



US 20090307140A1

(19) **United States**

(12) **Patent Application Publication**
Mardikar

(10) **Pub. No.: US 2009/0307140 A1**

(43) **Pub. Date: Dec. 10, 2009**

(54) **MOBILE DEVICE OVER-THE-AIR (OTA)
REGISTRATION AND POINT-OF-SALE (POS)
PAYMENT**

Publication Classification

(51) **Int. Cl.**
G06Q 20/00 (2006.01)
H04L 9/32 (2006.01)

(76) Inventor: **Upendra Mardikar**, San Jose, CA
(US)

(52) **U.S. Cl.** **705/71; 705/35; 705/17**

Correspondence Address:
Haynes and Boone, LLP
IP Section
2323 Victory Avenue, SUITE 700
Dallas, TX 75219 (US)

(57) **ABSTRACT**

A method for enabling secure registration of a mobile device OTA and for conducting a financial transaction at a point-of-sale (POS) has been described herein. In one embodiment, a method of mobile device registration over-the-air (OTA) comprises enabling a pre-loaded payment application having payment account information; enabling a certificate request; receiving payment credentials; associating the payment credentials with the payment account information; transmitting the payment account information and the certificate request OTA; and receiving a certificate of registration of the mobile device OTA.

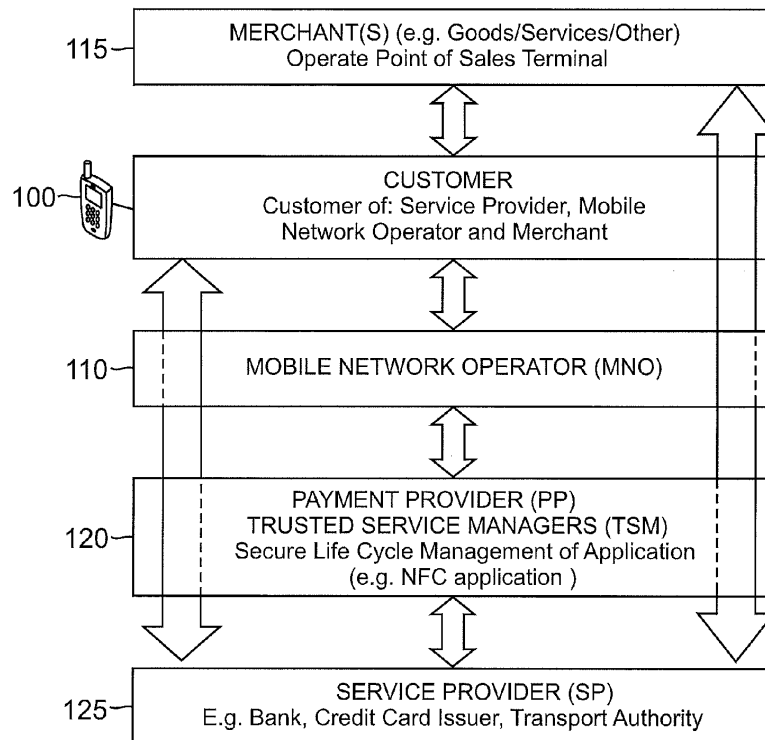
(21) Appl. No.: **12/249,145**

(22) Filed: **Oct. 10, 2008**

Related U.S. Application Data

(60) Provisional application No. 61/059,395, filed on Jun. 6, 2008, provisional application No. 61/059,907, filed on Jun. 9, 2008.

