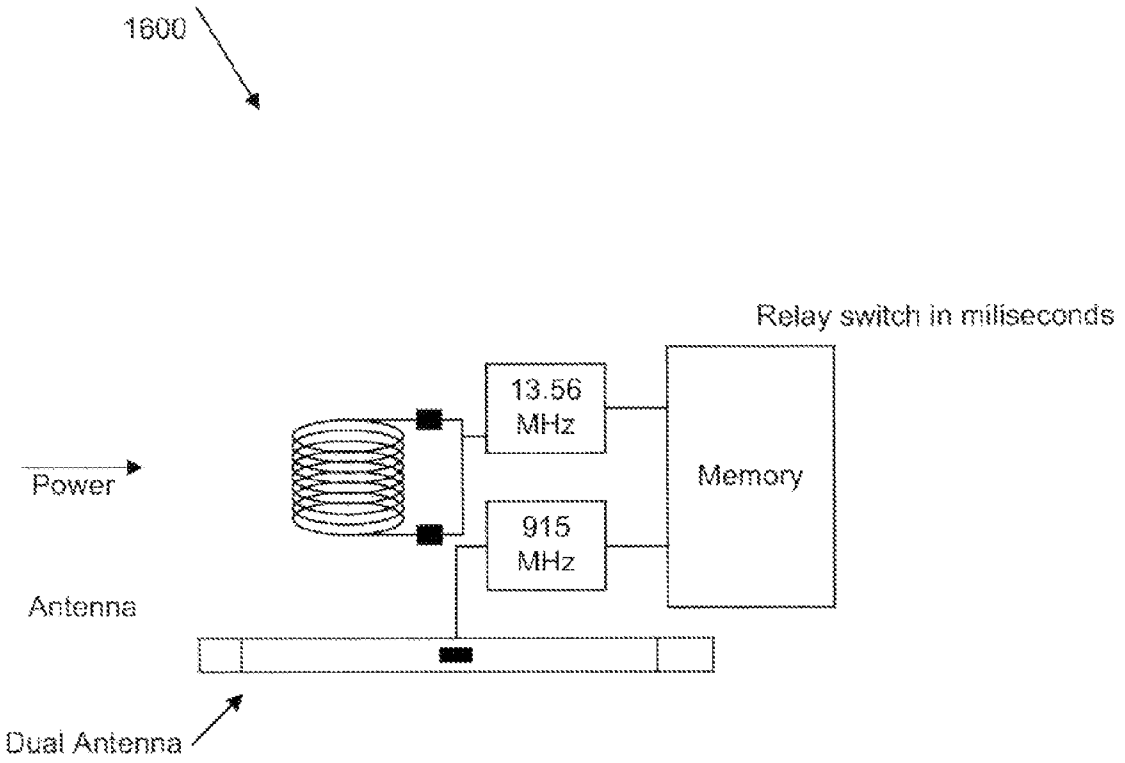

1600
Relay switch in miliseconds
13.56 MHz
915 MHz
Memory
Power
Antenna
Dual Antenna

FIG. 16

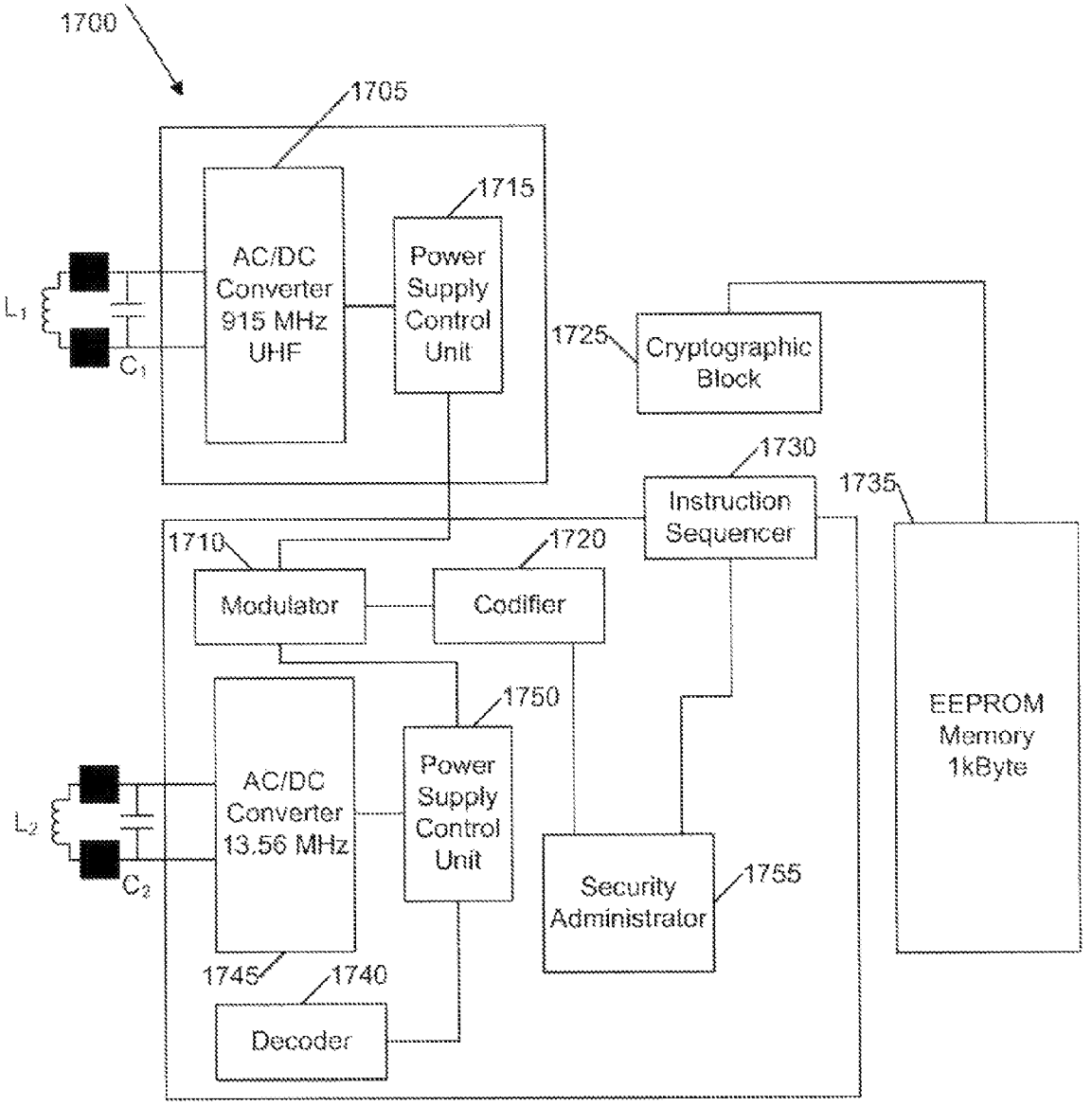

1700
1705
1715
AC/DC Converter 915 MHz UHF
Power Supply Control Unit
L1
C1
1725
Cryptographic Block
1730
1735
Instruction Sequencer
1710
1720
Modulator
Codifier
EEPROM Memory 1kByte
1750
AC/DC Converter 13.56 MHz
Power Supply Control Unit
L2
C2
Security Administrator
1755
1745
1740
Decoder

FIG. 17

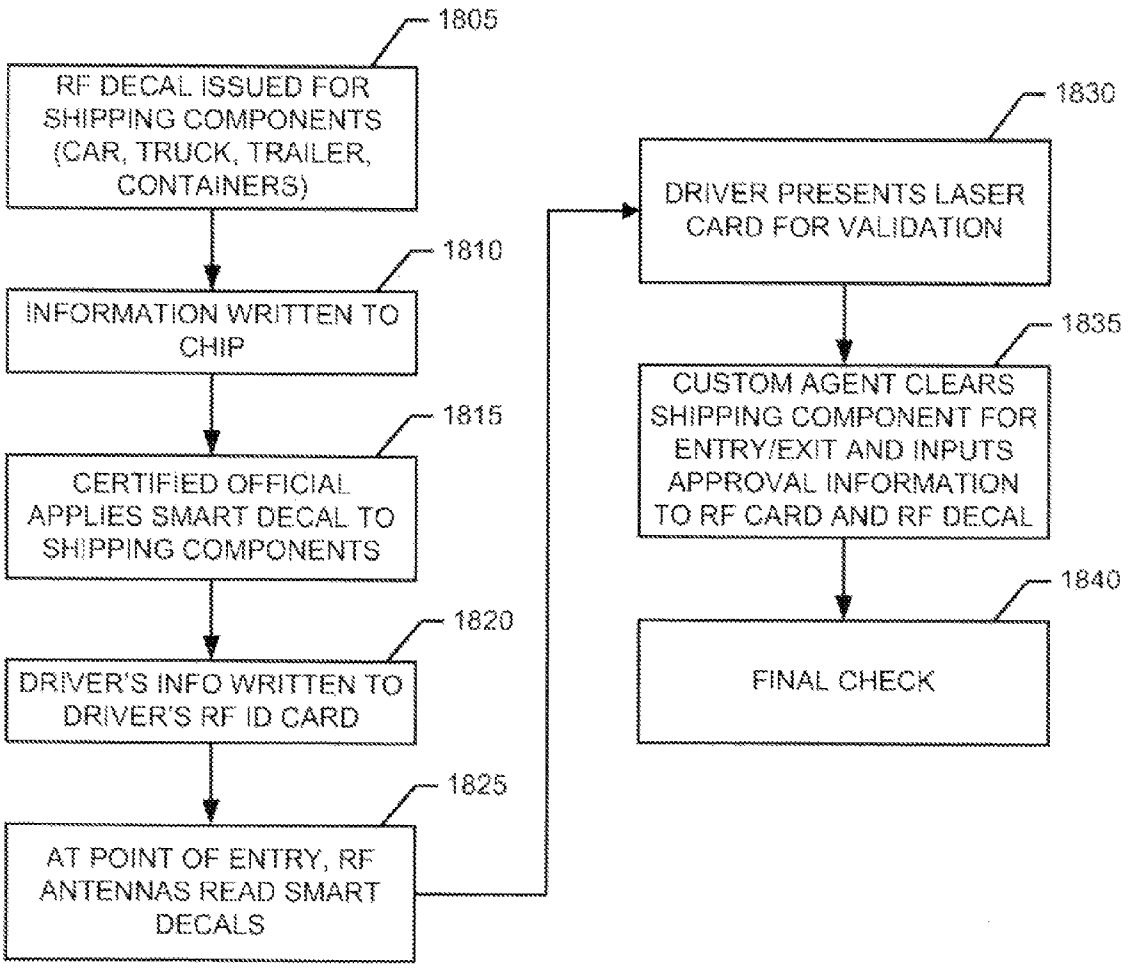

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS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

FIG. 18

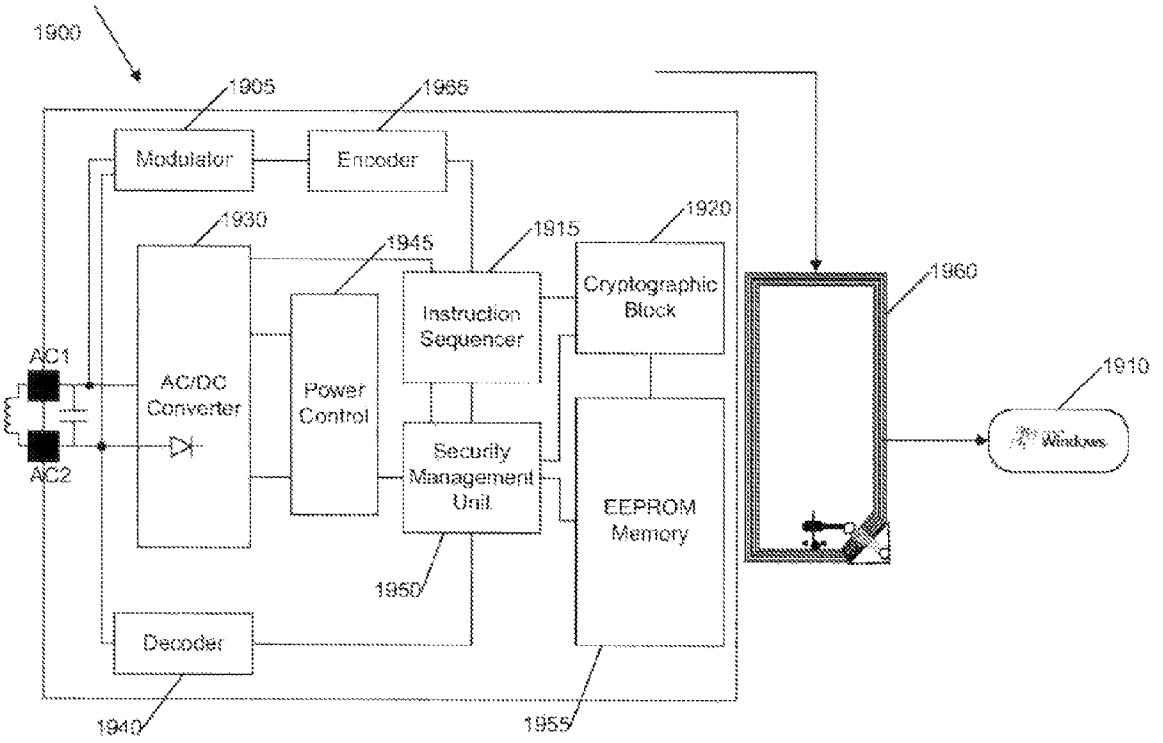

1900
1905
1965
Modulator
Encoder
1930
1945
1915
1920
Cryptographic Block
1960
Instruction Sequencer
AC1
AC/DC Converter
Power Control
1910
Windows
AC2
Security Management Unit
EEPROM Memory
1950
Decoder
1940
1955

FIG. 19

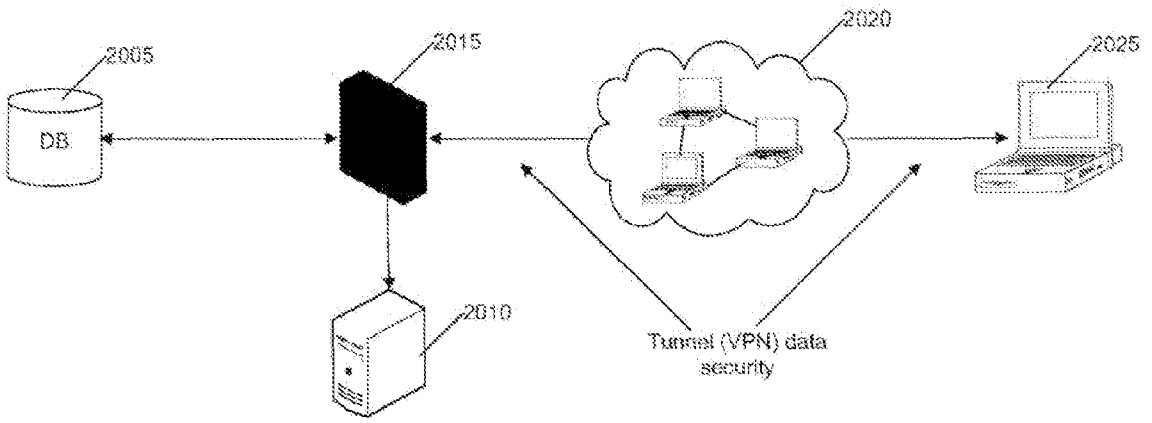


FIG. 20

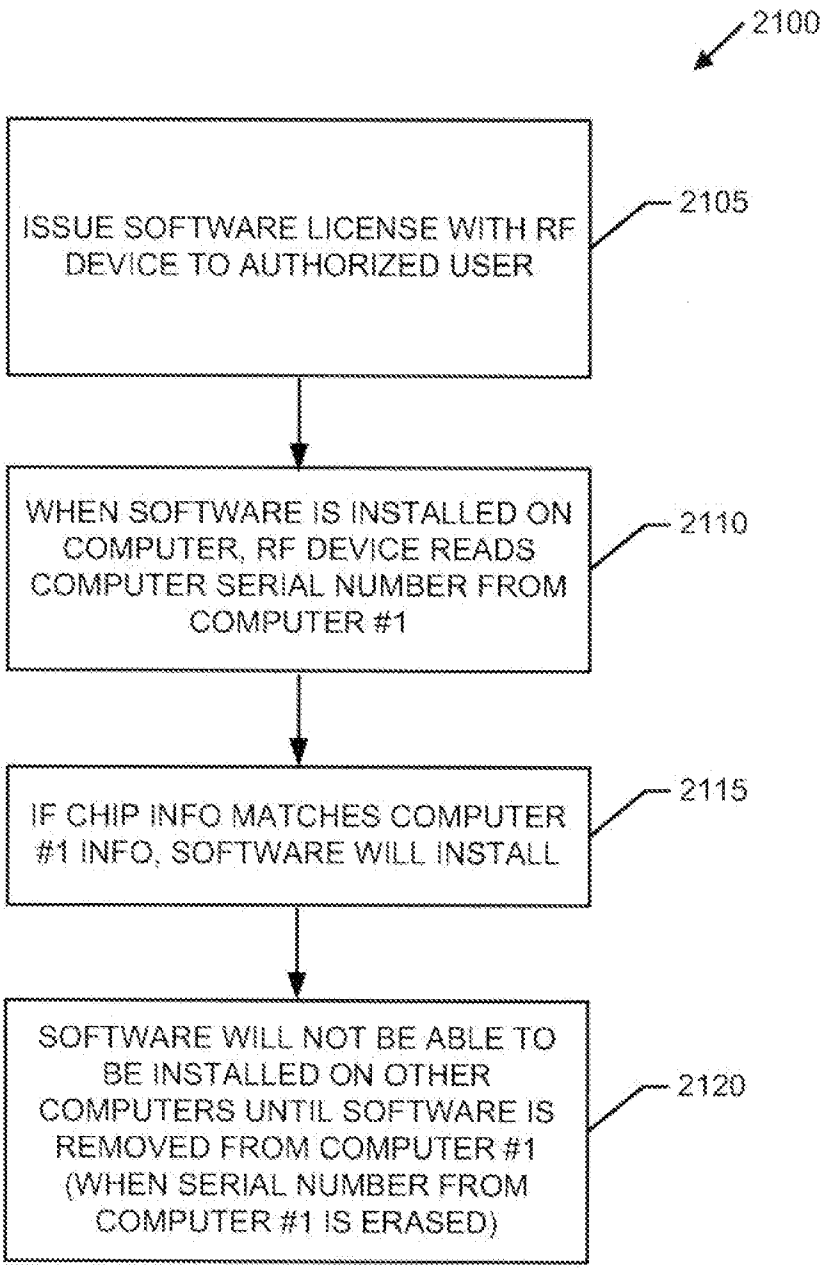

2100
ISSUE SOFTWARE LICENSE WITH RF DEVICE TO AUTHORIZED USER
2105
WHEN SOFTWARE IS INSTALLED ON COMPUTER, RF DEVICE READS COMPUTER SERIAL NUMBER FROM COMPUTER #1
2110
IF CHIP INFO MATCHES COMPUTER #1 INFO, SOFTWARE WILL INSTALL
2115
SOFTWARE WILL NOT BE ABLE TO BE INSTALLED ON OTHER COMPUTERS UNTIL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

FIG. 21

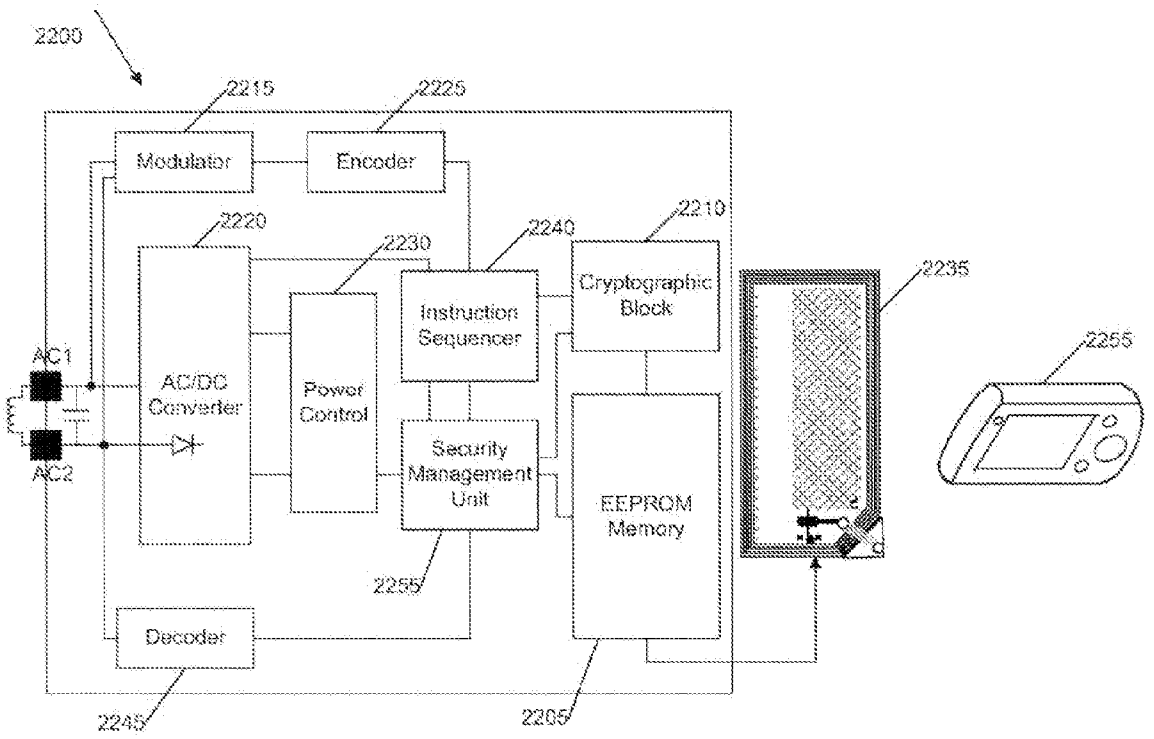

2200
2215
2225
Modulator
Encoder
2220
2230
2240
2210
Instruction Sequencer
Cryptographic Block
2235
2255
AC1
AC2
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
2255
Decoder
2245
2205

FIG. 22

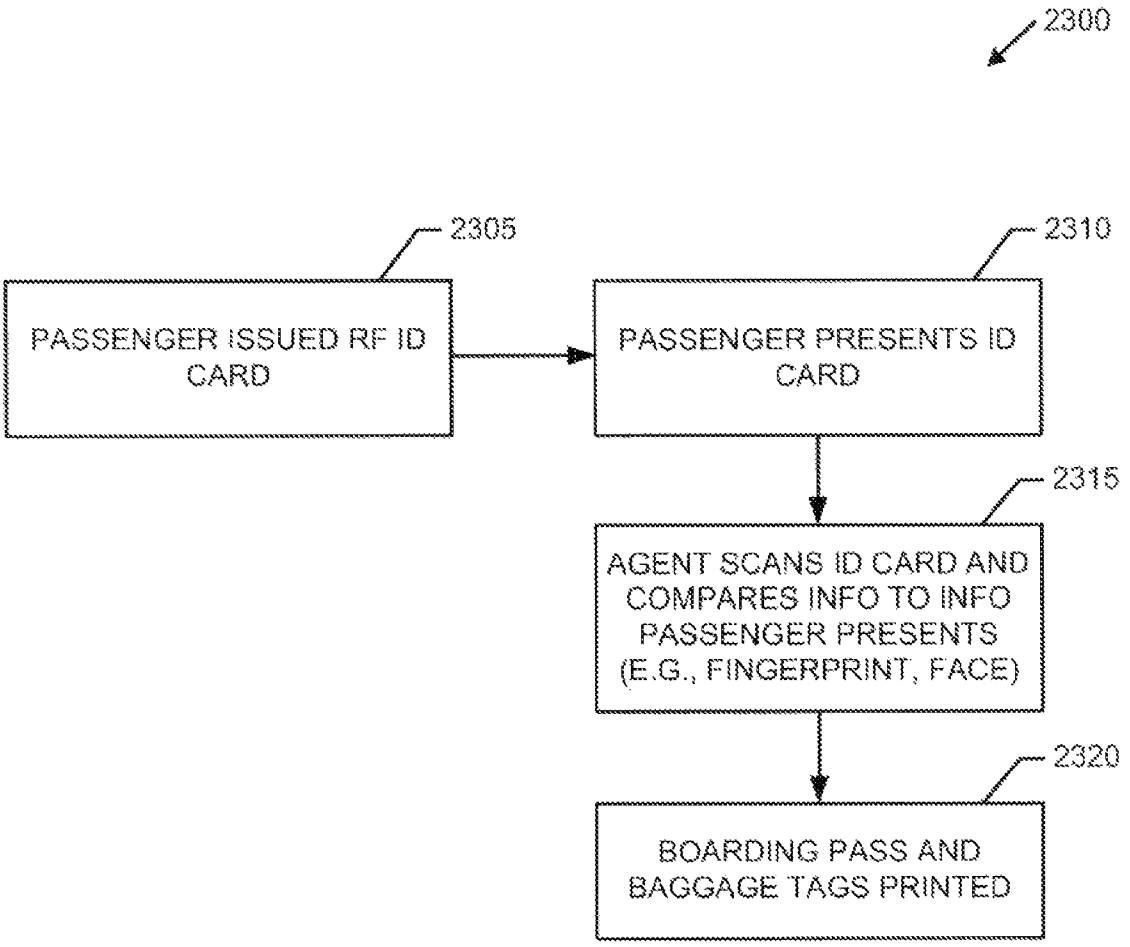

2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENT SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

FIG. 23

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

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

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

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

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

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

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

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

FIGS. **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

FIG. **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

FIG. **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.

FIG. **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.

A more detailed description of an RF device can be found in U.S. patent application Ser. No. 10/118,092 filed 9 Apr. 2002; PCT Patent Application PCT/IB02/01439, filed 30 Apr. 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 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.

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.

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.

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 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.

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 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.

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 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.

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

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

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 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.

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.

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 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.

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

FIG. **4** illustrates the methods 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

FIG. **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

FIG. **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.

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 FIG. **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 material, holographic foil, or another substrate with a high metal content.

FIG. **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) 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

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

FIG. **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

FIG. **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

FIG. **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 I**11 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

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 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.

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 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.

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

FIG. **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 ensures 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 FIG. **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.

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

FIG. **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 FIG. **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 **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.

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 Ser. No. 10/118,092, filed Apr. 2, 2002, and PCT Patent Application IB0201439, filed Apr. 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

FIG. **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 24×7; 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 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.

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 (PIPS) 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 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.

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 FIG. **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=capaticance (F)

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

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

N=number of windings around inductor
μ_o=permeability of freespace (Hm^{-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:

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

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

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

For substitution, the following values are used:

$$L_1 = 2.931\times10^{8} H$$

$$L_2 = 6.437\times10^{10} H$$

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

Multiple RF Chip Overview

FIG. **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

FIG. **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 demetalizing 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

FIG. **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.

FIG. **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.

FIG. **3**A illustrates the differences between transport mode and tunnel mode. The use of AH and ESP are illustrated in FIG. **38**.

B. Method of Limiting Software Downloads

FIG. **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 num-

ber 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

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

B. Method of Airport Security

FIG. **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:

1. A mobile device, comprising:
a biometric input device configured to receive biometric data; and
a radio frequency antenna and a chip, the chip comprising:
a memory, the memory configured to store a security key, transaction information, and biometric information for identifying an individual associated with the transaction, and
a processor coupled with the memory and the biometric input, the processor configured to provide access to the memory based on a security key, the processor further configured to:
receive a signal via the radio frequency antenna, the signal comprising a request to access the memory and a security key,
compare the security key included in the received access request with the security key stored in the memory, and
provide the transaction information in response to the access request when the security keys match.

2. The mobile device of claim 1, wherein the processor is further configured to receive biometric information from the biometric input device, compare the received biometric information with the biometric information stored in the memory.

3. The mobile device of claim 2, wherein the processor is further configured to provide the transaction information in response to the access request when the biometric information matches.

4. The mobile device of claim 1, wherein the mobile device is cellular device.

5. The mobile device of claim 1, wherein the biometric input device is a fingerprint scanner.

6. The mobile device of claim 1, wherein the processor is further configured to provide the received biometric information or the stored biometric information with the transaction information.

7. The mobile device of claim 1, wherein the transaction information is account information.

8. The mobile device of claim 1, wherein the transaction information is credit card information.

9. A mobile device, comprising:
a biometric input device configured to receive biometric data; and
a radio frequency antenna and a chip, the chip comprising:
a memory, the memory configured to store transaction information and biometric information for identifying an individual associated with the transaction, and
a processor coupled with the memory and the biometric input, the processor configured to:
receive a signal via the radio frequency antenna, the signal comprising a request to access the memory and retrieve the transaction information,
receive biometric information from the biometric input device,
compare the received biometric information with the biometric information stored in the memory, and
provide the transaction information in response to the access request when the biometric information matches.

10. The mobile device of claim 9, wherein the mobile device is one of a cellphone, smartphone, or tablet.

11. The mobile device of claim 9, wherein the biometric input device is a fingerprint scanner.

12. The mobile device of claim 9, wherein the processor is further configured to provide the received biometric information or the stored biometric information with the transaction information.

13. The mobile device of claim 9, wherein the transaction information is account information.

14. The mobile device of claim 9, wherein the transaction information is credit card information.

15. A cellular telephone, comprising:
a fingerprint scanner configured to receive fingerprint information; and
a radio frequency antenna and a chip, the chip comprising:
a memory, the memory configured to store transaction information and fingerprint information for identifying an individual associated with the transaction, and
a processor coupled with the memory and the fingerprint scanner, the processor configured to:
receive a signal via the radio frequency antenna, the signal comprising a request to access the memory and retrieve the transaction information,
receive fingerprint information from the fingerprint scanner,
compare the received fingerprint information with the fingerprint information stored in the memory, and
provide the transaction information in response to the access request when the fingerprint information matches.

16. The mobile device of claim 15, wherein the processor is further configured to provide the received fingerprint information or the stored fingerprint information with the transaction information.

17. The mobile device of claim 15, wherein the transaction information is account information.

18. The mobile device of claim 15, wherein the transaction information is credit card information.

* * * * *

EXHIBIT 4

US008933807B2

(12) **United States Patent**
Martinez de Velasco Cortina et al.

(10) **Patent No.: US 8,933,807 B2**
(45) **Date of Patent: Jan. 13, 2015**

(54) **SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS**

(71) Applicants: **Francisco Martinez de Velasco Cortina**, La Jolla, CA (US); **Manfred Rietzler**, Marktoberdorf (DE)

(72) Inventors: **Francisco Martinez de Velasco Cortina**, La Jolla, CA (US); **Manfred Rietzler**, Marktoberdorf (DE)

(73) Assignee: **Neology, Inc.**, Poway, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/028,469**

(22) Filed: **Sep. 16, 2013**

(65) **Prior Publication Data**

US 2014/0019355 A1 Jan. 16, 2014

Related U.S. Application Data

(63) Continuation of application No. 13/350,665, filed on Jan. 13, 2012, now Pat. No. 8,587,436, which is a continuation of application No. 13/175,768, filed on Jul. 1, 2011, now Pat. No. 8,237,568, which is a continuation of application No. 12/688,666, filed on Jan. 15, 2010, now Pat. No. 8,004,410, which is a continuation of application No. 11/279,912, filed on Apr. 17, 2006, now Pat. No. 7,671,746, which is a continuation of application No. 10/615,026, filed on Jul. 9, 2003, now Pat. No. 7,081,819.

(60) Provisional application No. 60/394,241, filed on Jul. 9, 2002.

(51) **Int. Cl.**
G08B 13/14 (2006.01)

(52) **U.S. Cl.**
USPC **340/572.4**; 340/572.1; 340/539.11

(58) **Field of Classification Search**
USPC 340/539.1, 539.11, 539.13, 568.1, 340/568.7, 572.1, 572.4, 572.7, 5.52, 5.53, 340/5.8, 5.82, 5.83, 5.86; 235/379, 380, 235/381; 455/419; 713/175, 189, 176, 186; 705/35, 44, 64
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,529,870 A * 7/1985 Chaum 235/380
5,552,789 A 9/1996 Schuermann
5,657,008 A 8/1997 Bantli
5,742,618 A 4/1998 Lowe

(Continued)

FOREIGN PATENT DOCUMENTS

DE 19608757 A1 9/1997
DE 10042805 A1 3/2002

(Continued)

OTHER PUBLICATIONS

Atmel Corporation, Solution Making Smart Cards Smarter, 2000, 12 pages.

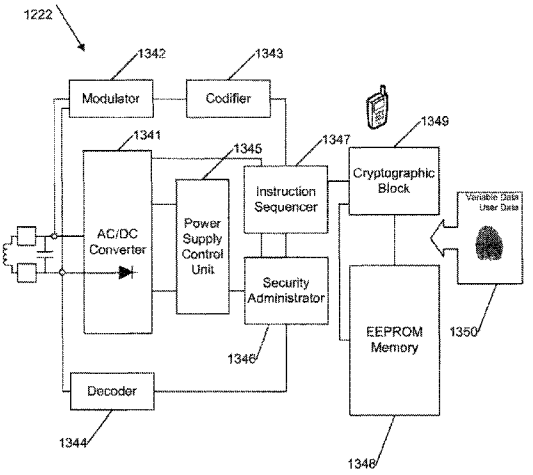
(Continued)

Primary Examiner — Van T. Trieu
(74) *Attorney, Agent, or Firm* — Procopio, Cory, Hargreaves & Savitch LLP; Noel C. Gillespie

(57) **ABSTRACT**

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

23 Claims, 24 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

5,787,174	A	7/1998	Tuttle	
5,864,580	A	1/1999	Lowe et al.	
5,874,896	A	2/1999	Small et al.	
5,974,500	A	10/1999	Maletsky et al.	
6,025,780	A	2/2000	Bowers et al.	
6,025,784	A	2/2000	Mish	
6,052,068	A	4/2000	Price et al.	
6,073,840	A	6/2000	Marion et al.	
6,098,879	A	8/2000	Terranova et al.	
6,104,281	A	8/2000	Heinrich et al.	
6,111,506	A	8/2000	Yap et al.	
6,140,941	A	10/2000	Dwyer et al.	
6,157,333	A	12/2000	Louagie et al.	
6,167,333	A	12/2000	Gehlot et al.	
6,175,922	B1 *	1/2001	Wang	713/182
6,203,952	B1	3/2001	O'Brien et al.	
6,211,790	B1	4/2001	Radomsky et al.	
6,268,796	B1	7/2001	Gnadinger et al.	
6,269,292	B1	7/2001	Kokubu et al.	
6,275,157	B1	8/2001	Mays et al.	
6,276,607	B1	8/2001	Sato	
6,334,059	B1	12/2001	Stilp et al.	
6,340,116	B1	1/2002	Cecil et al.	
6,360,208	B1	3/2002	Ohanian et al.	
6,388,579	B1	5/2002	Adcox et al.	
6,427,504	B1	8/2002	Janssen et al.	
6,570,487	B1	5/2003	Steeves	
6,617,961	B1	9/2003	Janssen et al.	
6,698,653	B1	3/2004	Diamond et al.	
6,753,759	B2	6/2004	Stegmaier et al.	
6,758,405	B2	7/2004	Look	
6,793,134	B2 *	9/2004	Clark	235/379
6,850,147	B2 *	2/2005	Prokoski et al.	340/5.53
6,894,615	B2	5/2005	Look	
6,950,013	B2	9/2005	Scaman et al.	
6,975,834	B1	12/2005	Forster	
7,031,946	B1	4/2006	Tamai et al.	
7,080,819	B2	7/2006	Tojo	
7,225,337	B2 *	5/2007	Baessler	713/175
7,310,734	B2 *	12/2007	Boate et al.	713/186
7,487,538	B2	2/2009	Mok	
7,533,809	B1	5/2009	Robinson et al.	
7,671,746	B2 *	3/2010	Martinez de Velasco Cortina et al.	340/572.4
7,844,505	B1	11/2010	Arneson et al.	
7,980,378	B2 *	7/2011	Jones et al.	194/217
8,004,410	B2 *	8/2011	Martinez De Velasco Cortina et al.	340/572.4
8,041,815	B2	10/2011	Bahl et al.	
8,126,449	B2 *	2/2012	Beenau et al.	455/419
8,401,539	B2 *	3/2013	Beenau et al.	455/419
8,548,927	B2 *	10/2013	Beenau et al.	705/76
2002/0089434	A1	7/2002	Ghazarian	
2002/0109580	A1 *	8/2002	Shreve et al.	340/5.61
2003/0074317	A1 *	4/2003	Hofi	705/44
2003/0200227	A1	10/2003	Ressler	
2005/0149764	A1	7/2005	Bahl et al.	
2010/0094754	A1 *	4/2010	Bertran et al.	705/44
2010/0095130	A1 *	4/2010	Bertran et al.	713/189

FOREIGN PATENT DOCUMENTS

EP	977145	A2	2/2000
EP	993999	A2	4/2000
JP	2002042076	A	2/2002
WO	9843104	A2	10/1998
WO	2004006165	A1	1/2004

OTHER PUBLICATIONS

Extended European Search Report issued by the European Patent Office in related European Application No. 10182033.0 dated Jan. 13, 2012 (7 pages).

Fancher, Carol Hovenga, In Your Pocket Smartcards, IEEE Spectrum, Feb. 2007, 7 pages.

Rakers, Patrick, et al., Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal of Solid-State Circuits, vol. 36, No. 3, Mar. 2001, 7 pages.

Official Action in Japanese Patent Application No. 2004-519130 dated May 12, 2009, 10 pages.

Anonymous, Read Write RFID Offers Standalone Advantages, Security, Aug. 1996, 1 page.

21 C.C.R. §1700.

21 C.C.R. § 1701(r).

21 C.C.R. § 1702.1.

21 C.C.R. § 1703(c).

21 C.C.R. § 1703(e-i).

21 C.C.R. § 1704.1.

21 C.C.R. § 1704.2.

21 C.C.R. § 1704.3.

21 C.C.R. § 1704.5(e)(1).

21 C.C.R. § 1704.6.

21 C.C.R. § 1705.1.

21 C.C.R. § 1705.2.

21 C.C.R. § 1705.3.

21 C.C.R. § 1705.4.

21 C.C.R. § 1705.5.

21 C.C.R. § 1705.5(d) and (e)(1).

21 C.C.R. 1705.8.

* cited by examiner

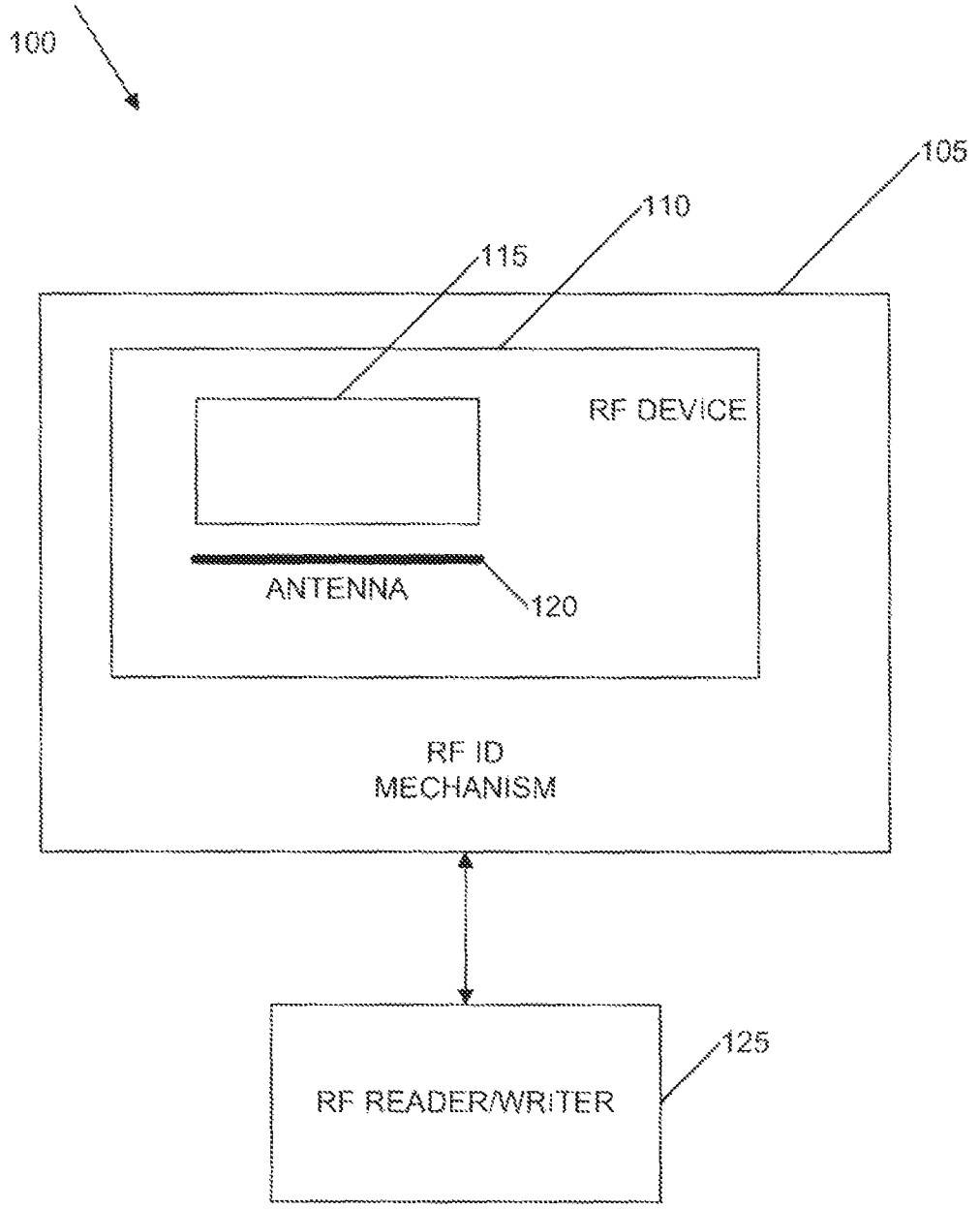

100
105
110
115
RF DEVICE
ANTENNA
120
RF ID
MECHANISM
125
RF READER/WRITER

FIG. 1

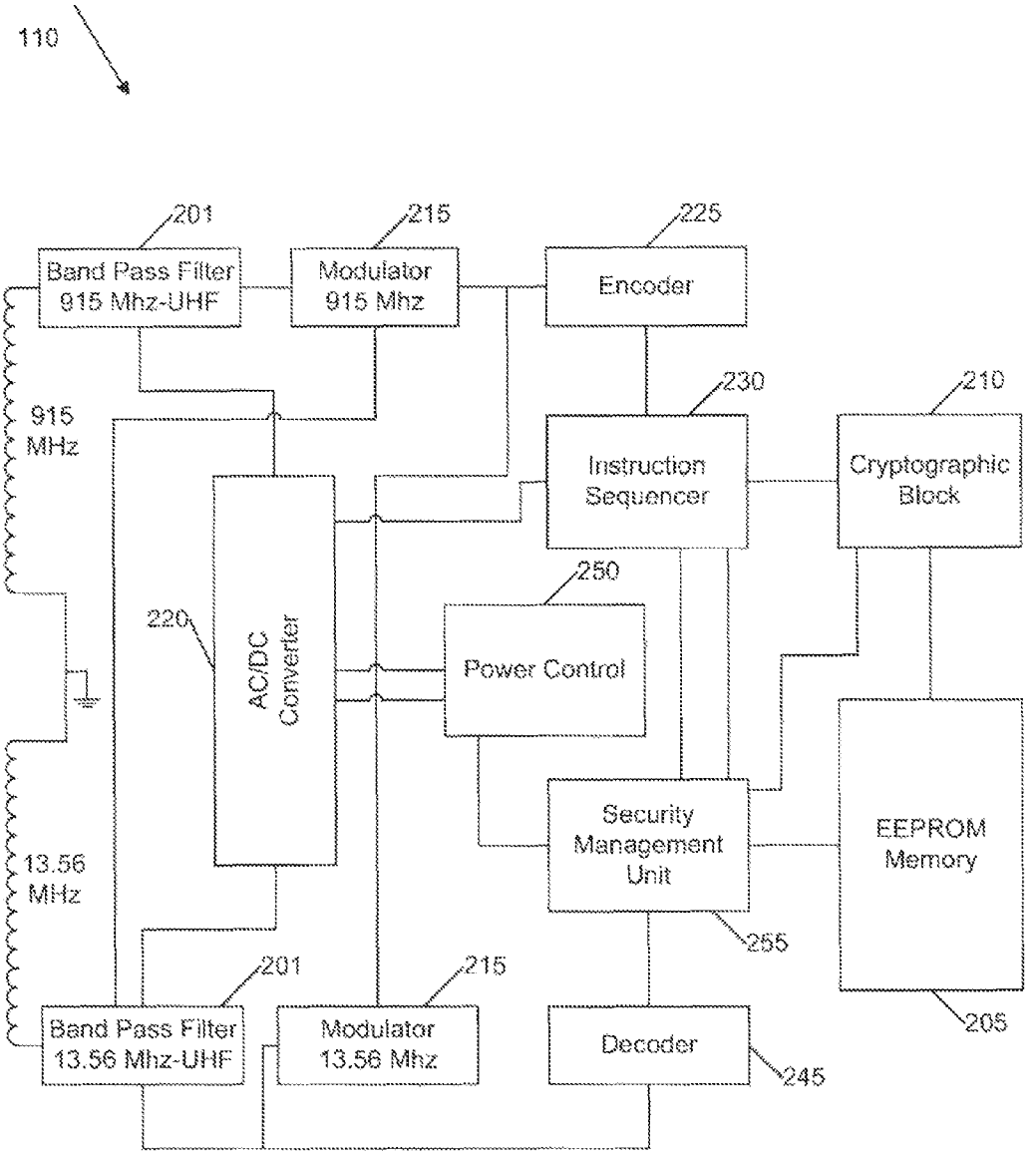

110
201
Band Pass Filter
915 Mhz-UHF
215
Modulator
915 Mhz
225
Encoder
230
Instruction
Sequencer
210
Cryptographic
Block
915
MHz
220
AC/DC
Converter
250
Power Control
Security
Management
Unit
EEPROM
Memory
255
205
13.56
MHz
201
Band Pass Filter
13.56 Mhz-UHF
215
Modulator
13.56 Mhz
Decoder
245

FIG. 2

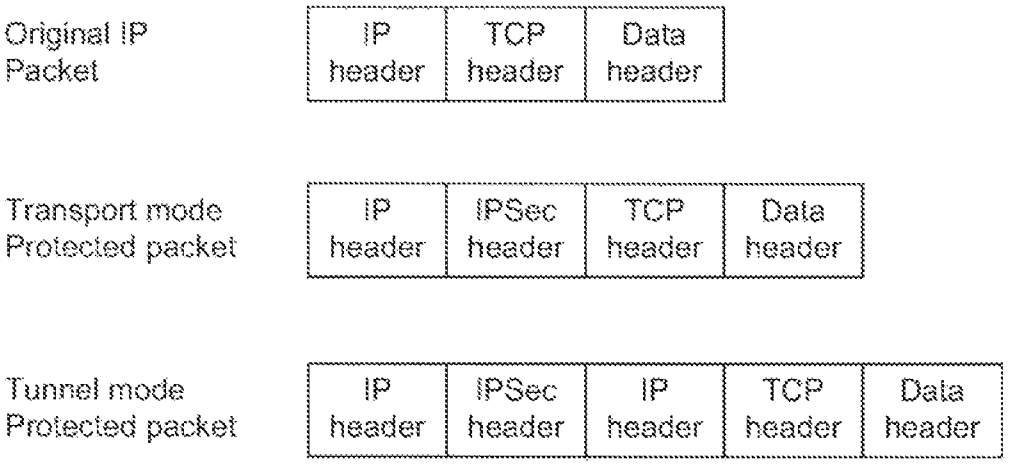

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIG. 3A

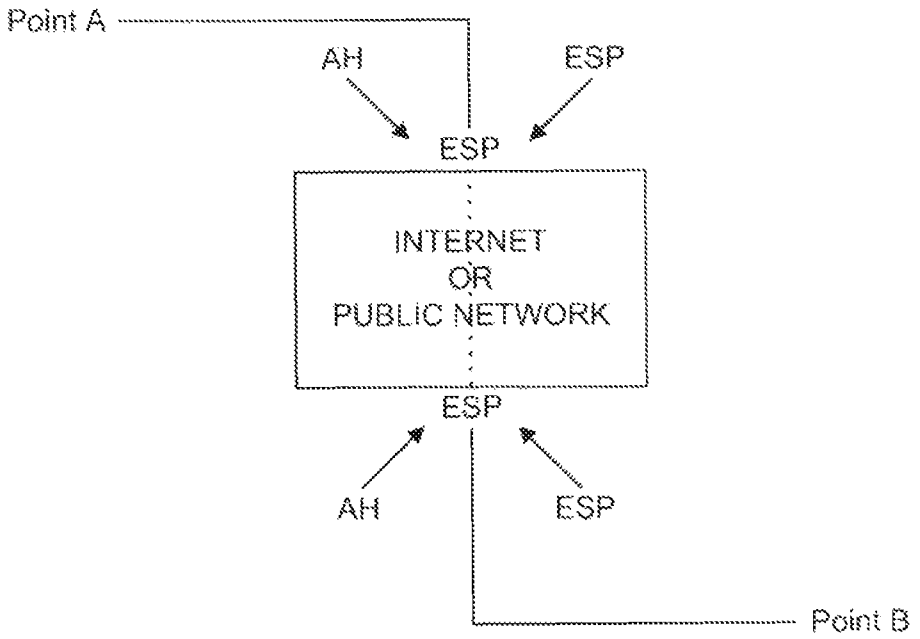

Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORK
ESP
AH
ESP
Point B

FIG. 3B

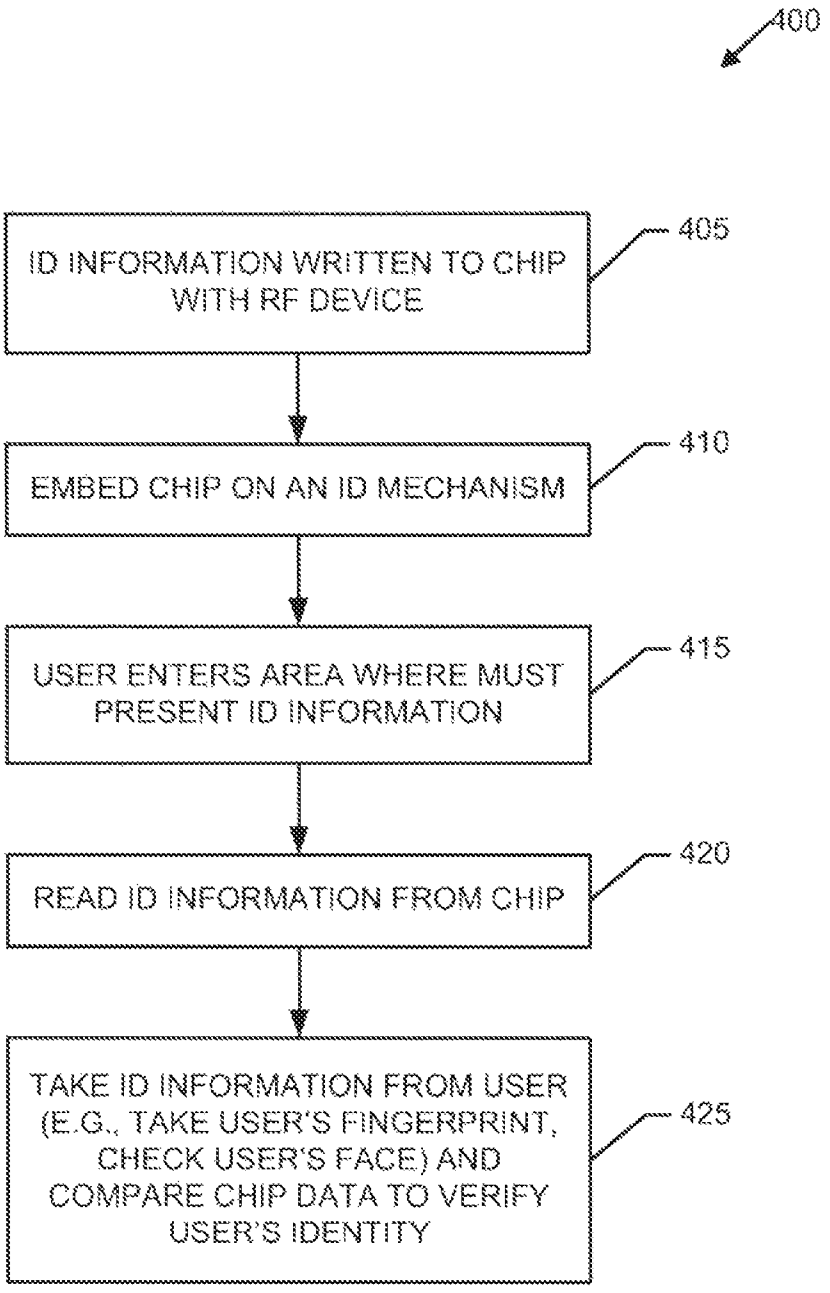

400
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
405
EMBED CHIP ON AN ID MECHANISM
410
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
415
READ ID INFORMATION FROM CHIP
420
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE CHIP DATA TO VERIFY USER'S IDENTITY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

FIG. 4

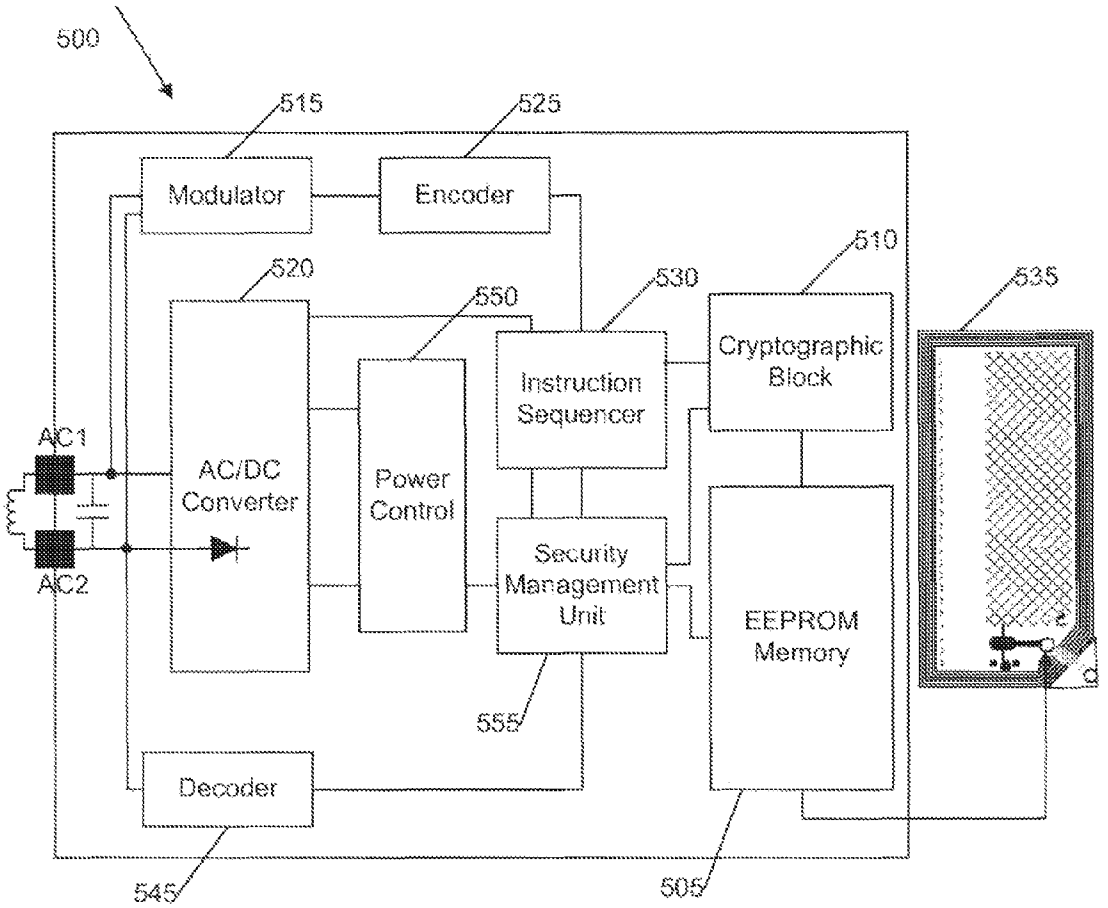

500
515
525
Modulator
Encoder
510
520
530
535
550
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
555
Decoder
545
505

FIG. 5

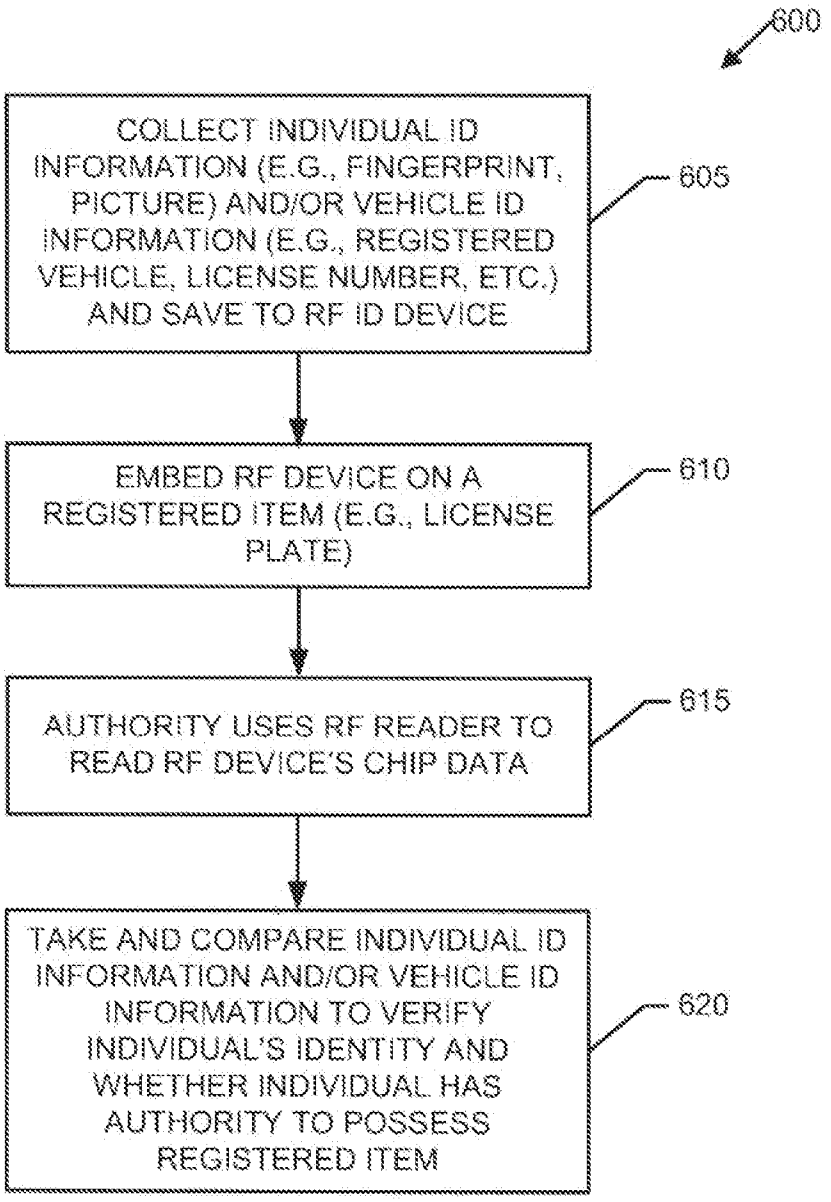

600
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
605
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
610
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
615
TAKE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

FIG. 6

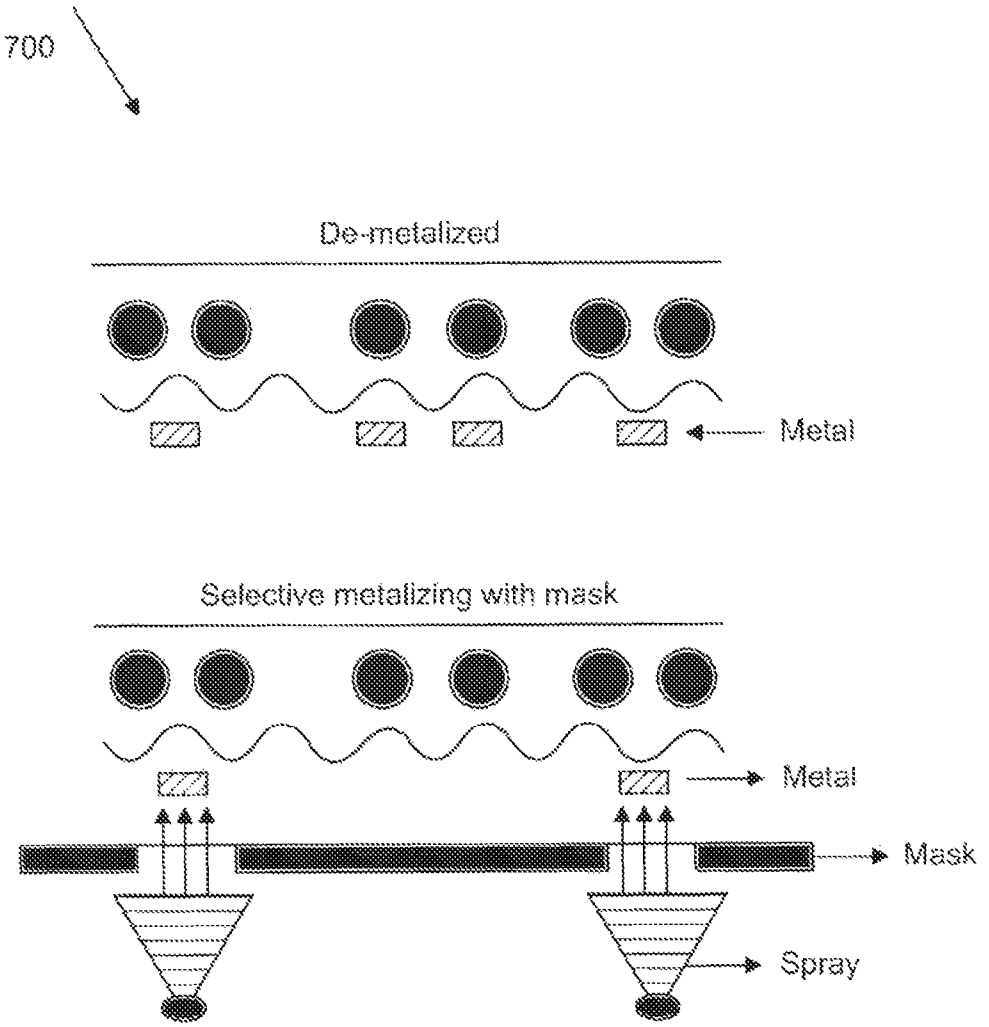

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIG. 7

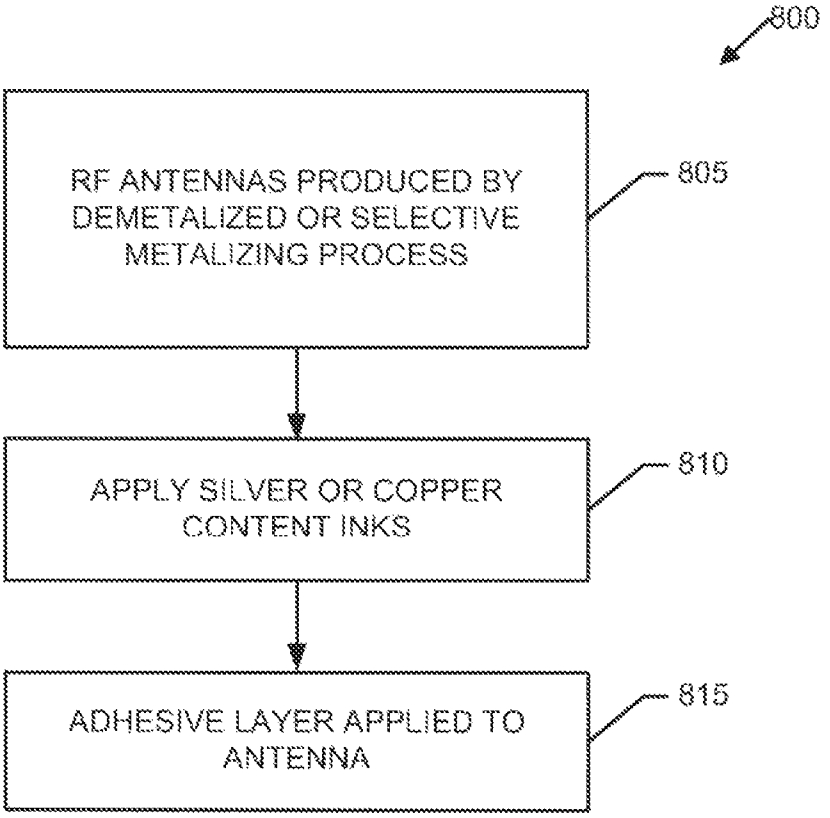

800
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
805
APPLY SILVER OR COPPER CONTENT INKS
810
ADHESIVE LAYER APPLIED TO ANTENNA
815

FIG. 8

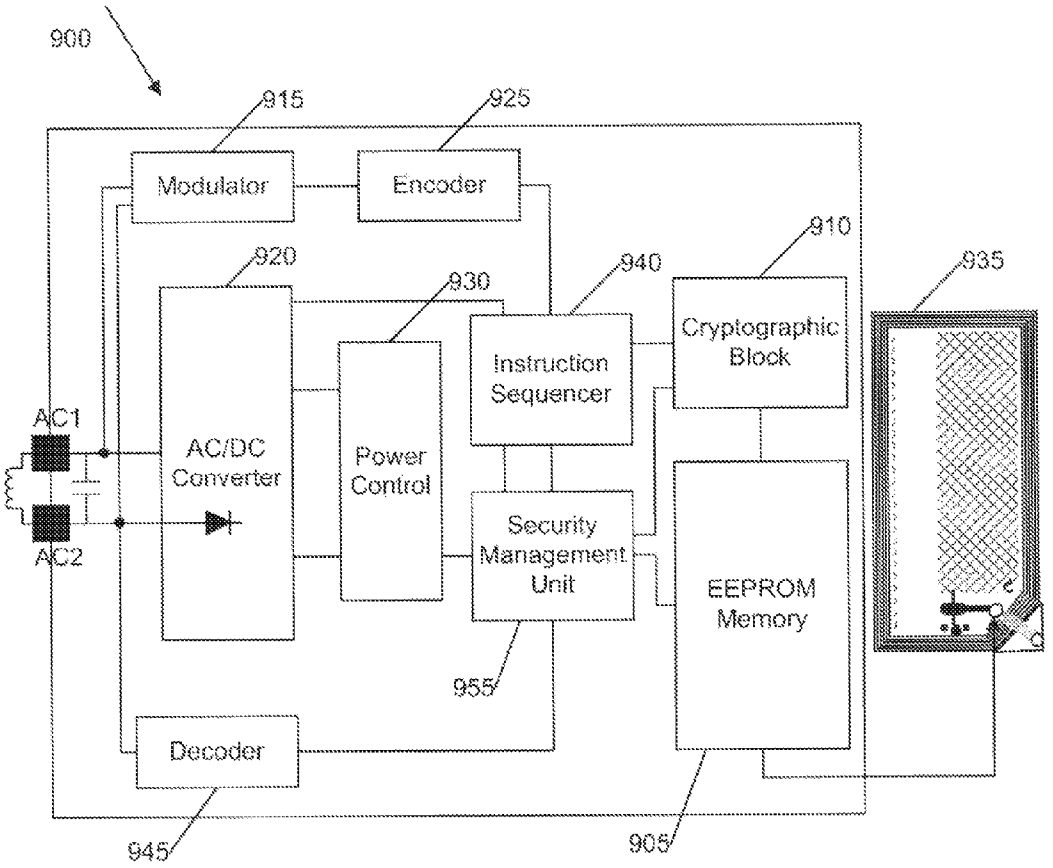

900
915
925
Modulator
Encoder
910
920
930
940
935
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
955
Decoder
945
905

FIG. 9

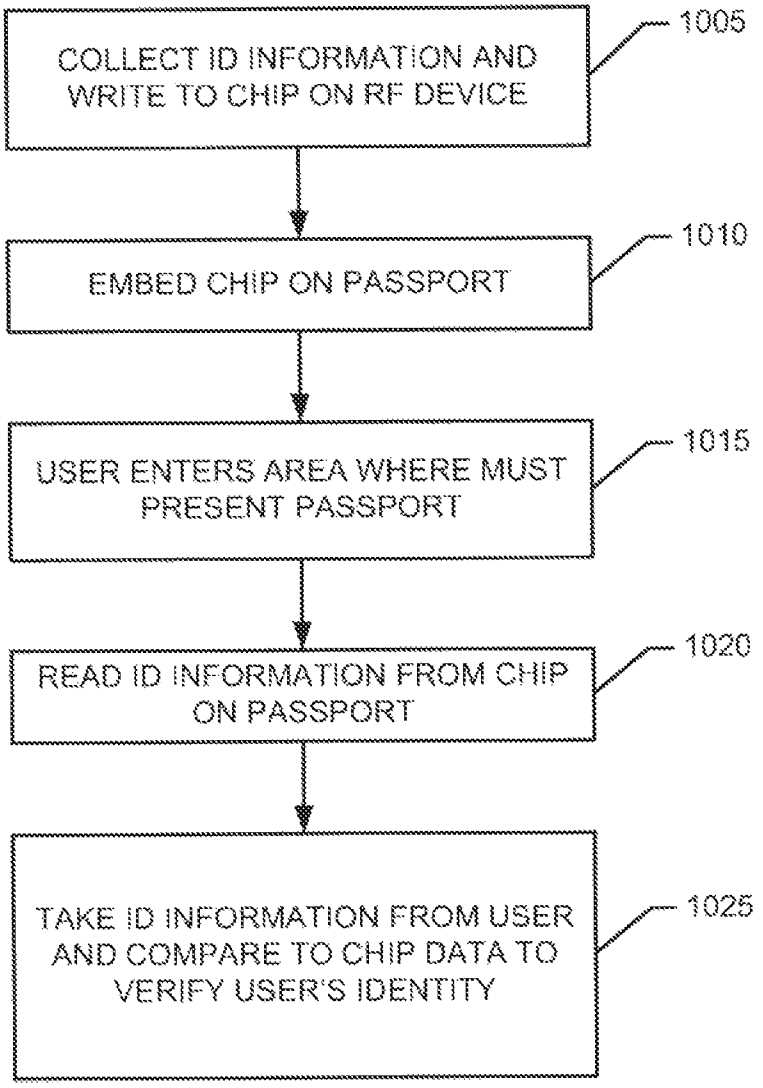

COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1005
EMBED CHIP ON PASSPORT
1010
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1015
READ ID INFORMATION FROM CHIP ON PASSPORT
1020
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY
1025

FIG. 10

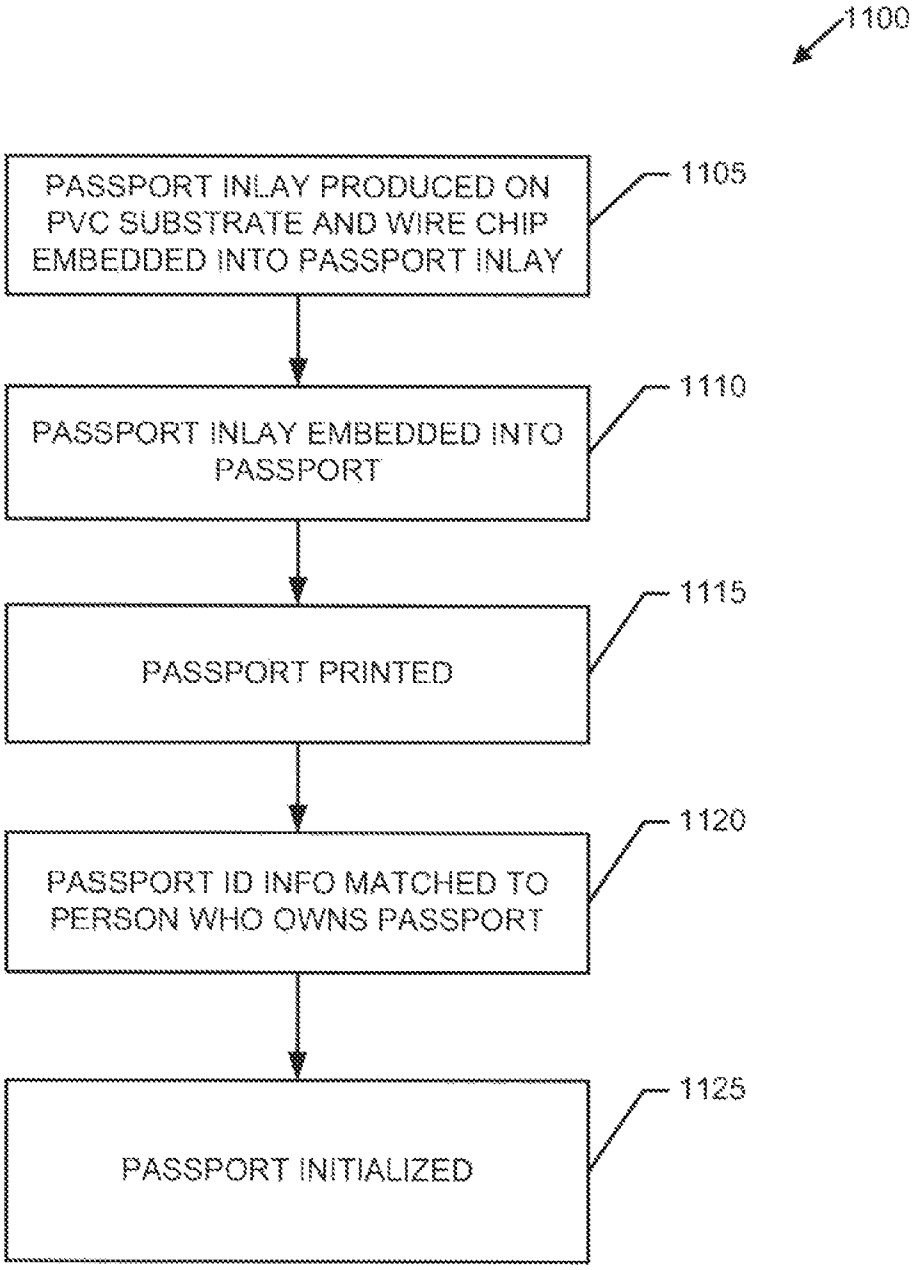

1100
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1105
PASSPORT INLAY EMBEDDED INTO PASSPORT
1110
PASSPORT PRINTED
1115
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1120
PASSPORT INITIALIZED
1125

FIG. 11

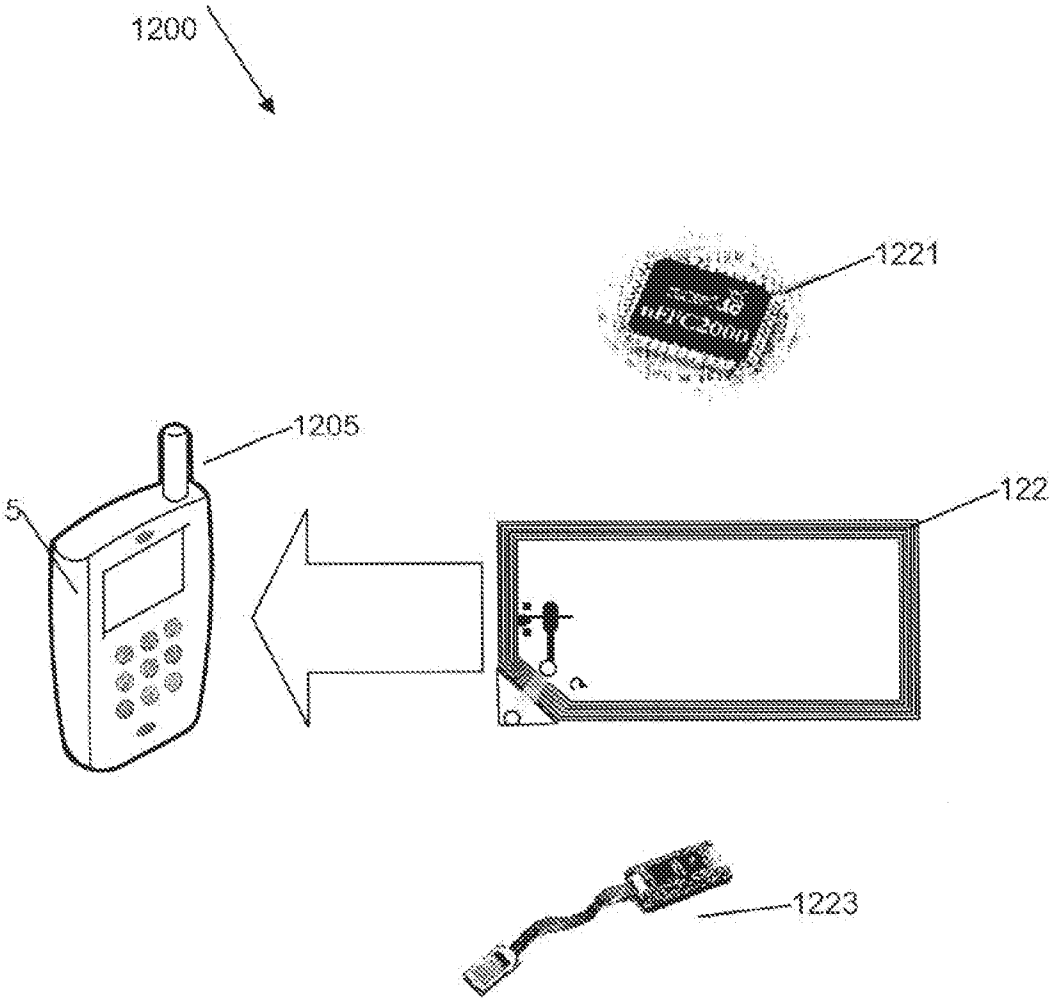


FIG. 12

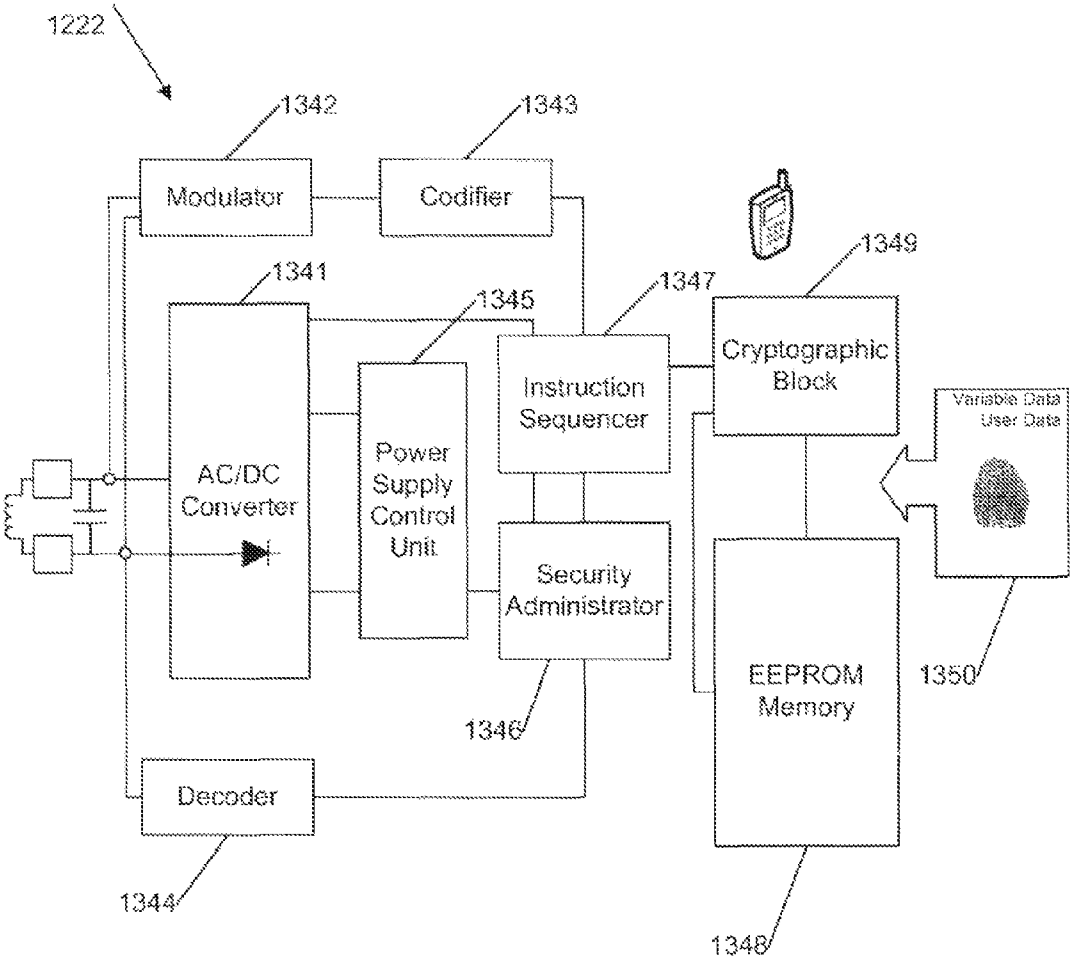

1222
1342
1343
Modulator
Codifier
1341
1345
1347
1349
AC/DC Converter
Power Supply Control Unit
Instruction Sequencer
Cryptographic Block
Variable Data
User Data
Security Administrator
EEPROM Memory
1350
1346
Decoder
1344
1348

FIG. 13

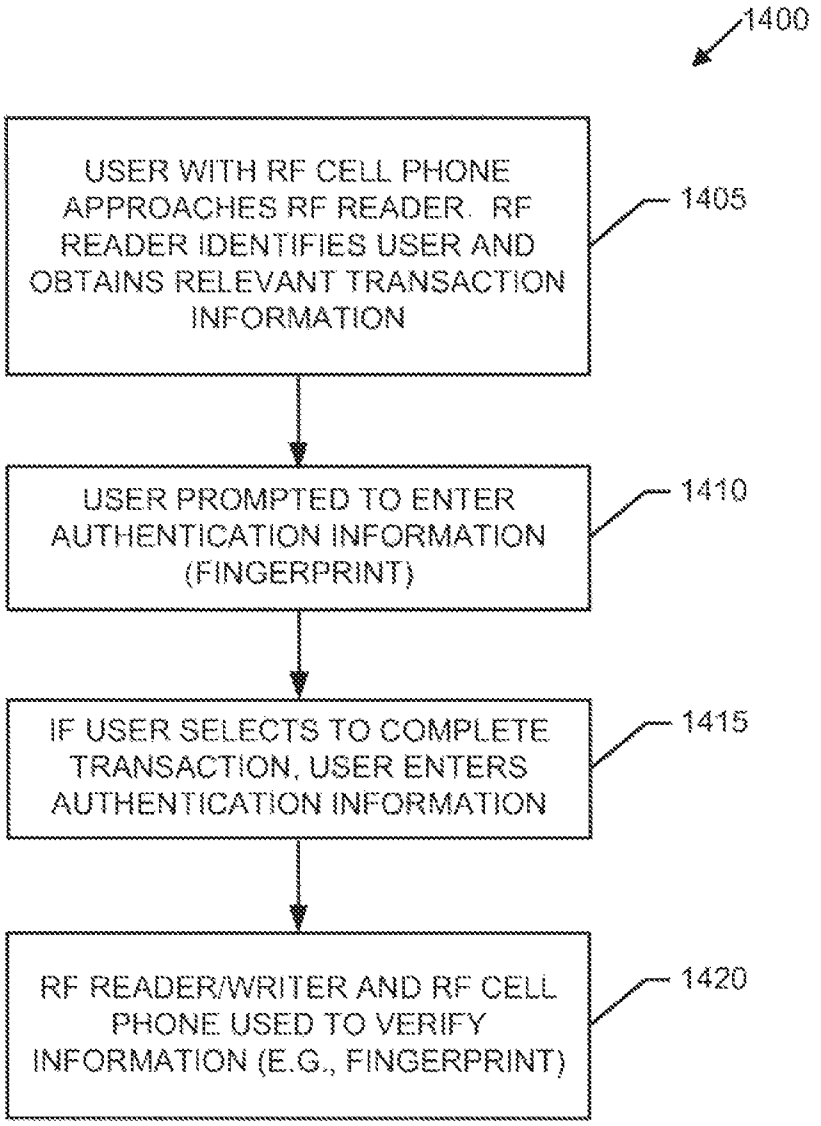

1400
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION
1405
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT)
1410
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION
1415
RF READER/WRITER AND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

FIG. 14

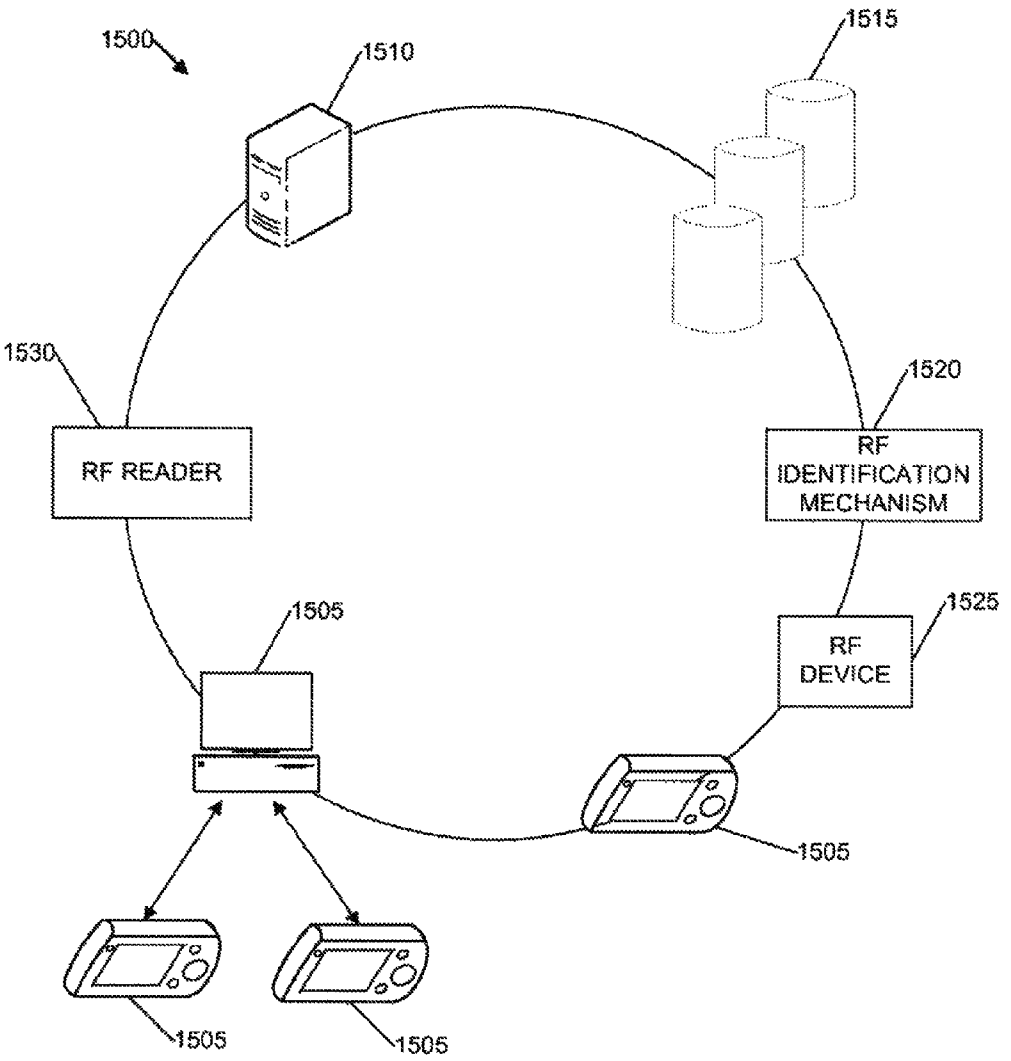

1500
1510
1515
1530
1520
RF READER
RF IDENTIFICATION MECHANISM
1505
1525
RF DEVICE
1505
1505
1505

FIG. 15

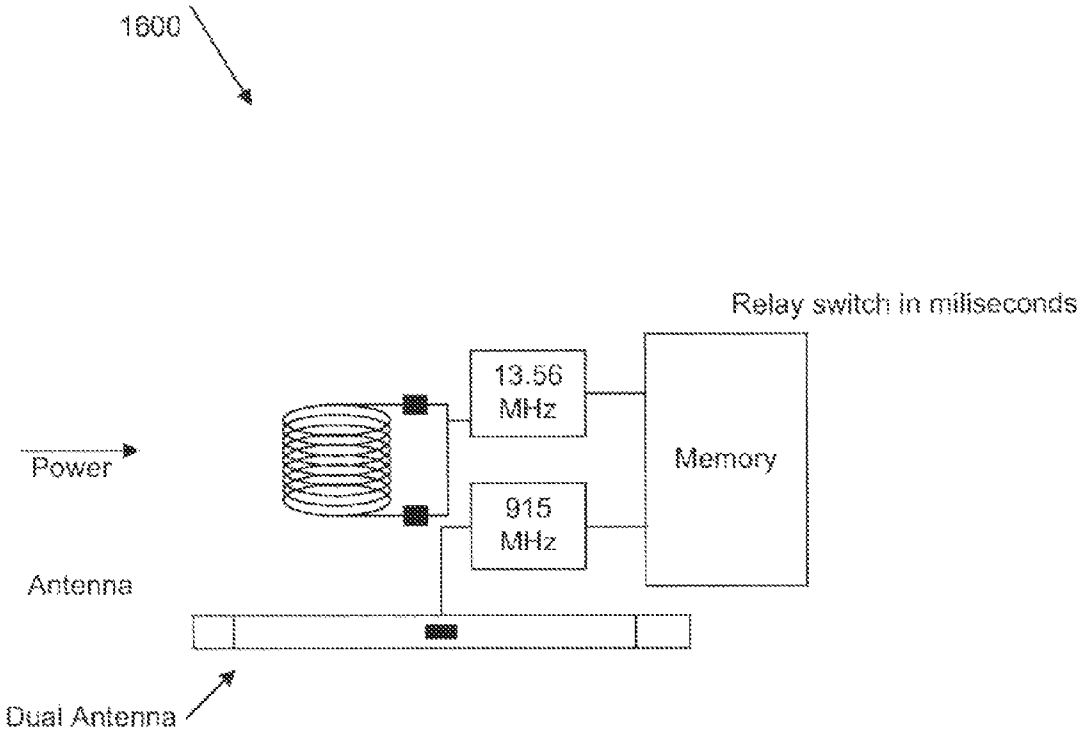

1600
Relay switch in milliseconds
13.56 MHz
915 MHz
Memory
Power
Antenna
Dual Antenna

FIG. 16

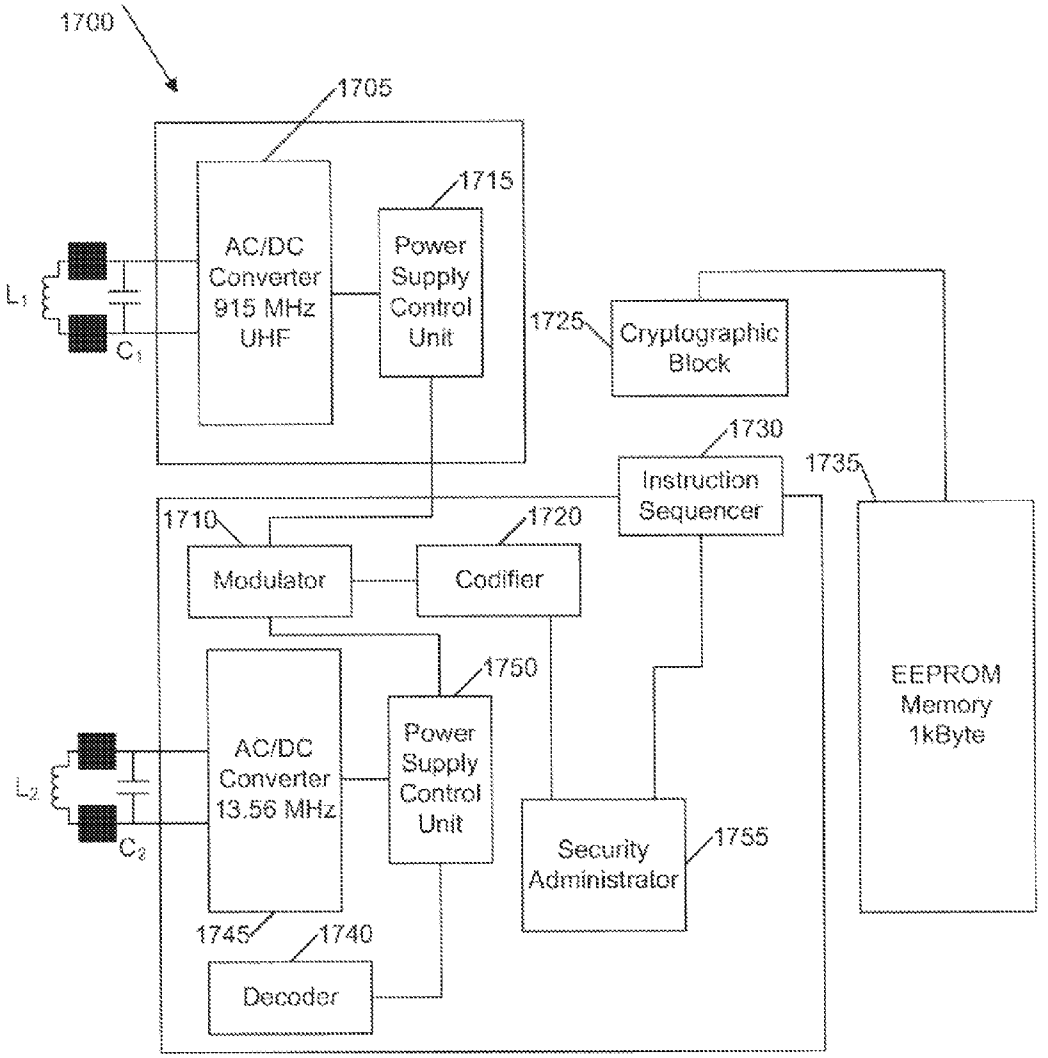

1700
1705
1715
AC/DC Converter 915 MHz UHF
Power Supply Control Unit
L1
C1
1725
Cryptographic Block
1730
Instruction Sequencer
1735
1710
1720
Modulator
Codifier
EEPROM Memory 1kByte
1750
AC/DC Converter 13.56 MHz
Power Supply Control Unit
L2
C2
Security Administrator
1755
1745
1740
Decoder

FIG. 17

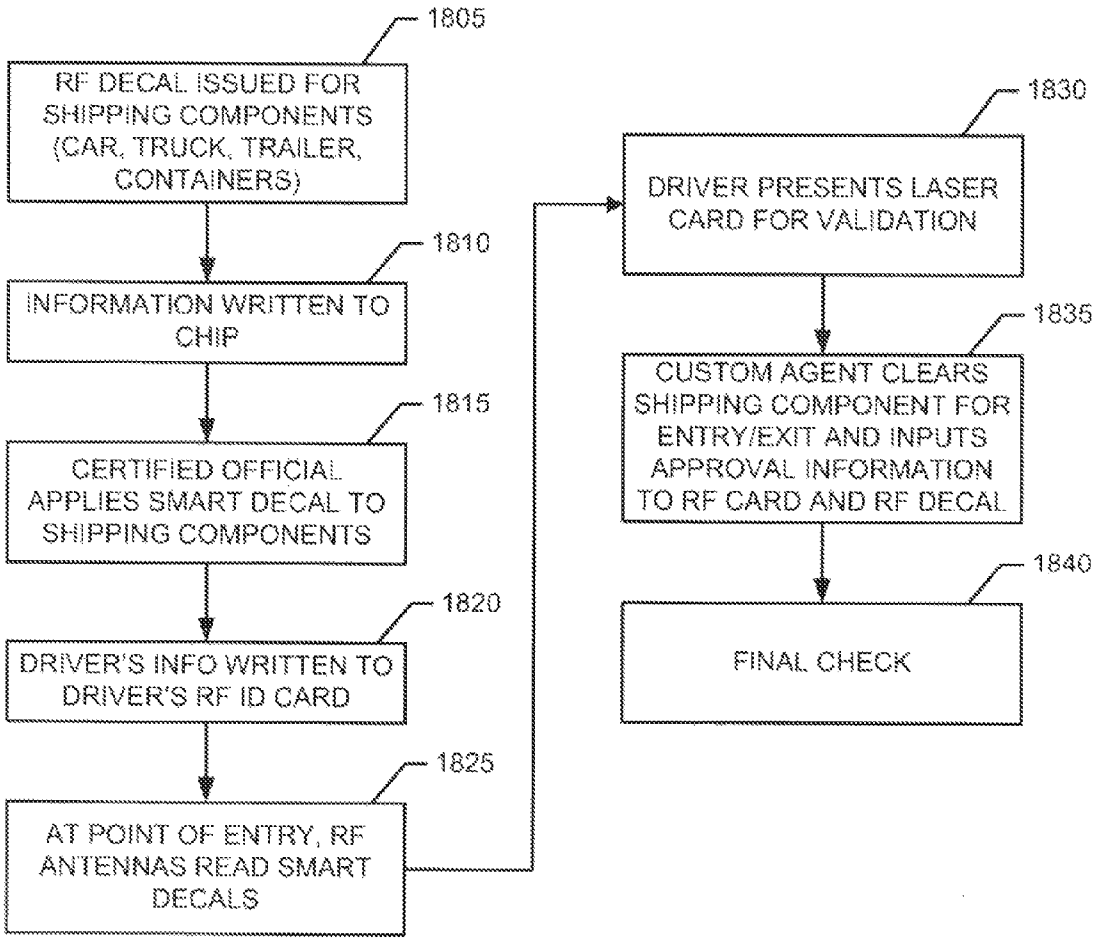

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS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

FIG. 18

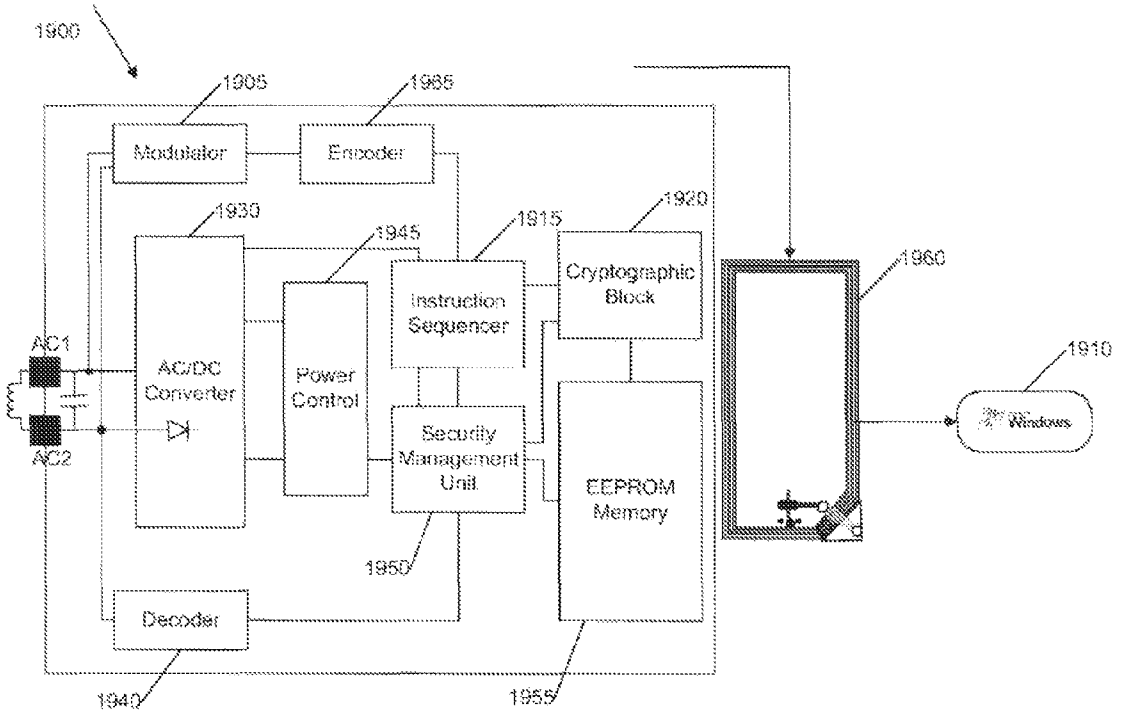

1900
1905
Modulator
1985
Encoder
1930
AC/DC Converter
1945
Power Control
1915
Instruction Sequencer
1920
Cryptographic Block
1960
AC1
AC2
Security Management Unit
1950
EEPROM Memory
1910
Windows
Decoder
1940
1955

FIG. 19

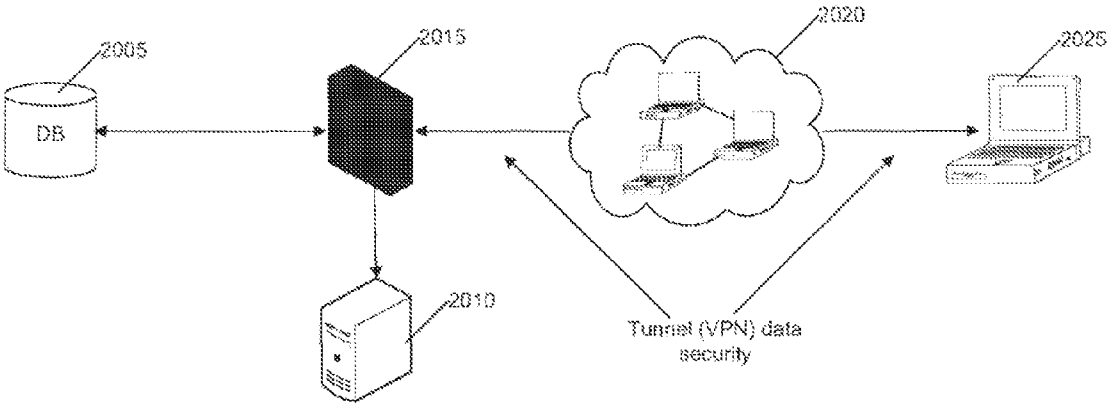


FIG. 20

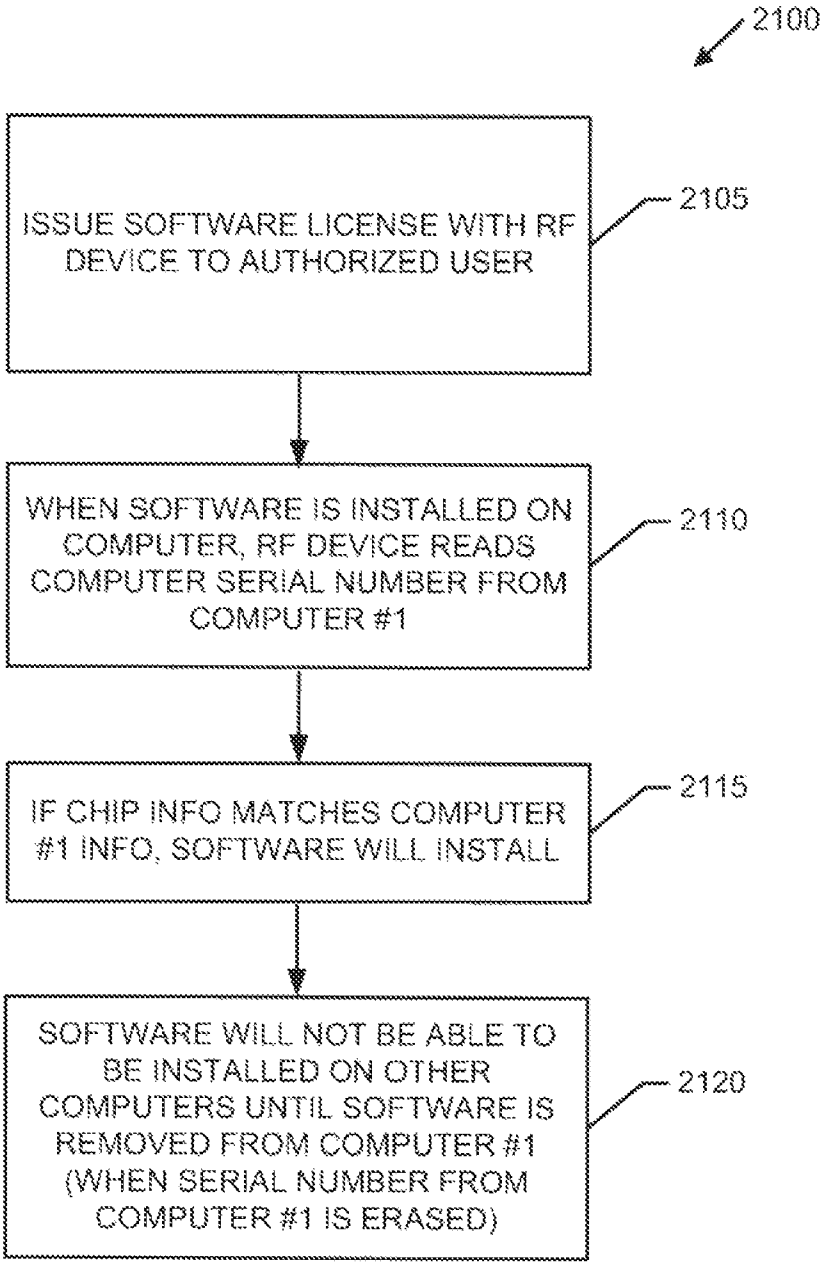

2100
ISSUE SOFTWARE LICENSE WITH RF DEVICE TO AUTHORIZED USER
2105
WHEN SOFTWARE IS INSTALLED ON COMPUTER, RF DEVICE READS COMPUTER SERIAL NUMBER FROM COMPUTER #1
2110
IF CHIP INFO MATCHES COMPUTER #1 INFO, SOFTWARE WILL INSTALL
2115
SOFTWARE WILL NOT BE ABLE TO BE INSTALLED ON OTHER COMPUTERS UNTIL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

FIG. 21

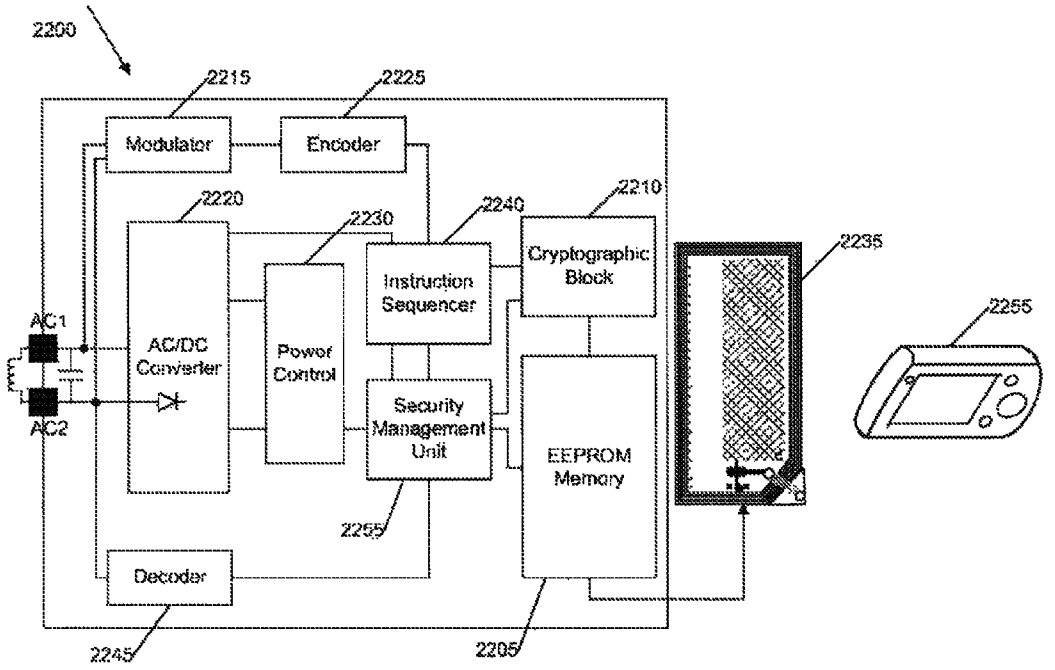

2200
2215
2225
Modulator
Encoder
2220
2230
2240
2210
Cryptographic Block
2235
Instruction Sequencer
AC1
AC/DC Converter
Power Control
2255
AC2
Security Management Unit
EEPROM Memory
2255
Decoder
2245
2205

FIG. 22

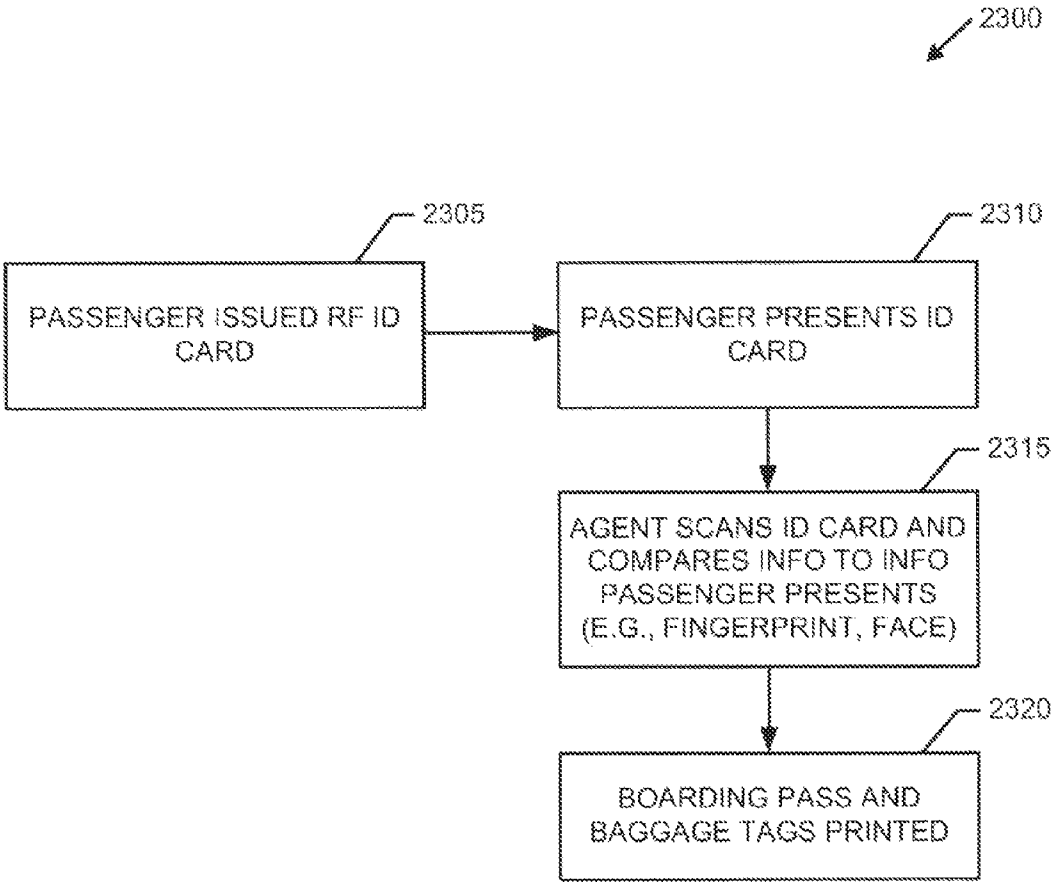

2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENT SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

FIG. 23

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

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

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

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

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

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

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

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

FIGS. **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

FIG. **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

FIG. **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.