105



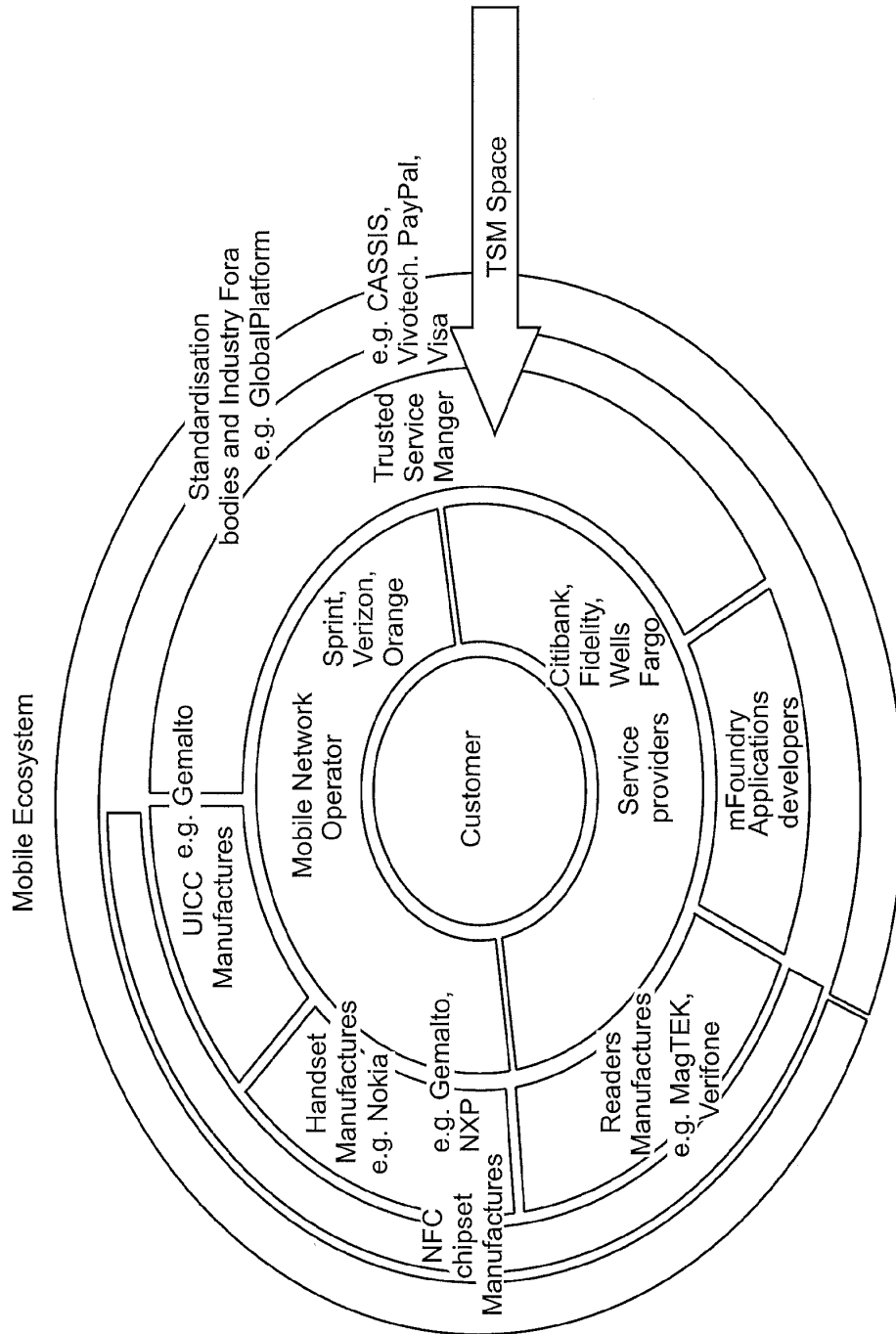


FIG. 1

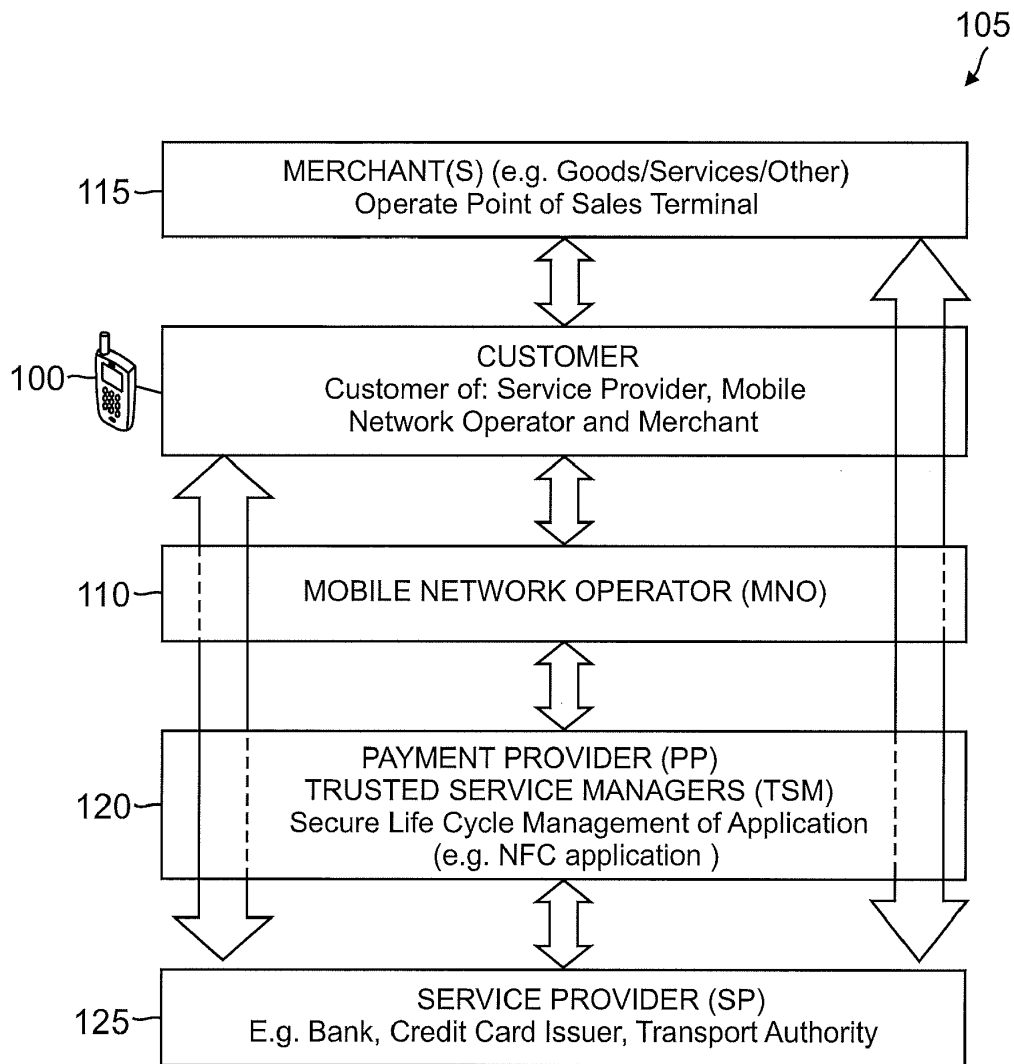


FIG. 2

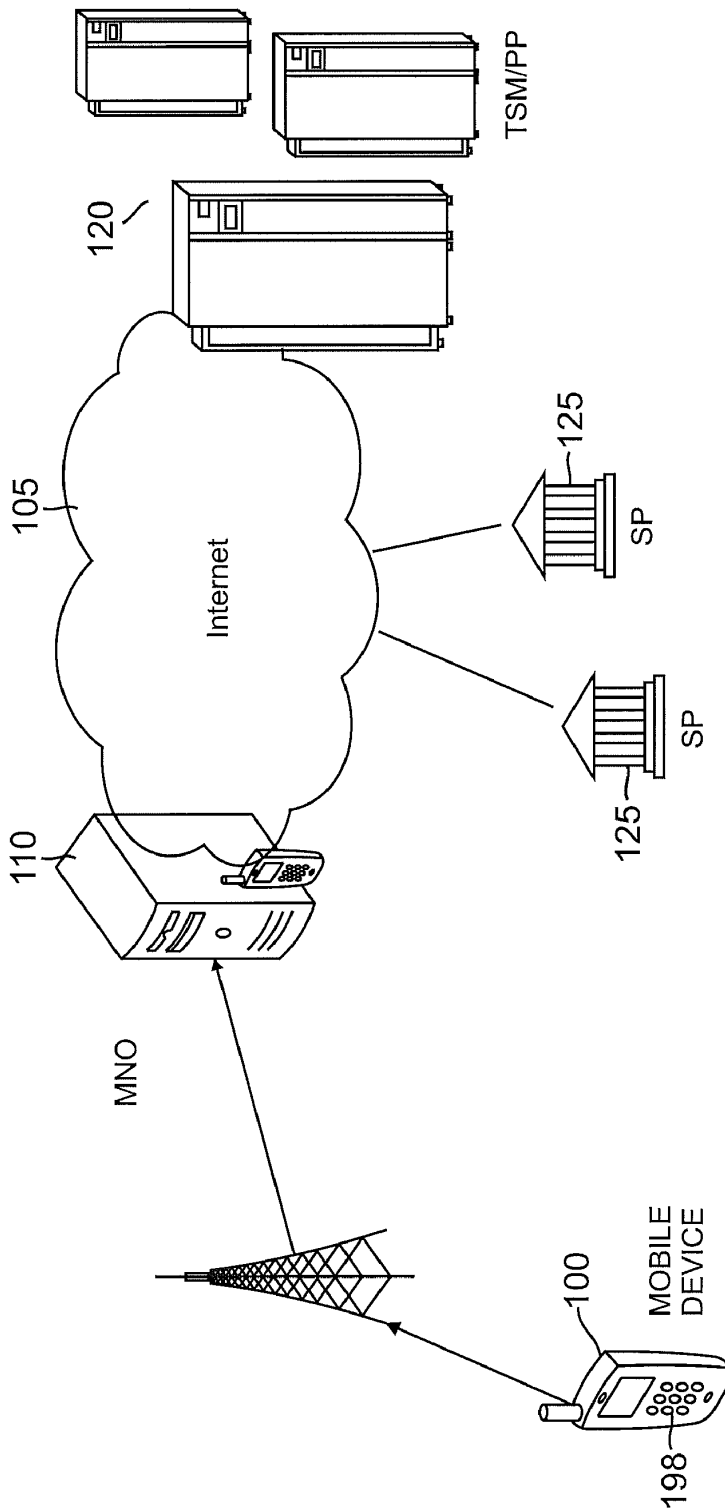


FIG. 3

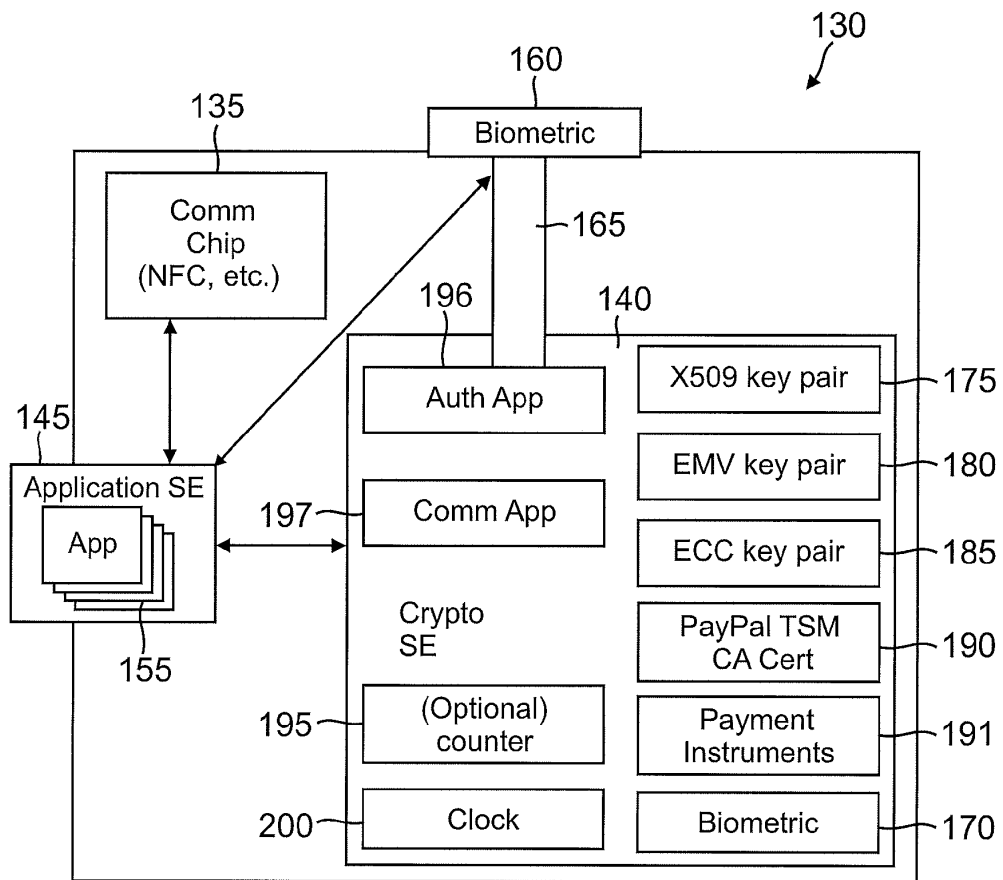


FIG. 4

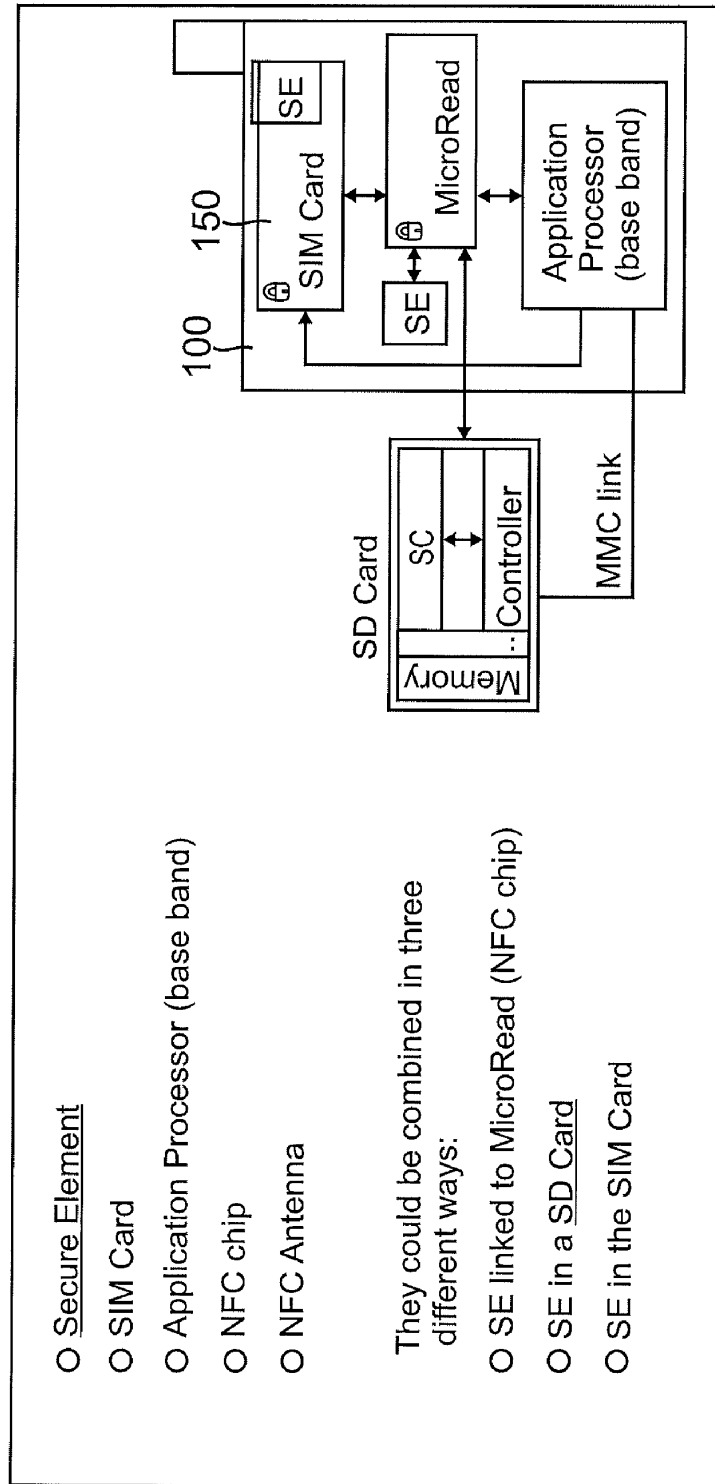


FIG. 5