FIG. **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.

A more detailed description of an RF device can be found in U.S. patent application Ser. No. 10/118,092 filed 9 Apr. 2002; PCT Patent Application PCT/IB02/01439, filed 30 Apr. 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 spe-

cial 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 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.

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 counter-

feiters 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 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.

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 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.

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 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.

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 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.

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

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

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 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.

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 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.

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

FIG. **4** illustrates the methods 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

FIG. **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

FIG. **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.

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 FIG. **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 material, holographic foil, or another substrate with a high metal content.

FIG. **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) 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

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

FIG. **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

FIG. **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

FIG. **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

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 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.

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 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.

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

FIG. **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 ensures 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 FIG. **13**. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt **1348**, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements are not met, a user cannot access the memory of the chip. The chip includes an ACDC converter **1341** and a connection to an RF antenna for power using a power supply control unit **1345**. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator **1342** is a device that receives baseband signals from an antenna. An AC/DC converter **1341** is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder **1343** is a device for encoding information received so that it may be utilized by another device or protocol. A decoder **1344** is a device that decodes information from the encoder output so it may be used by another device or display. A power control **1345** is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer **1347** is a device that queues instructions to be sent to the chip's internal memory. A security management unit **1346** is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block **1349** is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory **1348** stores data. Information can be read and written from or to this device.

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

FIG. **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 FIG. **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 Ser. No. 10/118,092, filed Apr. 2, 2002, and PCT Patent Application IB0201439, filed Apr. 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

FIG. **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 24×7; 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 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.

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 (PIPS) 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 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.

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 FIG. **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=capaticance (F)

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

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

N=number of windings around inductor
μ_o=permeability of freespace (Hm^{-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:

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

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

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

For substitution, the following values are used:

$$L_1 = 2.931\times10^{8} H$$

$$L_2 = 6.437\times10^{10} H$$

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

Multiple RF Chip Overview

FIG. **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

FIG. **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 demetalizing 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

FIG. **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.

FIG. **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.

FIG. **3**A illustrates the differences between transport mode and tunnel mode. The use of AH and ESP are illustrated in FIG. **38**.

B. Method of Limiting Software Downloads

FIG. **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

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

B. Method of Airport Security

FIG. **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 mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

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

a biometric reading device configured to read biometric information;

an authentication module configured to authenticate that the biometric information read by the biometric reading device is associated with the transaction information

based at least in part on the biometric authentication information stored in memory; and

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

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

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

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

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

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

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

8. The mobile device of claim **1**, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

9. A mobile device, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

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

a biometric reading device configured to read biometric information;

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

a transaction module configured to provide the transaction information via the short range RF circuitry for use in a transaction when the biometric information read by the biometric reading device is successfully authenticated by the authentication module as being associated with the transaction information by the authentication module; and

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

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

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

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

13. The mobile device of claim **9**, wherein the security block is a cryptographic block.

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

15. The mobile device of claim **9**, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

16. A cellular telephone, comprising:

Radio Frequency (RF) cellular circuitry;

short range RF circuitry;

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

a biometric reading device configured to read biometric information;

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

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

17. The cellular telephone of claim **16**, wherein the biometric reading device is a fingerprint reading device.

18. The cellular telephone of claim **17**, further comprising a security block configured to secure the transaction information before it is provided by the transaction module.

19. The cellular telephone of claim **18**, wherein the security block is a cryptographic block.

20. The cellular telephone of claim **16**, wherein the transaction information is generated based at least in part on credit card information.

21. The cellular telephone of claim **16**, wherein the transaction information is generated based at least in part on rewards card information.

22. The cellular telephone of claim **16**, wherein the short range RF circuitry includes a radio frequency identification (RFID) device.

23. The cellular phone of claim **16**, wherein the transaction module configured to provide the transaction information but not the biometric information via the short range RF circuitry for use in the transaction.

* * * * *

EXHIBIT 5

US010235513B2

(12) **United States Patent**
Martinez de Velasco Cortina et al.

(10) **Patent No.: US 10,235,513 B2**
(45) **Date of Patent: Mar. 19, 2019**

(54) **SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS**

(71) Applicant: **NEOLOGY, INC.**, Poway, CA (US)

(72) Inventors: **Francisco Martinez de Velasco Cortina**, La Jolla, CA (US); **Manfred Rietzler**, Marktoberdorf (DE)

(73) Assignee: **Neology, Inc.**, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **15/372,317**

(22) Filed: **Dec. 7, 2016**

(65) **Prior Publication Data**

US 2017/0094516 A1 Mar. 30, 2017

Related U.S. Application Data

(63) Continuation of application No. 14/084,565, filed on Nov. 19, 2013, now Pat. No. 9,558,385, which is a (Continued)

(51) **Int. Cl.**
G06F 21/31 (2013.01)
G06F 21/35 (2013.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06F 21/35*** (2013.01); ***G06F 21/31*** (2013.01); ***G06F 21/32*** (2013.01); ***G06F 21/34*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G06F 21/30; G06F 30/305; G06F 30/31; G06F 30/32; G06F 30/34; G06F 30/35; G06F 21/31; G06F 21/32; G06F 21/35; G06F 21/34; G06Q 20/20; G06Q 20/206; G06Q 20/40; G06Q 20/401; G06Q 20/405; G08B 13/2402; G08B 13/2417;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,529,870 A 7/1985 Chaum
5,552,789 A 9/1996 Schuermann
(Continued)

FOREIGN PATENT DOCUMENTS

DE 19608757 A1 9/1997
DE 10042805 A1 3/2002
(Continued)

OTHER PUBLICATIONS

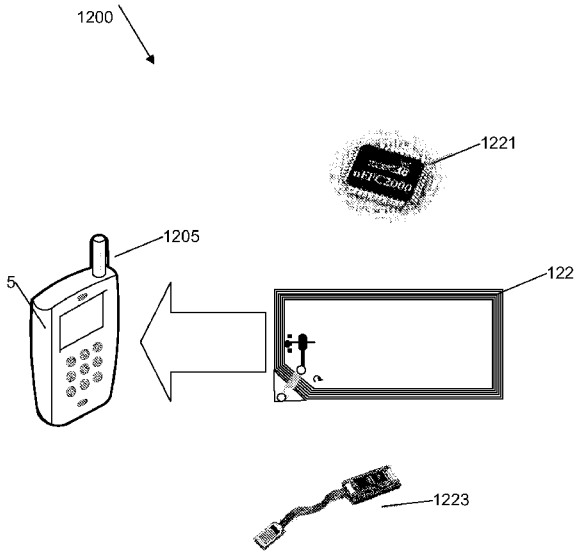
Mohammed et al., Smart Card Technology: Past Present and Future, International Journal of The Computer, the Internet and Management, vol. 12#1 (Jan.-Apr. 2004), pp. 12-22.
(Continued)

Primary Examiner — Van T Trieu
(74) *Attorney, Agent, or Firm* — Procopio; Mark W. Catanese; Noel C. Gillespie

(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.

26 Claims, 24 Drawing Sheets



Related U.S. Application Data

continuation of application No. 13/350,665, filed on Jan. 13, 2012, now Pat. No. 8,587,436, which is a continuation of application No. 13/175,768, filed on Jul. 1, 2011, now Pat. No. 8,237,568, which is a continuation of application No. 12/688,666, filed on Jan. 15, 2010, now Pat. No. 8,004,410, which is a continuation of application No. 11/279,912, filed on Apr. 17, 2006, now Pat. No. 7,671,746, which is a continuation of application No. 10/615,026, filed on Jul. 9, 2003, now Pat. No. 7,081,819.

(60) Provisional application No. 60/394,241, filed on Jul. 9, 2002.

(51) **Int. Cl.**

H04W 4/80	(2018.01)
G06F 21/34	(2013.01)
G06F 21/32	(2013.01)
G06K 19/07	(2006.01)
G06K 19/077	(2006.01)
G06K 19/10	(2006.01)
G06K 7/00	(2006.01)
G07C 9/00	(2006.01)
H04W 12/06	(2009.01)
H04W 12/08	(2009.01)
H04L 29/06	(2006.01)

(52) **U.S. Cl.**

CPC ... ***G06K 19/0723*** (2013.01); ***G06K 19/07758*** (2013.01); ***G06K 19/10*** (2013.01); ***H04W 4/80*** (2018.02); *G06K 7/0008* (2013.01); *G06K 19/0776* (2013.01); *G06K 19/07764* (2013.01); *G06Q 2220/00* (2013.01); *G07C 9/00087* (2013.01); *H04L 63/0861* (2013.01); *H04W 12/06* (2013.01); *H04W 12/08* (2013.01)

(58) **Field of Classification Search**

CPC G06C 20/20; G06C 20/206; G06C 20/40; G06C 20/401; G06C 20/405

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,590,197	A	12/1996	Chen et al.	
5,657,008	A	8/1997	Bantli	
5,742,618	A	4/1998	Lowe	
5,787,174	A	7/1998	Tuttle	
5,864,580	A	1/1999	Lowe et al.	
5,874,896	A	2/1999	Lowe et al.	
5,974,500	A	10/1999	Maletsky et al.	
6,025,780	A	2/2000	Bowers et al.	
6,025,784	A	2/2000	Mish	
6,052,068	A	4/2000	Price et al.	
6,073,840	A	6/2000	Marion	
6,098,879	A	8/2000	Terranova	
6,104,281	A	8/2000	Heinrich et al.	
6,111,506	A	8/2000	Yap et al.	
6,140,941	A	10/2000	Dwyer et al.	
6,157,333	A	12/2000	Louagie et al.	
6,163,771	A	12/2000	Walker et al.	
6,167,333	A	12/2000	Gehlot et al.	
6,175,922	B1	1/2001	Wang	
6,182,894	B1	2/2001	Hackett et al.	
6,203,952	B1	3/2001	O'Brien et al.	
6,211,790	B1	4/2001	Radomsky et al.	
6,268,796	B1	7/2001	Gnadinger et al.	
6,269,292	B1	7/2001	Kokubu et al.	
6,275,157	B1	8/2001	Mays et al.	
6,276,607	B1	8/2001	Sato	
6,334,059	B1	12/2001	Stilp et al.	
6,340,116	B1	1/2002	Cecil et al.	
6,360,208	B1	3/2002	Ghanian et al.	
6,388,579	B1	5/2002	Adcox et al.	
6,427,504	B1	8/2002	Janssen et al.	
6,570,487	B1	5/2003	Steeves	
6,617,961	B1	9/2003	Janssen et al.	
6,657,538	B1 *	12/2003	Ritter	G06F 21/32 340/5.8
6,698,653	B1	3/2004	Diamond et al.	
6,753,759	B2	6/2004	Stegmaier et al.	
6,758,405	B2	7/2004	Look	
6,793,134	B2	9/2004	Clark	
6,848,048	B1	1/2005	Holmes	
6,850,147	B2	2/2005	Prokoski	
6,894,615	B2	5/2005	Look	
6,934,861	B2 *	8/2005	Haala	G06Q 20/341 705/44
6,950,013	B2	9/2005	Scaman et al.	
6,975,834	B1	12/2005	Forster	
7,031,946	B1	4/2006	Tamai et al.	
7,080,819	B2	7/2006	Tojo	
7,225,337	B2	5/2007	Baessler	
7,310,734	B2	12/2007	Boate et al.	
7,487,538	B2	2/2009	Mok	
7,533,809	B1	5/2009	Robinson et al.	
7,671,746	B2	3/2010	Martinez de Velasco Cortina et al.	
7,844,505	B1	11/2010	Arneson et al.	
7,911,643	B2	3/2011	Yamada et al.	
7,980,378	B2	7/2011	Jones et al.	
8,004,410	B2	8/2011	Martinez de Velasco Cortina et al.	
8,041,815	B2	10/2011	Bahl et al.	
8,126,449	B2	2/2012	Beenau et al.	
8,401,539	B2	3/2013	Beenau et al.	
8,548,927	B2	10/2013	Beenau et al.	
2002/0089434	A1	7/2002	Ghazarian	
2002/0109580	A1	8/2002	Shreve et al.	
2002/0112177	A1	8/2002	Voltmer et al.	
2003/0001459	A1 *	1/2003	Scott	G06K 9/00885 310/339
2003/0074317	A1	4/2003	Hofi	
2003/0131247	A1 *	7/2003	Cannon	G06F 21/32 713/186
2003/0139984	A1 *	7/2003	Seigel	G06F 21/10 705/28
2003/0200227	A1	10/2003	Ressler	
2004/0059923	A1 *	3/2004	ShamRao	G06F 21/32 713/186
2004/0128249	A1 *	7/2004	Hoffman	G06F 21/32 705/44
2005/0149764	A1	7/2005	Bahl et al.	
2006/0020558	A1	1/2006	Bonalle	
2007/0022058	A1	1/2007	Labrou et al.	
2010/0094754	A1	4/2010	Bertran et al.	
2010/0095130	A1	4/2010	Bertran et al.	

FOREIGN PATENT DOCUMENTS

EP	0977145	A2	2/2000
EP	0993999	A2	4/2000
JP	2002042076	A	2/2002
WO	9843104	A2	10/1998
WO	2004006165	A1	1/2004

OTHER PUBLICATIONS

Extended European Search Report, European Patent Application No. 10182033.0, dated Jan. 13, 2012, 7 pages.

Fancher, Carol Hovenga. Motorola, Inc., In your pocket smartcards, IEEE Spectrum, Feb. 1997, 7 pages.

Rakers, et al. Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal of Solid-State Circuits, vol. 36, No. 3, Mar. 2001, 7 pages.

Japanese Office Action, Japanese Patent Application No. 2004-519130, dated May 12, 2009, 10 pages.

(56) **References Cited**

OTHER PUBLICATIONS

Anonymous, Read/write RFID offers standalone advantages, Security, Aug. 1996; 33, 8; ProQuest, 1 page.
Response to Office Action filed on Nov. 18, 2016 for U.S. Appl. No. 14/321,781.
US Office Action dated May 19, 2016 received in U.S. Appl. No. 14/321,781.
Response to Office Action filed on Dec. 24, 2015 for U.S. Appl. No. 14/321,781.
US Office Action dated Jun. 24, 2015 received in U.S. Appl. No. 14/321,781.
US Notice of Allowance dated Jul. 11, 2014 received in U.S. Appl. No. 14/022,135.
Response to Office Action filed on Mar. 14, 2014 for U.S. Appl. No. 14/022,135.
US Office Action dated Mar. 7, 2014 received in U.S. Appl. No. 14/022,135.
Response to Office Action filed on Feb. 3, 2014 for U.S. Appl. No. 14/022,135.
US Office Action dated Dec. 5, 2013 received in U.S. Appl. No. 14/022,135.
Appeal Brief filed Feb. 9, 2017 for U.S. Appl. No. 14/585,057.
Pre-Brief Appeal Conference Decision dated Nov. 30, 2016 and received in U.S. Appl. No. 14/585,057.
Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Nov. 9, 2016 for U.S. Appl. No. 14/585,057.
US Office Action dated May 9, 2016 received in U.S. Appl. No. 14/585,057.
Response to Office Action filed on Jan. 7, 2016 for U.S. Appl. No. 14/585,057.
US Office Action dated Oct. 7, 2015 received in U.S. Appl. No. 14/585,057.
US Notice of Allowance dated Dec. 3, 2014 received in U.S. Appl. No. 14/028,469.
Supplemental response to Office Action filed on Oct. 31, 2014 for U.S. Appl. No. 14/028,469.
Response to Office Action filed on Oct. 14, 2014 for U.S. Appl. No. 14/028,469.
US Office Action dated Aug. 18, 2014 received in U.S. Appl. No. 14/028,469.
US Office Action dated Jul. 9, 2014 received in U.S. Appl. No. 14/028,469.
Response to Office Action filed on Jun. 13, 2014 for U.S. Appl. No. 14/028,469.
US Office Action dated Apr. 3, 2014 received in U.S. Appl. No. 14/028,469.
Response to Office Action filed on Mar. 14, 2014 for U.S. Appl. No. 14/028,469.
US Office Action dated Mar. 6, 2014 received in U.S. Appl. No. 14/028,469.
Response to Office Action filed on Feb. 3, 2014 for U.S. Appl. No. 14/028,469.
US Office Action dated Dec. 6, 2013 received in U.S. Appl. No. 14/028,469.
Appeal Brief filed Jan. 30, 2017 for U.S. Appl. No. 14/639,034.
Pre-Brief Appeal Conference Decision dated Jul. 21, 2016 and received in U.S. Appl. No. 14/639,034.
Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Jun. 30, 2016 for U.S. Appl. No. 14/639,034.
US Office Action dated Dec. 30, 2015 received in U.S. Appl. No. 14/639,034.
Response to Office Action filed on Nov. 30, 2015 for U.S. Appl. No. 14/639,034.
US Office Action dated May 29, 2015 received in U.S. Appl. No. 14/639,034.
Response to Office Action filed on Apr. 26, 2017 for U.S. Appl. No. 14/724,593.
US Office Action dated Feb. 17, 2017 received in U.S. Appl. No. 14/724,593.
Pre-Brief Appeal Conference Decision dated Dec. 12, 2016 and received in U.S. Appl. No. 14/724,593.
Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Nov. 7, 2016 for U.S. Appl. No. 14/724,593.
US Office Action dated May 6, 2016 received in U.S. Appl. No. 14/724,593.
Response to Office Action filed on Jan. 7, 2016 for U.S. Appl. No. 14/724,593.
US Office Action dated Aug. 4, 2015 received in U.S. Appl. No. 14/724,593.
Appeal Brief filed Apr. 18, 2017 for U.S. Appl. No. 14/659,502.
Pre-Brief Appeal Conference Decision dated Nov. 30, 2016 and received in U.S. Appl. No. 14/659,502.
Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Nov. 16, 2016 for U.S. Appl. No. 14/659,502.
US Office Action dated May 16, 2016 received in U.S. Appl. No. 14/659,502.
Response to Office Action filed on Dec. 22, 2015 for U.S. Appl. No. 14/659,502.
US Office Action dated Jun. 22, 2015 received in U.S. Appl. No. 14/659,502.

* cited by examiner

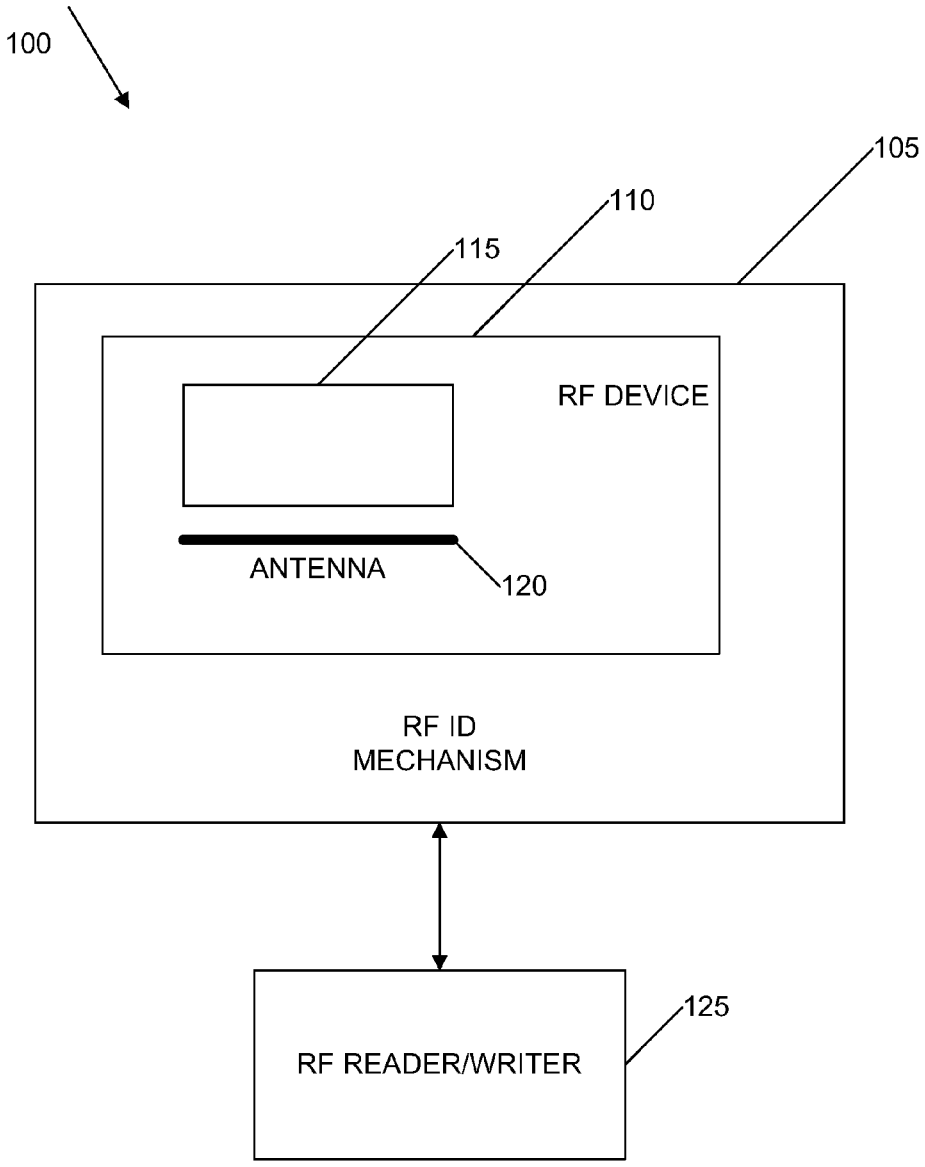

100
105
110
115
RF DEVICE
ANTENNA
120
RF ID
MECHANISM
125
RF READER/WRITER

FIG. 1

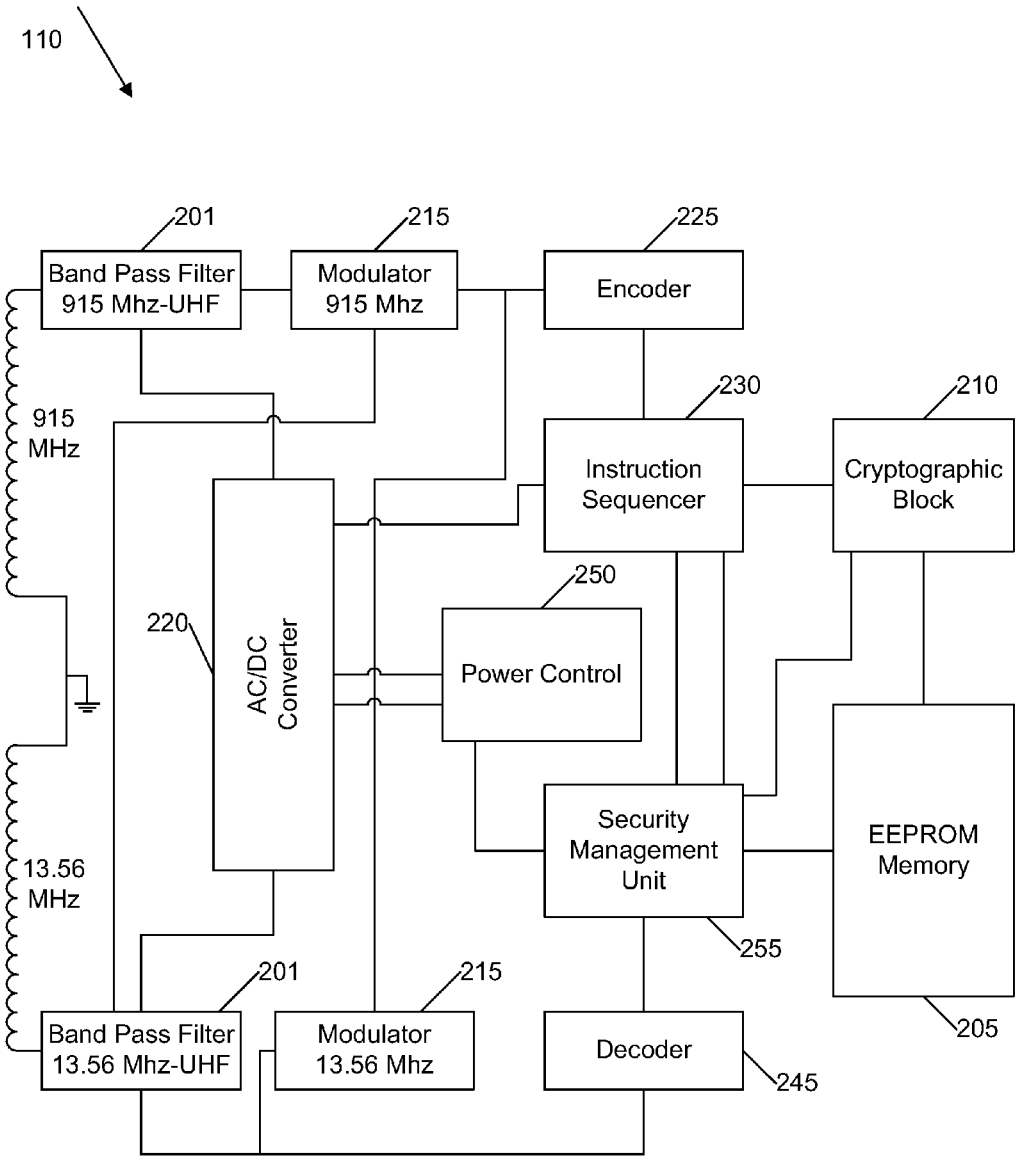

110
201
215
225
Band Pass Filter
915 Mhz-UHF
Modulator
915 Mhz
Encoder
915
MHz
230
210
Instruction
Sequencer
Cryptographic
Block
250
220
AC/DC
Converter
Power Control
Security
Management
Unit
EEPROM
Memory
13.56
MHz
255
201
215
205
Band Pass Filter
13.56 Mhz-UHF
Modulator
13.56 Mhz
Decoder
245

FIG. 2

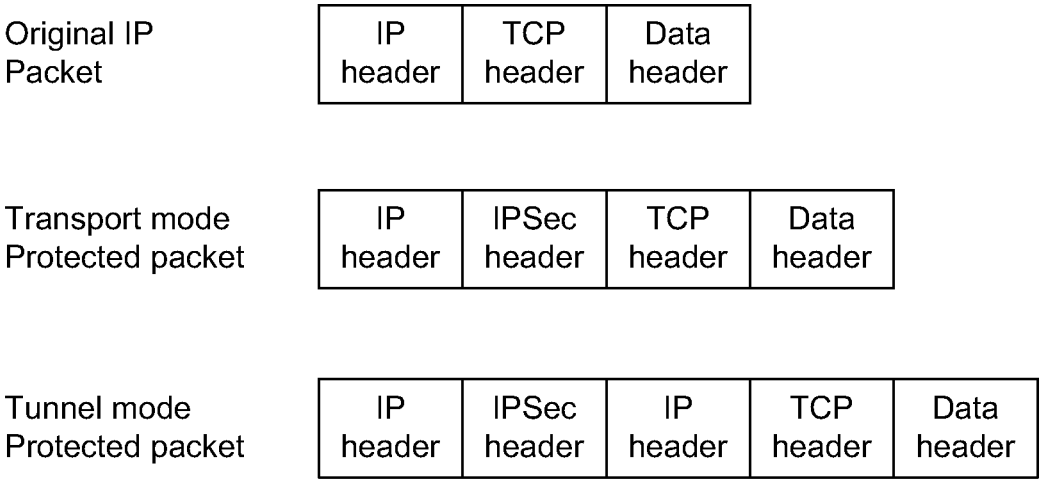

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIG. 3A

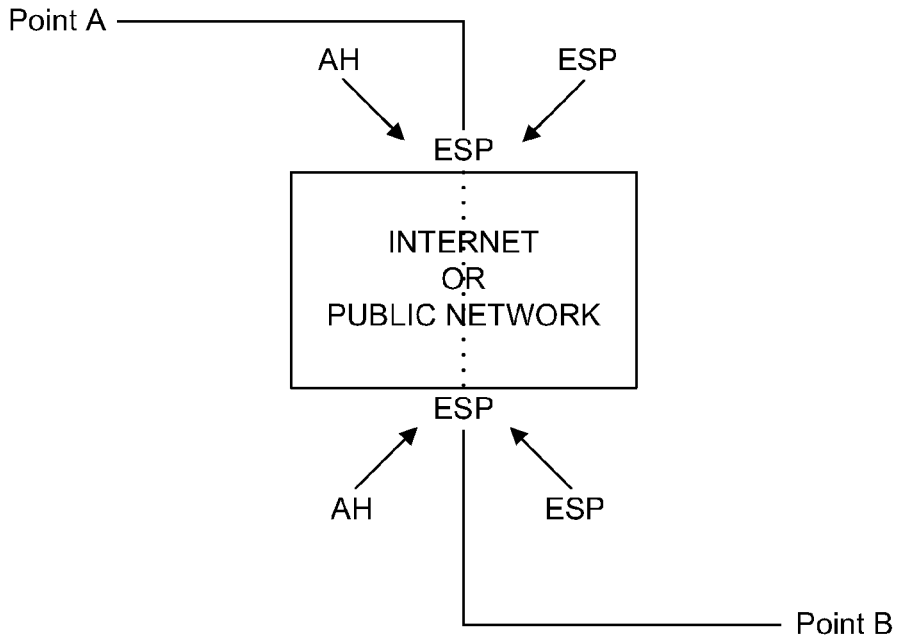

Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORK
ESP
AH
ESP
Point B

FIG. 3B

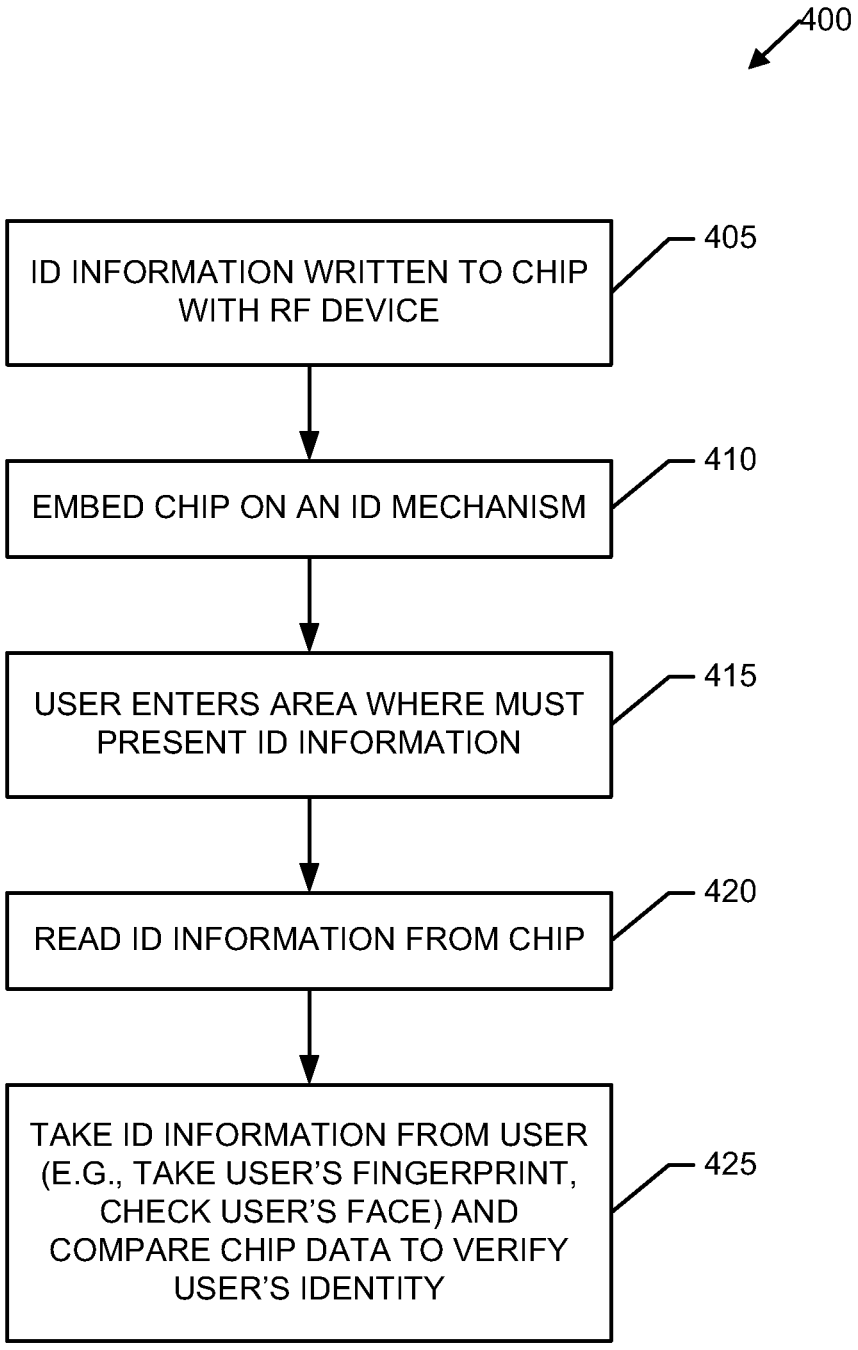

400
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
405
EMBED CHIP ON AN ID MECHANISM
410
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
415
READ ID INFORMATION FROM CHIP
420
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE CHIP DATA TO VERIFY USER'S IDENTITY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

FIG. 4

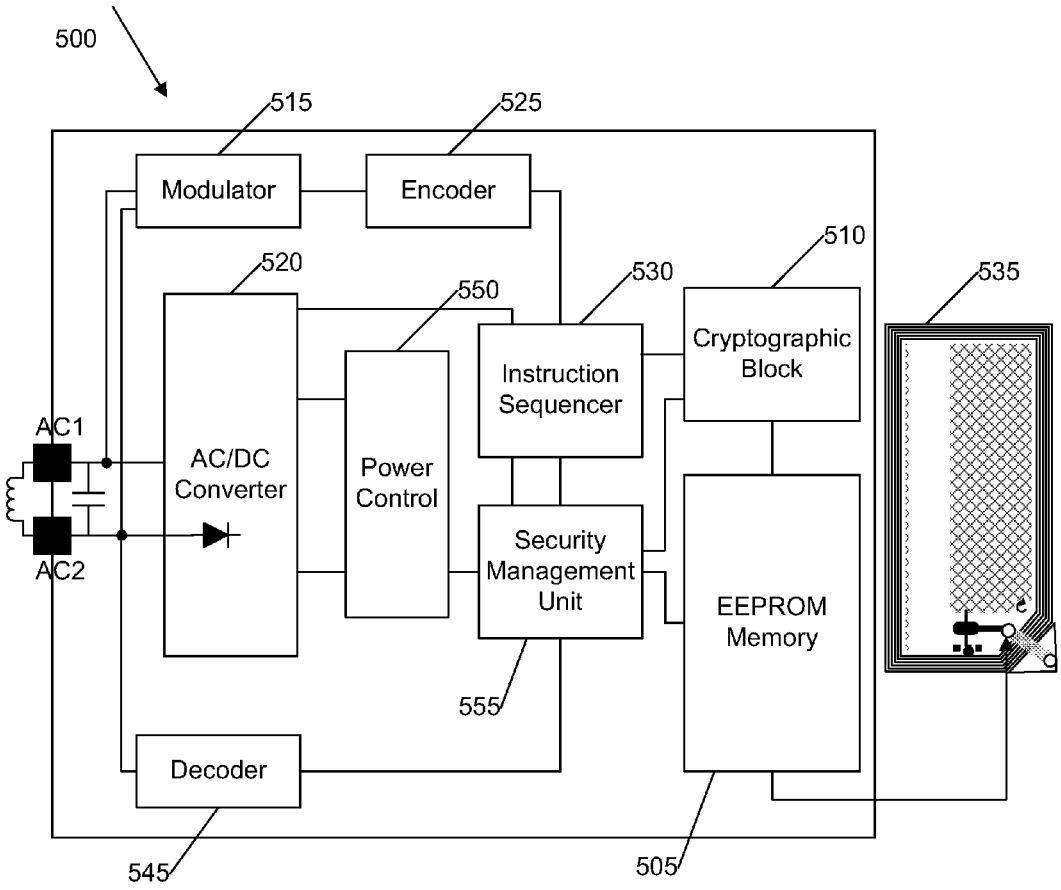

500
515
525
Modulator
Encoder
510
520
530
535
550
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
555
Decoder
545
505

FIG. 5

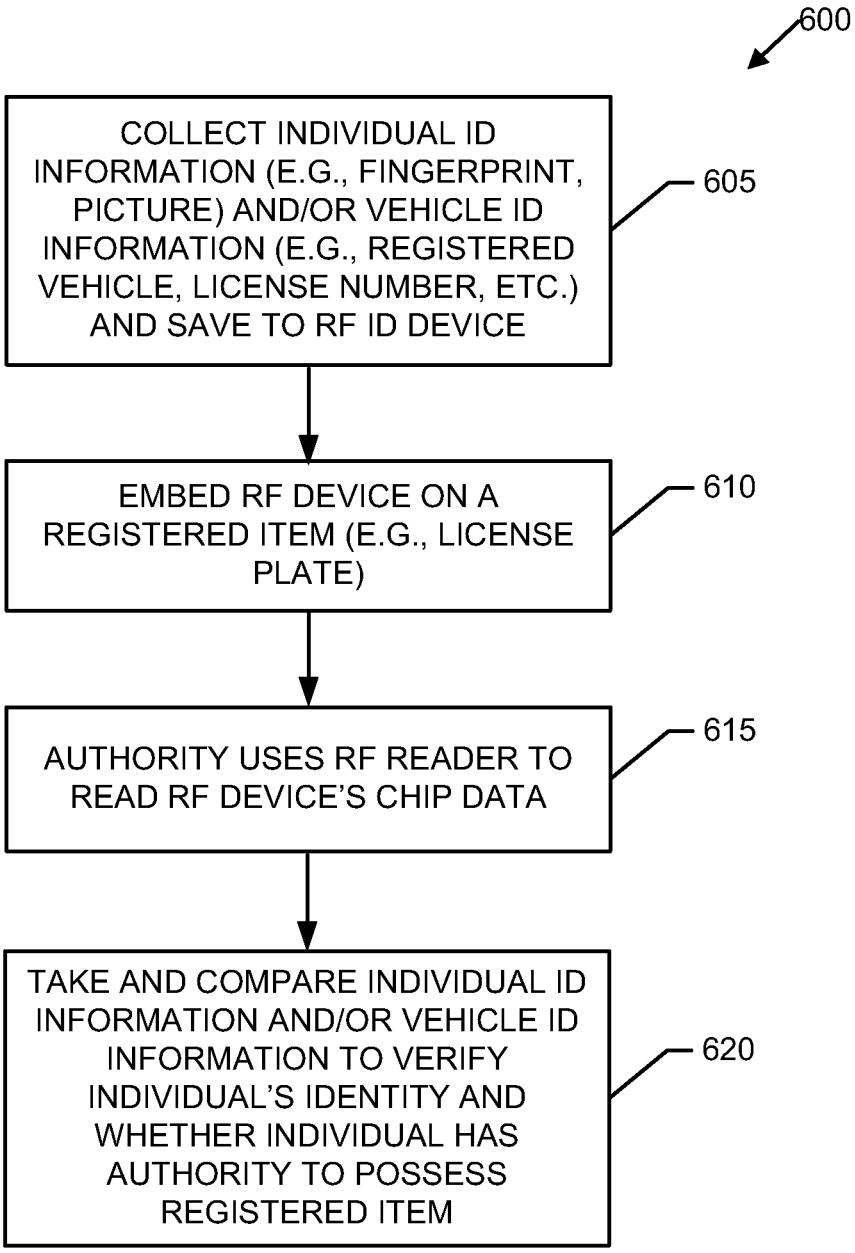

600
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
605
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
610
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
615
TAKE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

FIG. 6

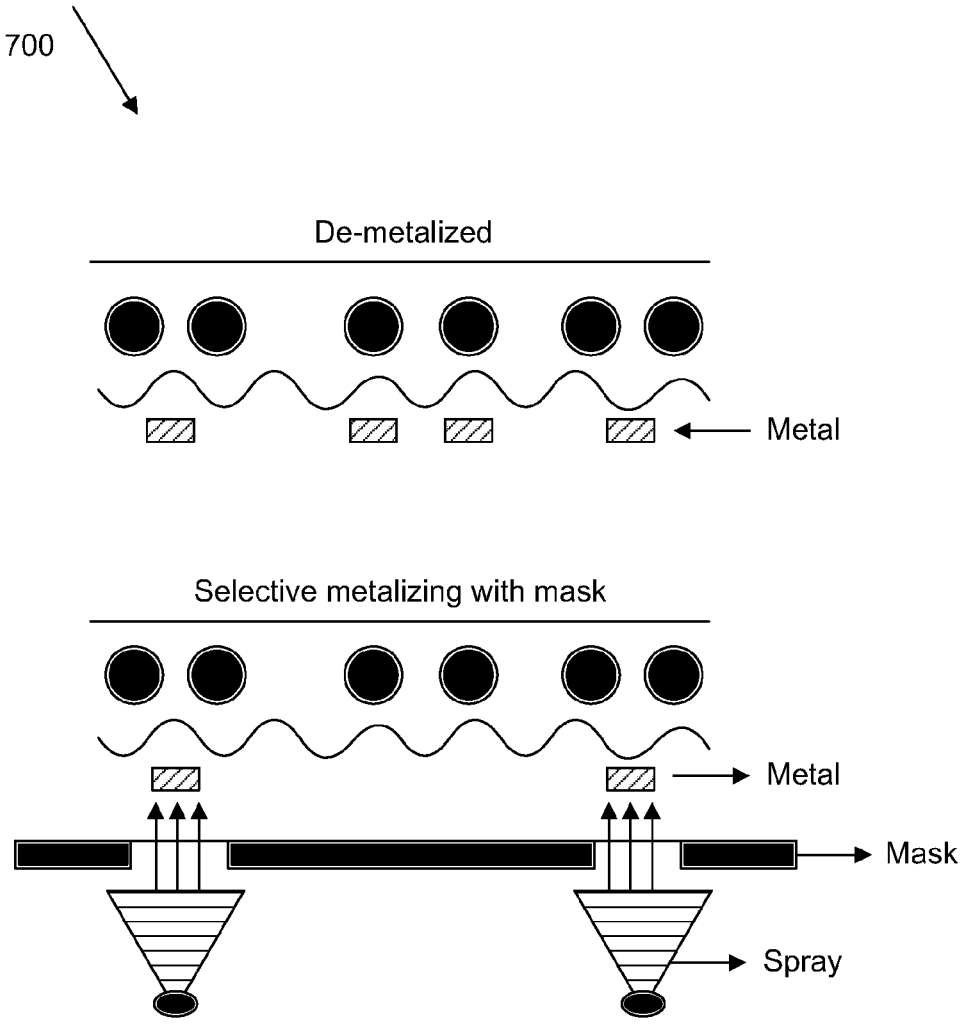

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIG. 7

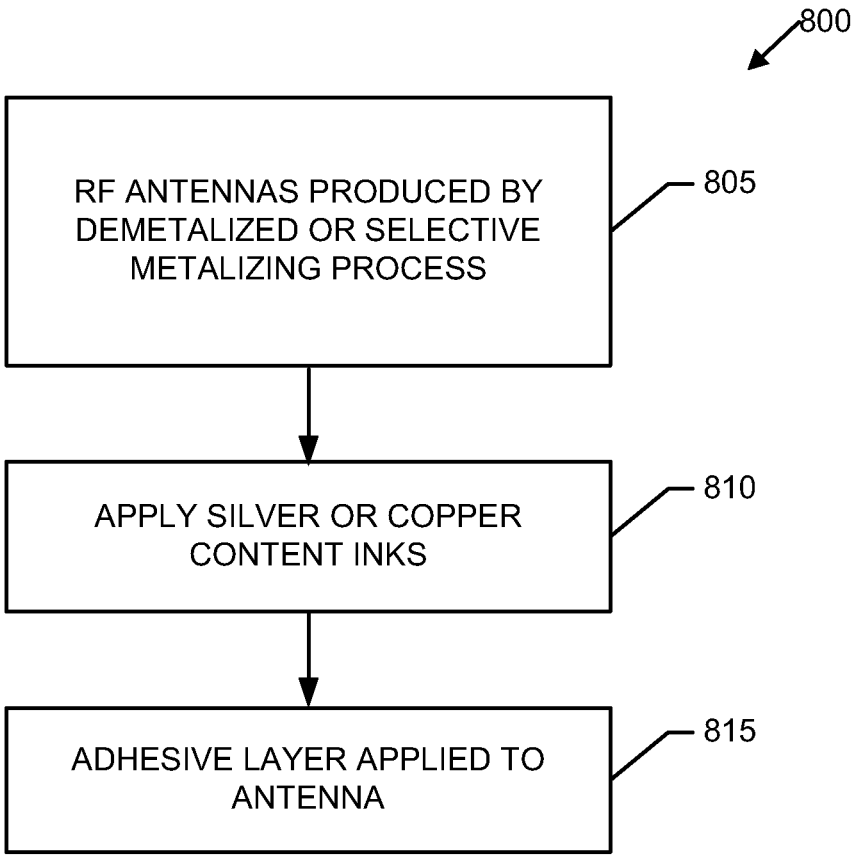

800
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
805
APPLY SILVER OR COPPER CONTENT INKS
810
ADHESIVE LAYER APPLIED TO ANTENNA
815

FIG. 8

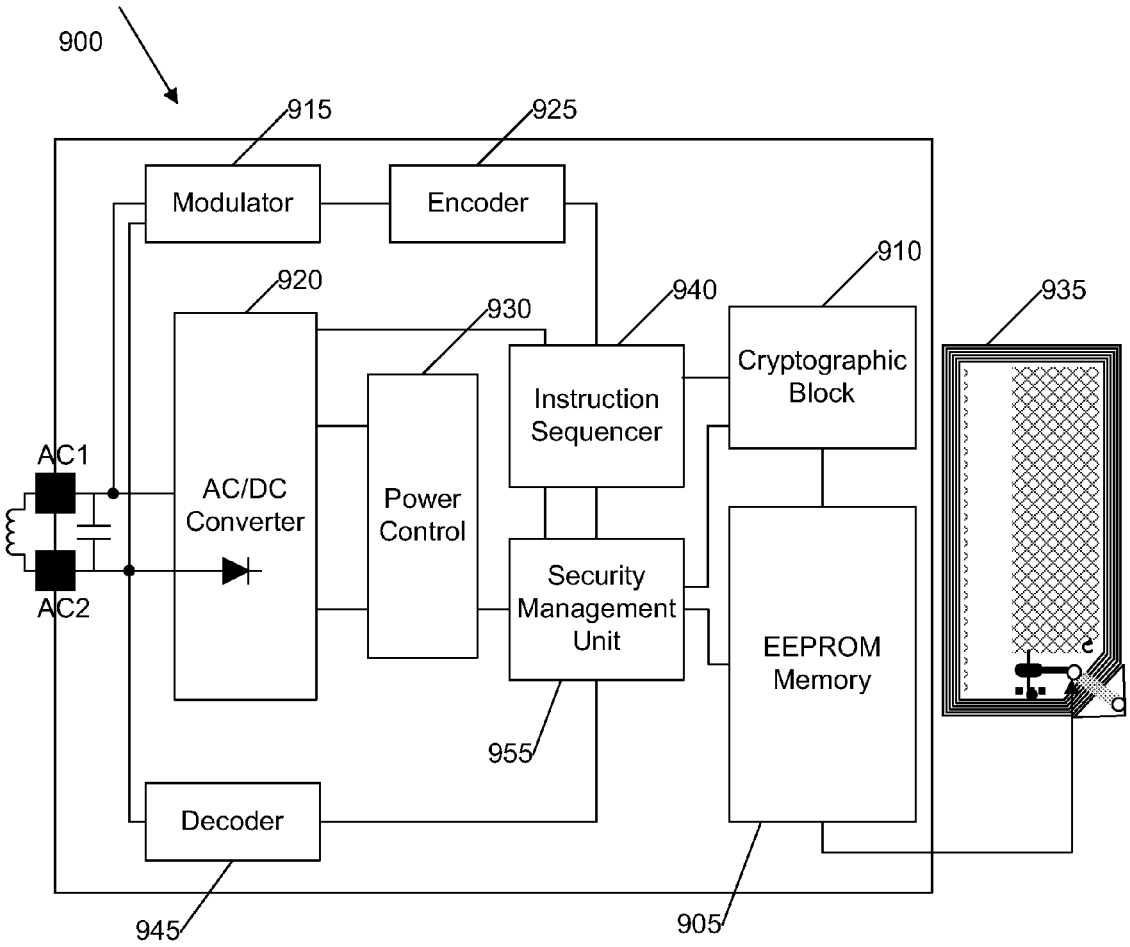

900
915
925
Modulator
Encoder
910
920
940
935
930
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
955
Decoder
945
905

FIG. 9

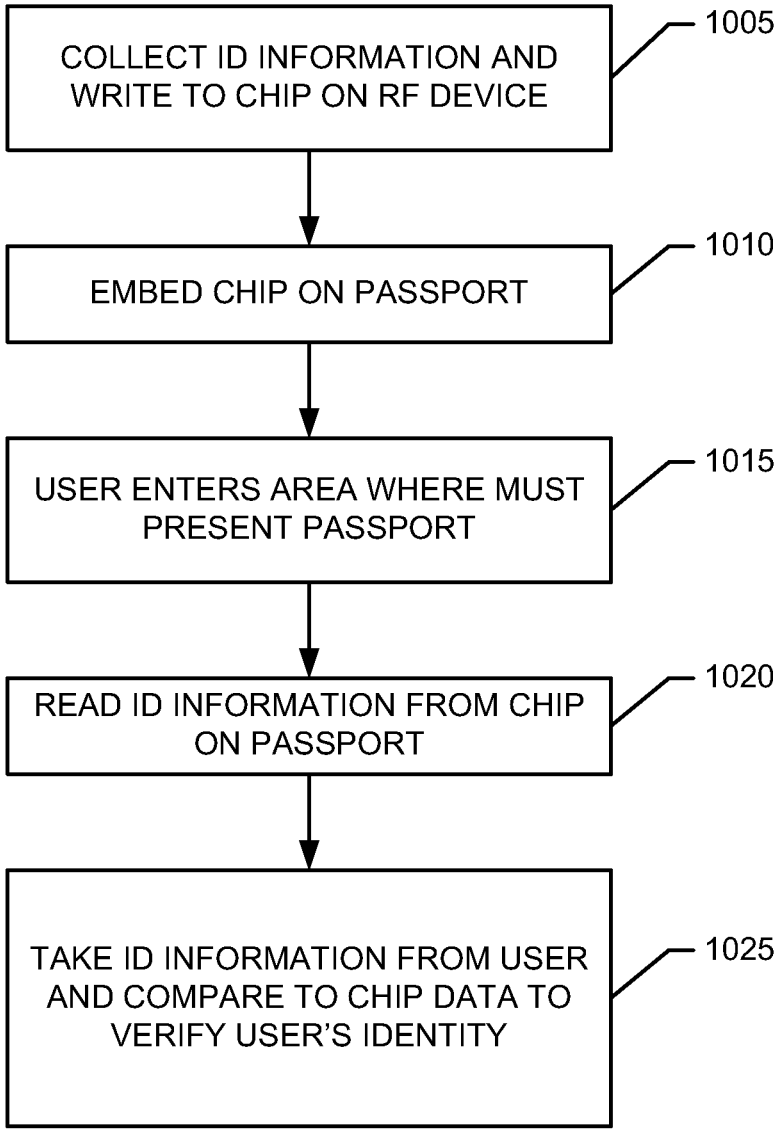

COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1005
EMBED CHIP ON PASSPORT
1010
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1015
READ ID INFORMATION FROM CHIP ON PASSPORT
1020
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY
1025

FIG. 10

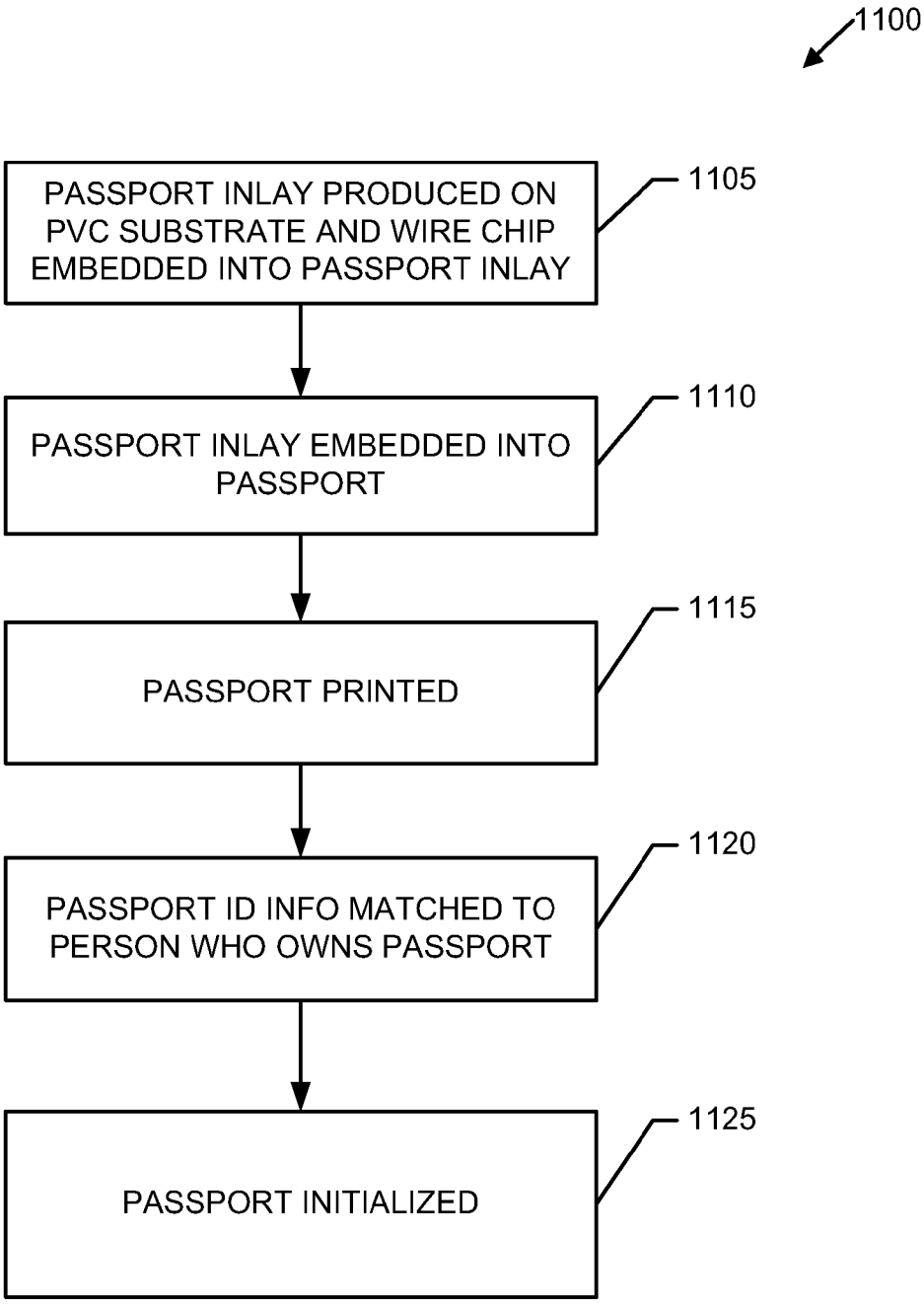

1100
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1105
PASSPORT INLAY EMBEDDED INTO PASSPORT
1110
PASSPORT PRINTED
1115
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1120
PASSPORT INITIALIZED
1125

FIG. 11

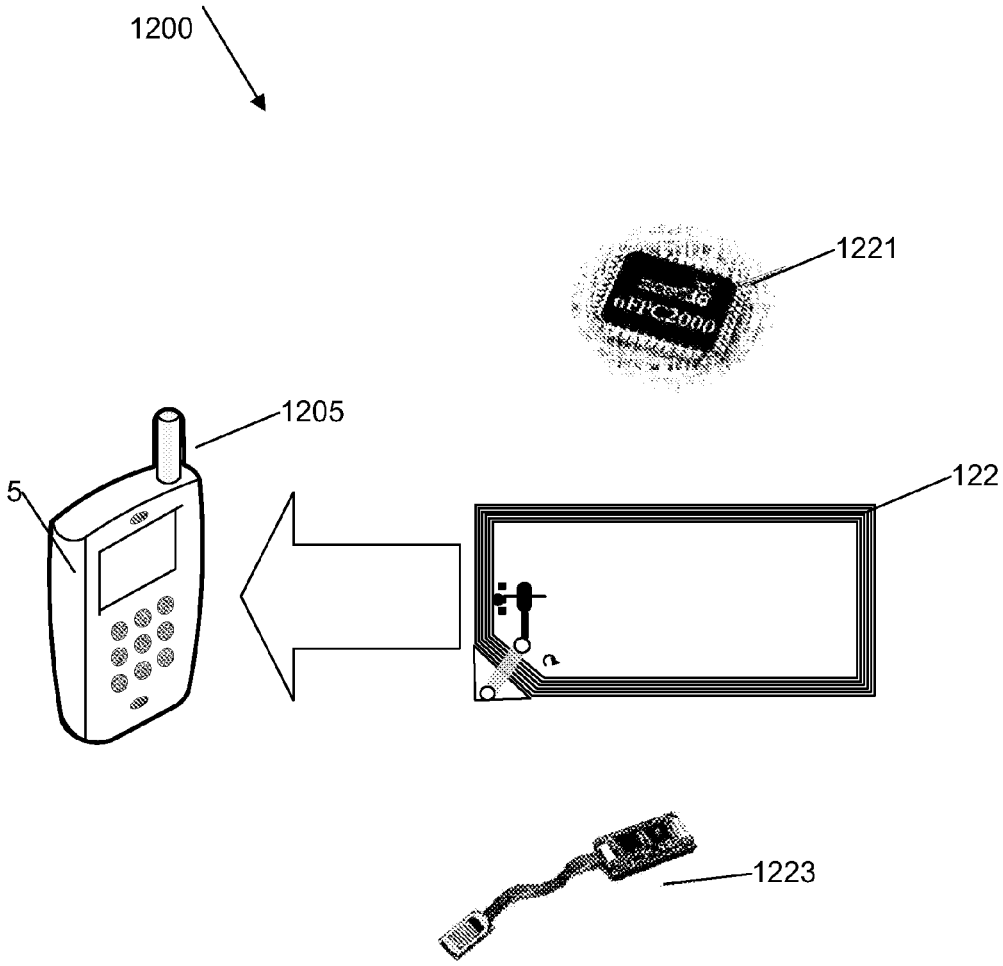


FIG. 12

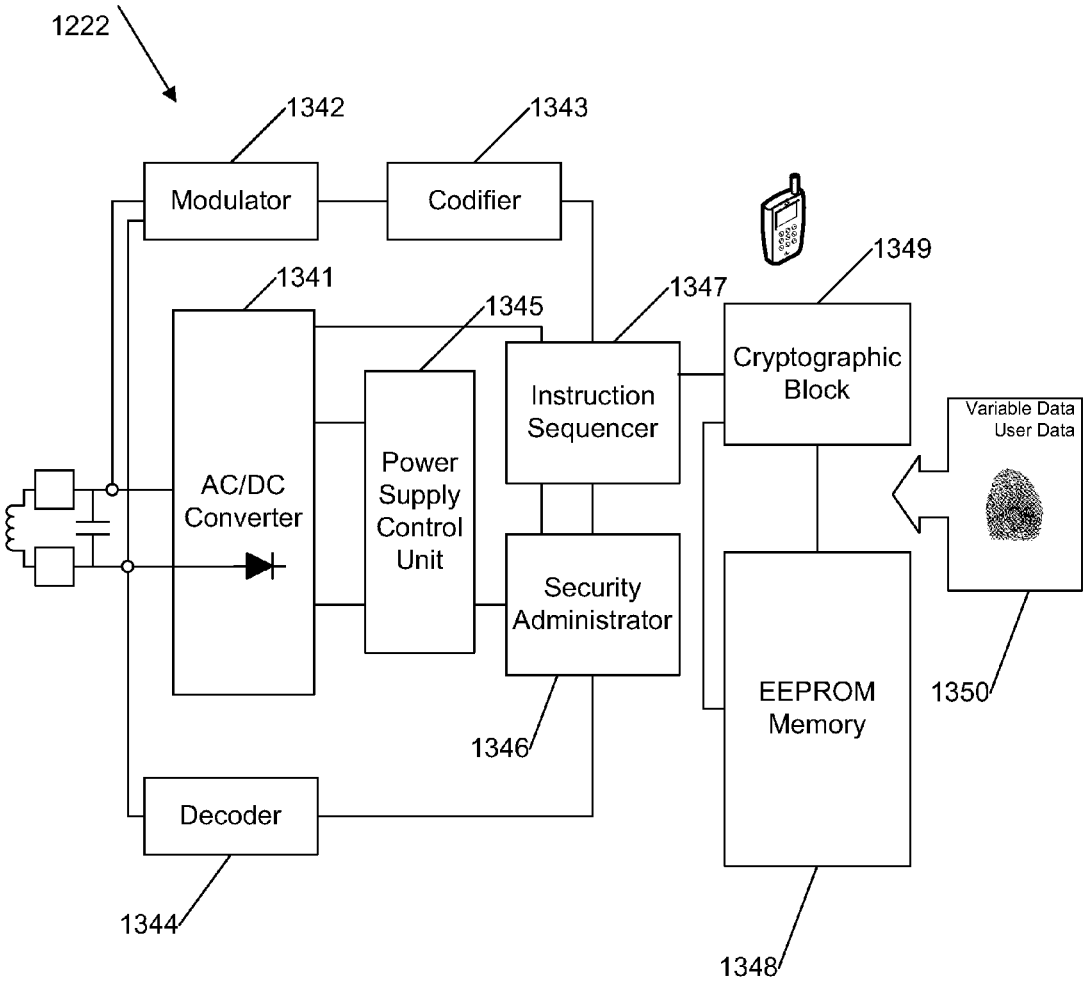

1222
1342
1343
Modulator
Codifier
1349
1341
1345
1347
Cryptographic Block
Instruction Sequencer
Variable Data
User Data
AC/DC Converter
Power Supply Control Unit
Security Administrator
EEPROM Memory
1350
1346
Decoder
1344
1348

FIG. 13

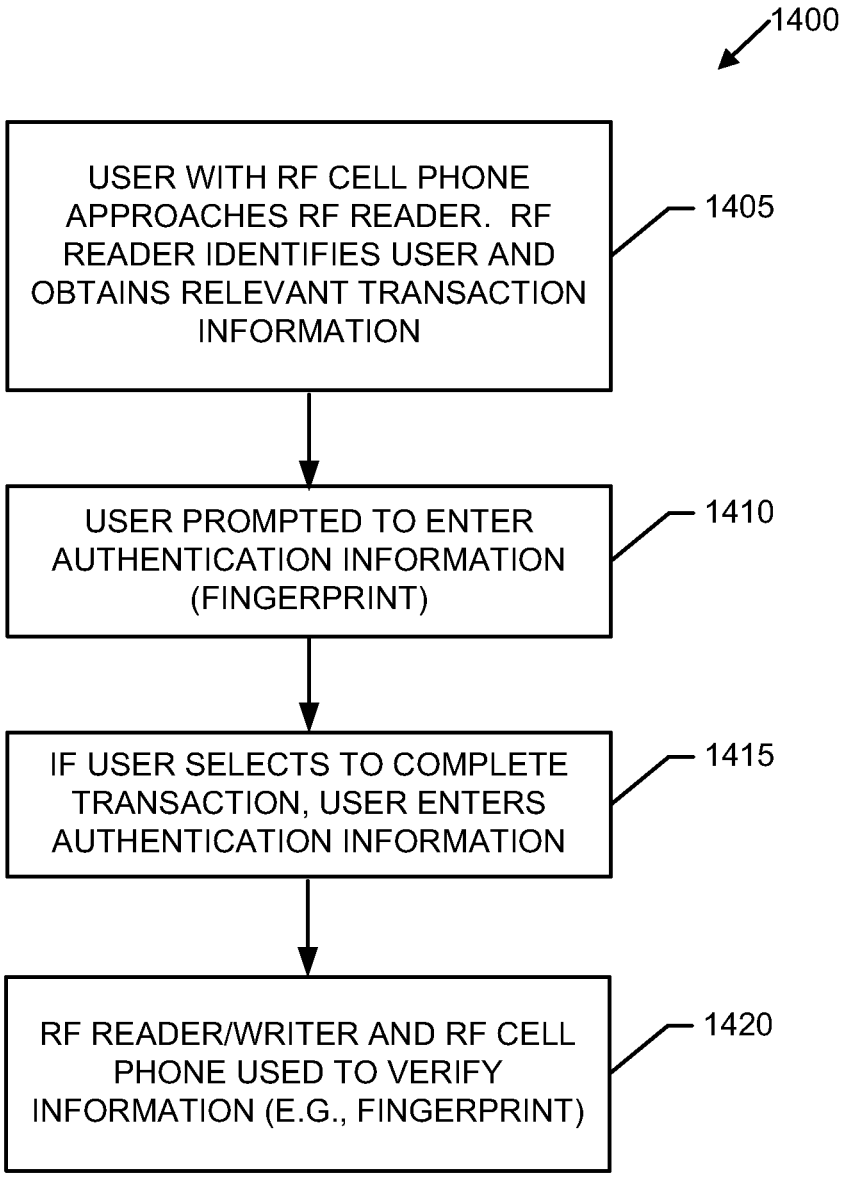

1400
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION
1405
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT)
1410
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION
1415
RF READER/WRITER AND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

FIG. 14

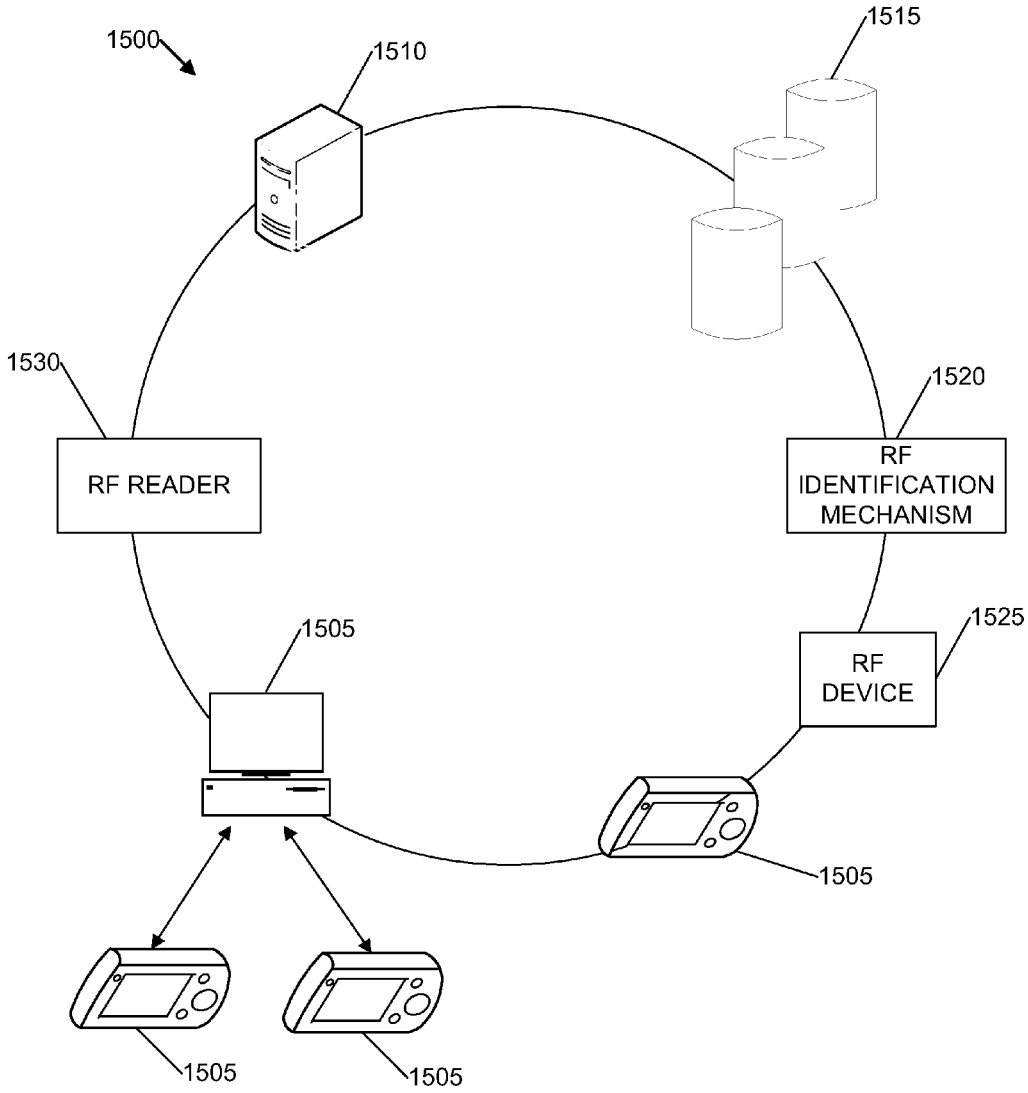

1500
1510
1515
1530
1520
RF READER
RF IDENTIFICATION MECHANISM
1505
1525
RF DEVICE
1505
1505
1505

FIG. 15

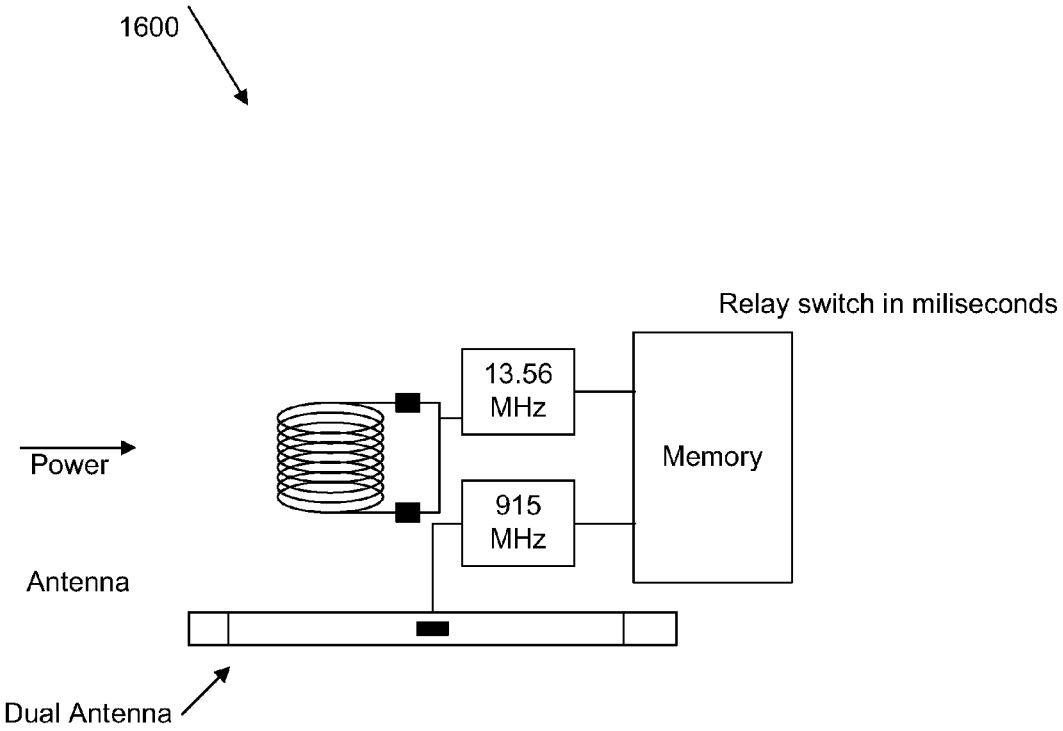

1600
Relay switch in miliseconds
13.56 MHz
915 MHz
Memory
Power
Antenna
Dual Antenna

FIG. 16

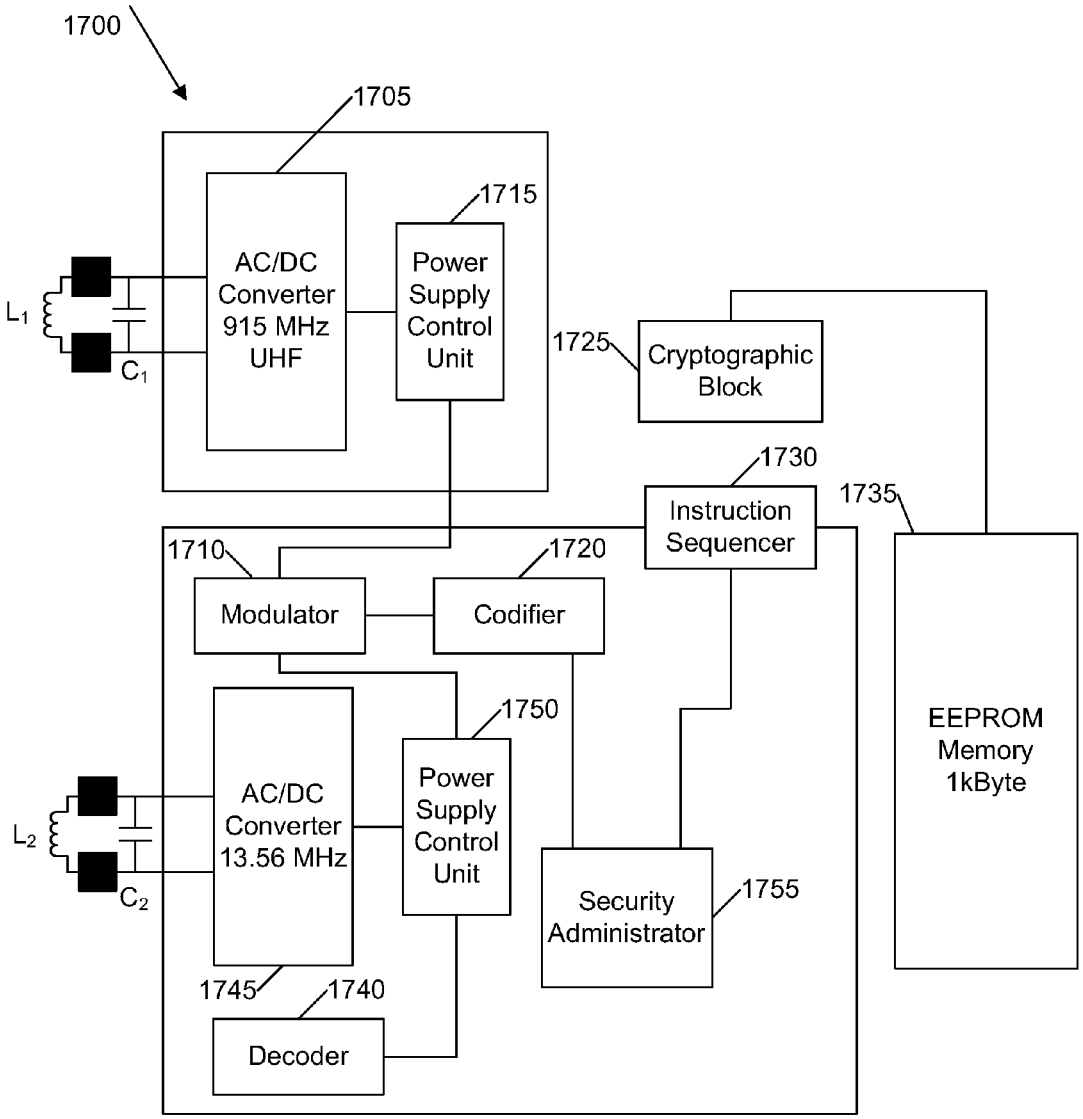

1700
1705
1715
AC/DC Converter 915 MHz UHF
Power Supply Control Unit
L1
C1
1725
Cryptographic Block
1730
Instruction Sequencer
1735
1710
1720
Modulator
Codifier
1750
AC/DC Converter 13.56 MHz
Power Supply Control Unit
L2
C2
Security Administrator
1755
EEPROM Memory 1kByte
1745
1740
Decoder

FIG. 17

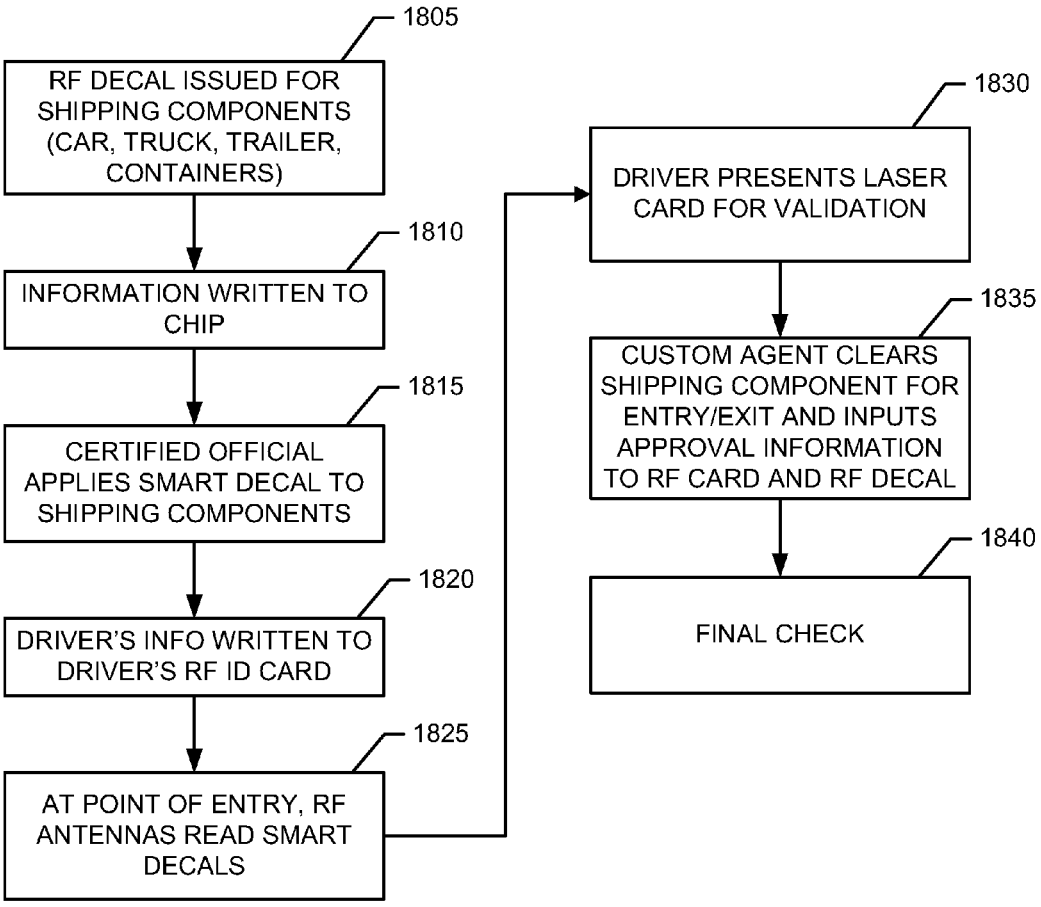

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS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

FIG. 18

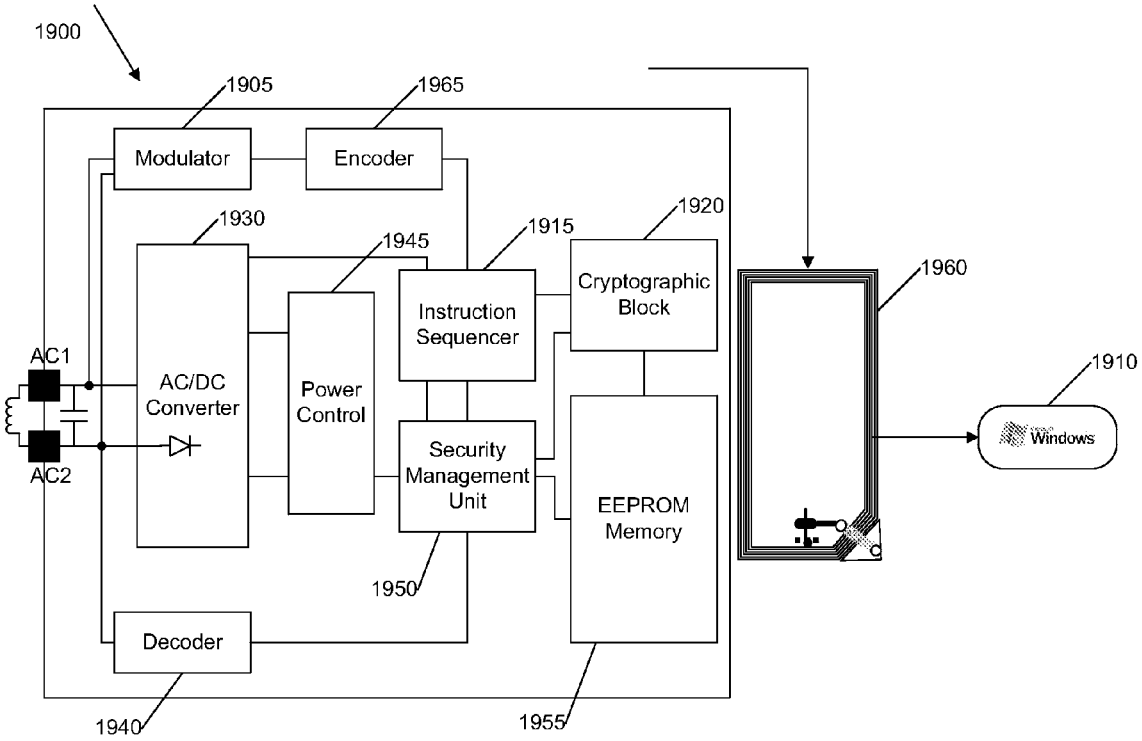

1900
1905
1965
Modulator
Encoder
1930
1945
1915
1920
Cryptographic Block
Instruction Sequencer
1960
AC1
AC/DC Converter
Power Control
1910
Windows
AC2
Security Management Unit
EEPROM Memory
1950
Decoder
1940
1955

FIG. 19

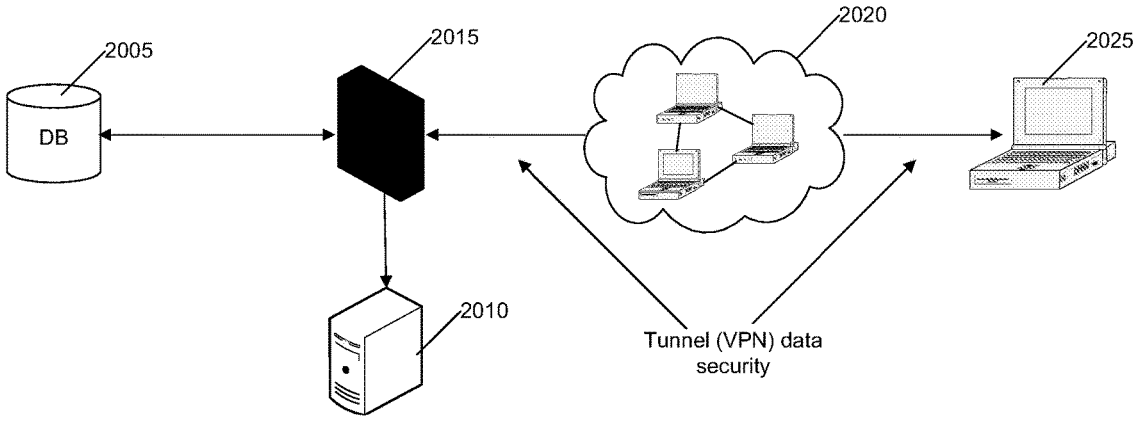


FIG. 20

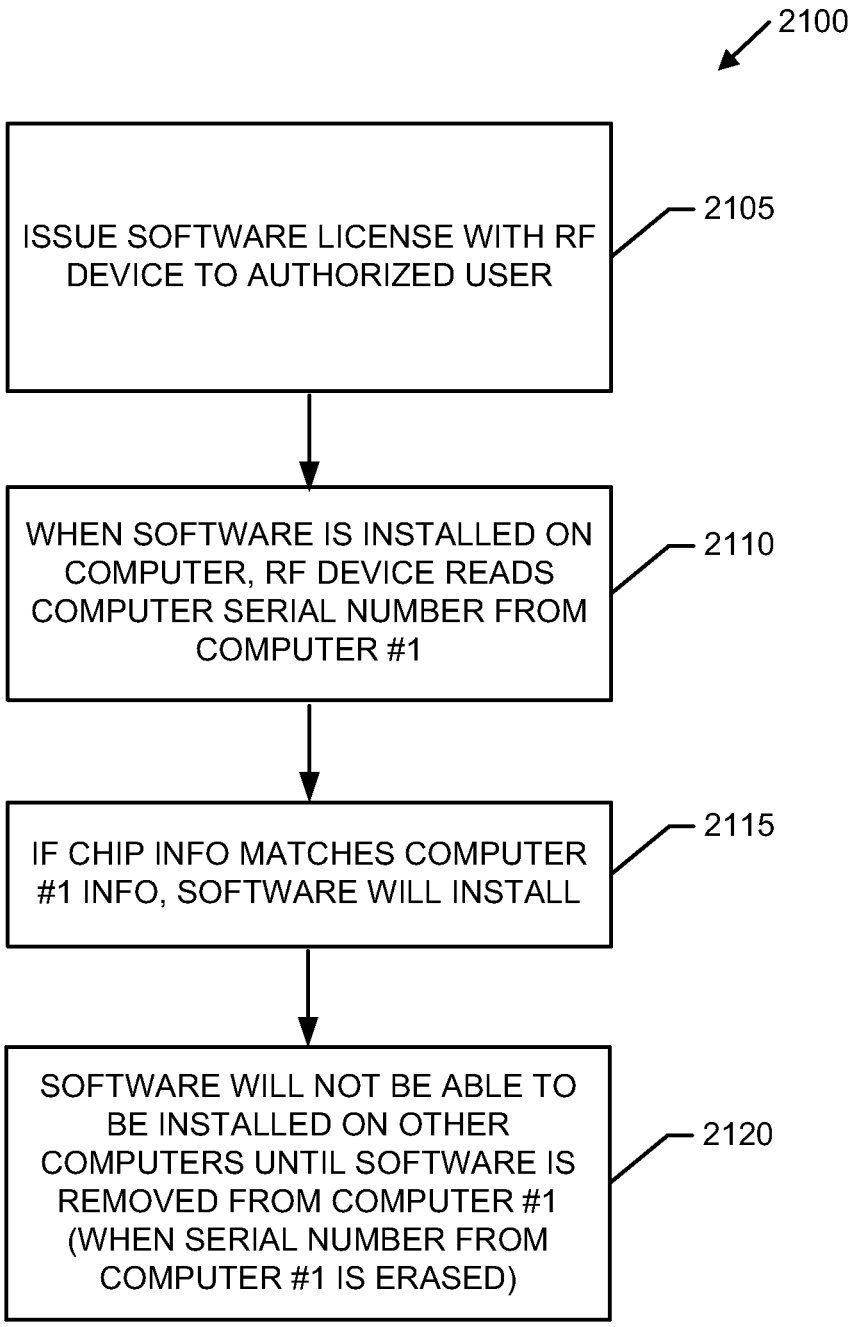

2100
ISSUE SOFTWARE LICENSE WITH RF DEVICE TO AUTHORIZED USER
2105
WHEN SOFTWARE IS INSTALLED ON COMPUTER, RF DEVICE READS COMPUTER SERIAL NUMBER FROM COMPUTER #1
2110
IF CHIP INFO MATCHES COMPUTER #1 INFO, SOFTWARE WILL INSTALL
2115
SOFTWARE WILL NOT BE ABLE TO BE INSTALLED ON OTHER COMPUTERS UNTIL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

FIG. 21

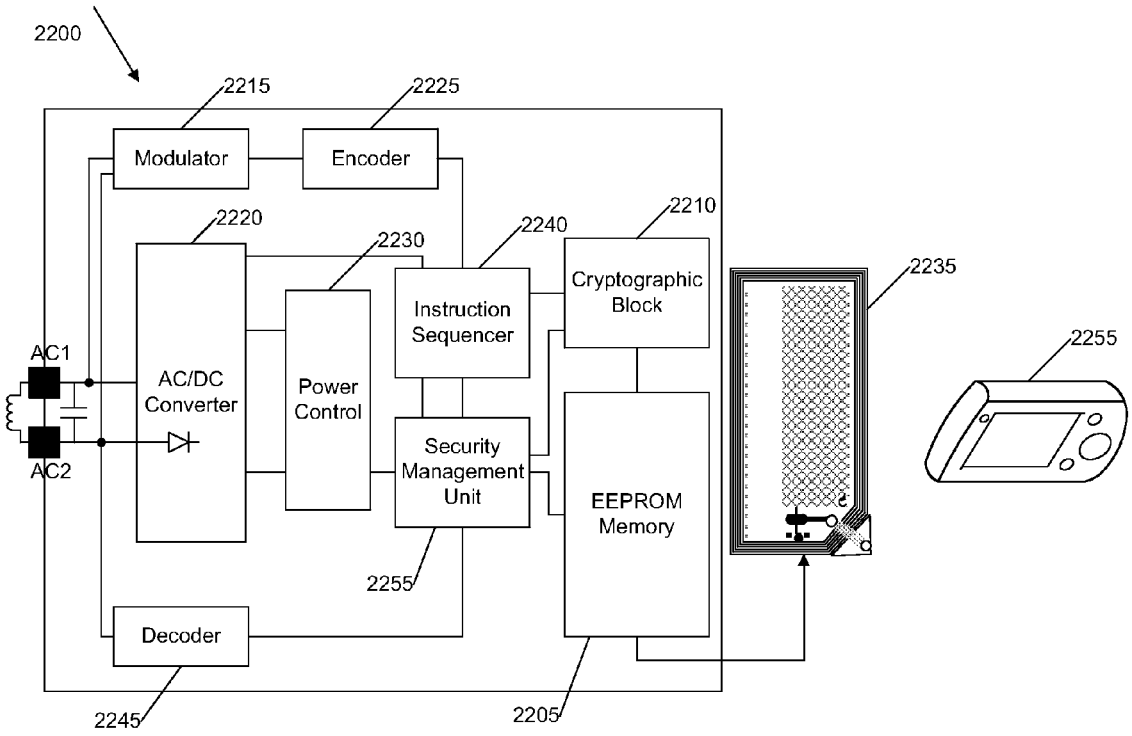

2200
2215
2225
Modulator
Encoder
2220
2230
2240
2210
2235
2255
AC1
AC2
AC/DC Converter
Power Control
Instruction Sequencer
Cryptographic Block
Security Management Unit
EEPROM Memory
2255
Decoder
2245
2205

FIG. 22

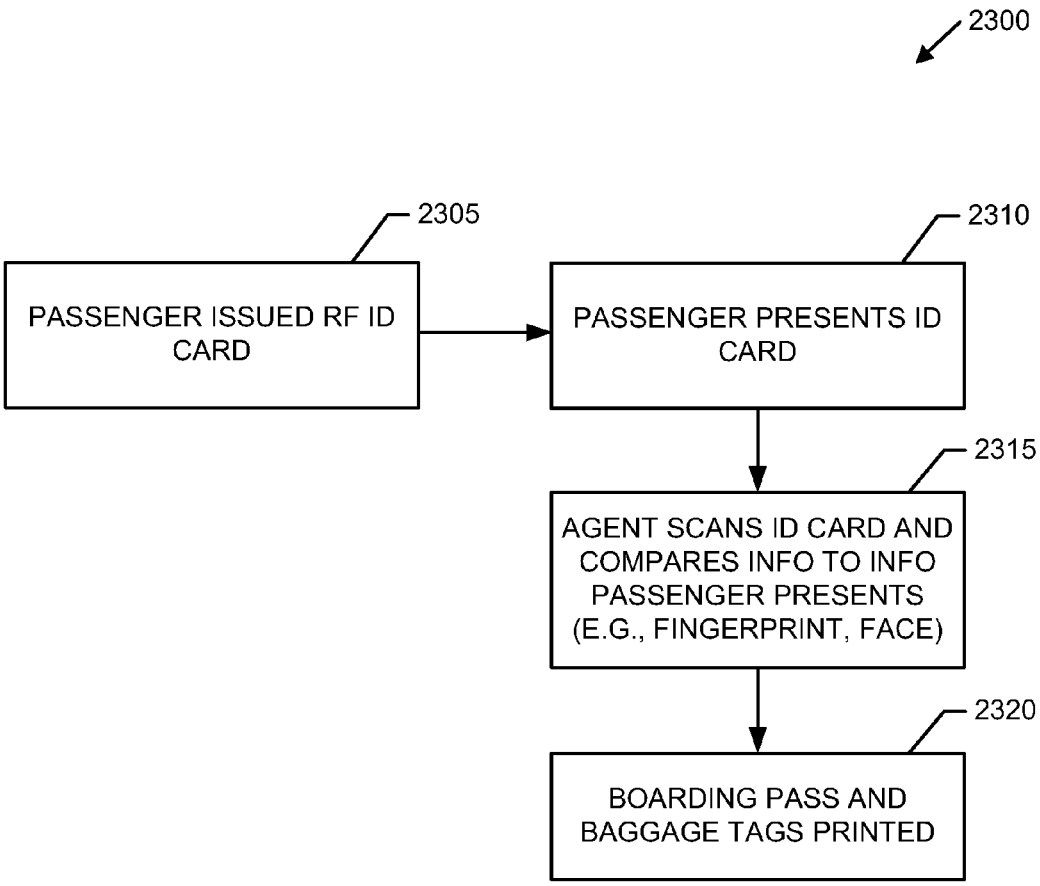

2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENT SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

FIG. 23

SYSTEM AND METHOD FOR PROVIDING SECURE IDENTIFICATION SOLUTIONS

RELATED APPLICATIONS INFORMATION

This application is a continuation of application Ser. No. 14/084,565, filed on Nov. 19, 2013 now U.S. Pat. No. 9,558,385, issued on Jan. 31, 2017, which is a continuation of Ser. No. 13/350,665, filed on Jan. 13, 2012, now U.S. Pat. No. 8,587,436, issued on Nov. 19, 2013, which is a continuation of U.S. patent application Ser. No. 13/175,768, filed on Jul. 1, 2011, now U.S. Pat. No. 8,237,568, issued on Aug. 7 2012, which is a continuation of U.S. Ser. No. 12/688,666, filed on Jan. 15, 2010, now U.S. Pat. No. 8,004,410, issued on Aug. 23, 2011, which is a continuation of U.S. application Ser. No. 11/279,912, filed on Apr. 17, 2006, now U.S. Pat. No. 7,671,746, issued on Mar. 2, 2010, which is a continuation of U.S. application Ser. No. 10/615,026, filed on Jul. 9, 2003, now U.S. Pat. No. 7,081,819, issued on Jul. 25, 2006, which in turn claims the benefit under 35 U.S.C. 119(e) to U.S. Provisional Patent Application Ser. No. 60/394,241, filed Jul. 9, 2002, all of which are incorporated herein by reference in their entirety as if set forth in full.

BACKGROUND OF THE INVENTION

Field of the Invention

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

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

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

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

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

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

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

FIGS. **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

FIG. **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

FIG. **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.

FIG. **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.

A more detailed description of an RF device can be found in U.S. patent application Ser. No. 10/118,092 filed 9 Apr. 2002; PCT Patent Application PCT/IB02/01439, filed 30 Apr. 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 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.

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, VisuaVMachine-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 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.

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 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.

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 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.

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 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.

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

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

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 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.

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 "upconversion" concept. The white powder is ground into particles that are 2-3 nm in diameter and is mixed into a clear ink media in very small concentrations. Again, as before, the combination of the white color, the small particle sizes and the low concentration causes the material to be invisible to the eye. However, this special material can be activated by several wavelengths and each activation wavelength results in a different response.

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

FIG. **4** illustrates the methods 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

FIG. **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

FIG. **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.

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 FIG. **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 material, holographic foil, or another substrate with a high metal content.

FIG. **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

FIG. **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

FIG. **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

FIG. **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 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.

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

FIG. **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 ensures 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 FIG. **13**. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt **1348**, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements are not met, a user cannot access the memory of the chip. The chip includes an ACDC converter **1341** and a connection to an RF antenna for power using a power supply control unit **1345**. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator **1342** is a device that receives baseband signals from an antenna. An AC/DC converter **1341** is a device that receives

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

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

FIG. **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 FIG. **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 Ser. No. 10/118,092, filed Apr. 2, 2002, and PCT Patent Application 180201439, filed Apr. 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

FIG. **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 24×7; 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 1Developer, Oracle's flagship J2EE and XML development environment that supports the full development life cycle of J2EE applications and Web services. It also includes Oracle9i Forms Developer for easily and quickly construct sophisticated database forms and business logic delivered through any Internet browser as a high performance, rich Java client.

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 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.

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 FIG. **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

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

N = number of windings around inductor

μ_o = permeability of freespace $((\mathrm{Hm})^{-1})$

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:

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

-continued

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

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

For substitution, the following values are used:

$$L_1 = 2.931 \times 10^8 \text{H}$$

$$L_2 = 6.437 \times 10^{10} \text{H}$$

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

FIG. **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

FIG. **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

FIG. **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.

FIG. **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 appro-

priate 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.

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

B. Method of Limiting Software Downloads

FIG. **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

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

B. Method of Airport Security

FIG. **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 mobile device, comprising:
- a biometric input device configured to receive biometric data;
- a short range radio frequency circuit;
- memory configured to store biometric information for identifying an individual associated with transaction information;
- a processor coupled with the memory and the biometric input device, the processor configured to:
  - receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,
  - receive the biometric data from the biometric input device,
  - compare the received biometric data with the biometric information stored in the memory, and
  - transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received biometric data matches the stored biometric information; and
- a mobile device body housing the biometric input device, short range radio frequency circuit, memory, and processor.

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

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

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

5. The mobile device of claim **1**, wherein the transaction information is account information.

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

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

8. The mobile device of claim **7**, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

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

10. The mobile device of claim **1**, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

11. A cellular telephone, comprising:
- a fingerprint scanner configured to receive fingerprint data;
- a short range radio frequency circuit;
- memory configured to store fingerprint information for identifying an individual associated with transaction information;
- a processor coupled with the memory and the fingerprint scanner, the processor configured to:
  - receive a signal from a point of sale terminal via the short range radio frequency circuit, the signal comprising a request to access the memory and retrieve the transaction information,
  - receive the fingerprint data from the fingerprint scanner,
  - compare the received fingerprint data with the fingerprint information stored in the memory, and
  - transmit the transaction information to the point of sale terminal using the short range radio frequency circuit when the received fingerprint data matches the stored fingerprint information; and
- a mobile device body housing the fingerprint scanner, short range radio frequency circuit, memory, and processor.

12. The cellular telephone of claim **11**, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.

13. The cellular telephone of claim **11**, wherein the transaction information is account information.

14. The cellular telephone of claim **11**, wherein the transaction information is credit card information.

15. The cellular telephone of claim **11**, further comprising memory configured to store the transaction information.

16. The cellular telephone of claim **15**, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

17. The cellular telephone of claim **11**, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

18. The cellular telephone of claim **11**, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

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

20. The cellular telephone of claim 19, wherein the processor is further configured to transmit the received fingerprint data or the stored fingerprint information with the transaction information.

21. The cellular telephone of claim 19, wherein the transaction information is account information.

22. The cellular telephone of claim 19, wherein the transaction information is credit card information.

23. The cellular telephone of claim 19, further comprising memory configured to store the transaction information.

24. The cellular telephone of claim 23, wherein the memory configured to store the biometric information and the memory configured to store the transaction information are the same memory.

25. The cellular telephone of claim 19, wherein the processor is configured to compare the received fingerprint data with the fingerprint information stored in the memory in response to receiving the request to retrieve the transaction information.

26. The cellular telephone of claim 19, wherein the short range radio frequency circuit operates at a frequency of approximately 13.56 MHz.

* * * * *

EXHIBIT 6

US010706412B2

(12) **United States Patent**
Martinez de Velasco Cortina et al.

(10) **Patent No.: US 10,706,412 B2**
(45) **Date of Patent: *Jul. 7, 2020**

(54) **SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS**

(71) Applicant: **NEOLOGY, INC.**, Poway, CA (US)

(72) Inventors: **Francisco Martinez de Velasco Cortina**, La Jolla, CA (US); **Manfred Rietzler**, Marktoberdorf (DE)

(73) Assignee: **NEOLOGY, INC.**, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/639,034**

(22) Filed: **Mar. 4, 2015**

(65) **Prior Publication Data**

US 2015/0186884 A1 Jul. 2, 2015

Related U.S. Application Data

(63) Continuation of application No. 14/321,781, filed on Jul. 1, 2014, which is a continuation of application No. 14/022,135, filed on Sep. 9, 2013, now Pat. No. 8,766,772, which is a continuation of application No. 13/350,665, filed on Jan. 13, 2012, now Pat. No.
(Continued)

(51) **Int. Cl.**

G06Q 20/36	(2012.01)
G06Q 20/32	(2012.01)
H04W 4/80	(2018.01)
H04W 12/06	(2009.01)
H04W 12/00	(2009.01)
H04W 12/08	(2009.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/3674*** (2013.01); ***G06Q 20/3278*** (2013.01); *H04W 4/80* (2018.02); *H04W 12/00* (2013.01); *H04W 12/06* (2013.01); *H04W 12/08* (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,529,870 A 7/1985 Chaum
5,552,789 A 9/1996 Schuermann
(Continued)

FOREIGN PATENT DOCUMENTS

DE 19608757 A1 9/1997
DE 10042805 A1 3/2002
(Continued)

OTHER PUBLICATIONS

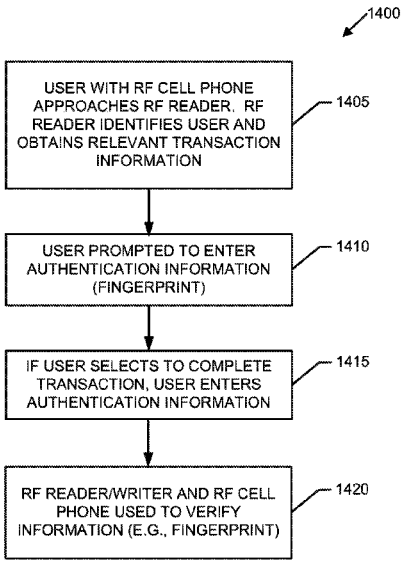
RFID Handbook—Active Load Modulation.*
(Continued)

Primary Examiner — El Mehdi Oussir
(74) *Attorney, Agent, or Firm* — Procopio, Cory, Hargreaves & Savitch LLP; Mark W. Catanese

(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.

7 Claims, 24 Drawing Sheets



Related U.S. Application Data

8,587,436, which is a continuation of application No. 13/175,768, filed on Jul. 1, 2011, now Pat. No. 8,237,568, which is a continuation of application No. 12/688,666, filed on Jan. 15, 2010, now Pat. No. 8,004,410, which is a continuation of application No. 11/279,912, filed on Apr. 17, 2006, now Pat. No. 7,671,746, which is a continuation of application No. 10/615,026, filed on Jul. 9, 2003, now Pat. No. 7,081,819.

(60) Provisional application No. 60/394,241, filed on Jul. 9, 2002.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,590,197	A *	12/1996	Chen	G06Q 20/04 380/30
5,627,544	A	5/1997	Snodgrass et al.	
5,657,008	A	8/1997	Bantli	
5,742,618	A	4/1998	Lowe	
5,787,174	A	7/1998	Tuttle	
5,819,234	A	10/1998	Slavin et al.	
5,864,580	A	1/1999	Lowe et al.	
5,874,896	A	2/1999	Lowe et al.	
5,940,006	A	8/1999	MacLellan et al.	
5,974,500	A	10/1999	Maletsky et al.	
6,016,476	A	1/2000	Maes	
6,025,780	A	2/2000	Bowers et al.	
6,025,784	A	2/2000	Mish	
6,044,382	A *	3/2000	Martino	G06F 9/466 348/E7.081
6,049,710	A *	4/2000	Nilsson	H04M 3/42204 379/88.03
6,052,068	A	4/2000	Price et al.	
6,073,840	A	6/2000	Marion et al.	
6,089,284	A	7/2000	Kaehler	
6,098,879	A	8/2000	Terranova et al.	
6,104,281	A	8/2000	Heinrich et al.	
6,111,506	A	8/2000	Yap et al.	
6,140,941	A	10/2000	Dwyer et al.	
6,157,333	A	12/2000	Louagie et al.	
6,163,771	A *	12/2000	Walker	G06Q 20/04 705/18
6,167,333	A	12/2000	Gehlot et al.	
6,175,922	B1	1/2001	Wang	
6,182,894	B1	2/2001	Hackett et al.	
6,203,952	B1	3/2001	O'Brien et al.	
6,211,790	B1	4/2001	Radomsky et al.	
6,259,405	B1 *	7/2001	Stewart	H04M 15/8033 342/457
6,268,796	B1	7/2001	Gnadinger et al.	
6,269,292	B1	7/2001	Kokubu et al.	
6,275,157	B1	8/2001	Mays et al.	
6,276,607	B1	8/2001	Sato	
6,334,059	B1	12/2001	Stilp et al.	
6,340,116	B1	1/2002	Cecil et al.	
6,360,208	B1	3/2002	Ohanian et al.	
6,388,579	B1	5/2002	Adcox et al.	
6,427,504	B1	8/2002	Janssen et al.	
6,570,487	B1	5/2003	Steeves	
6,570,488	B2	5/2003	Kucharczyk et al.	
6,617,961	B1	9/2003	Janssen et al.	
6,698,653	B1	3/2004	Diamond et al.	
6,753,759	B2	6/2004	Stegmaier et al.	
6,758,405	B2	7/2004	Look	
6,793,134	B2	9/2004	Clark	
6,796,490	B1 *	9/2004	Drummond	G06Q 20/32 235/379
6,848,048	B1 *	1/2005	Holmes	G06F 21/64 713/162
6,850,147	B2	2/2005	Prokoski	
6,894,615	B2	5/2005	Look	
6,934,689	B1 *	8/2005	Ritter	G06Q 20/04 705/16
6,934,861	B2	8/2005	Haala	
6,950,013	B2	9/2005	Scaman et al.	
6,975,834	B1	12/2005	Forster	
7,031,946	B1	4/2006	Tamai et al.	
7,080,819	B2	7/2006	Tojo	
7,081,819	B2	7/2006	Martinez de Velasco Cortina et al.	
7,096,363	B2	8/2006	Kon	
7,225,337	B2	5/2007	Baessler	
7,310,734	B2	12/2007	Boate et al.	
7,487,538	B2	2/2009	Mok	
7,533,809	B1	5/2009	Robinson et al.	
7,671,746	B2	3/2010	Martinez de Velasco Cortina et al.	
7,844,505	B1	11/2010	Arneson et al.	
7,911,643	B2 *	3/2011	Yamada	H04N 1/33307 358/1.15
7,980,378	B2	7/2011	Jones et al.	
7,987,501	B2	7/2011	Miller et al.	
8,004,410	B2	8/2011	Martinez de Velasco Cortina et al.	
8,041,815	B2	10/2011	Bahl et al.	
8,126,449	B2	2/2012	Beenau et al.	
8,237,568	B2	8/2012	Martinez de Velasco Cortina et al.	
8,325,044	B2	12/2012	Martinez de Velasco Cortina et al.	
8,401,539	B2	3/2013	Beenau et al.	
8,548,927	B2	10/2013	Beenau et al.	
8,587,436	B2	11/2013	Martinez de Velasco Cortina et al.	
8,766,772	B2 *	7/2014	Martinez de Velasco Cortina	H04W 12/00 340/5.8
9,558,385	B2	1/2017	Martinez de Velasco Cortina et al.	
9,858,566	B2 *	1/2018	Mardikar	H04W 12/06
2001/0044900	A1 *	11/2001	Uchida	G06Q 20/40 713/186
2002/0010684	A1 *	1/2002	Moskowitz	G06F 21/10 705/75
2002/0040327	A1 *	4/2002	Owa	G06Q 10/10 705/26.1
2002/0073416	A1 *	6/2002	Ramsey Catan	G07C 9/37 725/6
2002/0089434	A1	7/2002	Ghazarian	
2002/0109580	A1	8/2002	Shreve	
2002/0112171	A1 *	8/2002	Ginter	G06F 21/10 713/185
2002/0112177	A1 *	8/2002	Voltmer	G06Q 20/40145 726/26
2002/0123325	A1 *	9/2002	Cooper	H04L 63/0492 455/411
2002/0157029	A1 *	10/2002	French	G06F 21/31 726/21
2002/0193142	A1 *	12/2002	Stavenow	G06F 21/41 455/556.1
2002/0194499	A1 *	12/2002	Audebert	H04L 63/0853 726/35
2003/0004827	A1	1/2003	Wang	
2003/0018522	A1 *	1/2003	Denimarck	G06Q 30/0267 705/14.23
2003/0019929	A1	1/2003	Stewart et al.	
2003/0055738	A1	3/2003	Alie	
2003/0074317	A1	4/2003	Hofi	
2003/0112120	A1 *	6/2003	K.	G05B 19/0425 340/5.53
2003/0137403	A1	7/2003	Carrender et al.	
2003/0149662	A1 *	8/2003	Shore	G06Q 20/04 705/39
2003/0200227	A1	10/2003	Ressler	
2004/0044627	A1	3/2004	Russell	
2004/0049451	A1	3/2004	Beraardi	
2004/0128249	A1	7/2004	Hoffman	
2005/0149764	A1	7/2005	Bahl et al.	

(56) **References Cited**

U.S. PATENT DOCUMENTS

2006/0020558	A1*	1/2006	Bonalle	G06Q 20/382 705/64
2006/0204048	A1*	9/2006	Morrison	G06F 21/32 382/115
2007/0022058	A1*	1/2007	Labrou	G06Q 20/32 705/67
2007/0198436	A1*	8/2007	Weiss	G06Q 20/401 705/75
2010/0094754	A1	4/2010	Bertran et al.	
2010/0095130	A1	4/2010	Bertran et al.	

FOREIGN PATENT DOCUMENTS

EP	0977145	A2	2/2000
EP	0993999	A2	4/2000
JP	2002042076	A	2/2002
WO	9843104	A2	10/1998
WO	2004006165	A1	1/2004

OTHER PUBLICATIONS

Smart Card Technology Past Present and Future Mohammmed 2004.*

Understanding the Requirements of ISO IEC 14443.*

Alliance, S. C. (May 2002). 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).*

IEEE. (Mar. 24, 1997). IEEE xplore. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=570830 (Year: 1997).*

Atmel Corporation, Silicon solutions making smart cards smarter, 2000, 12 pages.

Extended European Search Report received in European patent application No. 10182033.0, dated Jan. 13, 2012, 7 pages.

Fancher, Carol Hovenga, In your pocket smartcards, Feb. 1997, 7 pages.

Rakers et al., Secure contactless smartcard ASIC with DPA protection, Mar. 2001, 7 pages.

Japanese Office Action received in Japanese patent application No. 2004-519130, dated May 12, 2009, 3 pages (including partial English translation).

Anonymous, Read/write RFID offers standalone advantages, Security, Aug. 1996, 1 page.

Appeal Brief filed Apr. 18, 2017 for U.S. Appl. No. 14/659,502.

Pre-Brief Appeal Conference Decision dated Nov. 30, 2016 and received in U.S. Appl. No. 14/659,502.

Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Nov. 16, 2016 for U.S. Appl. No. 14/659,502.

U.S. Office Action dated May 16, 2016 received in U.S. Appl. No. 14/659,502.

Response to Office Action filed on Dec. 23, 2015 for U.S. Appl. No. 14/659,502.

U.S. Office Action dated Jun. 22, 2015 received in U.S. Appl. No. 14/659,502.

Response to Office Action filed on May 2, 2017 for U.S. Appl. No. 15/372,317.

U.S. Office Action dated Feb. 2, 2017 received in U.S. Appl. No. 15/372,317.

Response to Office Action filed on Nov. 18, 2016 for U.S. Appl. No. 14/321,781.

U.S. Office Action dated May 19, 2016 received in U.S. Appl. No. 14/321,781.

Response to Office Action filed on Dec. 24, 2015 for U.S. Appl. No. 14/321,781.

U.S. Office Action dated Jun. 24, 2015 received in U.S. Appl. No. 14/321,781.

U.S. Notice of Allowance dated Apr. 11, 2014 received in U.S. Appl. No. 14/022,135.

Response to Office Action filed on Mar. 14, 2014 for U.S. Appl. No. 14/022,135.

U.S. Office Action dated Mar. 7, 2014 received in U.S. Appl. No. 14/022,135.

Response to Office Action filed on Feb. 3, 2014 for U.S. Appl. No. 14/022,135.

U.S. Office Action dated Dec. 5, 2013 received in U.S. Appl. No. 14/022,135.

Response to Office Action filed on Apr. 26, 2017 for U.S. Appl. No. 14/724,593.

U.S. Office Action dated Feb. 17, 2017 received in U.S. Appl. No. 14/724,593.

Pre-Brief Appeal Conference Decision dated Dec. 12, 2016 and received in U.S. Appl. No. 14/724,593.

Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Nov. 7, 2016 for U.S. Appl. No. 14/724,593.

U.S. Office Action dated May 6, 2016 received in U.S. Appl. No. 14/724,593.

Response to Office Action filed on Jan. 7, 2016 for U.S. Appl. No. 14/724,593.

U.S. Office Action dated Aug. 4, 2015 received in U.S. Appl. No. 14/724,593.

U.S. Notice of Allowance dated Dec. 3, 2014 received in U.S. Appl. No. 14/028,469.

Supplemental response to Office Action filed on Oct. 31, 2014 for U.S. Appl. No. 14/028,469.

Response to Office Action filed on Oct. 14, 2014 for U.S. Appl. No. 14/028,469.

U.S. Office Action dated Aug. 18, 2014 received in U.S. Appl. No. 14/028,469.

U.S. Office Action dated Jul. 9, 2014 received in U.S. Appl. No. 14/028,469.

Response to Office Action filed on Jun. 13, 2014 for U.S. Appl. No. 14/028,469.

U.S. Office Action dated Apr. 3, 2014 received in U.S. Appl. No. 14/028,469.

Response to Office Action filed on Mar. 14, 2014 for U.S. Appl. No. 14/028,469.

U.S. Office Action dated Mar. 6, 2014 received in U.S. Appl. No. 14/028,469.

Response to Office Action filed on Feb. 3, 2014 for U.S. Appl. No. 14/028,469.

U.S. Office Action dated Dec. 6, 2013 received in U.S. Appl. No. 14/028,469.

Appeal Brief filed Feb. 9, 2017 for U.S. Appl. No. 14/585,057.

Pre-Brief Appeal Conference Decision dated Nov. 30, 2016 and received in U.S. Appl. No. 14/585,057.

Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Nov. 9, 2016 for U.S. Appl. No. 14/585,057.

U.S. Office Action dated May 9, 2016 received in U.S. Appl. No. 14/585,057.

Response to Office Action filed on Jan. 7, 2016 for U.S. Appl. No. 14/585,057.

U.S. Office Action dated Oct. 7, 2015 received in U.S. Appl. No. 14/585,057.

U.S. Office Action dated Jan. 8, 2020 received in U.S. Appl. No. 14/321,781(21 pages).

Appeal Brief filed Jun. 10, 2019 filed in U.S. Appl. No. 14/724,593. (46 pages).

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 Ortidam .pdf (10 pages).

U.S. Notice of Allowance dated Jul. 24, 2019 received in U.S. Appl. No. 16/051,751 (16 pages).

U.S. Notice of Allowance dated Jun. 4, 2019 received in U.S. Appl. No. 16/051,751 (22 pages).

Response to Office Action filed on Apr. 30, 2019 in U.S. Appl. No. 16/051,751. (11 pages).

U.S. Applicant Interview Summary dated Apr. 22, 2019 received in U.S. Appl. No. 16/051,751.

U.S. Office Action dated Feb. 4, 2019 received in U.S. Appl. No. 16/051,751. (21 pages).

(56) **References Cited**

OTHER PUBLICATIONS

Preliminary Amendment filed on Aug. 28, 2018 in U.S. Appl. No. 16/051,751. (9 pages).
U.S. Office Action dated Oct. 24, 2019 received in U.S. Appl. No. 14/724,593. (29 pages).
Notice of Appeal dated Apr. 10, 2019 filed in U.S. Appl. No. 14/724,593. (4 pages).
U.S. Office Action dated Jan. 11, 2019 received in U.S. Appl. No. 14/724,593. (48 pages).
Response to Office Action filed on Sep. 11, 2018 for U.S. Appl. No. 14/724,593 (24 pages).
U.S. Office Action dated Jul. 12, 2018 received in U.S. Appl. No. 14/724,593. (45 pages).
Response to Office Action filed on Jan. 10, 2018 for U.S. Appl. No. 14/724,593 (17 pages).
U.S. Applicant Interview Summary dated Dec. 6, 2017 received in U.S. Appl. No. 14/724,593. (3 pages).
U.S. Office Action dated Jul. 28, 2017 received in U.S. Appl. No. 14/724,593. (36 pages).
U.S. Notice of Allowance dated May 28, 2019 received in U.S. Appl. No. 14/659,502 (31 pages).
Patent Board Decision dated May 10, 2019 received in U.S. Appl. No. 14/659,502 (11 pages).
Reply Brief filed Sep. 26, 2017 for U.S. Appl. No. 14/659,502 (13 pages).
Examiner's Answer to Appeal Brief dated Jul. 26, 2017 received in U.S. Appl. No. 14/659,502.(28 pages).
U.S. Applicant Interview Summary dated Dec. 20, 2019 received in U.S. Appl. No. 14/585,057 (3 pages).
U.S. Office Action dated Sep. 19, 2019 received in U.S. Appl. No. 14/585,057 (21 pages).
Response to Office Action filed on Apr. 30, 2019 for U.S. Appl. No. 14/585,057 (20 pages).
Patent Board Decision dated Mar. 4, 2019 for U.S. Appl. No. 14/585,057. (11 pages).
Reply Brief filed dated Aug. 21, 2017 in the U.S. Appl. No. 14/585,057 (11 pages).
Examiner's Answer to Appeal Brief dated Jun. 21, 2017 received in U.S. Appl. No. 14/585,057 (24 pages).
Advisory Action dated Dec. 16, 2019 received in U.S. Appl. No. 14/321,781 (7 pages).
Response to Office Action dated Dec. 3, 2019 for U.S. Appl. No. 14/321,781 (30 pages).
U.S. Office Action dated Oct. 4, 2019 received in U.S. Appl. No. 14/321,781. (21 pages).
Response to Office Action filed on Jun. 7, 2019 for U.S. Appl. No. 14/321,781. (31 pages).
U.S. Office Action dated Mar. 7, 2019 received in U.S. Appl. No. 14/321,781. (19 pages).
Response to Office Action filed on Aug. 14, 2018 for U.S. Appl. No. 14/321,781. (28 pages).
U.S. Office Action dated Mar. 22, 2018 received in U.S. Appl. No. 14/321,781. (37 pages).
Response to Office Action filed on Dec. 5, 2017 for U.S. Appl. No. 14/321,781. (16 pages).
U.S. Office Action dated Jun. 5, 2017 received in U.S. Appl. No. 14/321,781. (51 pages).
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).
U.S. Office Action dated Apr. 13, 2020 received in U.S. Appl. No. 16/519,961 (38 pages).
Notice of Allowance and Examiner Initiated Interview Summary dated Apr. 8, 2020 received in U.S. Appl. No. 14/724,593 (48 pages).
U.S. Applicant Interview Summary dated Jan. 22, 2020 received in U.S. Appl. No. 14/724,593 (7 pages).
U.S. Applicant Interview Summary dated Jan. 22, 2020 received in U.S. Appl. No. 14/585,057 (7 pages).
Notice of Allowance and Examiner Initiated Interview Summary dated Apr. 2, 2020 received in U.S. Appl. No. 14/321,781 (41 pages).

* cited by examiner

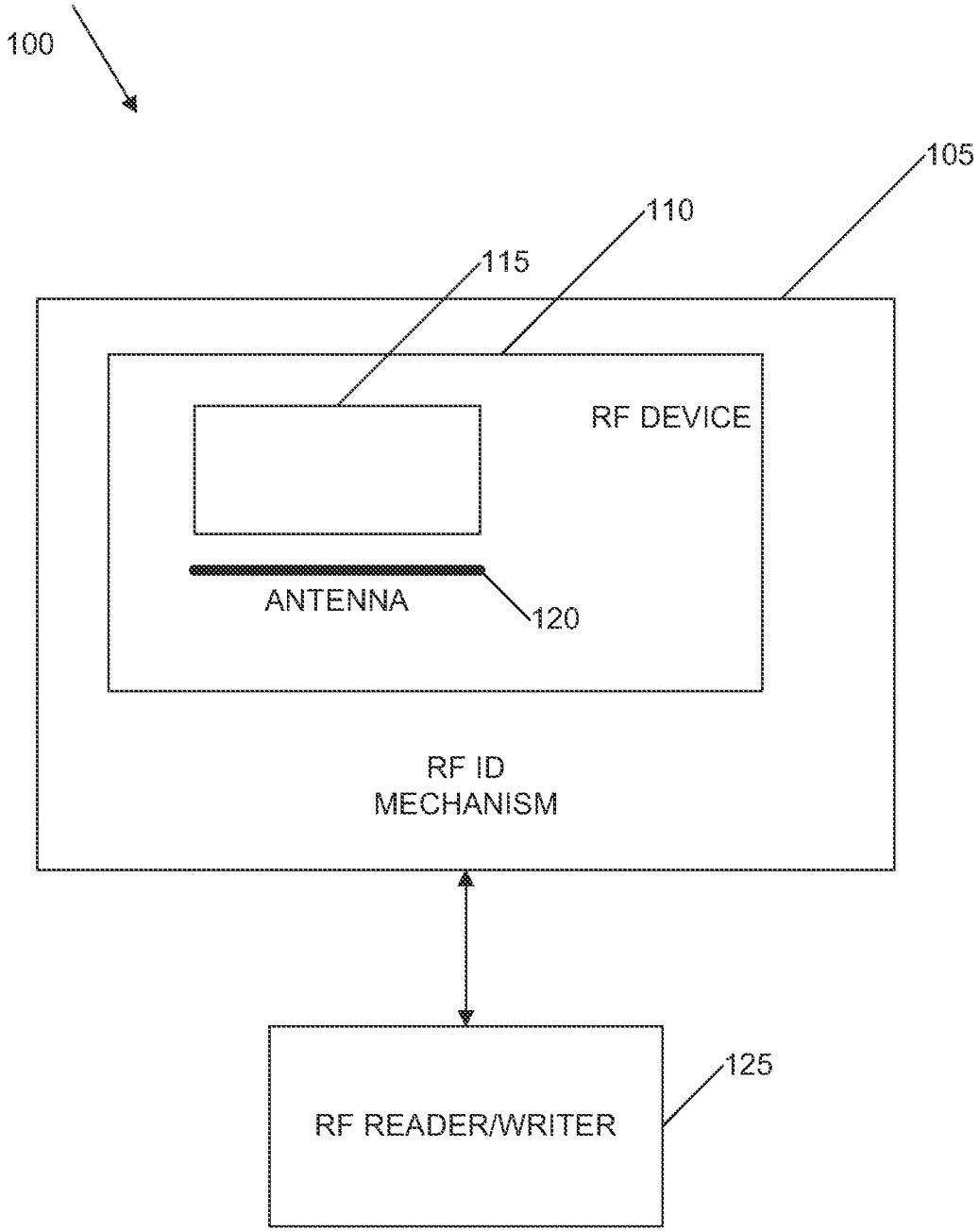

100
105
110
115
RF DEVICE
ANTENNA
120
RF ID
MECHANISM
125
RF READER/WRITER

FIG. 1

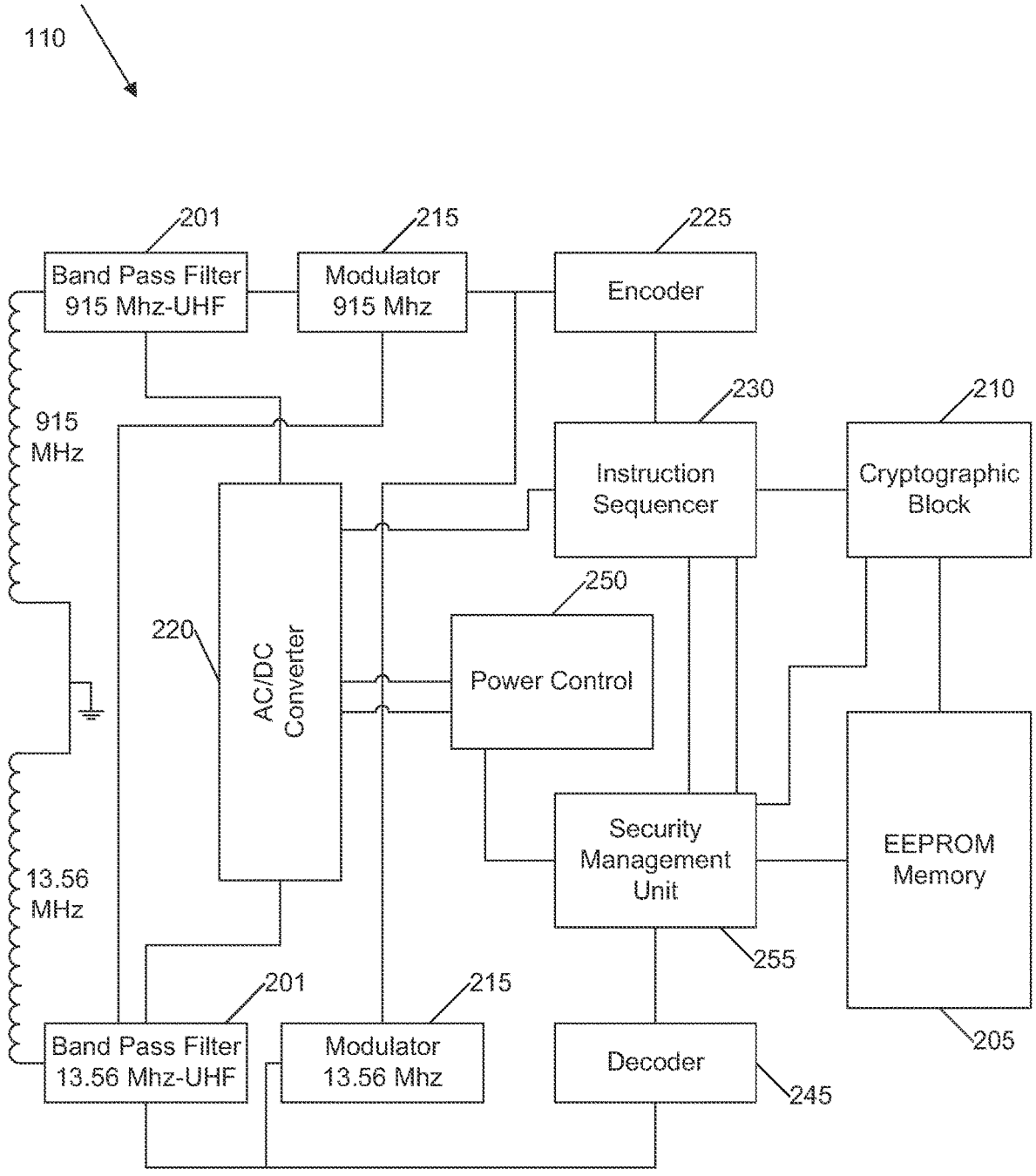

110
201
Band Pass Filter
915 Mhz-UHF
215
Modulator
915 Mhz
225
Encoder
915
MHz
230
Instruction
Sequencer
210
Cryptographic
Block
250
220
AC/DC
Converter
Power Control
Security
Management
Unit
EEPROM
Memory
13.56
MHz
255
205
201
Band Pass Filter
13.56 Mhz-UHF
215
Modulator
13.56 Mhz
Decoder
245

FIG. 2

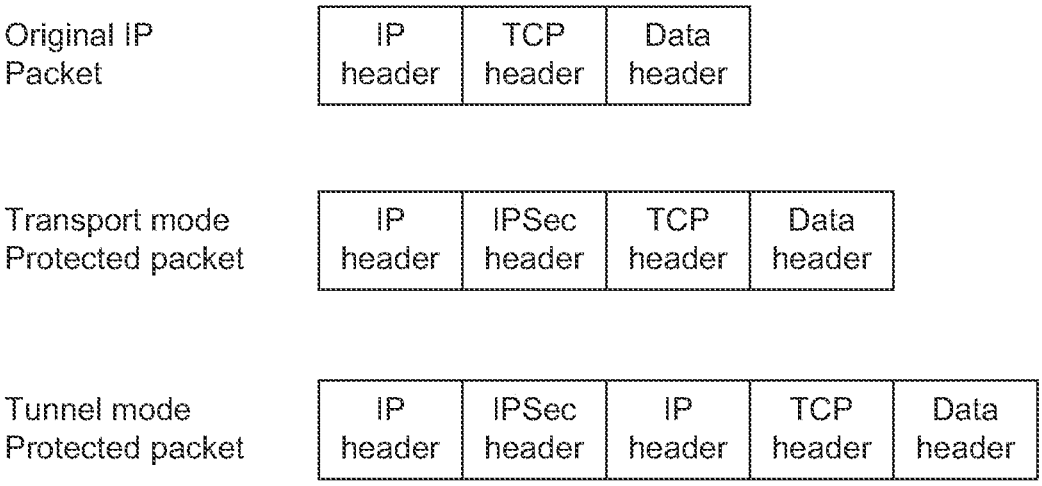

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIG. 3A

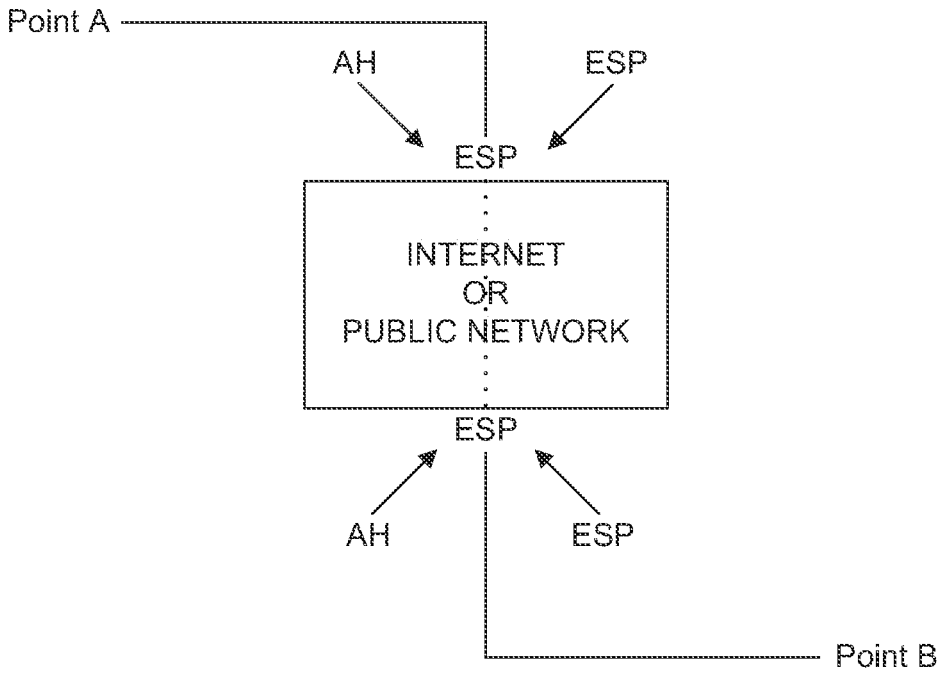

Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORK
ESP
AH
ESP
Point B

FIG. 3B

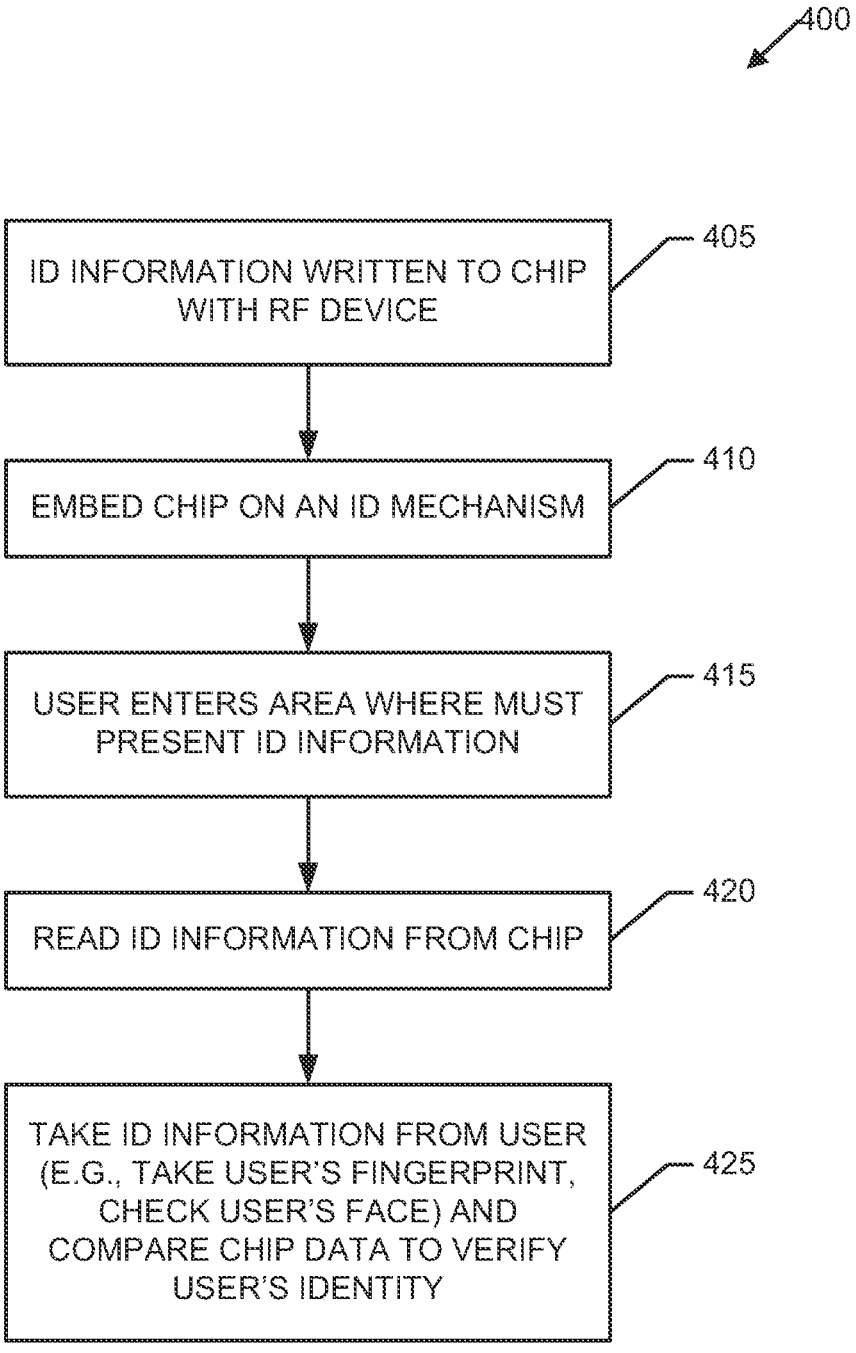

400
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
405
EMBED CHIP ON AN ID MECHANISM
410
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
415
READ ID INFORMATION FROM CHIP
420
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE CHIP DATA TO VERIFY USER'S IDENTITY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

FIG. 4

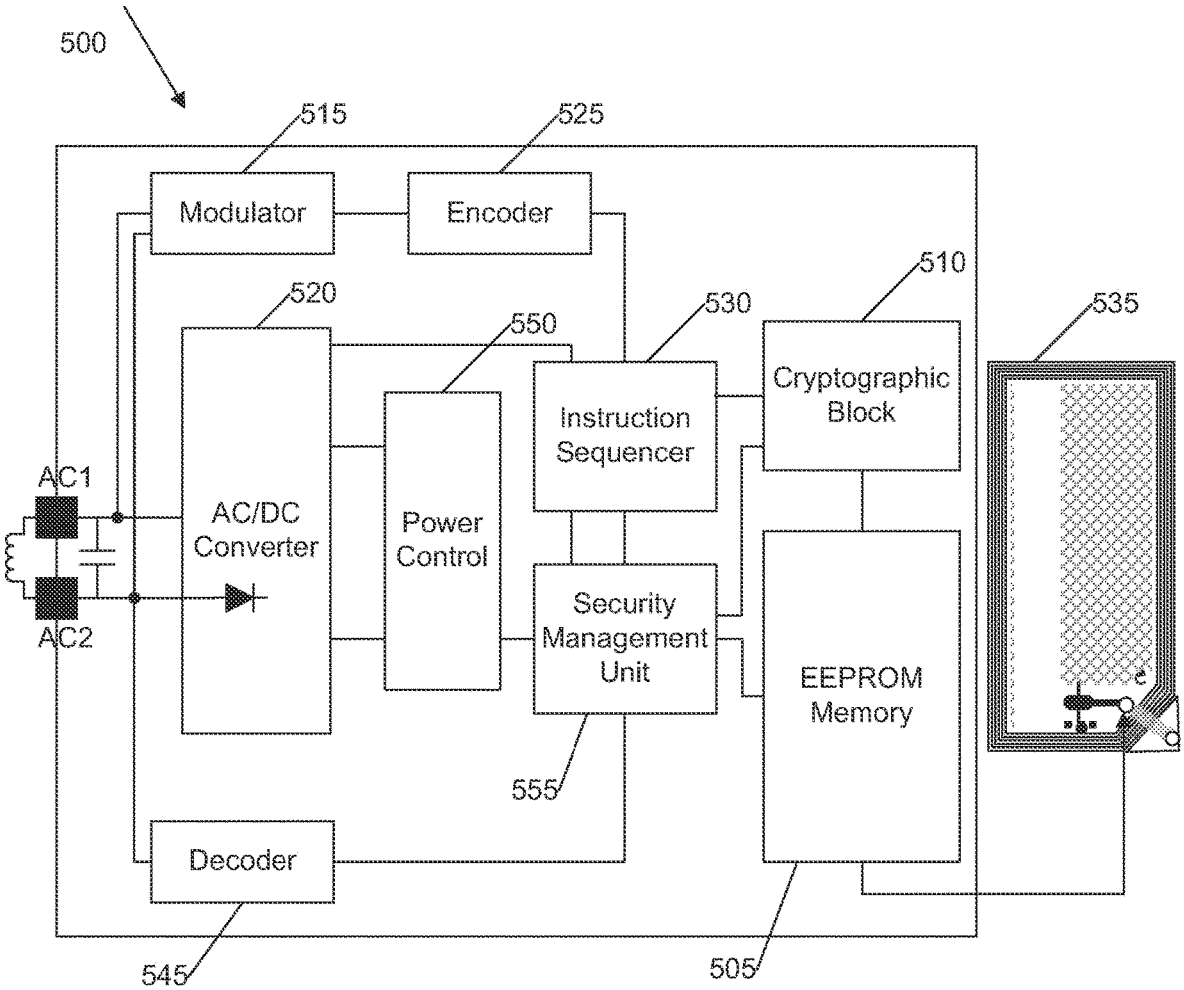

500
515
525
Modulator
Encoder
510
520
530
535
550
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
555
Decoder
545
505

FIG. 5

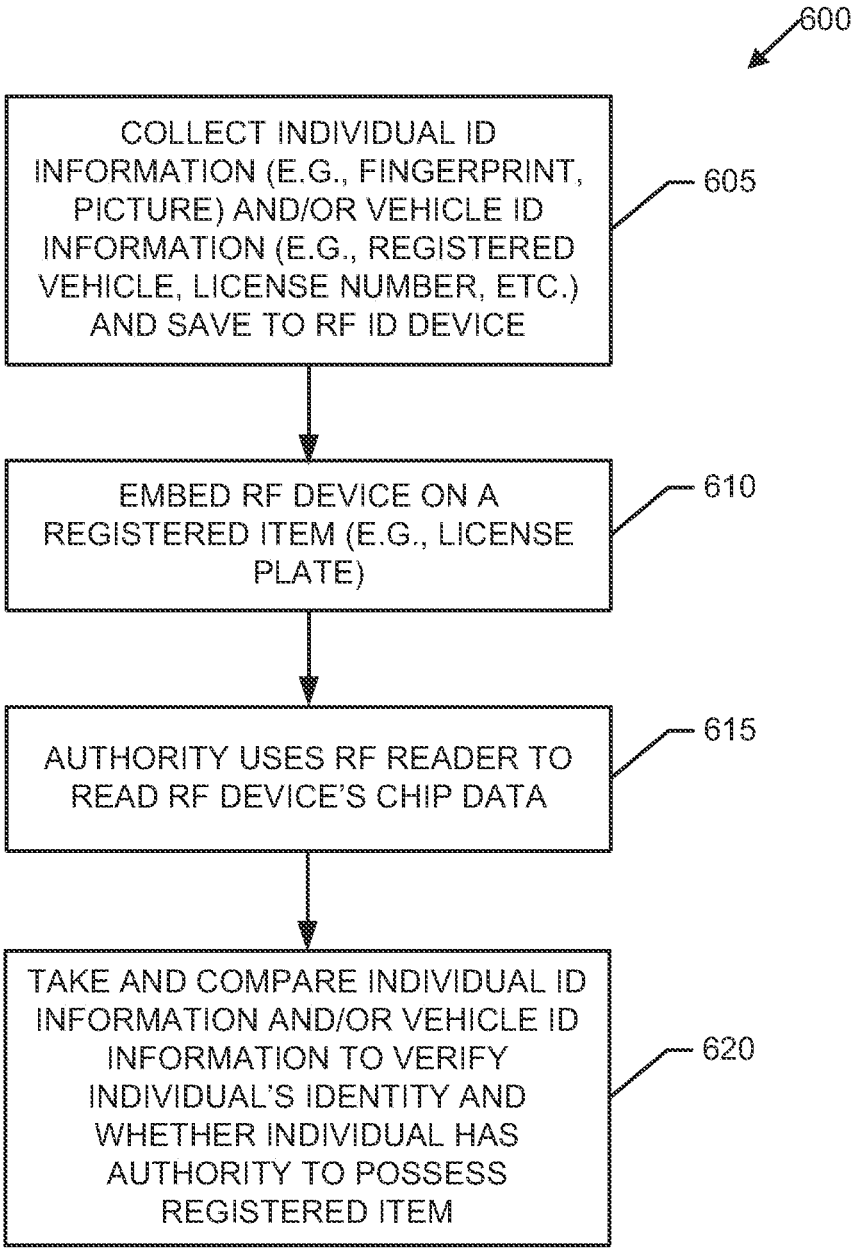

600
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
605
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
610
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
615
TAKE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

FIG. 6

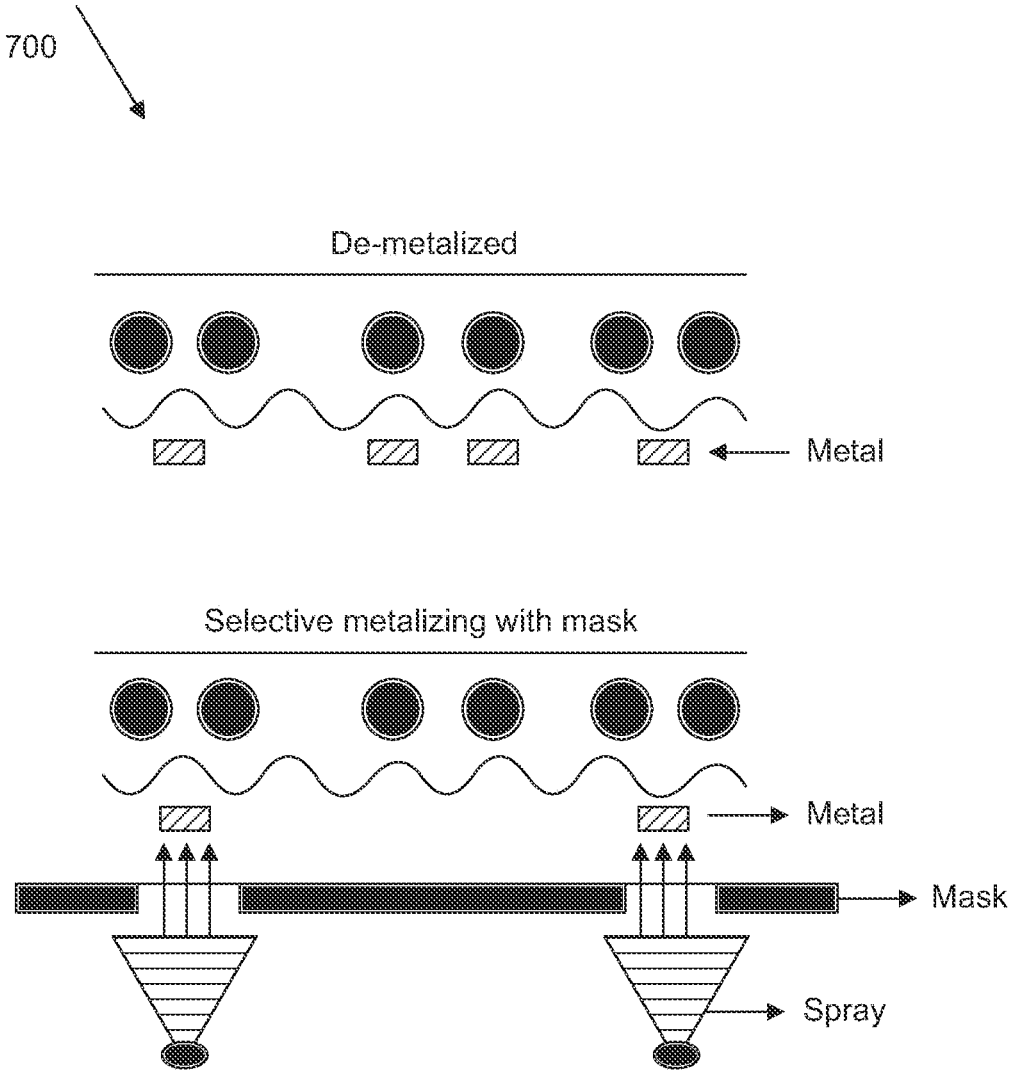

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIG. 7

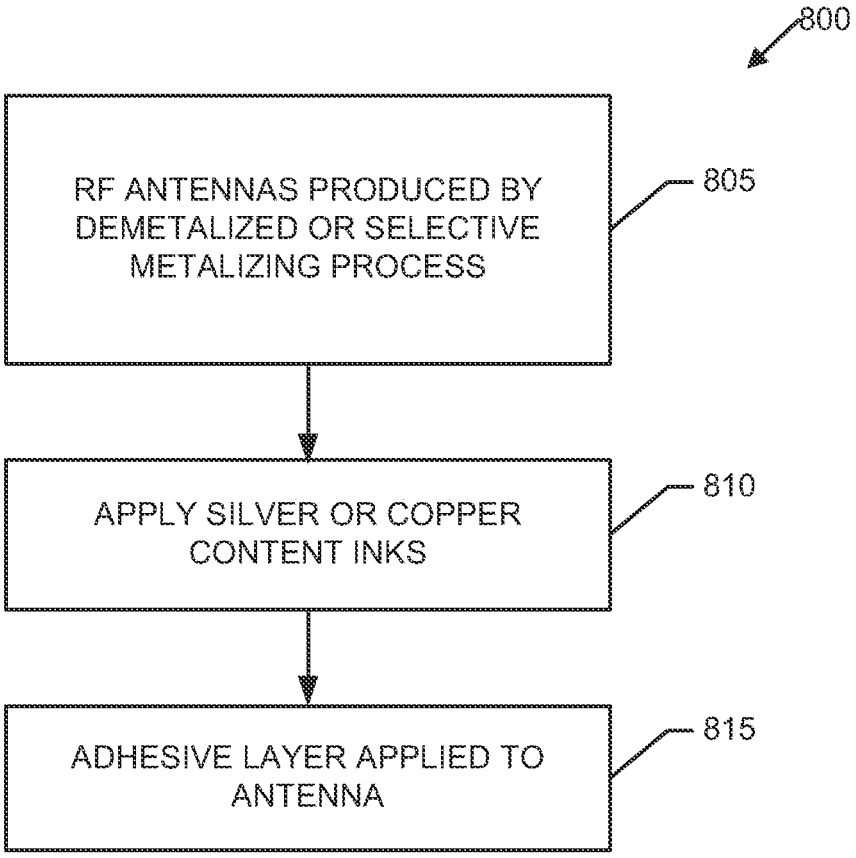

800
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
805
APPLY SILVER OR COPPER CONTENT INKS
810
ADHESIVE LAYER APPLIED TO ANTENNA
815

FIG. 8

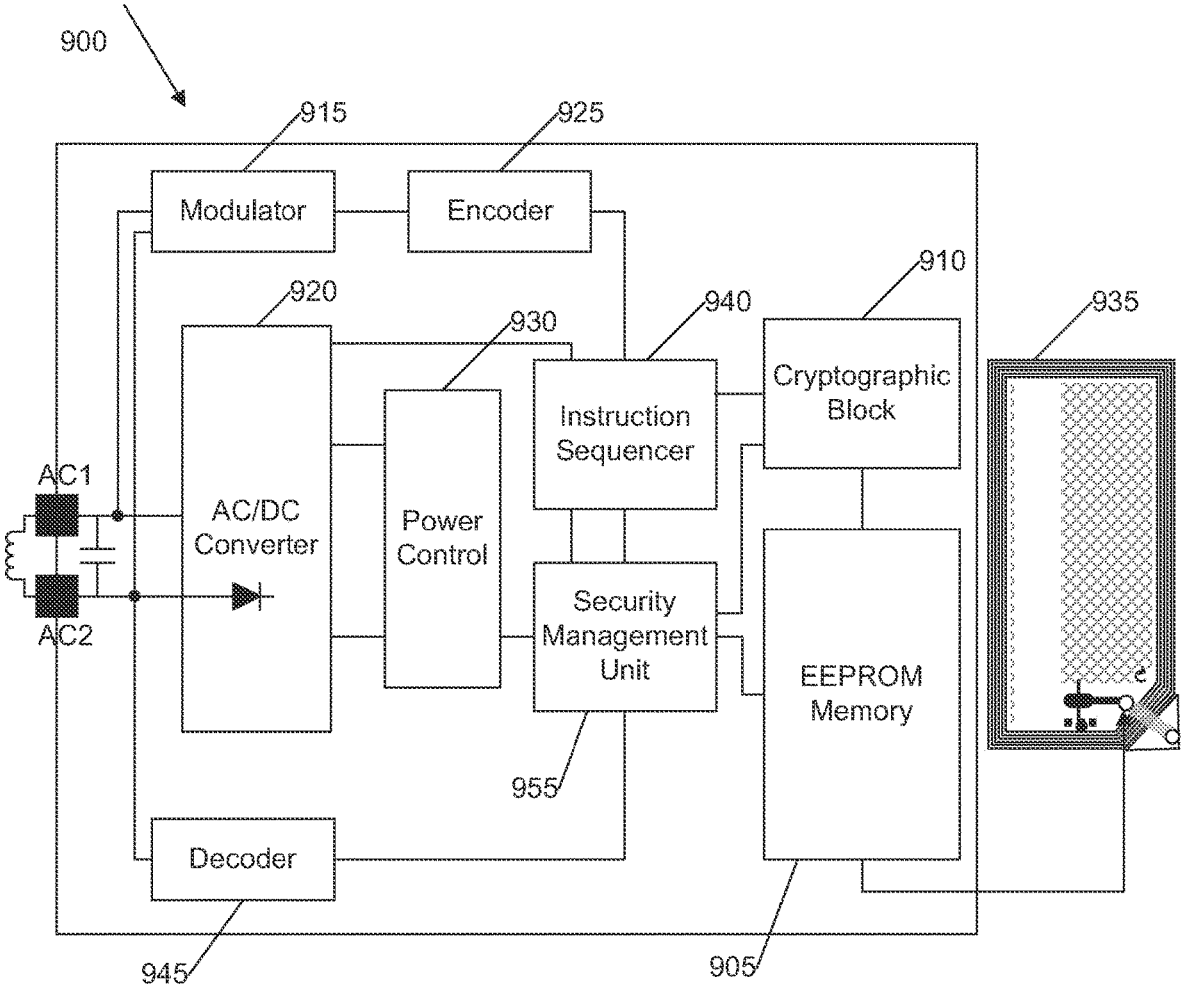

900
915
925
Modulator
Encoder
910
920
940
935
930
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
955
Decoder
945
905

FIG. 9

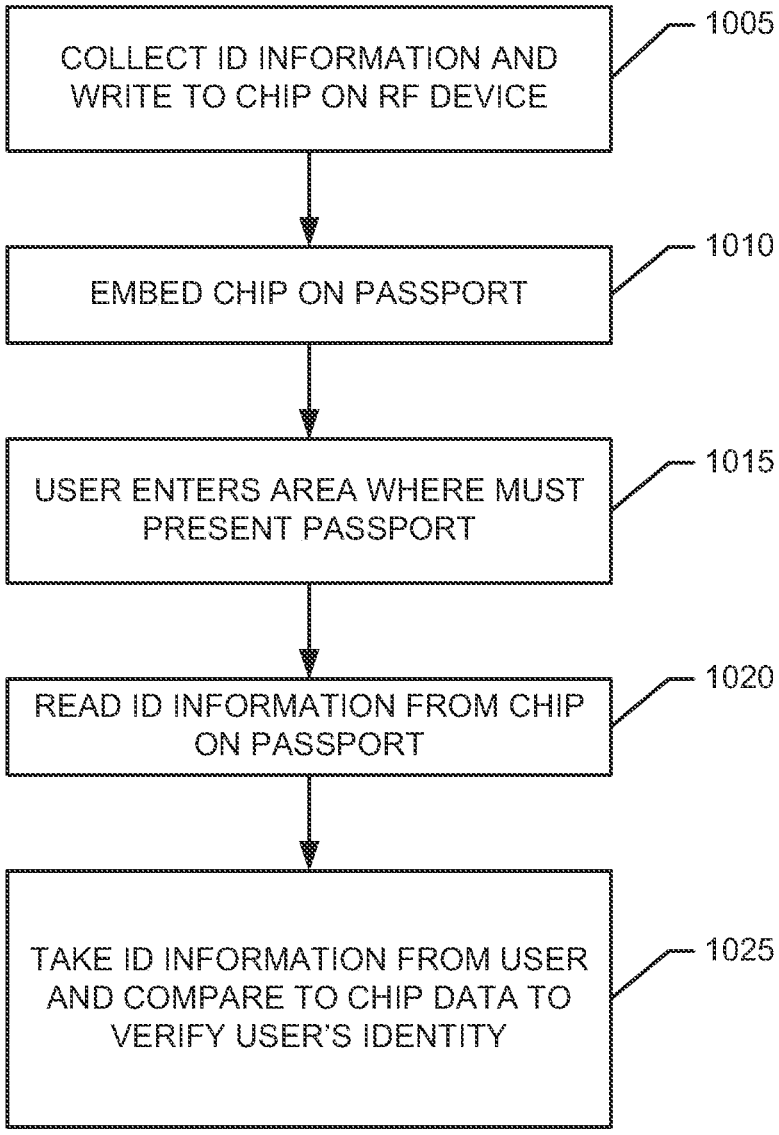

COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1005
EMBED CHIP ON PASSPORT
1010
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1015
READ ID INFORMATION FROM CHIP ON PASSPORT
1020
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY
1025

FIG. 10

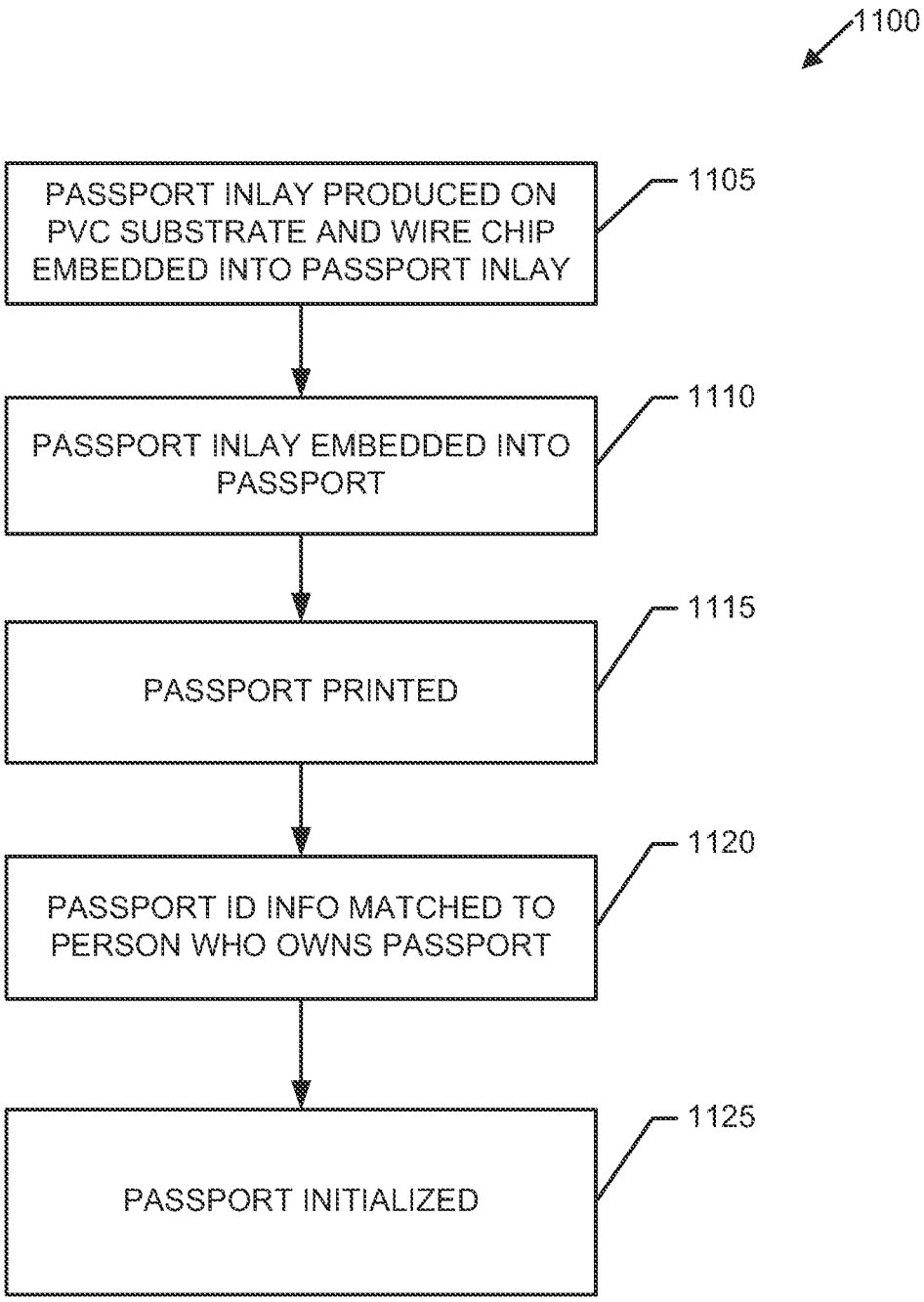

1100
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1105
PASSPORT INLAY EMBEDDED INTO PASSPORT
1110
PASSPORT PRINTED
1115
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1120
PASSPORT INITIALIZED
1125

FIG. 11

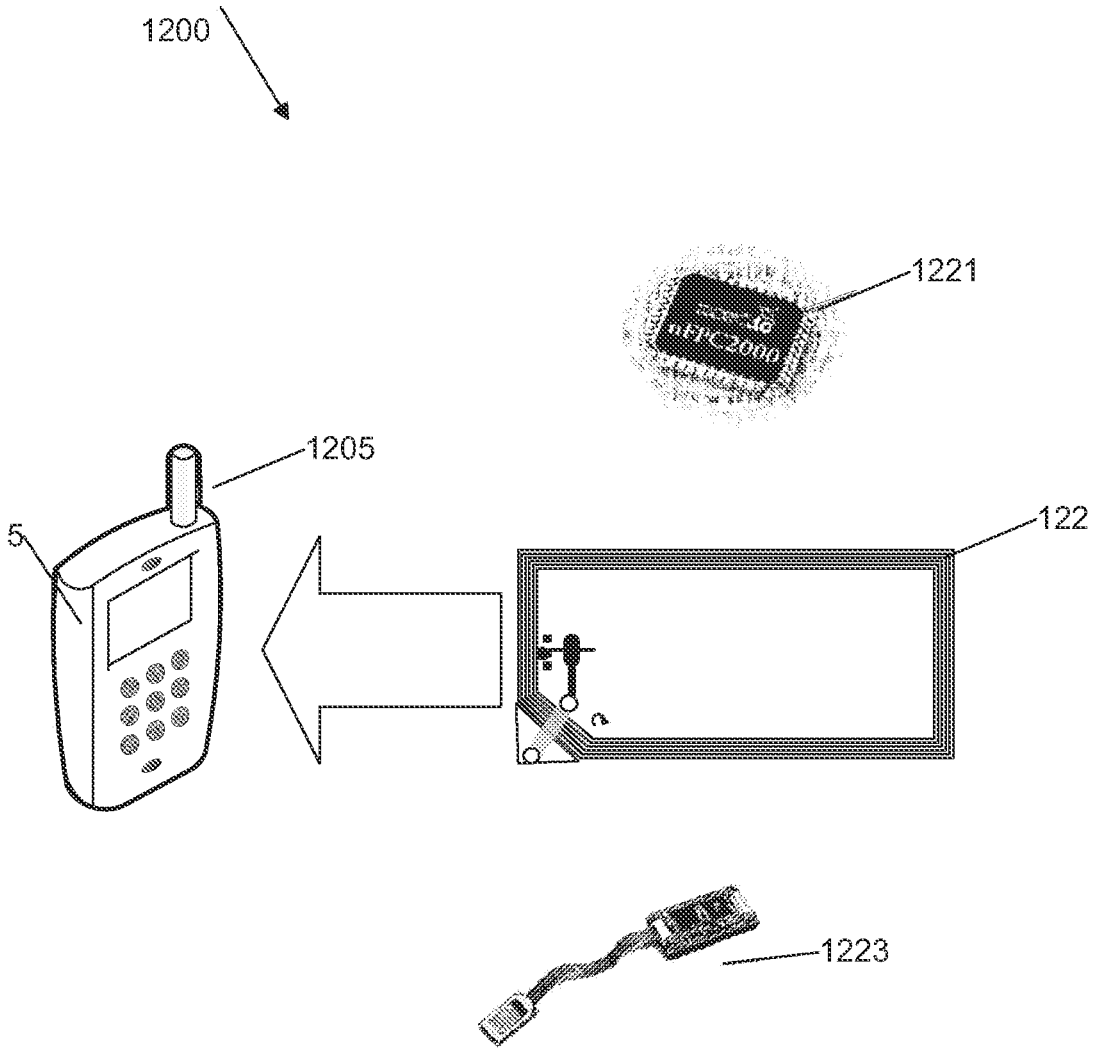


FIG. 12

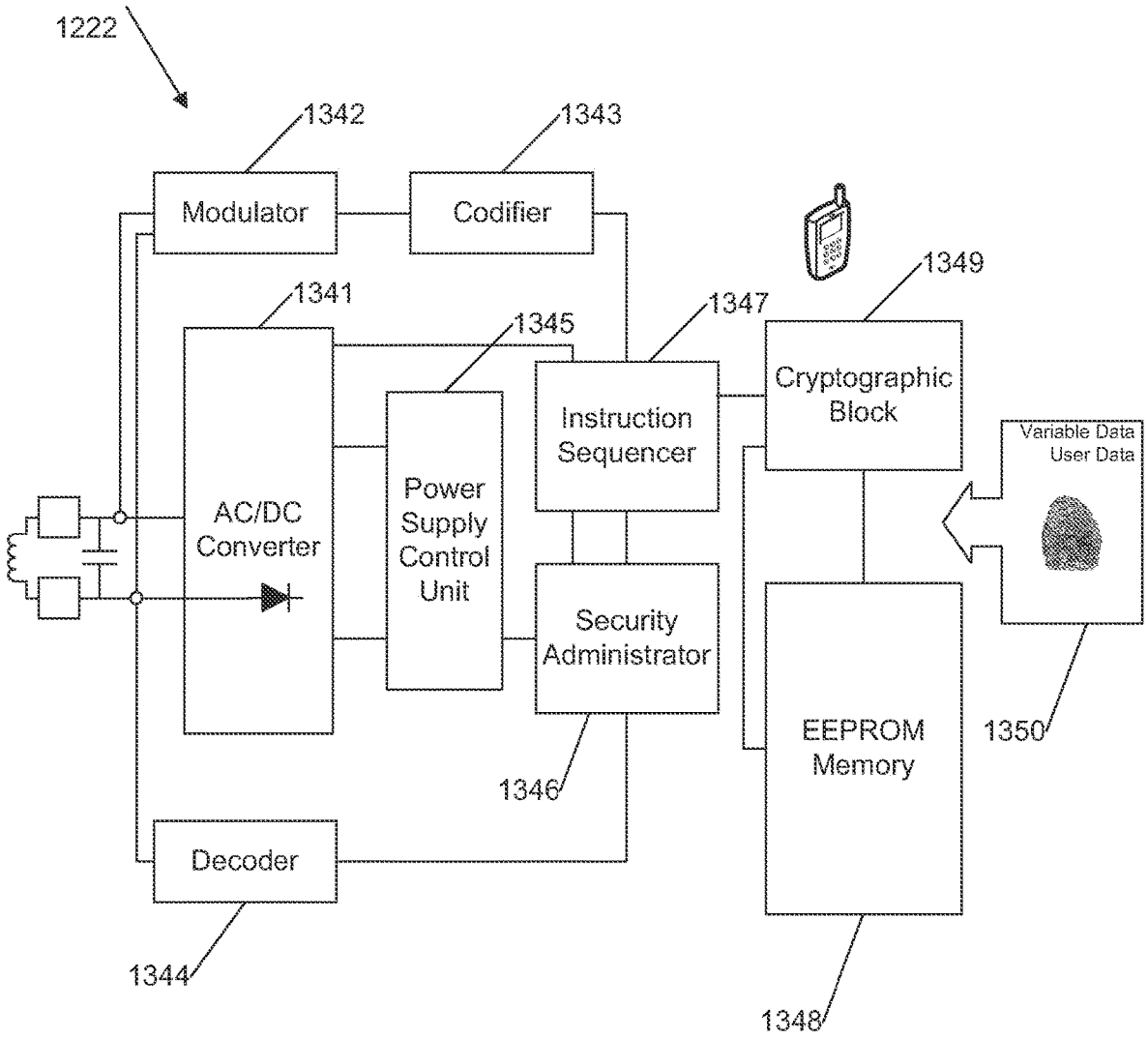

1222
1342
1343
Modulator
Codifier
1341
1345
1347
1349
AC/DC Converter
Power Supply Control Unit
Instruction Sequencer
Cryptographic Block
Variable Data
User Data
Security Administrator
EEPROM Memory
1350
1346
Decoder
1344
1348

FIG. 13

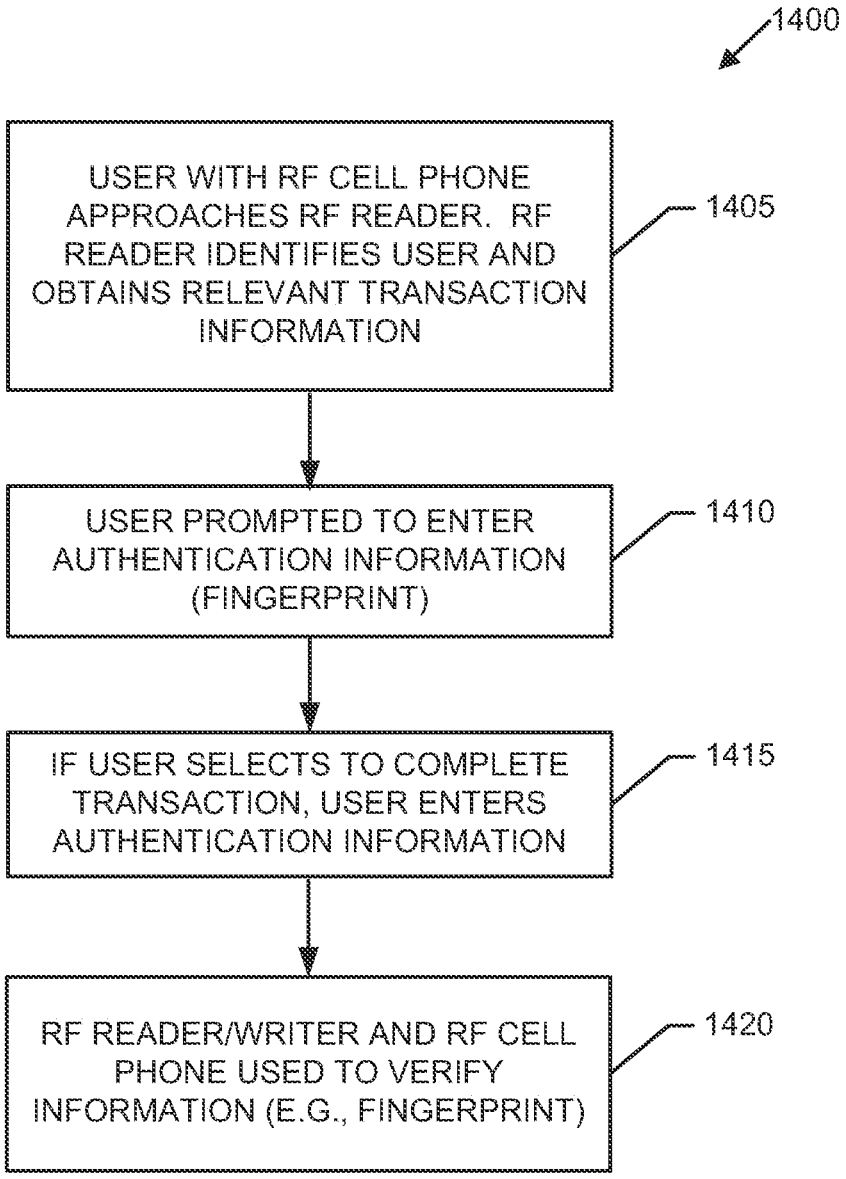

1400
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION
1405
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT)
1410
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION
1415
RF READER/WRITER AND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

FIG. 14

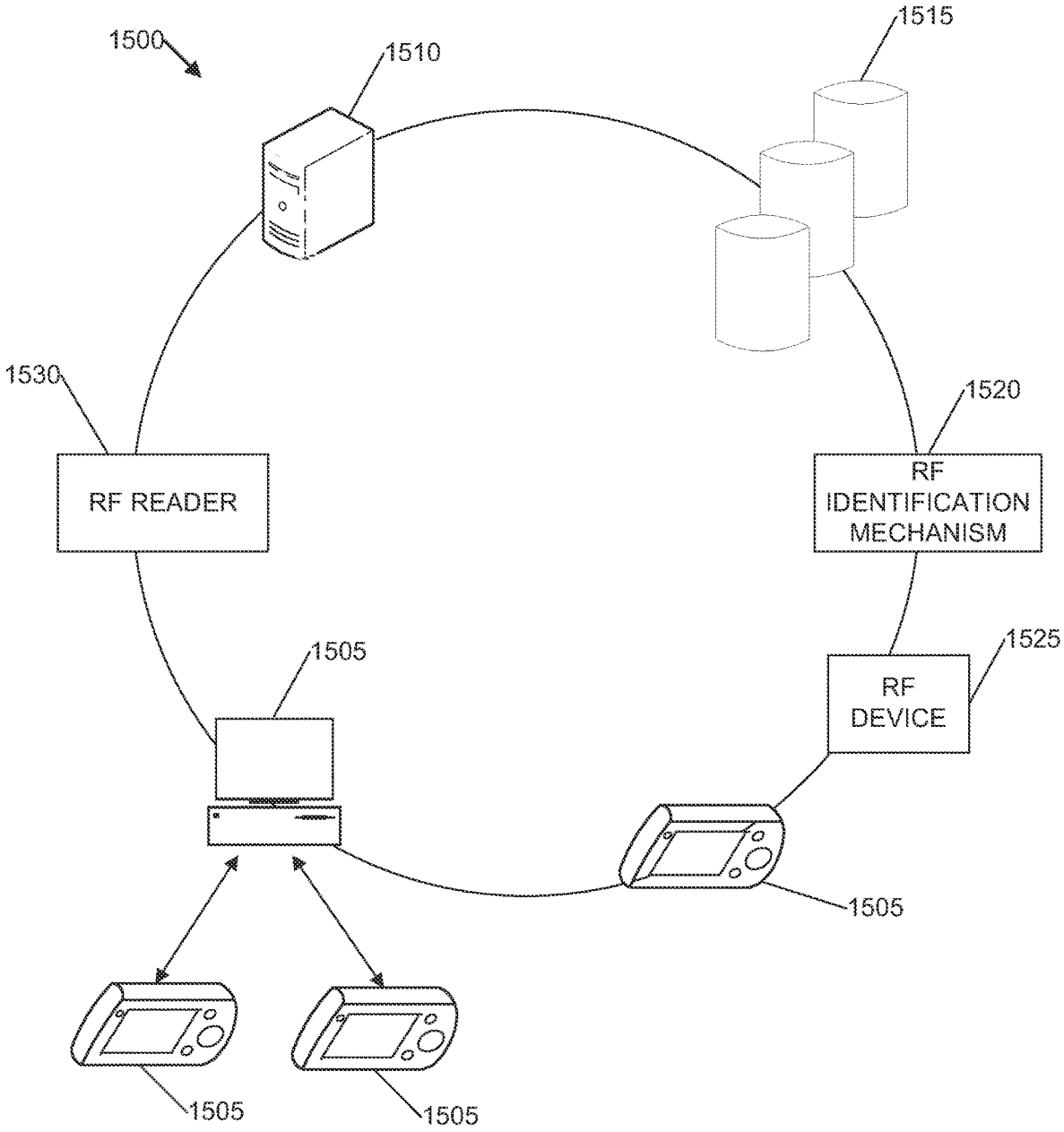

1500
1510
1515
1530
1520
RF READER
RF IDENTIFICATION MECHANISM
1505
1525
RF DEVICE
1505
1505
1505

FIG. 15

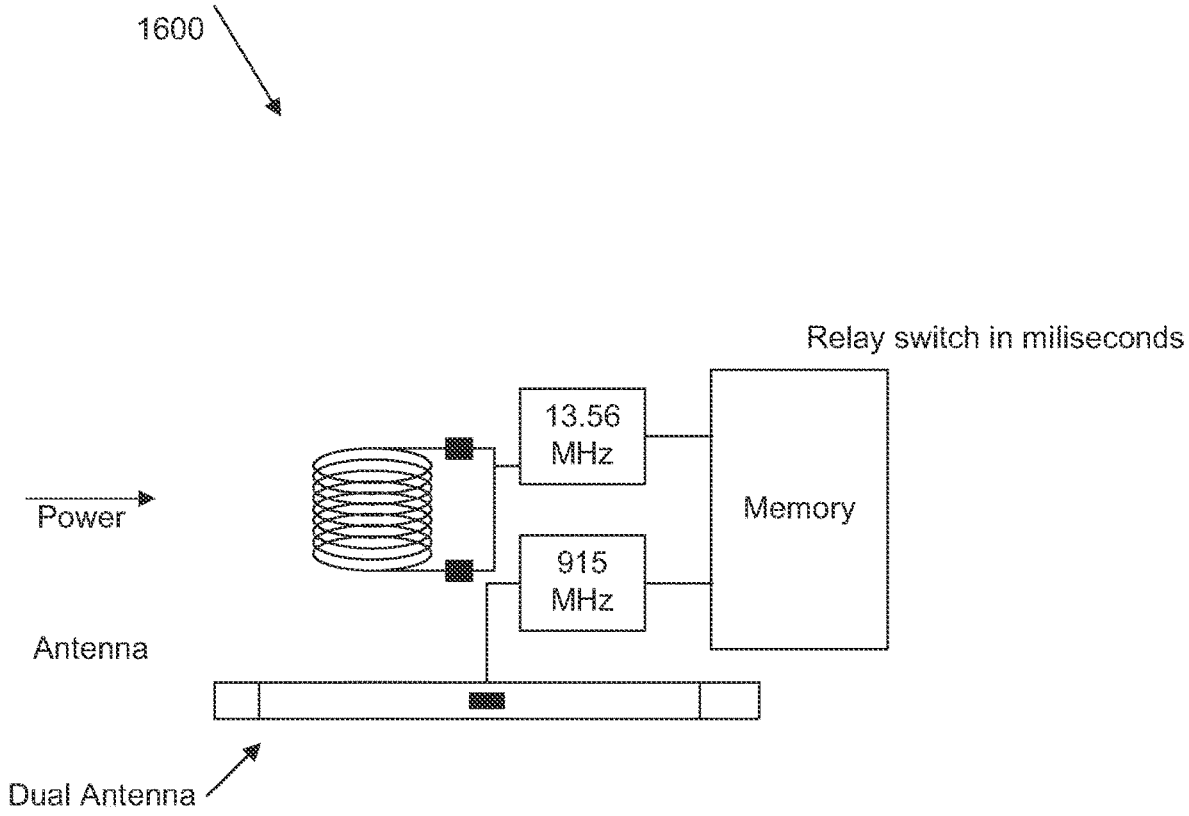

1600
Relay switch in miliseconds
13.56 MHz
915 MHz
Memory
Power
Antenna
Dual Antenna

FIG. 16

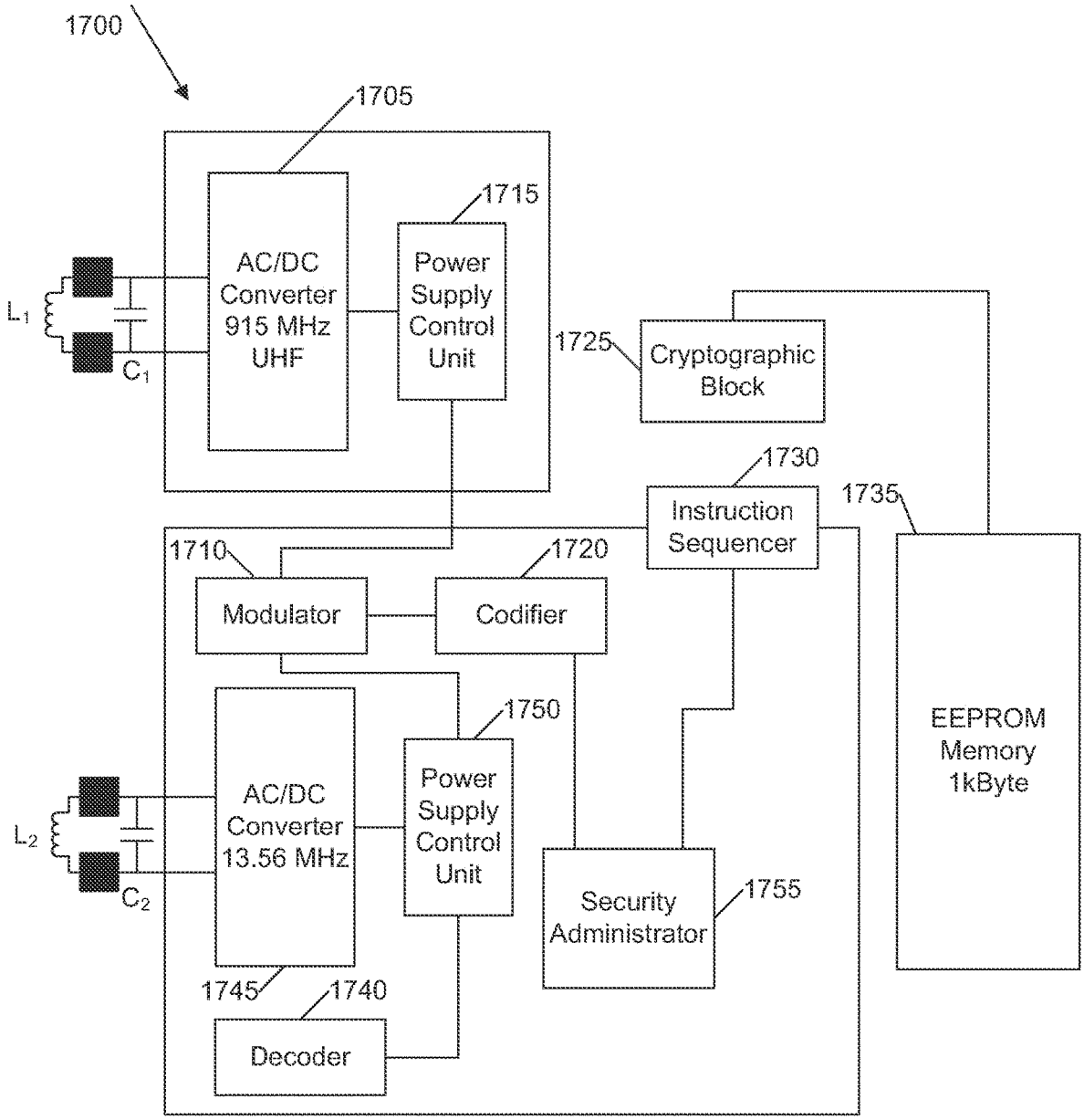

1700
1705
1715
AC/DC Converter 915 MHz UHF
Power Supply Control Unit
L1
C1
1725
Cryptographic Block
1730
Instruction Sequencer
1735
1710
1720
Modulator
Codifier
EEPROM Memory 1kByte
1750
AC/DC Converter 13.56 MHz
Power Supply Control Unit
L2
C2
Security Administrator
1755
1745
1740
Decoder

FIG. 17

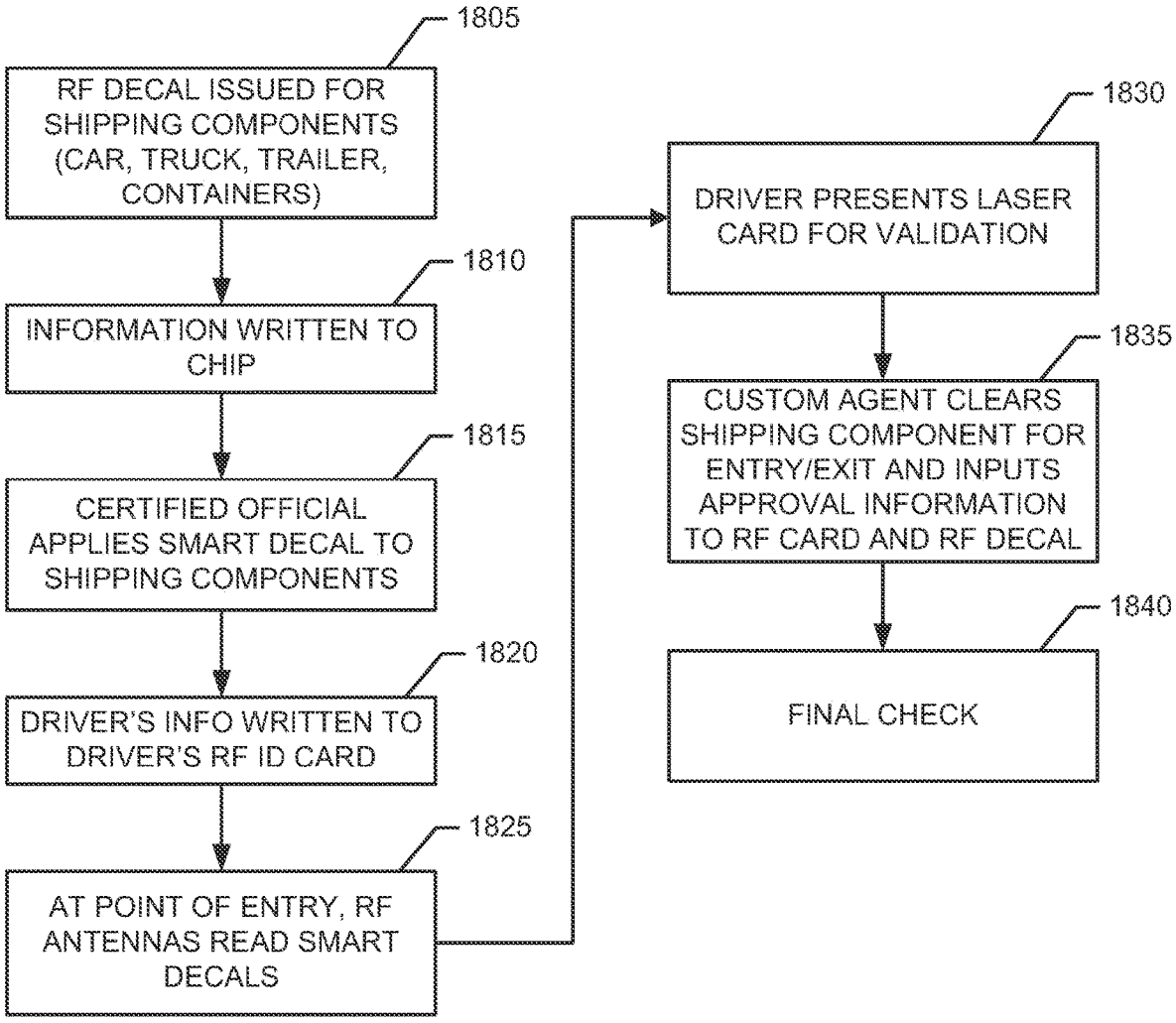

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS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

FIG. 18

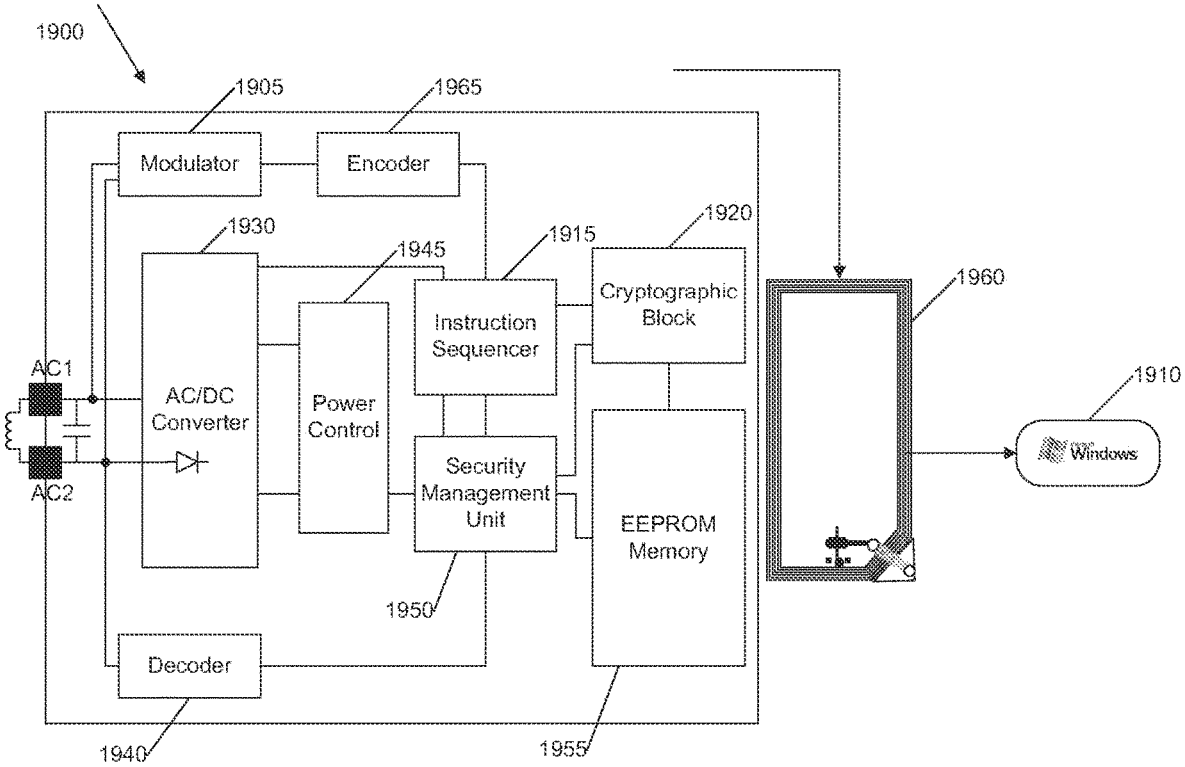

1900
1905
1965
Modulator
Encoder
1930
1945
1915
1920
Cryptographic Block
1960
Instruction Sequencer
AC1
AC/DC Converter
Power Control
1910
Windows
AC2
Security Management Unit
EEPROM Memory
1950
Decoder
1940
1955

FIG. 19

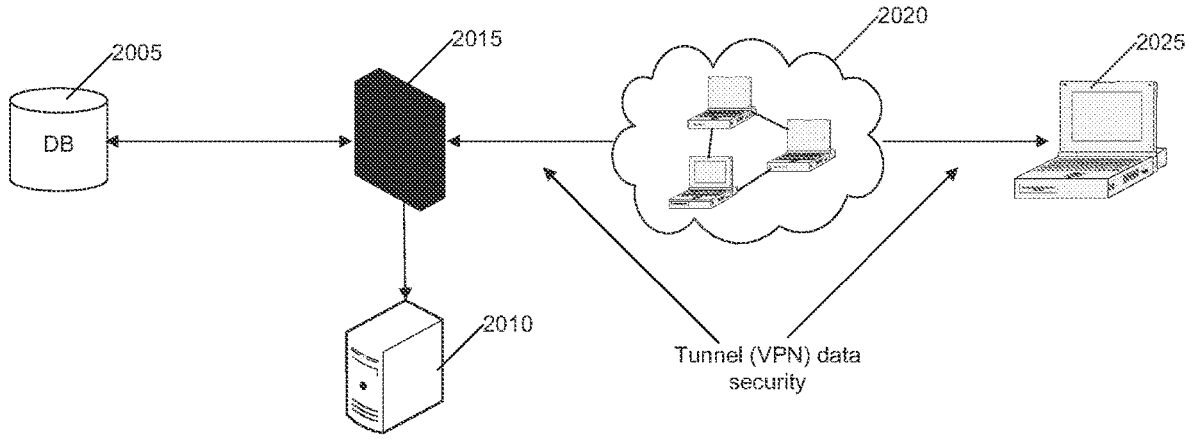


FIG. 20

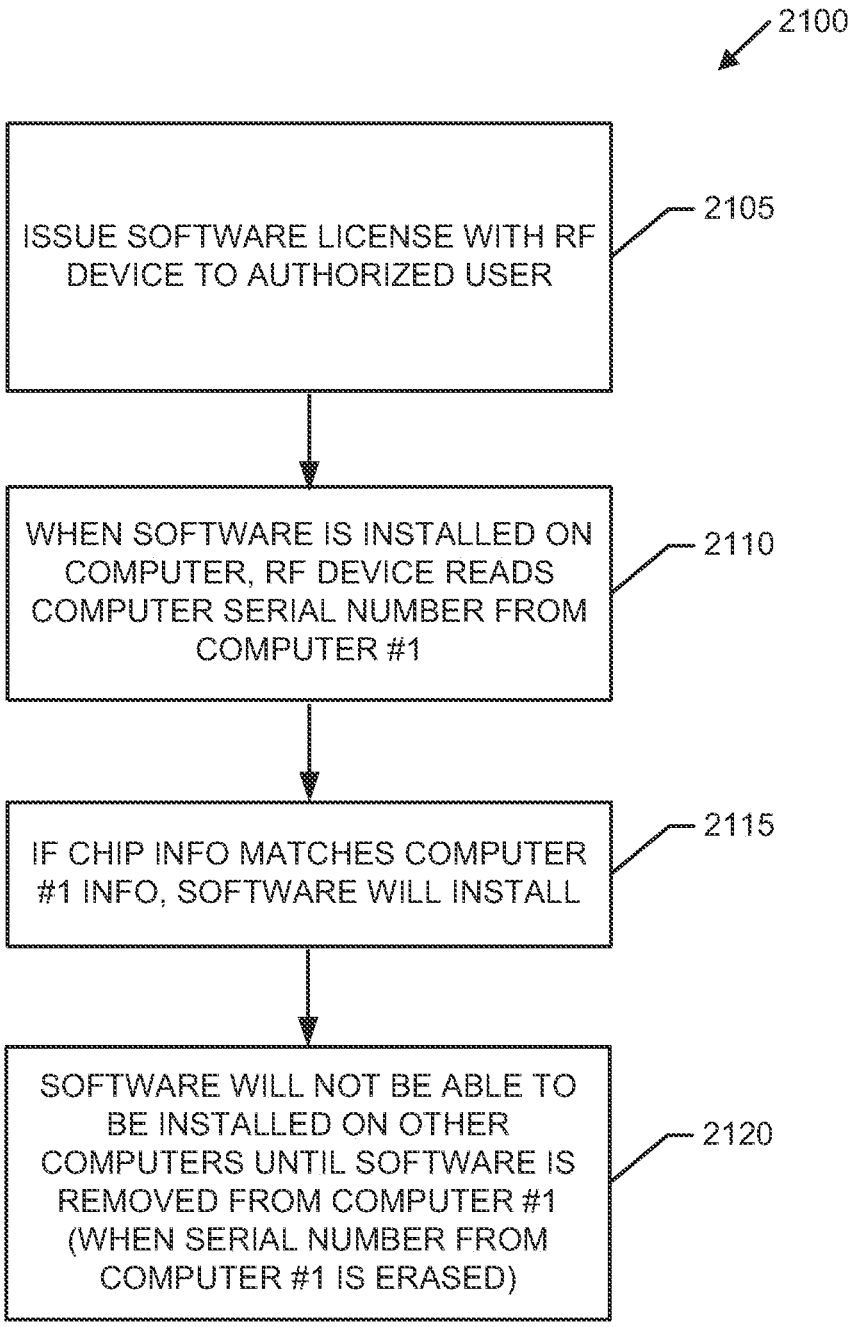

2100
ISSUE SOFTWARE LICENSE WITH RF DEVICE TO AUTHORIZED USER
2105
WHEN SOFTWARE IS INSTALLED ON COMPUTER, RF DEVICE READS COMPUTER SERIAL NUMBER FROM COMPUTER #1
2110
IF CHIP INFO MATCHES COMPUTER #1 INFO, SOFTWARE WILL INSTALL
2115
SOFTWARE WILL NOT BE ABLE TO BE INSTALLED ON OTHER COMPUTERS UNTIL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

FIG. 21

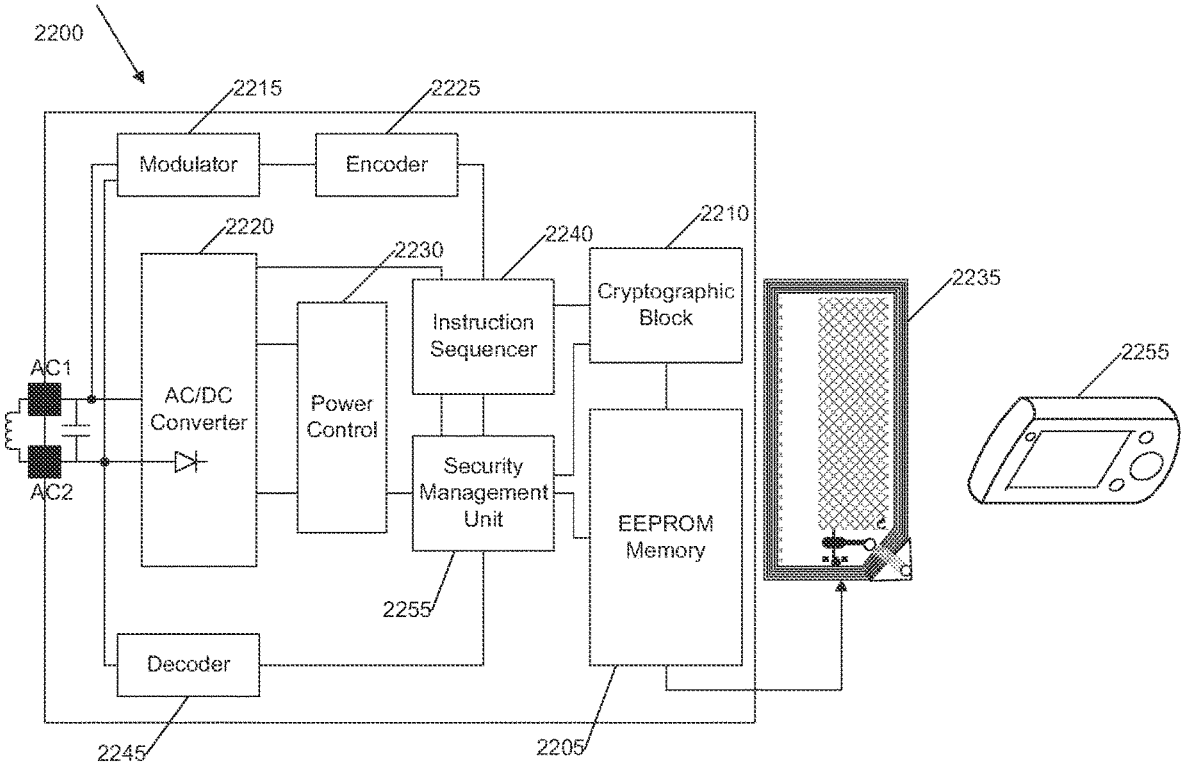

2200
2215
2225
Modulator
Encoder
2220
2230
2240
2210
Cryptographic Block
Instruction Sequencer
2235
2255
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
2255
Decoder
2245
2205

FIG. 22

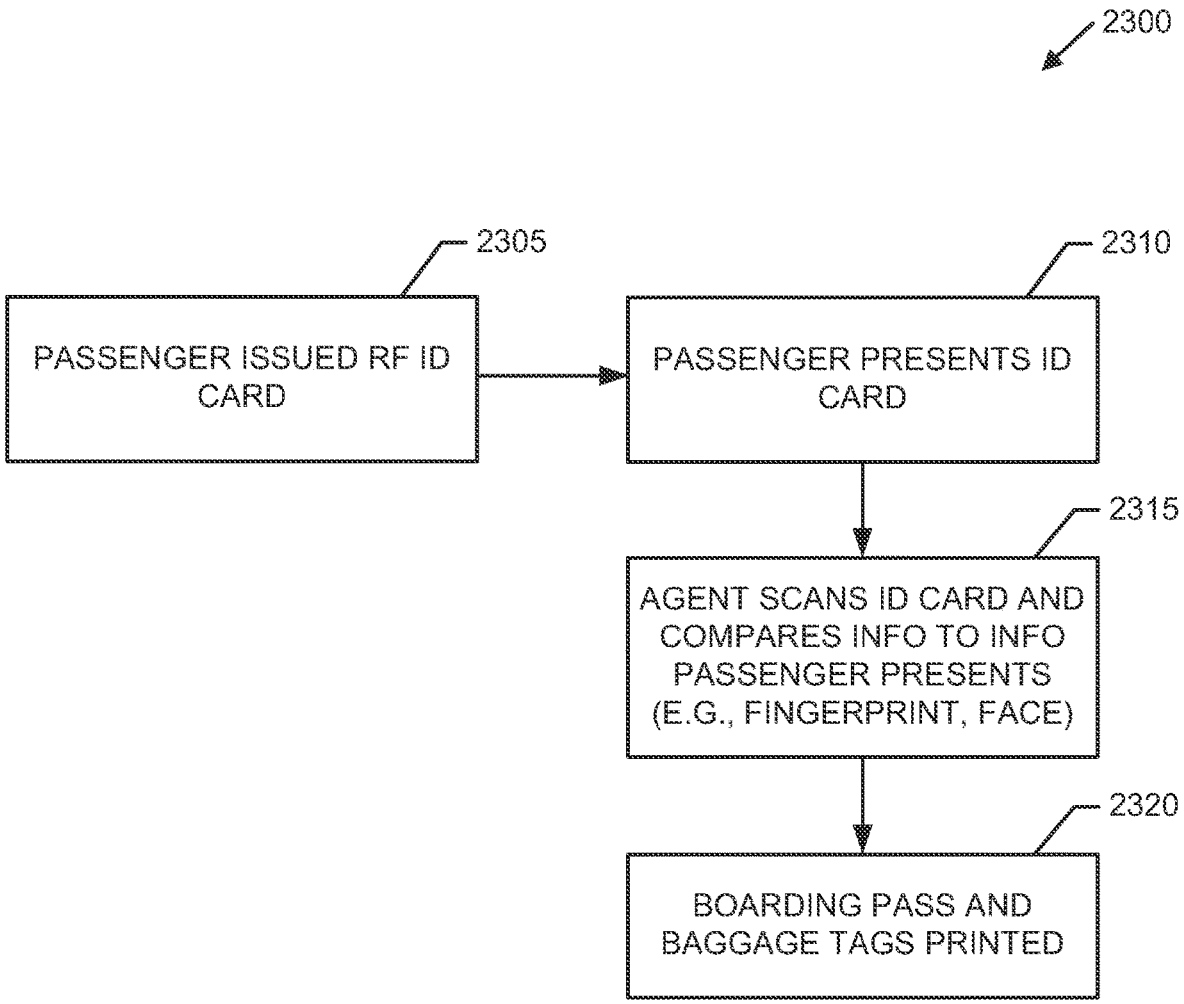

2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENT SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

FIG. 23

SYSTEM AND METHODS FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

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

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

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

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

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

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

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

FIGS. **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

FIG. **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

FIG. **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.

FIG. **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.

A more detailed description of an RF device can be found in U.S. patent application Ser. No. 10/118,092 filed 9 Apr. 2002; PCT Patent Application PCT/IB02/01439, filed 30 Apr. 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 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.

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.

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.

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 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.

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 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.

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 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.

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

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

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 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.

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.

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 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.

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

FIG. **4** illustrates the methods 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

FIG. **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

FIG. **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.

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 FIG. **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 material, holographic foil, or another substrate with a high metal content.

FIG. **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) 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

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

FIG. **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

FIG. **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

FIG. **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

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 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.

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 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.

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

FIG. **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 ensures 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 FIG. **13**. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt **1348**, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements are not met, a user cannot access the memory of the chip. The chip includes an ACDC converter **1341** and a connection to an RF antenna for power using a power supply control unit **1345**. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator **1342** is a device that receives baseband signals from an antenna. An AC/DC converter **1341** is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder **1343** is a device for encoding information received so that it may be utilized by another device or protocol. A decoder **1344** is a device that decodes information from the encoder output so it may be used by another device or display. A power control **1345** is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer **1347** is a device that queues instructions to be sent to the chip's internal memory. A security management unit **1346** is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block **1349** is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory **1348** stores data. Information can be read and written from or to this device.

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

FIG. **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 FIG. **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 Ser. No. 10/118,092, filed Apr. 2, 2002, and PCT Patent Application IB0201439, filed Apr. 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

FIG. **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 24×7; 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 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.

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 (PIPS) 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 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.

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 FIG. **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 = capaticance(F)

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

$$f_1 = 13.56\ MH_z$$

$$f_2 = 915\ MH_z$$

$$L = \frac{N^3\mu_\circ A}{1}$$

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)

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:

$$l = \frac{N^3\mu_\circ A}{1} \Rightarrow \frac{N^3\mu_\circ A}{1}\ \frac{l}{f^2 4\pi^2 C} \Rightarrow l = f^2 4\pi^2 N^2 \mu_\circ A$$

For substitution, the following values are used:

$$L_1 = 2.931\times10^{8} H$$

$$L_1 = 6.437\times10^{10} H$$

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

Multiple RF Chip Overview

FIG. **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

FIG. **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

FIG. **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.

FIG. **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.

FIG. **3**A illustrates the differences between transport mode and tunnel mode. The use of AH and ESP are illustrated in FIG. **38**.

B. Method of Limiting Software Downloads

FIG. **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

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

B. Method of Airport Security

FIG. **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 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:

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.

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

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

4. 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:

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.

5. The system of claim **4**, wherein the payment information is associated with a primary account number.

6. The system of claim **4**, wherein the POS device includes an RF reader.

7. The system of claim **4**, wherein the biometric authentication information is stored separately from the secured payment information.

* * * * *

EXHIBIT 7

US010762187B2

(12) **United States Patent**
Martinez de Velasco Cortina et al.

(10) **Patent No.: US 10,762,187 B2**
(45) **Date of Patent: *Sep. 1, 2020**

(54) **SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS**

(71) Applicant: **Neology, Inc.**, Poway, CA (US)

(72) Inventors: **Francisco Martinez de Velasco Cortina**, La Jolla, CA (US); **Manfred Rietzler**, Marktoberdorf (DE)

(73) Assignee: **NEOLOGY, INC.**, San Diego, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 533 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **14/659,502**

(22) Filed: **Mar. 16, 2015**

(65) **Prior Publication Data**

US 2015/0193766 A1 Jul. 9, 2015

Related U.S. Application Data

(63) Continuation of application No. 14/585,057, filed on Dec. 29, 2014, which is a continuation of application (Continued)

(51) **Int. Cl.**
G06F 21/35 (2013.01)
H04W 4/80 (2018.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06F 21/35*** (2013.01); ***G06F 21/31*** (2013.01); ***G06F 21/32*** (2013.01); ***G06F 21/34*** (2013.01); ***G06K 7/0008*** (2013.01); ***G06K 7/10*** (2013.01); ***G06K 7/10316*** (2013.01); ***G06K 7/10366*** (2013.01); ***G06K 19/025*** (2013.01); ***G06K 19/0723*** (2013.01); ***G06K 19/0776*** (2013.01);
(Continued)

(58) **Field of Classification Search**
None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,529,870 A 7/1985 Chaum
5,552,789 A 9/1996 Schuermann
(Continued)

FOREIGN PATENT DOCUMENTS

DE 19608757 A1 9/1997
DE 10042805 A1 3/2002
(Continued)

OTHER PUBLICATIONS

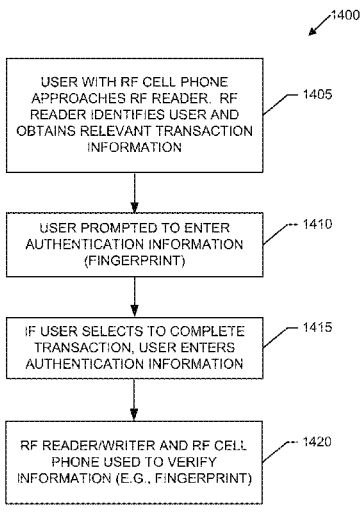
RFID Handbook—Active Load Modulation.*
(Continued)

Primary Examiner — Neha Patel
Assistant Examiner — El Mehdi Oussir
(74) *Attorney, Agent, or Firm* — Procopio, Cory, Hargreaves & Savitch LLP

(57) **ABSTRACT**

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

21 Claims, 24 Drawing Sheets



Related U.S. Application Data

No. 14/028,469, filed on Sep. 16, 2013, now Pat. No. 8,933,807, which is a continuation of application No. 13/350,665, filed on Jan. 13, 2012, now Pat. No. 8,587,436, which is a continuation of application No. 13/175,768, filed on Jul. 1, 2011, now Pat. No. 8,237,568, which is a continuation of application No. 12/688,666, filed on Jan. 15, 2010, now Pat. No. 8,004,410, which is a continuation of application No. 11/279,912, filed on Apr. 17, 2006, now Pat. No. 7,671,746, which is a continuation of application No. 10/615,026, filed on Jul. 9, 2003, now Pat. No. 7,081,819.

(60) Provisional application No. 60/394,241, filed on Jul. 9, 2002.

(51) **Int. Cl.**

G06F 21/34	(2013.01)
G06F 21/32	(2013.01)
G06F 21/31	(2013.01)
G06K 7/00	(2006.01)
G06K 19/07	(2006.01)
G06K 19/077	(2006.01)
G06K 19/10	(2006.01)
G07C 9/00	(2020.01)
H04W 12/06	(2009.01)
H04W 12/08	(2009.01)
G06K 7/10	(2006.01)
G06K 19/02	(2006.01)
H04L 29/06	(2006.01)
H04W 12/00	(2009.01)

(52) **U.S. Cl.**

CPC . ***G06K 19/07758*** (2013.01); ***G06K 19/07764*** (2013.01); ***G06K 19/10*** (2013.01); ***G07C 9/00087*** (2013.01); ***H04W 4/80*** (2018.02); ***H04W 12/06*** (2013.01); ***H04W 12/08*** (2013.01); *G06Q 2220/00* (2013.01); *H04L 63/0861* (2013.01); *H04M 2203/6009* (2013.01); *H04M 2203/6054* (2013.01); *H04W 12/00522* (2019.01)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,590,197	A *	12/1996	Chen	G06Q 20/04 380/30
5,627,544	A	5/1997	Snodgrass et al.	
5,657,008	A	8/1997	Bantli	
5,742,618	A	4/1998	Lowe	
5,787,174	A	7/1998	Tuttle	
5,819,234	A	10/1998	Slavin et al.	
5,864,580	A	1/1999	Lowe et al.	
5,874,896	A	2/1999	Lowe et al.	
5,940,006	A	8/1999	MacLellan et al.	
5,974,500	A	10/1999	Maletsky et al.	
6,025,780	A	2/2000	Bowers et al.	
6,025,784	A	2/2000	Mish	
6,052,068	A	4/2000	Price R et al.	
6,073,840	A	6/2000	Marion et al.	
6,089,284	A	7/2000	Kaehler et al.	
6,098,879	A	8/2000	Terranova et al.	
6,104,281	A	8/2000	Heinrich et al.	
6,111,506	A	8/2000	Yap et al.	
6,140,941	A	10/2000	Dwyer et al.	
6,157,333	A	12/2000	Louagie et al.	
6,163,771	A *	12/2000	Walker	G06Q 20/04 705/18
6,167,333	A	12/2000	Gehlot et al.	
6,175,922	B1	1/2001	Wang	
6,182,894	B1	2/2001	Hackett et al.	
6,203,952	B1	3/2001	O'Brien et al.	
6,211,790	B1	4/2001	Radomsky et al.	
6,268,796	B1	7/2001	Gnadinger et al.	
6,269,292	B1	7/2001	Kokubu et al.	
6,275,157	B1	8/2001	Mays et al.	
6,276,607	B1	8/2001	Sato	
6,334,059	B1	12/2001	Stilp et al.	
6,340,116	B1	1/2002	Cecil et al.	
6,360,208	B1	3/2002	Ohanian et al.	
6,388,579	B1	5/2002	Adcox et al.	
6,427,504	B1	8/2002	Janssen et al.	
6,570,487	B1	5/2003	Steeves	
6,570,488	B2	5/2003	Kucharczyk et al.	
6,617,961	B1	9/2003	Janssen et al.	
6,698,653	B1	3/2004	Diamond et al.	
6,753,759	B2	6/2004	Stegmaier et al.	
6,758,405	B2	7/2004	Look	
6,793,134	B2	9/2004	Clark	
6,848,048	B1 *	1/2005	Holmes	G06F 21/64 713/162
6,850,147	B2	2/2005	Prokoski	
6,894,615	B2	5/2005	Look	
6,934,689	B1 *	8/2005	Ritter	G06Q 20/04 705/16
6,934,861	B2	8/2005	Haala	
6,950,013	B2	9/2005	Scaman et al.	
6,975,834	B1	12/2005	Forster	
7,031,946	B1	4/2006	Tamai et al.	
7,080,819	B2	7/2006	Tojo	
7,081,819	B2	7/2006	Martinez de Velasco Cortina et al.	
7,096,363	B2	8/2006	Kon et al.	
7,225,337	B2	5/2007	Baessler	
7,310,734	B2	12/2007	Boate et al.	
7,487,538	B2	2/2009	Mok	
7,533,809	B1	5/2009	Robinson et al.	
7,671,746	B2	3/2010	Martinez de Velasco Cortina et al.	
7,844,505	B1	11/2010	Arneson et al.	
7,911,643	B2 *	3/2011	Yamada	H04N 1/33307 358/1.15
7,980,378	B2	7/2011	Jones et al.	
7,987,501	B2	7/2011	Miller et al.	
8,004,410	B2	8/2011	Martinez de Velasco Cortina et al.	
8,041,815	B2	10/2011	Bahl et al.	
8,126,449	B2	2/2012	Beenau et al.	
8,237,568	B2	8/2012	Martinez de Velasco Cortina et al.	
8,325,044	B2	12/2012	Martinez de Velasco Cortina et al.	
8,401,539	B2	3/2013	Beenau et al.	
8,548,927	B2	10/2013	Beenau et al.	
8,587,436	B2	11/2013	Martinez de Velasco Cortina et al.	
9,558,385	B2	1/2017	Martinez de Velasco Cortina et al.	
9,858,566	B2 *	1/2018	Mardikar	G06Q 20/1085
2002/0089434	A1	7/2002	Ghazarian	
2002/0109580	A1	8/2002	Shreve et al.	
2002/0112171	A1 *	8/2002	Ginter	G06F 21/10 713/185
2002/0112177	A1	8/2002	Voltmer	
2002/0123325	A1 *	9/2002	Cooper	H04L 63/0492 455/411
2002/0157029	A1 *	10/2002	French	G06F 21/31 726/21
2002/0193142	A1 *	12/2002	Stavenow	G06F 21/41 455/556.1
2002/0194499	A1 *	12/2002	Audebert	H04L 63/0853 726/35
2003/0018522	A1 *	1/2003	Denimarck	G06Q 20/40145 705/14.23
2003/0019929	A1	1/2003	Stewart et al.	
2003/0074317	A1	4/2003	Hofi	
2003/0137403	A1	7/2003	Carrender et al.	

(56) **References Cited**

U.S. PATENT DOCUMENTS

2003/0200227	A1	10/2003	Ressler	
2004/0128249	A1	7/2004	Hoffman	
2005/0149764	A1	7/2005	Bahl et al.	
2006/0020558	A1*	1/2006	Bonalle	G06Q 20/341 705/64
2006/0204048	A1*	9/2006	Morrison	G06F 21/31 382/115
2007/0022058	A1*	1/2007	Labrou	G06Q 20/32 705/67
2007/0198436	A1*	8/2007	Weiss	G06F 21/32 705/75
2010/0094754	A1	4/2010	Bertran et al.	
2010/0095130	A1	4/2010	Bertran et al.	

FOREIGN PATENT DOCUMENTS

EP	0977145	A2	2/2000
EP	0993999	A2	4/2000
JP	2002042076	A	2/2002
WO	9843104	A2	10/1998
WO	2004006165	A1	1/2004

OTHER PUBLICATIONS

Smart Card Technology Past Present and Future Mohammed 2004.*
Understanding the Requirements of ISO IEC 14443.*
Ewa Syta, S. K. (2010). RFID-based Authentication Middleware for Mobile Devices. IEEE, 1-10. Retrieved from http://www.cs.ccsu.edu/~stan/research/pervasive/pubs/hicss2010rfidam.pdf.*
Atmel, Atmel Smart Card ICs, Silicon solutions making smart cards smarter, 12 pages.
Extended European Search Report, European Patent Application No. 10182033.0, dated Jan. 13, 2012, 7 pages.
Fancher, Carol Hovenga. Motorola, Inc., In your pocket smartcards, IEEE Spectrum, Feb. 1997, 7 pages.
Rakers, et al. Secure Contactless Smartcard ASIC with DPA Protection, IEEE Journal of Solid-State Circuits, vol. 36, No. 36, Mar. 2001, 7 pages.
Japanese Office Action, Japanese Patent Application No. 2004-519130, dated May 12, 2009, 10 pages.
Anonymous, Read/write RFID offers standalone advantages, Security, Aug. 1996; 33, 8; ProQuest, 1 page.
Response to Office Action filed on May 2, 2017 for U.S. Appl. No. 15/372,317.
U.S. Office Action dated Feb. 2, 2017 received in U.S. Appl. No. 15/372,317.
Response to Office Action filed on Nov. 18, 2016 for U.S. Appl. No. 14/321,781.
U.S. Office Action dated May 19, 2016 received in U.S. Appl. No. 14/321,781.
Response to Office Action filed on Dec. 24, 2015 for U.S. Appl. No. 14/321,781.
U.S. Office Action dated Jun. 24, 2015 received in U.S. Appl. No. 14/321,781.
U.S. Notice of Allowance dated Jul. 11, 2014 received in U.S. Appl. No. 14/022,135.
Response to Office Action filed on Mar. 14, 2014 for U.S. Appl. No. 14/022,135.
U.S. Office Action dated Mar. 7, 2014 received in U.S. Appl. No. 14/022,135.
Response to Office Action filed on Feb. 3, 2014 for U.S. Appl. No. 14/022,135.
U.S. Office Action dated Dec. 5, 2013 received in U.S. Appl. No. 14/022,135.
Appeal Brief filed Feb. 9, 2017 for U.S. Appl. No. 14/585,057.
Pre-Brief Appeal Conference Decision dated Nov. 30, 2016 and received in U.S. Appl. No. 14/585,057.
Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Nov. 9, 2016 for U.S. Appl. No. 14/585,057.
U.S. Office Action dated May 9, 2016 received in U.S. Appl. No. 14/585,057.
Response to Office Action filed on Jan. 7, 2016 for U.S. Appl. No. 14/585,057.
U.S. Office Action dated Oct. 7, 2015 received in U.S. Appl. No. 14/585,057.
U.S. Notice of Allowance dated Dec. 3, 2014 received in U.S. Appl. No. 14/028,469.
Supplemental response to Office Action filed on Oct. 31, 2014 for U.S. Appl. No. 14/028,469.
Response to Office Action filed on Oct. 14, 2014 for U.S. Appl. No. 14/028,469.
U.S. Office Action dated Aug. 18, 2014 received in U.S. Appl. No. 14/028,469.
U.S. Office Action dated Jul. 9, 2014 received in U.S. Appl. No. 14/028,469.
Response to Office Action filed on Jun. 13, 2014 for U.S. Appl. No. 14/028,469.
U.S. Office Action dated Apr. 3, 2014 received in U.S. Appl. No. 14/028,469.
Response to Office Action filed on Mar. 14, 2014 for U.S. Appl. No. 14/028,469.
U.S. Office Action dated Mar. 6, 2014 received in U.S. Appl. No. 14/028,469.
Response to Office Action filed on Feb. 3, 2014 for U.S. Appl. No. 14/028,469.
U.S. Office Action dated Dec. 6, 2013 received in U.S. Appl. No. 14/028,469.
Appeal Brief filed Jan. 30, 2017 for U.S. Appl. No. 14/639,034.
Pre-Brief Appeal Conference Decision dated Jul. 21, 2016 and received in U.S. Appl. No. 14/639,034.
Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Jun. 30, 2016 for U.S. Appl. No. 14/639,034.
U.S. Office Action dated Dec. 30, 2015 received in U.S. Appl. No. 14/639,034.
Response to Office Action filed on Nov. 30, 2015 for U.S. Appl. No. 14/639,034.
U.S. Office Action dated May 29, 2015 received in U.S. Appl. No. 14/639,034.
Response to Office Action filed on Apr. 26, 2017 for U.S. Appl. No. 14/724,593.
U.S. Office Action dated Feb. 17, 2017 received in U.S. Appl. No. 14/724,593.
Pre-Brief Appeal Conference Decision dated Dec. 12, 2016 and received in U.S. Appl. No. 14/724,593.
Pre-Appeal Brief Request for Review, Notice of Appeal, and Pre-Brief Brief filed on Nov. 7, 2016 for U.S. Appl. No. 14/724,593.
U.S. Office Action dated May 6, 2016 received in U.S. Appl. No. 14/724,593.
Response to Office Action filed on Jan. 7, 2016 for U.S. Appl. No. 14/724,593.
U.S. Office Action dated Aug. 4, 2015 received in U.S. Appl. No. 14/724,593.
Preliminary Amendment filed on Aug. 28, 2018 in U.S. Appl. No. 16/051,751. (6 pages).
U.S. Office Action dated Feb. 4, 2019 received in U.S. Appl. No. 16/051,751.(17 pages).
Response to Office Action filed Apr. 30, 2019 in U.S. Appl. No. 16/051,751.(8 pages).

* cited by examiner

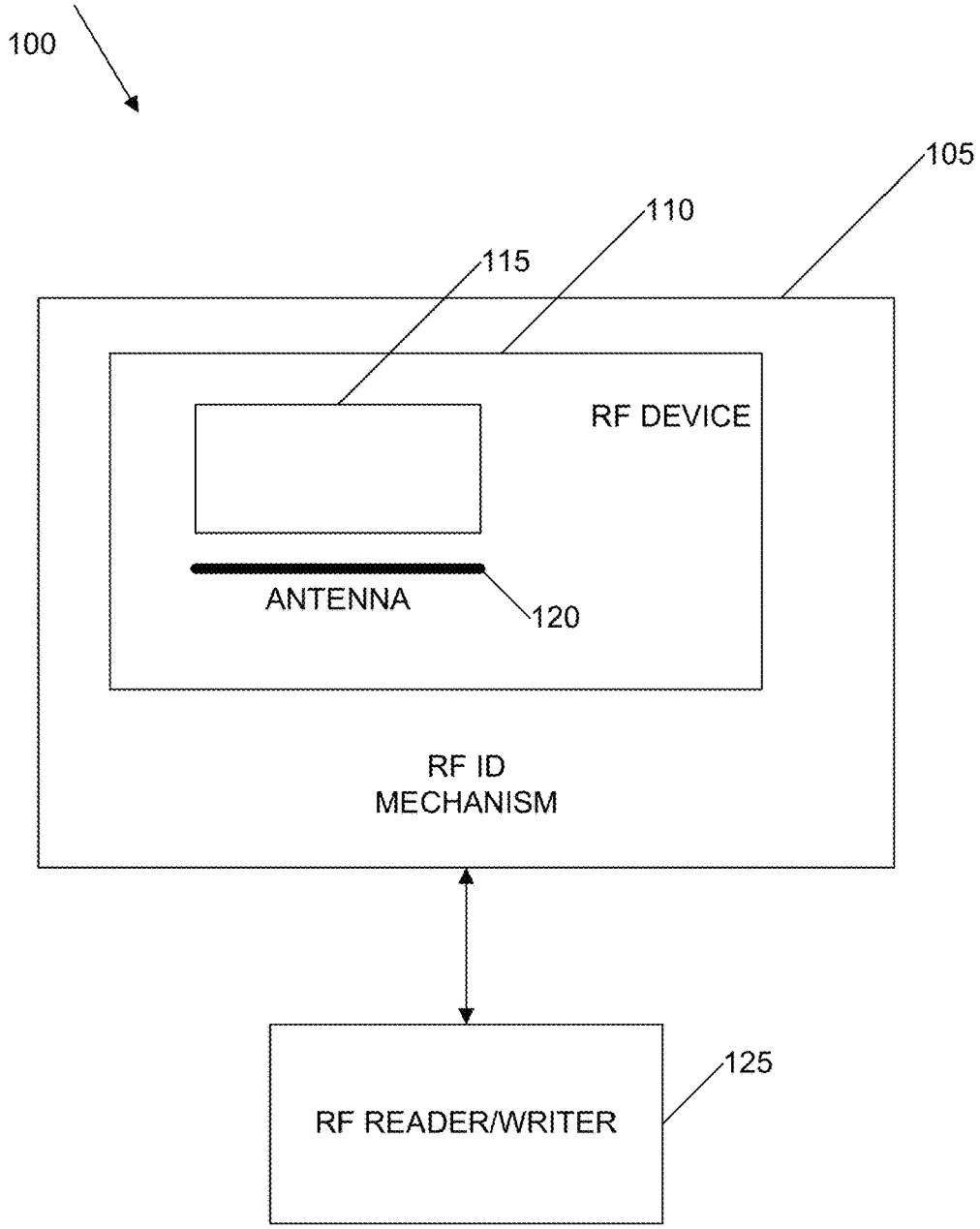

100
105
110
115
RF DEVICE
ANTENNA
120
RF ID
MECHANISM
RF READER/WRITER
125

FIG. 1

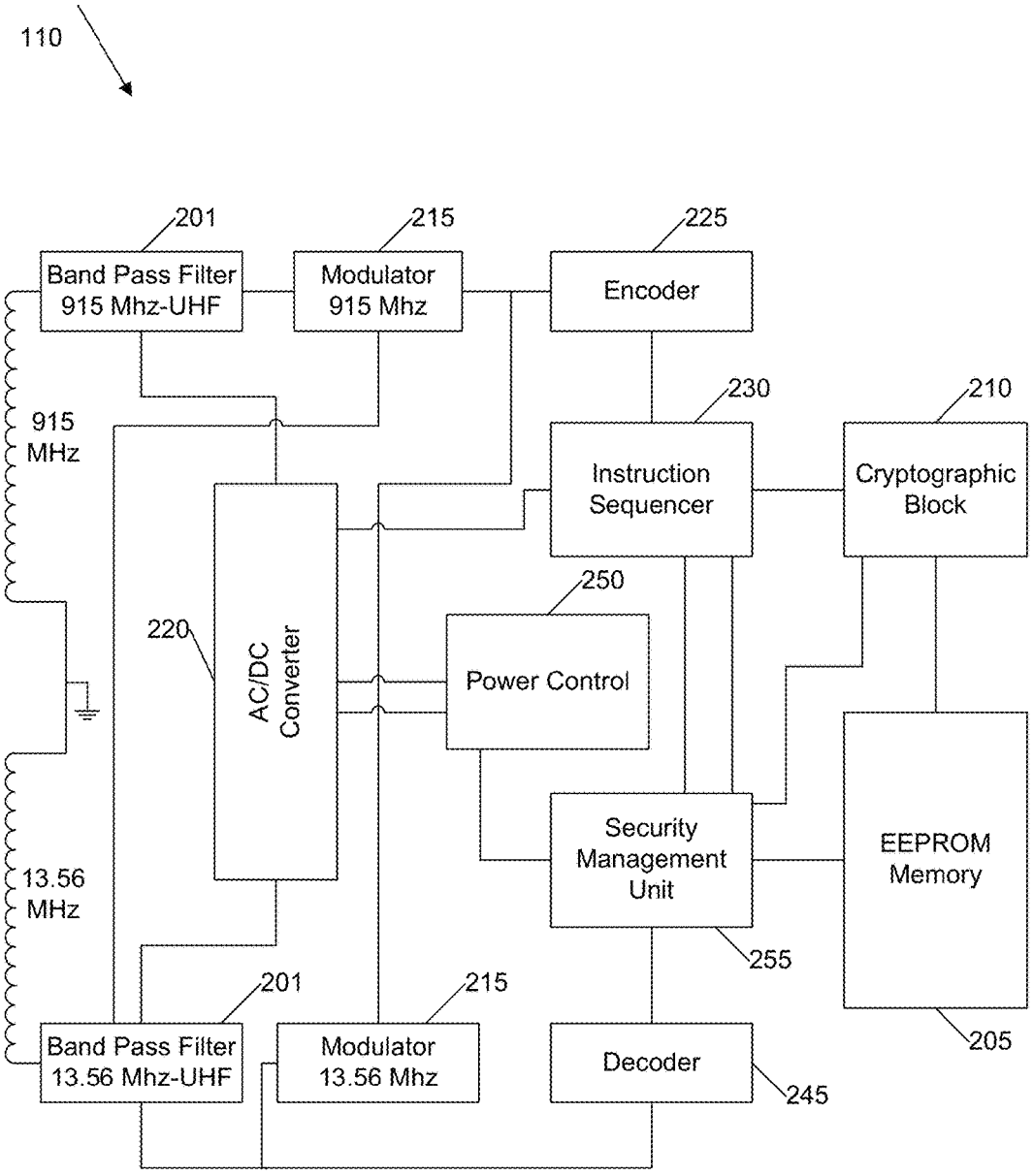

110
201
Band Pass Filter
915 Mhz-UHF
215
Modulator
915 Mhz
225
Encoder
915
MHz
230
Instruction
Sequencer
210
Cryptographic
Block
250
220
AC/DC
Converter
Power Control
Security
Management
Unit
EEPROM
Memory
255
205
13.56
MHz
201
Band Pass Filter
13.56 Mhz-UHF
215
Modulator
13.56 Mhz
Decoder
245

FIG. 2

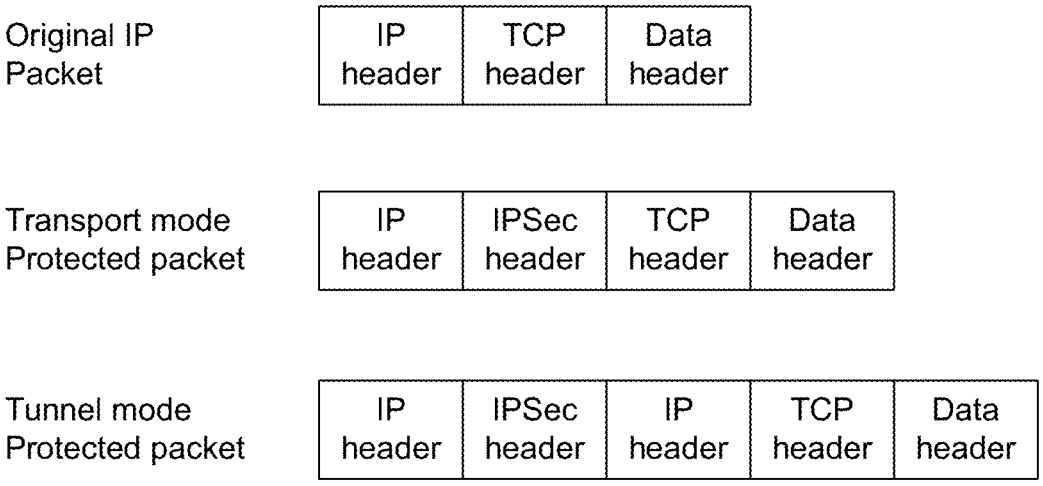

Original IP Packet
IP header
TCP header
Data header
Transport mode Protected packet
IP header
IPSec header
TCP header
Data header
Tunnel mode Protected packet
IP header
IPSec header
IP header
TCP header
Data header

FIG. 3A

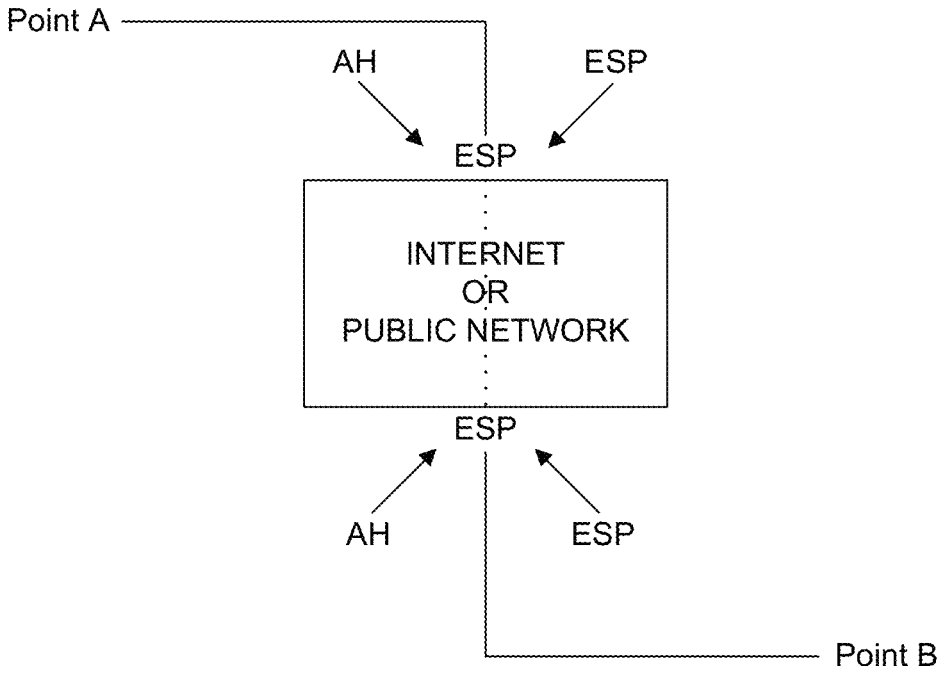

Point A
AH
ESP
ESP
INTERNET
OR
PUBLIC NETWORK
ESP
AH
ESP
Point B

FIG. 3B

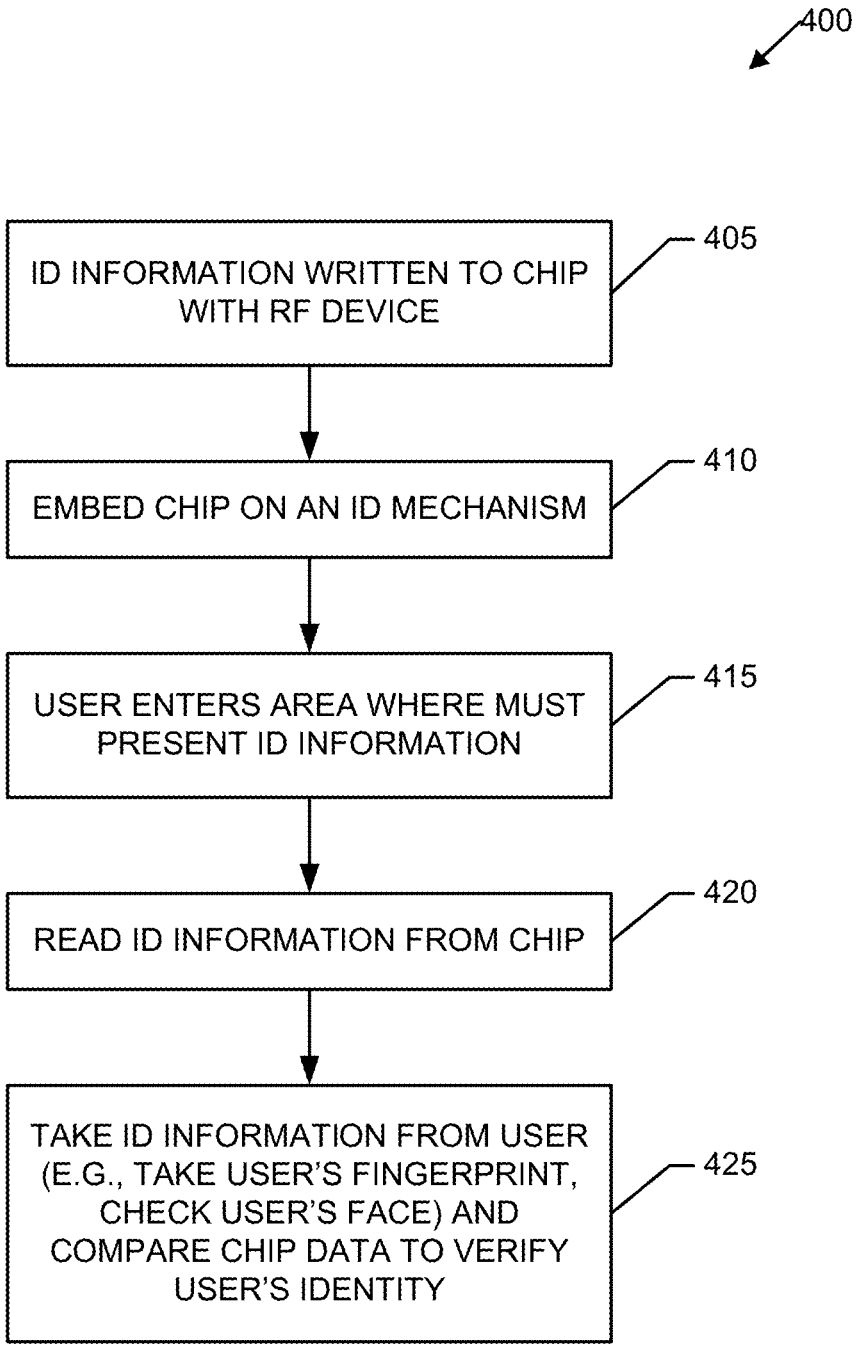

400
ID INFORMATION WRITTEN TO CHIP WITH RF DEVICE
405
EMBED CHIP ON AN ID MECHANISM
410
USER ENTERS AREA WHERE MUST PRESENT ID INFORMATION
415
READ ID INFORMATION FROM CHIP
420
TAKE ID INFORMATION FROM USER (E.G., TAKE USER'S FINGERPRINT, CHECK USER'S FACE) AND COMPARE CHIP DATA TO VERIFY USER'S IDENTITY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

FIG. 4

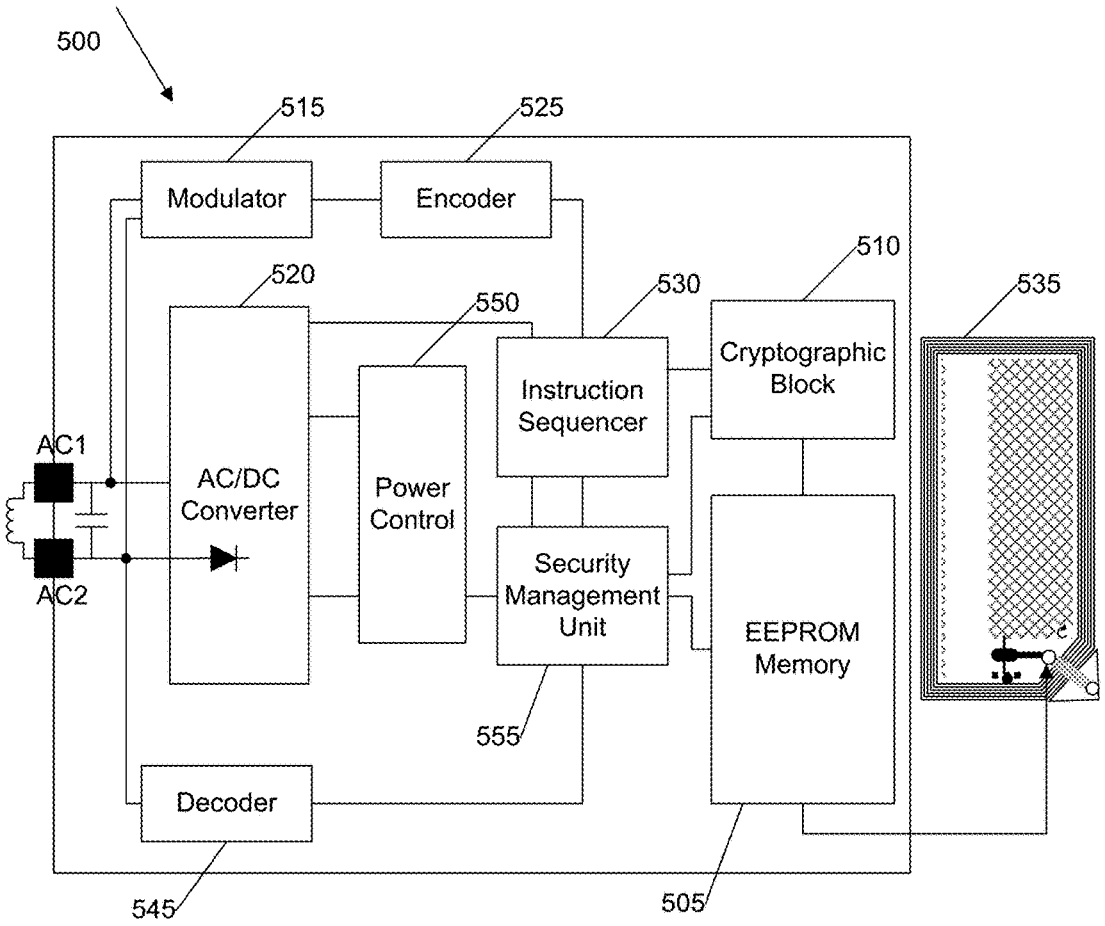

500
515
525
Modulator
Encoder
510
520
530
535
550
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
555
Decoder
545
505

FIG. 5

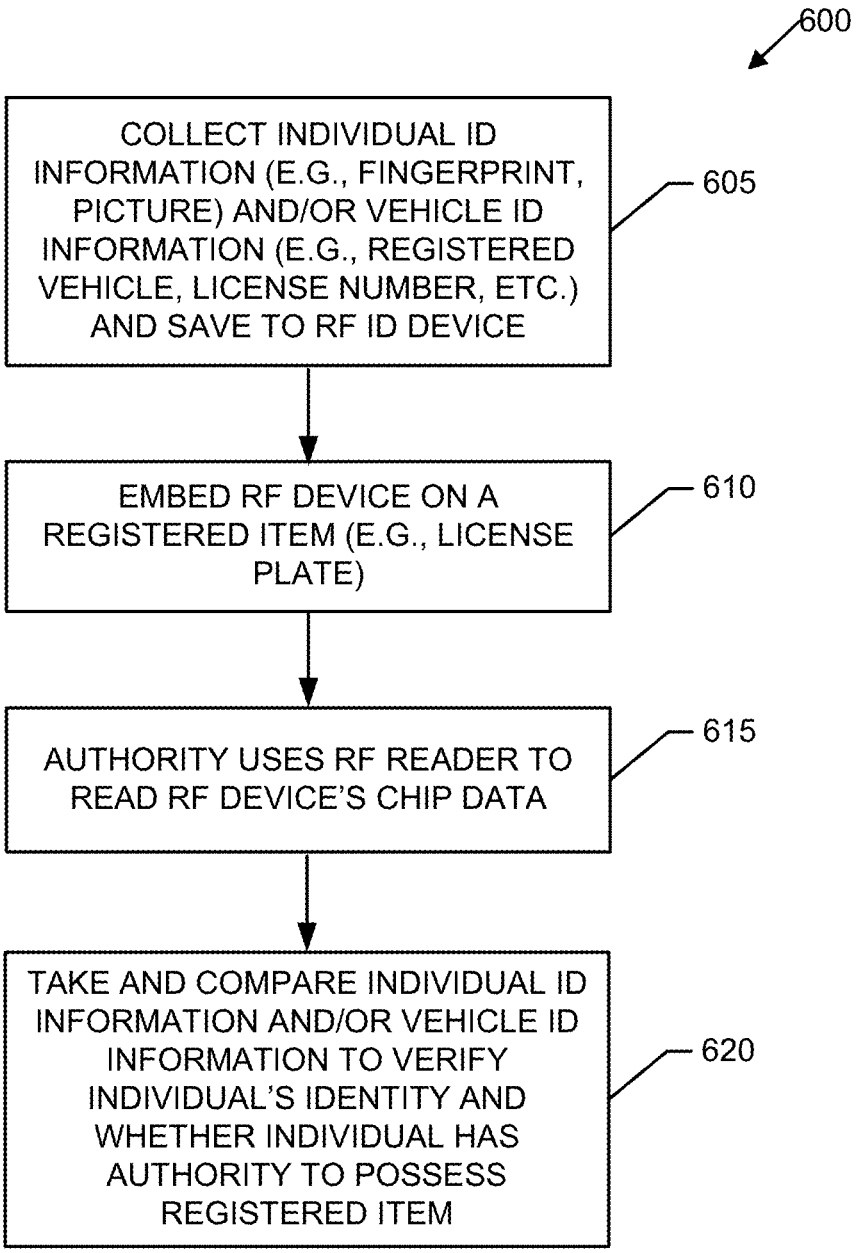

600
COLLECT INDIVIDUAL ID INFORMATION (E.G., FINGERPRINT, PICTURE) AND/OR VEHICLE ID INFORMATION (E.G., REGISTERED VEHICLE, LICENSE NUMBER, ETC.) AND SAVE TO RF ID DEVICE
605
EMBED RF DEVICE ON A REGISTERED ITEM (E.G., LICENSE PLATE)
610
AUTHORITY USES RF READER TO READ RF DEVICE'S CHIP DATA
615
TAKE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

FIG. 6

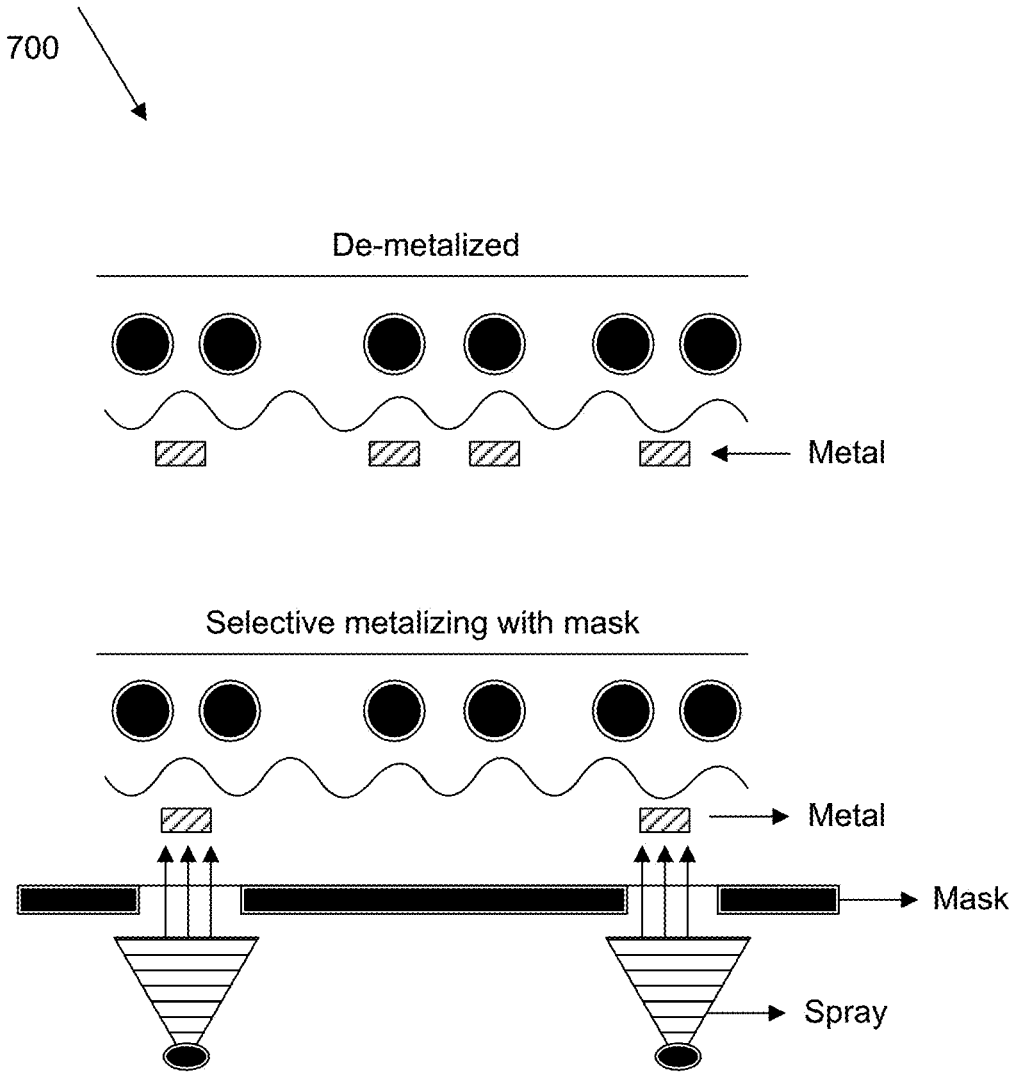

700
De-metalized
Metal
Selective metalizing with mask
Metal
Mask
Spray

FIG. 7

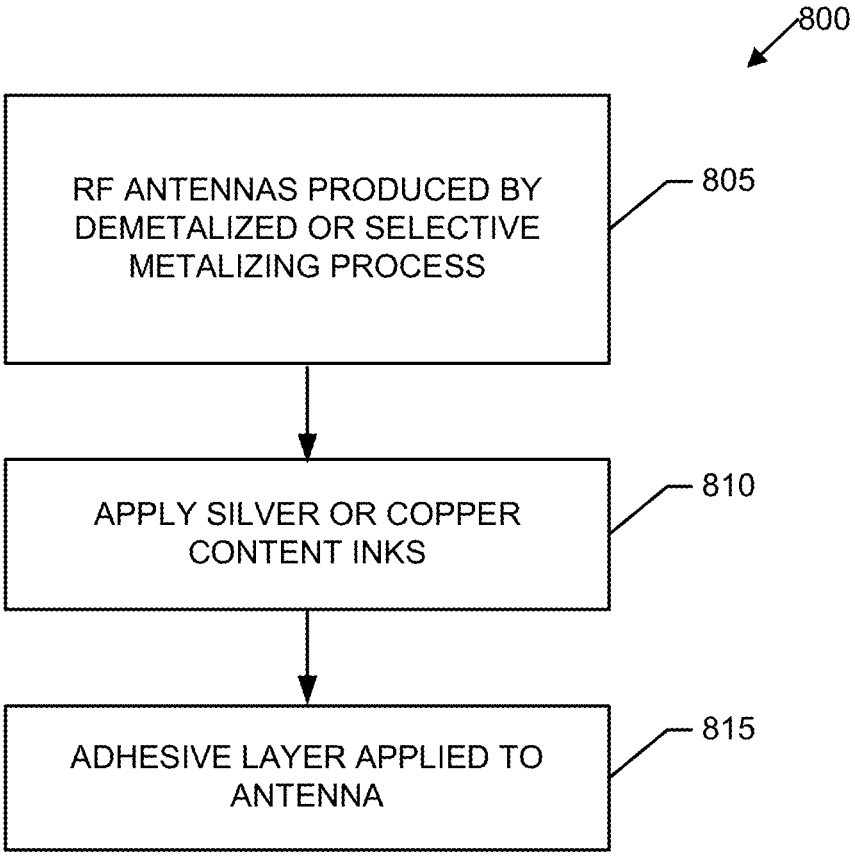

800
RF ANTENNAS PRODUCED BY DEMETALIZED OR SELECTIVE METALIZING PROCESS
805
APPLY SILVER OR COPPER CONTENT INKS
810
ADHESIVE LAYER APPLIED TO ANTENNA
815

FIG. 8

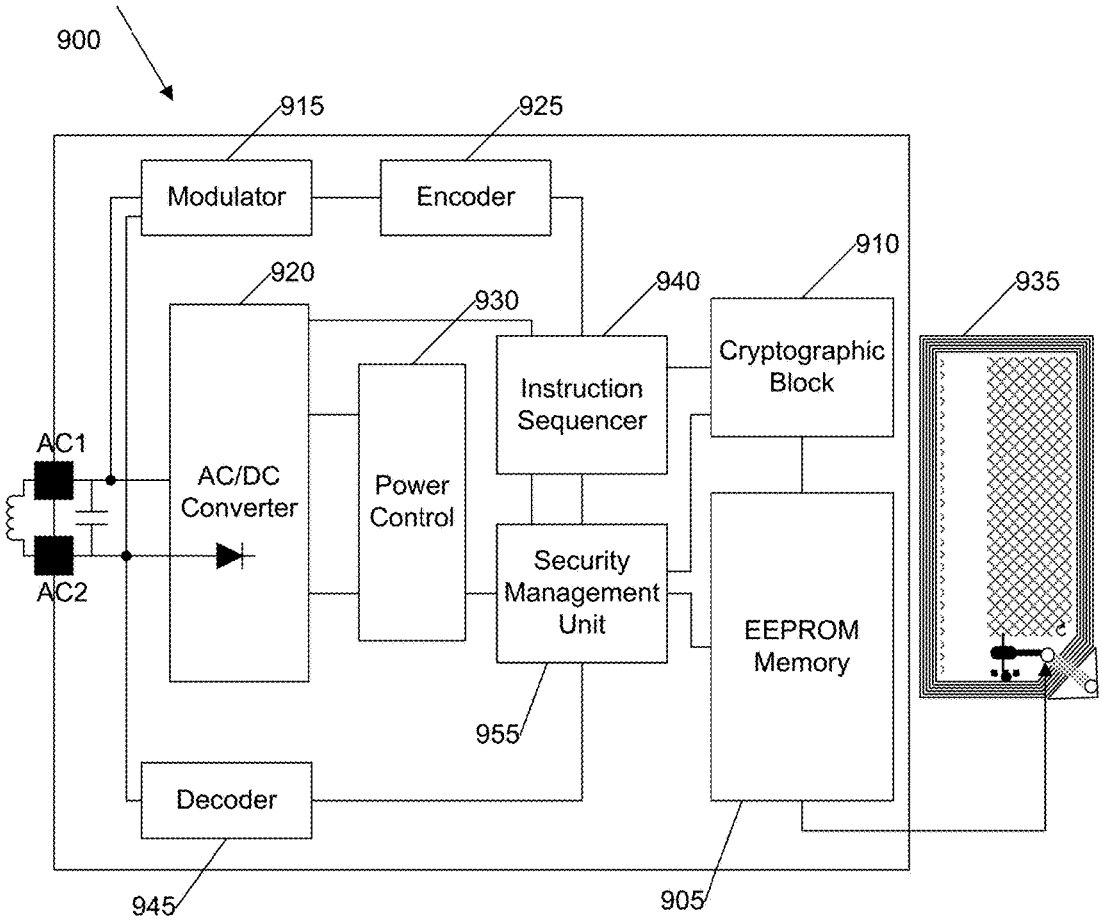

900
915
925
Modulator
Encoder
910
920
930
940
935
Cryptographic Block
Instruction Sequencer
AC1
AC/DC Converter
Power Control
Security Management Unit
EEPROM Memory
AC2
955
Decoder
945
905

FIG. 9

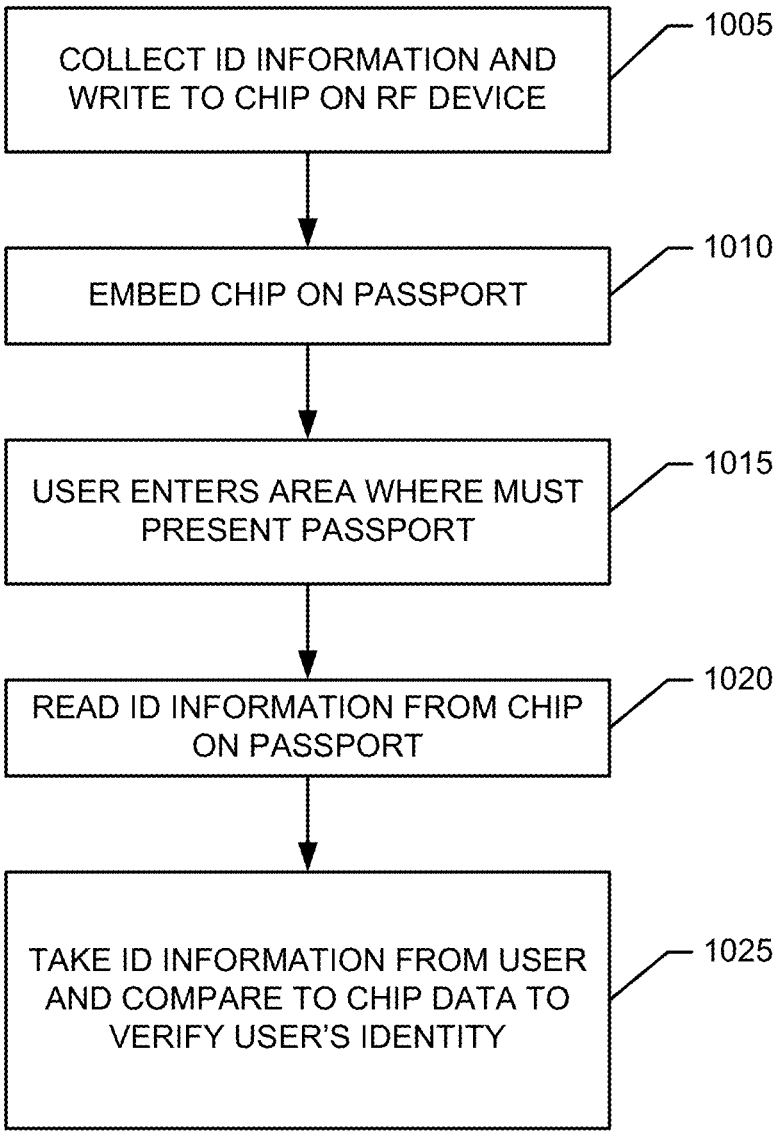

COLLECT ID INFORMATION AND WRITE TO CHIP ON RF DEVICE
1005
EMBED CHIP ON PASSPORT
1010
USER ENTERS AREA WHERE MUST PRESENT PASSPORT
1015
READ ID INFORMATION FROM CHIP ON PASSPORT
1020
TAKE ID INFORMATION FROM USER AND COMPARE TO CHIP DATA TO VERIFY USER'S IDENTITY
1025

FIG. 10

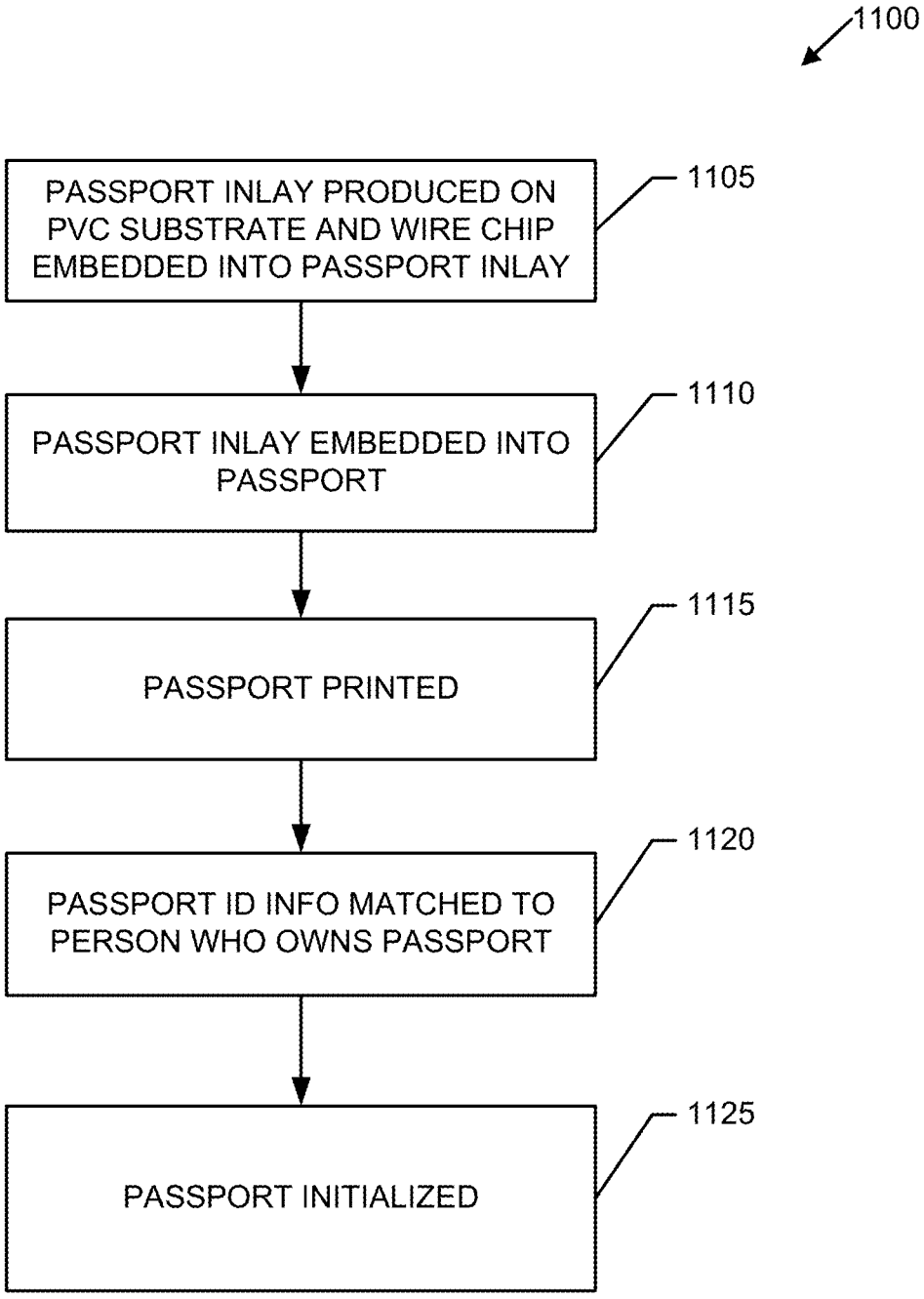

1100
PASSPORT INLAY PRODUCED ON PVC SUBSTRATE AND WIRE CHIP EMBEDDED INTO PASSPORT INLAY
1105
PASSPORT INLAY EMBEDDED INTO PASSPORT
1110
PASSPORT PRINTED
1115
PASSPORT ID INFO MATCHED TO PERSON WHO OWNS PASSPORT
1120
PASSPORT INITIALIZED
1125

FIG. 11

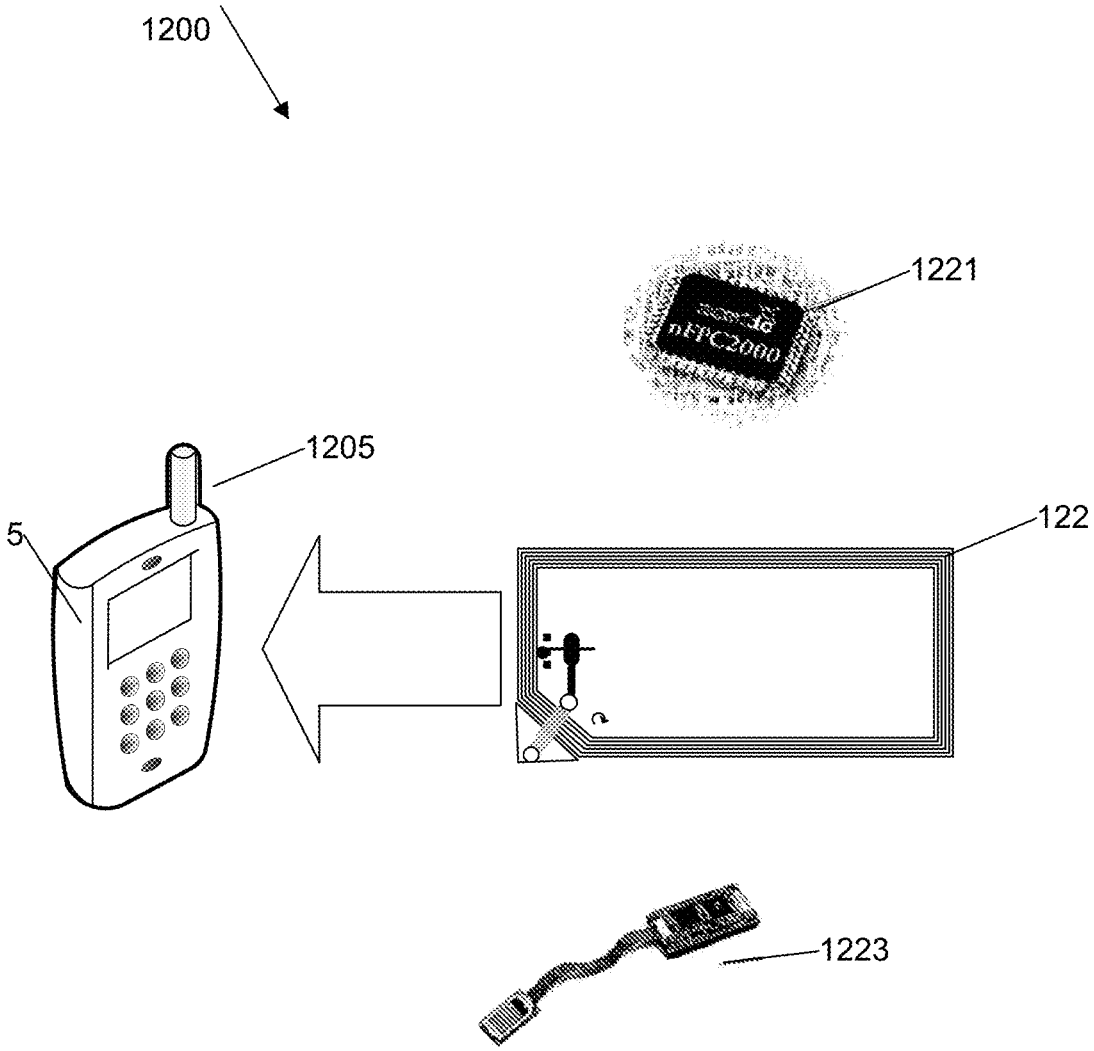


FIG. 12

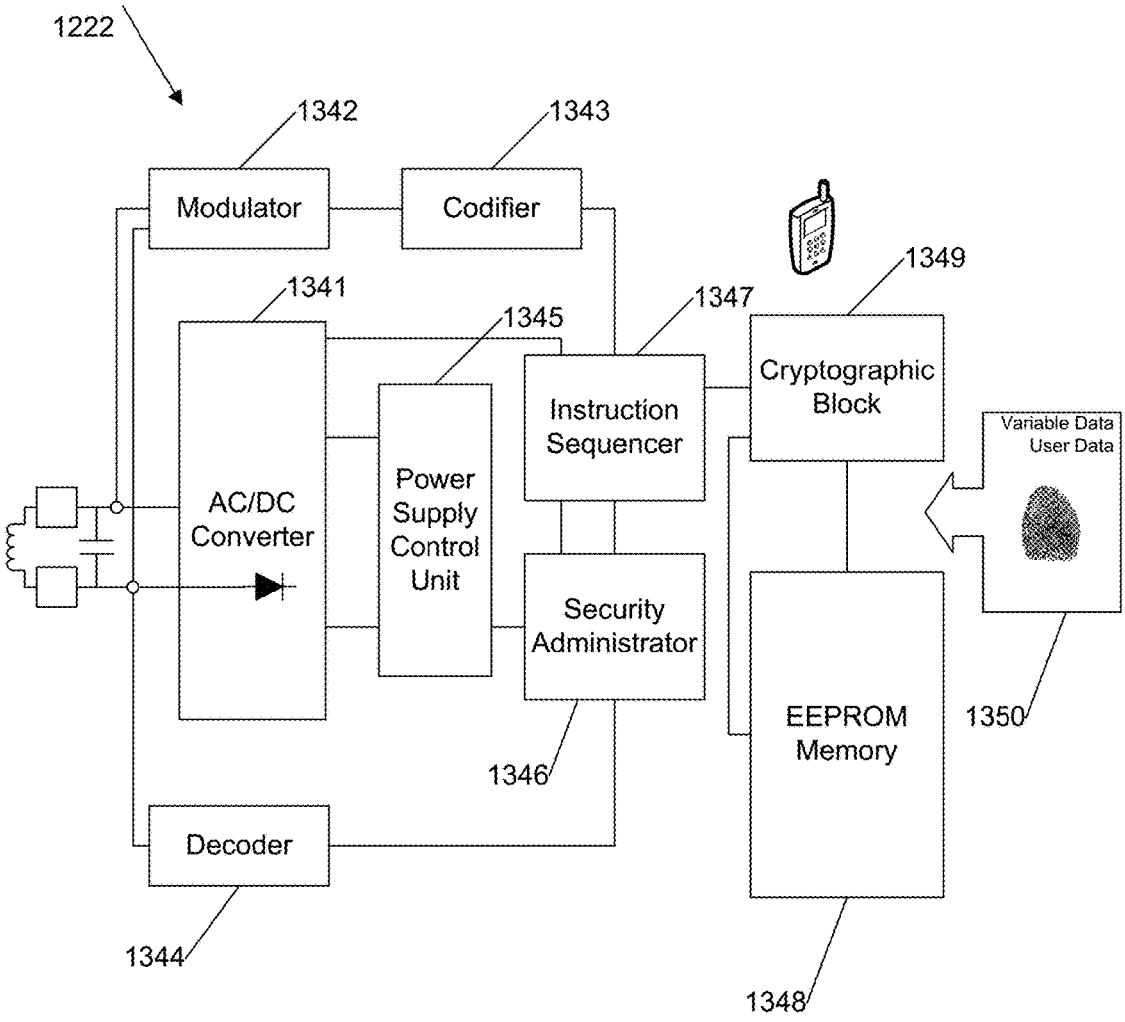

1222
1342
1343
Modulator
Codifier
1341
1345
1347
1349
Cryptographic Block
Instruction Sequencer
Variable Data
User Data
AC/DC Converter
Power Supply Control Unit
Security Administrator
EEPROM Memory
1350
1346
Decoder
1344
1348

FIG. 13

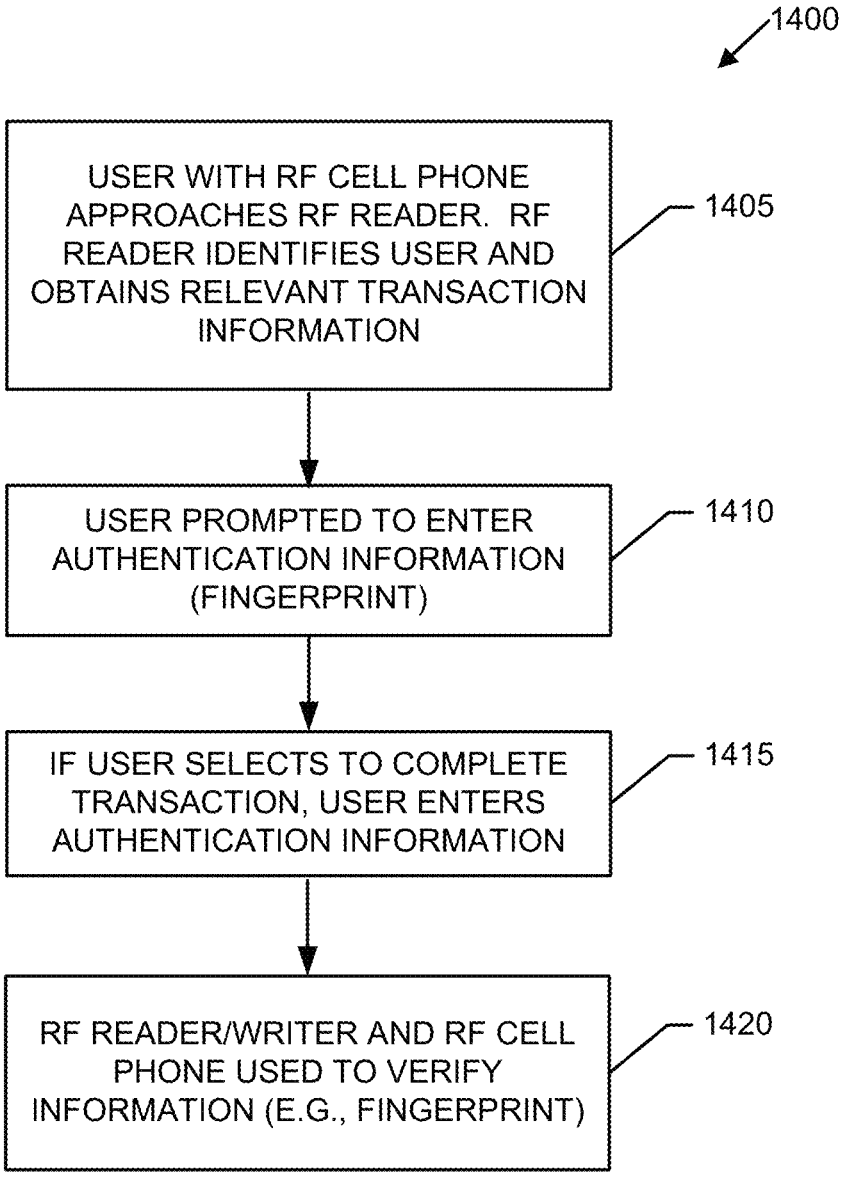

1400
USER WITH RF CELL PHONE APPROACHES RF READER. RF READER IDENTIFIES USER AND OBTAINS RELEVANT TRANSACTION INFORMATION
1405
USER PROMPTED TO ENTER AUTHENTICATION INFORMATION (FINGERPRINT)
1410
IF USER SELECTS TO COMPLETE TRANSACTION, USER ENTERS AUTHENTICATION INFORMATION
1415
RF READER/WRITER AND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

FIG. 14

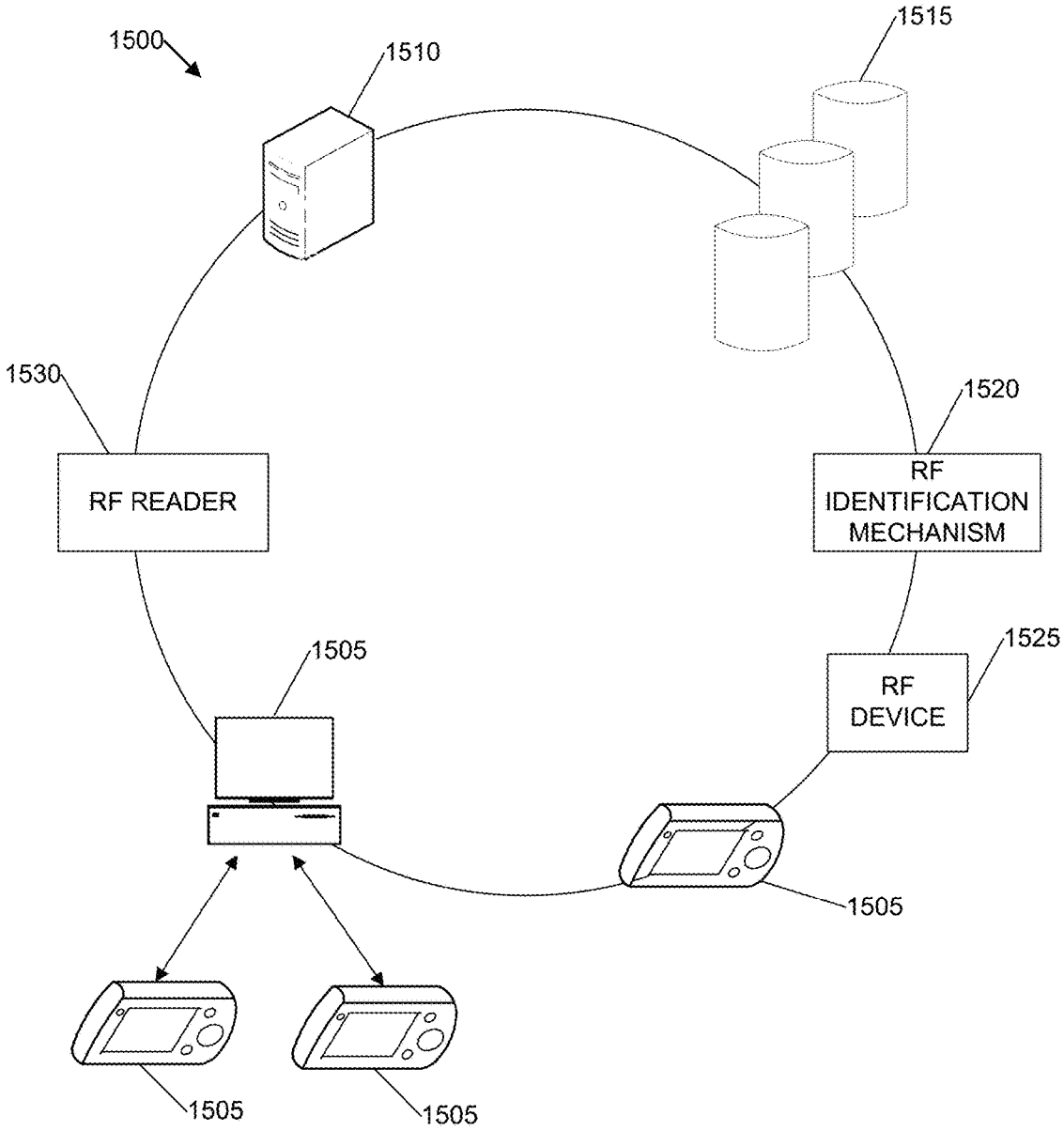

1500
1510
1515
1530
1520
RF READER
RF IDENTIFICATION MECHANISM
1505
1525
RF DEVICE
1505
1505
1505

FIG. 15

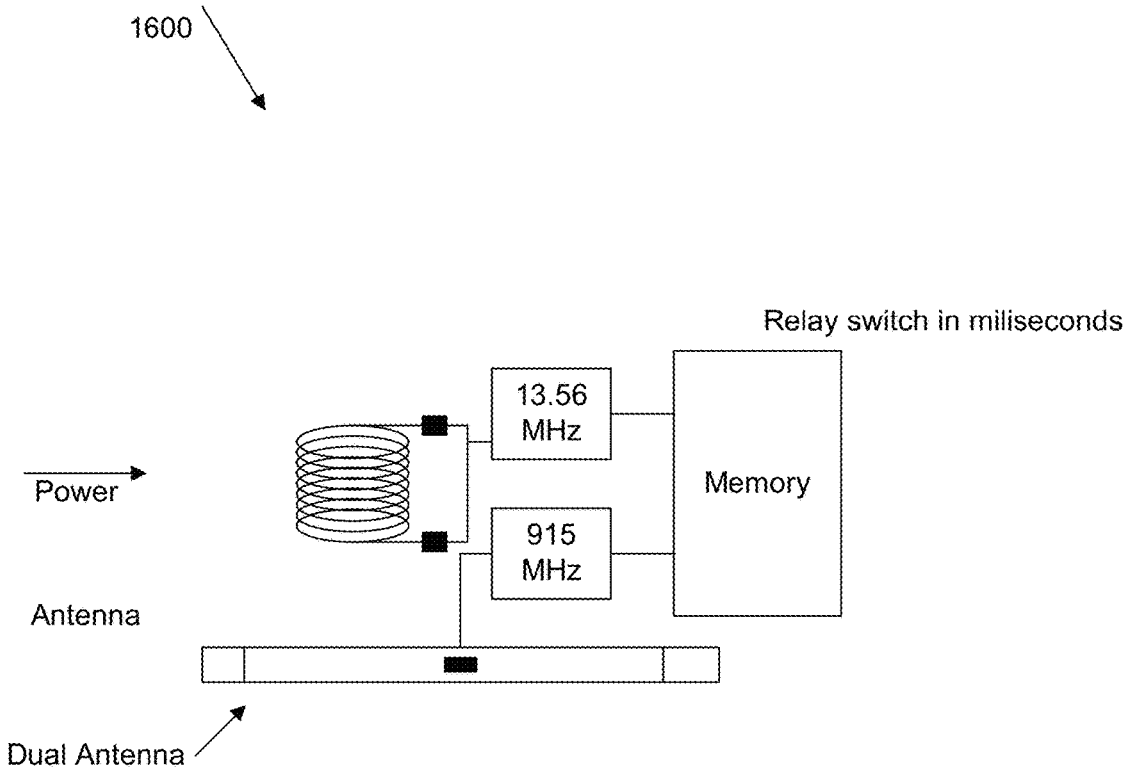

1600
Relay switch in miliseconds
13.56 MHz
915 MHz
Memory
Power
Antenna
Dual Antenna

FIG. 16

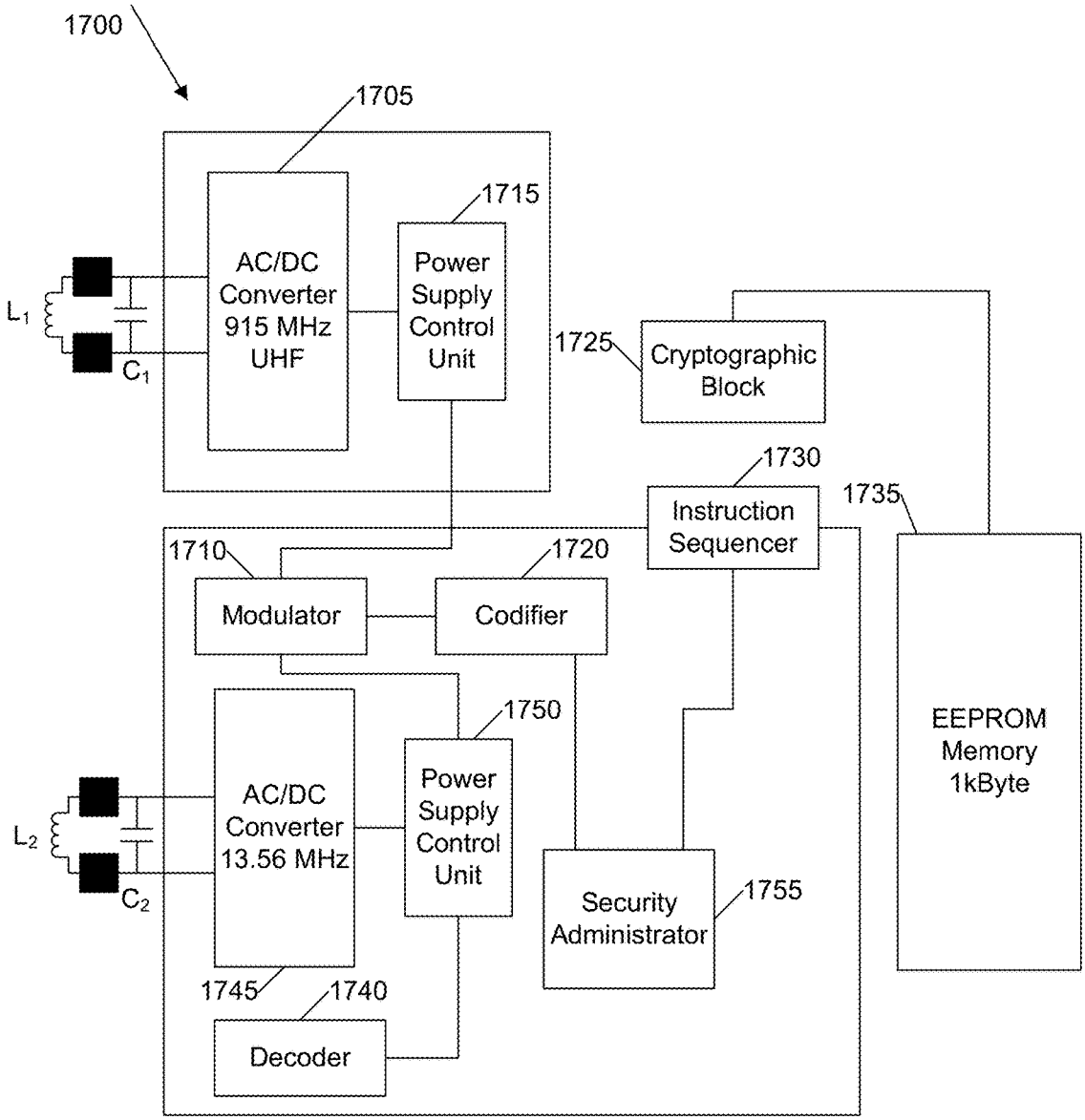

1700
1705
1715
AC/DC Converter 915 MHz UHF
Power Supply Control Unit
L1
C1
1725
Cryptographic Block
1730
Instruction Sequencer
1735
1710
1720
Modulator
Codifier
EEPROM Memory 1kByte
1750
AC/DC Converter 13.56 MHz
Power Supply Control Unit
L2
C2
Security Administrator
1755
1745
1740
Decoder

FIG. 17

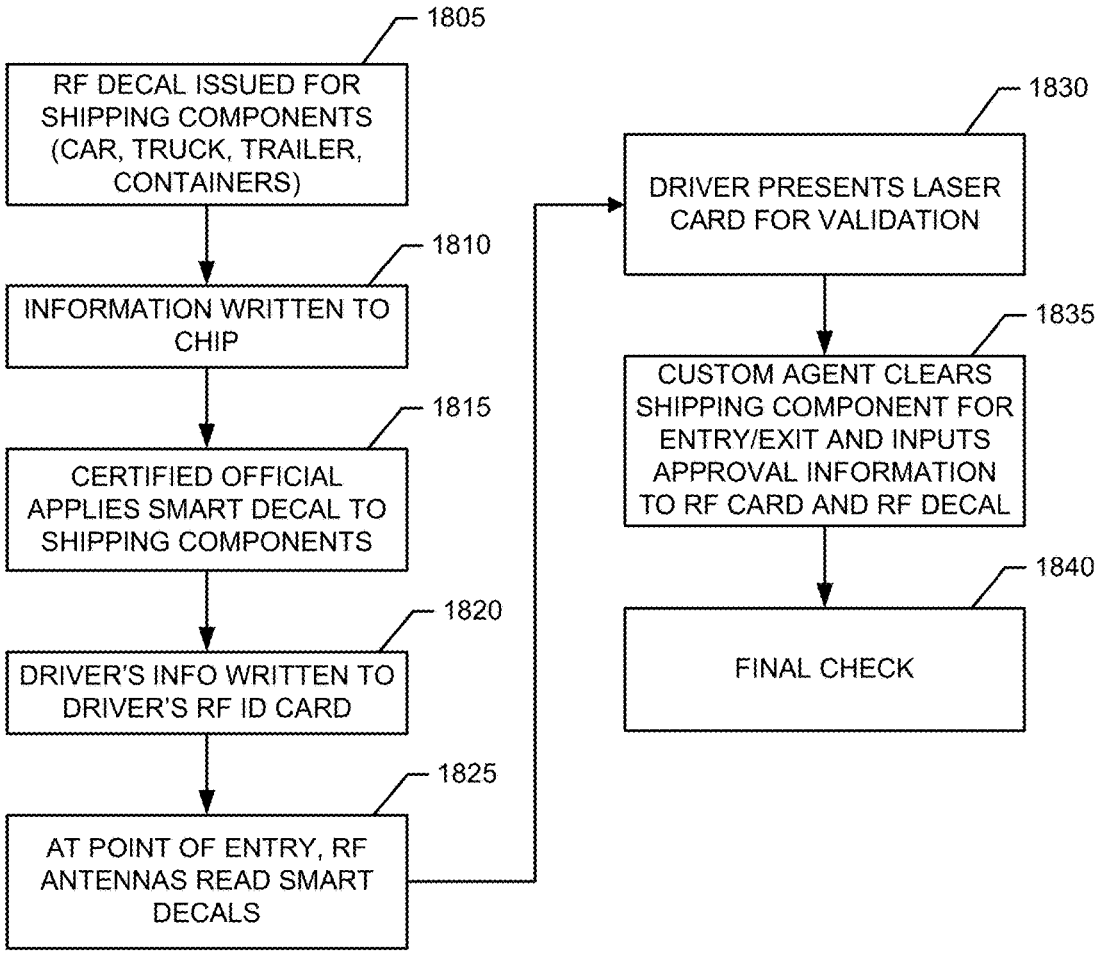

1805
RF DECAL ISSUED FOR SHIPPING COMPONENTS (CAR, TRUCK, TRAILER, CONTAINERS)
1810
INFORMATION WRITTEN TO CHIP
1815
CERTIFIED OFFICIAL APPLIES SMART DECAL TO SHIPPING COMPONENTS
1820
DRIVER'S INFO WRITTEN TO DRIVER'S RF ID CARD
1825
AT POINT OF ENTRY, RF ANTENNAS READ SMART DECALS
1830
DRIVER PRESENTS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

FIG. 18

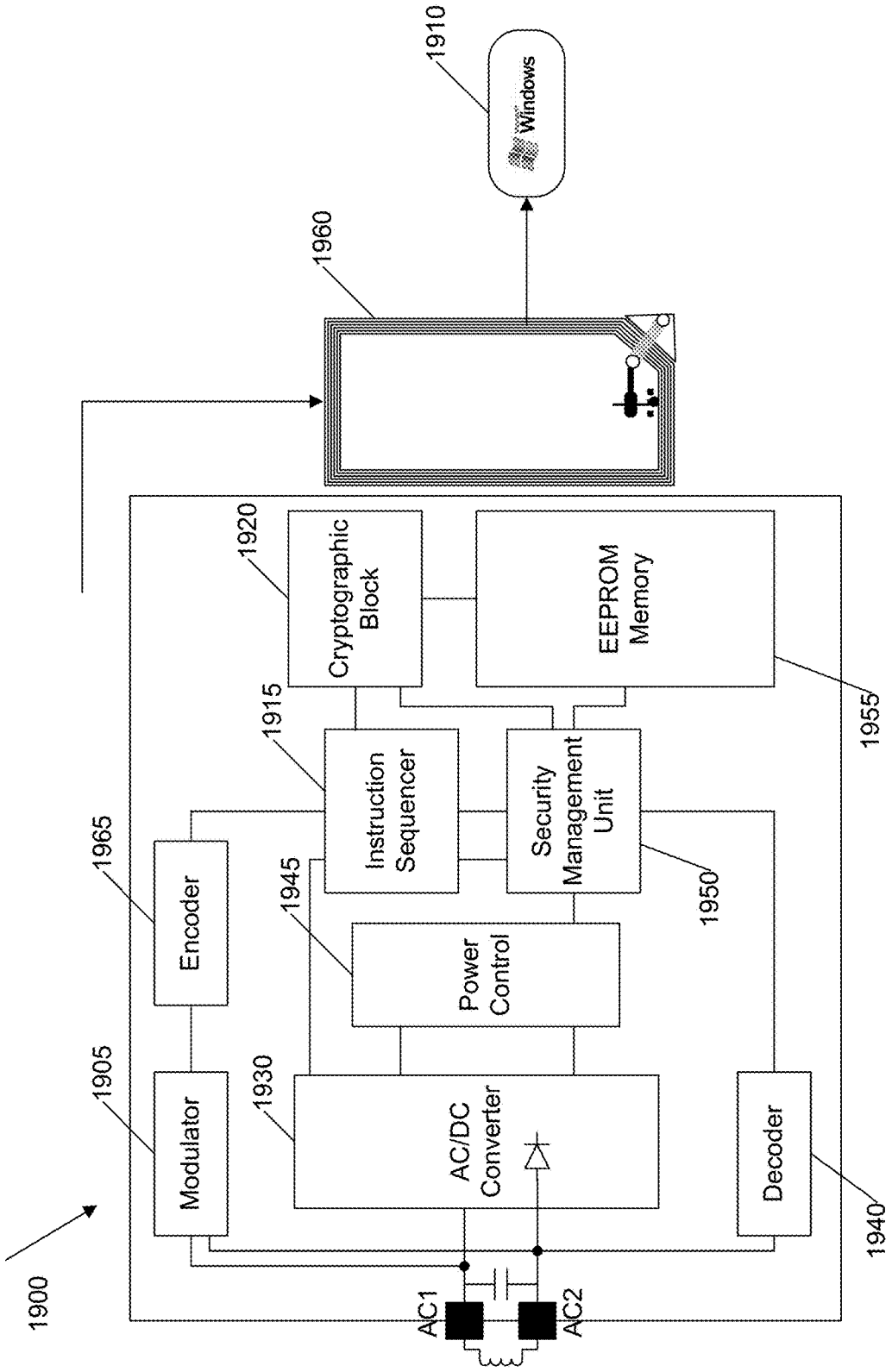

1910
Windows
1960
1920
Cryptographic Block
EEPROM Memory
1955
1915
Instruction Sequencer
Security Management Unit
1950
1965
Encoder
1945
Power Control
1905
Modulator
1930
AC/DC Converter
Decoder
1940
1900
AC1
AC2

FIG. 19

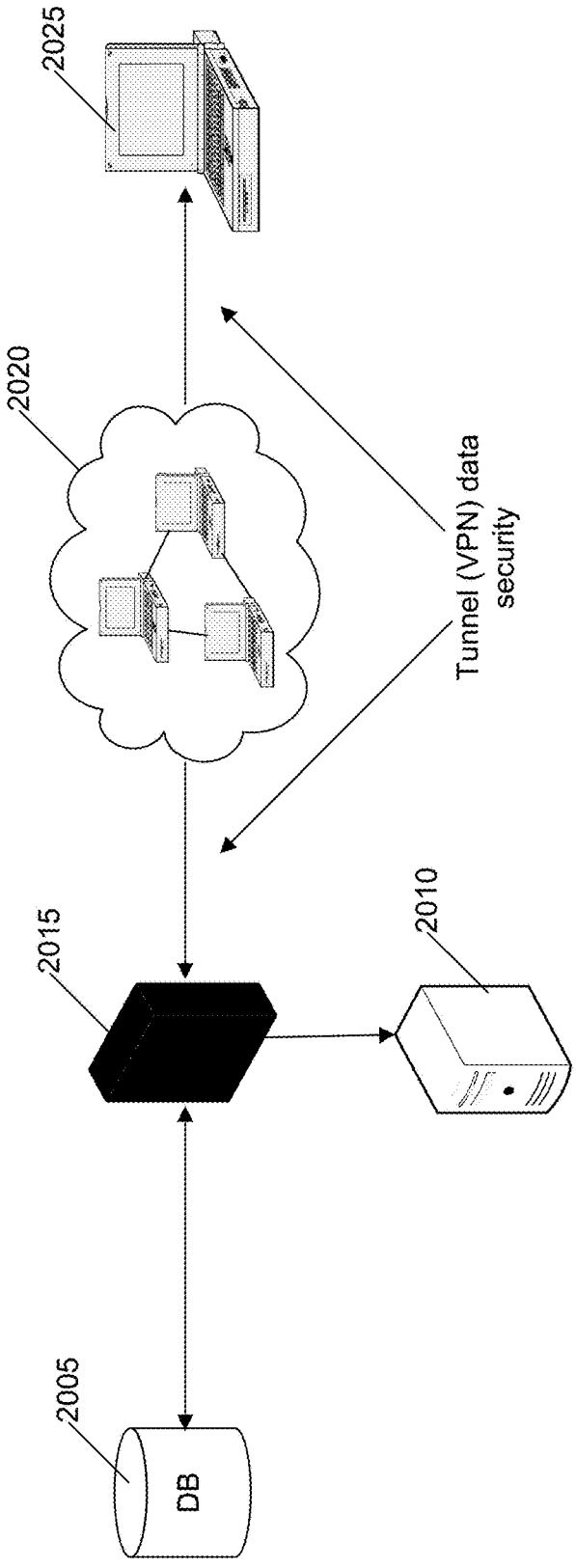


FIG. 20

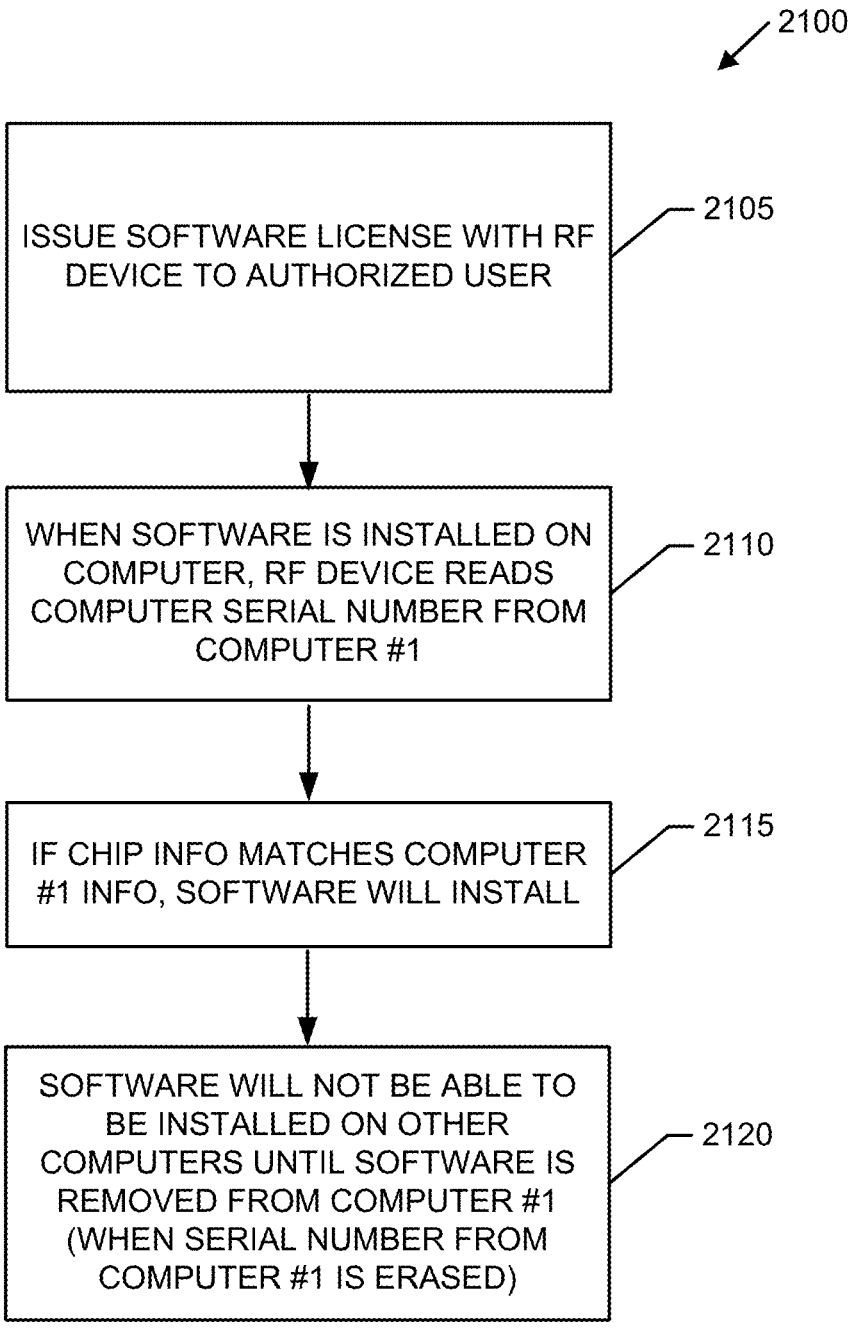

2100
ISSUE SOFTWARE LICENSE WITH RF DEVICE TO AUTHORIZED USER
2105
WHEN SOFTWARE IS INSTALLED ON COMPUTER, RF DEVICE READS COMPUTER SERIAL NUMBER FROM COMPUTER #1
2110
IF CHIP INFO MATCHES COMPUTER #1 INFO, SOFTWARE WILL INSTALL
2115
SOFTWARE WILL NOT BE ABLE TO BE INSTALLED ON OTHER COMPUTERS UNTIL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

FIG. 21

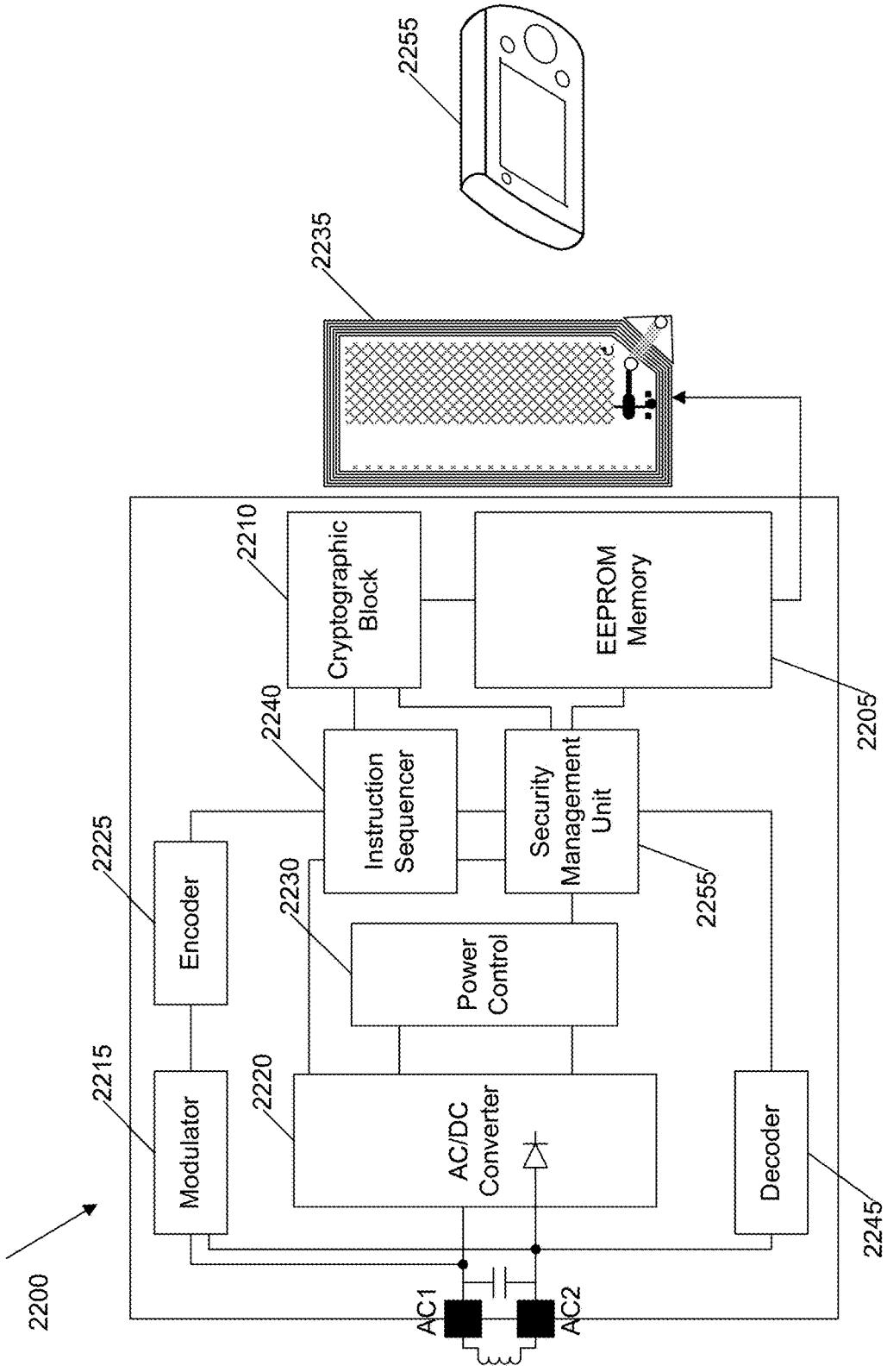

2255
2235
2210
Cryptographic Block
EEPROM Memory
2205
2240
Instruction Sequencer
Security Management Unit
2225
Encoder
2230
Power Control
2255
2215
Modulator
2220
AC/DC Converter
Decoder
2245
2200
AC1
AC2

FIG. 22

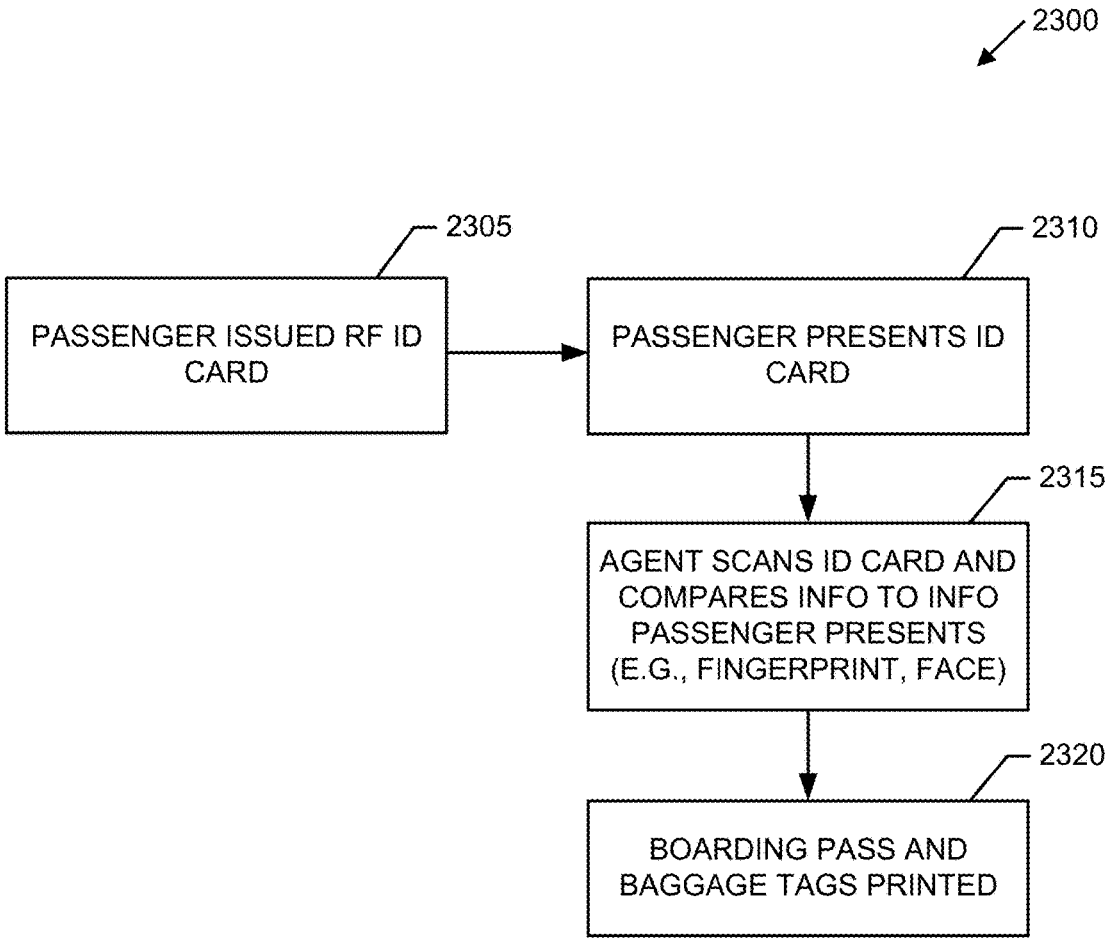

2300
2305
PASSENGER ISSUED RF ID CARD
2310
PASSENGER PRESENTS ID CARD
2315
AGENT SCANS ID CARD AND COMPARES INFO TO INFO PASSENGER PRESENTS (E.G., FINGERPRINT, FACE)
2320
BOARDING PASS AND BAGGAGE TAGS PRINTED

FIG. 23

SYSTEM AND METHOD FOR PROVIDING SECURE TRANSACTIONAL SOLUTIONS

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

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

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

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

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

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

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

FIGS. **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

FIG. **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

FIG. **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.

FIG. **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.

A more detailed description of an RF device can be found in U.S. patent application Ser. No. 10/118,092 filed 9 Apr. 2002; PCT Patent Application PCT/IB02/01439, filed 30 Apr. 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 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.

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.

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.

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 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.

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 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.

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 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.

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

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

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 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.

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.

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 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.

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

FIG. **4** illustrates the methods 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

FIG. **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

FIG. **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.

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 FIG. **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 material, holographic foil, or another substrate with a high metal content.

FIG. **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) 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

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

FIG. **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

FIG. **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

FIG. **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

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 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.

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 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.

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

FIG. **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 ensures 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 FIG. **13**. The chip is a passive chip that is secure. These chips have a power unit converter and are secure. The e-prompt **1348**, the memory of the chip, is totally separated from the rest of the communication, so if the security requirements are not met, a user cannot access the memory of the chip. The chip includes an ACDC converter **1341** and a connection to an RF antenna for power using a power supply control unit **1345**. The chip communicates with information stored on the telephone by coupling to an input device in the cellular telephone. A modulator **1342** is a device that receives baseband signals from an antenna. An AC/DC converter **1341** is a device that receives an alternating current (AC) and converts it to direct current (DC). An encoder **1343** is a device for encoding information received so that it may be utilized by another device or protocol. A decoder **1344** is a device that decodes information from the encoder output so it may be used by another device or display. A power control **1345** is a device which regulates voltage and current to protect an apparatus from both power surges and low power. An instruction sequencer **1347** is a device that queues instructions to be sent to the chip's internal memory. A security management unit **1346** is a device that checks and validates the cryptographic keys that will be sent to the cryptographic block. A cryptographic block **1349** is a device that stores the security keys. These keys are checked and validated to grant or deny access to the memory chip. EEPROM memory **1348** stores data. Information can be read and written from or to this device.

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

FIG. **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 FIG. **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 Ser. No. 10/118,092, filed Apr. 2, 2002, and PCT Patent Application IB0201439, filed Apr. 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

FIG. **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 24×7; 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 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.

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 (PIPS) 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 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.

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 FIG. **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 MH_z
f_2=915 MH_z

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

N=number of windings around inductor
μ_o=permeability of freespace (Hm^{-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:

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

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

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

For substitution, the following values are used:

L_1=2.931×10^8 H

L_2=6.437×10^10 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 1\ (NRZ clock).

Multiple RF Chip Overview

FIG. **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

FIG. **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

FIG. **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.

FIG. **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.

FIG. **3**A illustrates the differences between transport mode and tunnel mode. The use of AH and ESP are illustrated in FIG. **38**.

B. Method of Limiting Software Downloads

FIG. **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

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

B. Method of Airport Security

FIG. **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 mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information;

a biometric module configured to read biometric information;

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

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

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

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

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

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

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

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

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

8. A system, comprising:

a mobile device, comprising:

short range radio frequency (RF) circuitry;

memory configured to store biometric authentication information and payment information;

a biometric module configured to read biometric information;

an authentication module configured to determine whether the biometric information read by the biometric module corresponds to the biometric authentication information stored in memory; and

a secure module configured to:

generate a key when the biometric information read by the biometric reading device is determined by the authentication module to correspond to the biometric authentication information stored in memory;

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

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

a point of sale (POS) device configured to:

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

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

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

9. The system of claim **8**, wherein the biometric module is configured to read biometric information provided by a user to complete the transaction.

10. The system of claim **8**, wherein the payment information is associated with a primary account number.

11. The system of claim **8**, wherein the POS device includes an RF reader.

12. The system of claim **8**, wherein the biometric authentication information is stored separately from the payment information.

13. The system of claim **8**, wherein the payment information is stored in a memory accessible only by the secure module.

14. The system of claim **8**, wherein the short range RF circuitry comprises a radio frequency identification (RFID) device.

15. A method for secure transactions using a mobile device, comprising:

storing biometric authentication information and payment information in memory;

reading biometric information using a biometric reader;

determining whether the biometric information read by the biometric reader corresponds to the biometric authentication information stored in memory;

generating a key when the biometric information read by the biometric reader is determined to correspond to the biometric authentication information stored in memory;

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

providing the encrypted key and payment information for use in a transaction.

16. The method of claim **15**, further comprising reading biometric information provided by a user to complete the transaction.

17. The method of claim **15**, wherein the payment information is associated with a primary account number.

18. The method of claim **15**, further comprising providing the encrypted key and payment information to a point of sale (POS) device.

19. The method of claim **15**, wherein the biometric authentication information is stored separately from the payment information.

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

21. The method of claim **15**, wherein the payment information is provided using a short range RF circuitry.

* * * * *