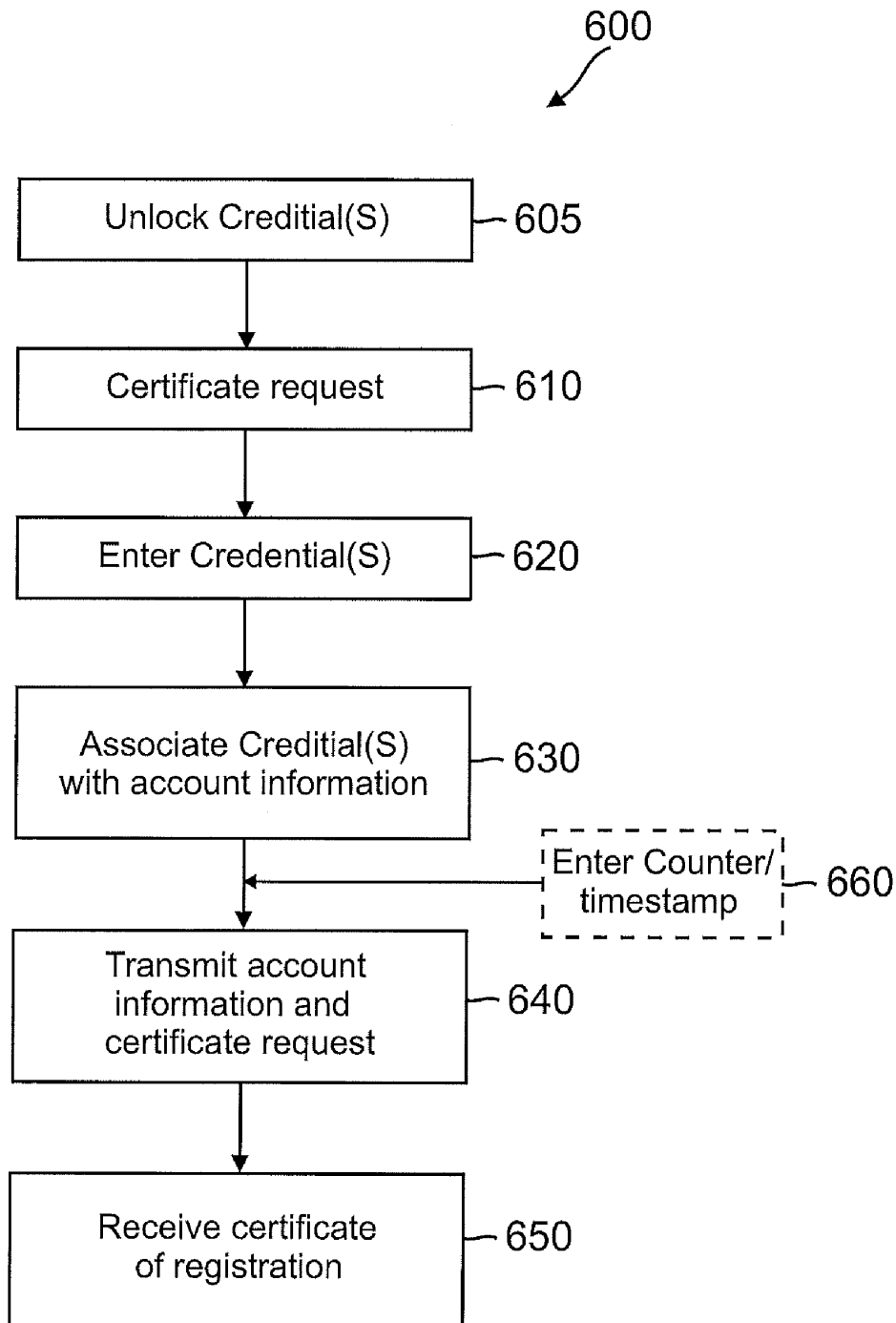


FIG. 6

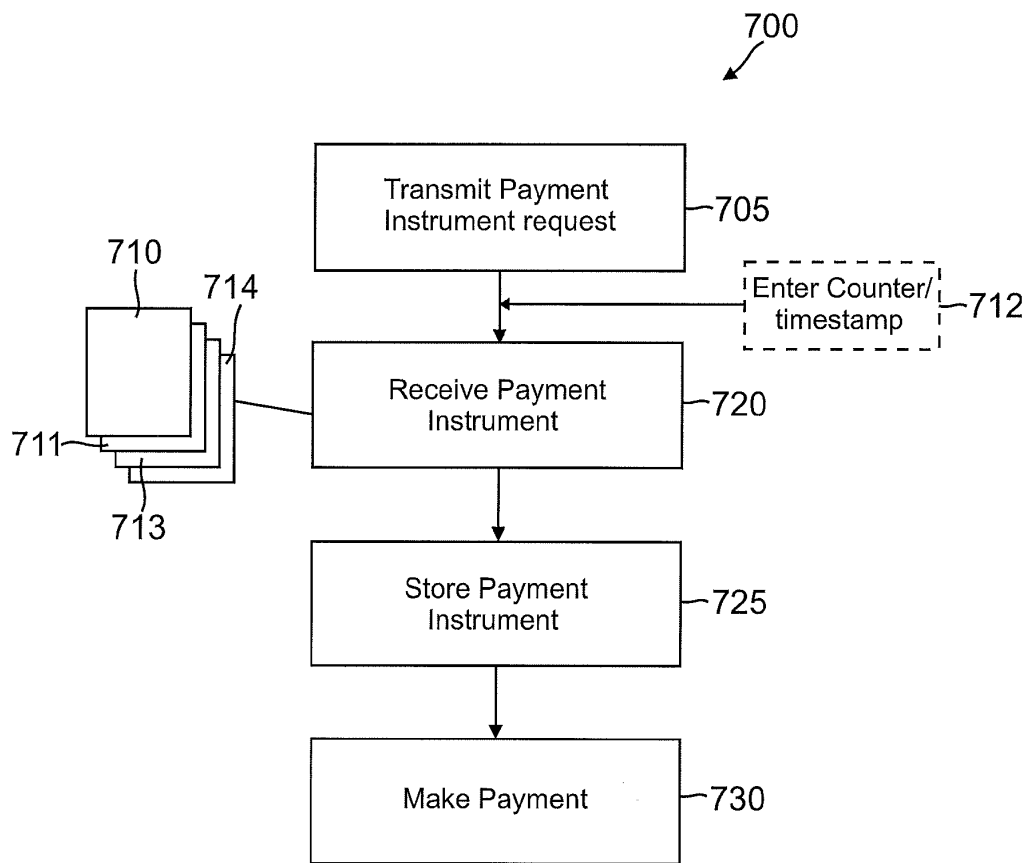


FIG. 7

**MOBILE DEVICE OVER-THE-AIR (OTA)
REGISTRATION AND POINT-OF-SALE (POS)
PAYMENT**

RELATED APPLICATIONS

[0001] This application claims priority and the benefit of U.S. Provisional Application No. 61/059,395, filed Jun. 6, 2008; and U.S. Provisional Application No. 61/059,907 filed Jun. 9, 2008, the entire disclosures of which are incorporated herein by reference.

BACKGROUND

[0002] 1. Field of the Invention

[0003] The present invention generally relates to financial transactions and more particularly to secure financial transactions initiated from an electronic device.

[0004] 2. Related Art

[0005] In direct (face-to-face) or online financial transactions customers may search for and purchase products and/or services from a merchant. In the case of online shopping, transactions are conducted through electronic communications with online merchants over electronic networks. A variety of electronic devices and various electronic techniques may be utilized to conduct such electronic transactions. Methods of initiating or making financial transactions from an electronic device include wireless communication as well as mobile Internet-based payments to name a few.

[0006] One such wireless technology, Near Field Communication, herein referred to a "NFC" is the most recently explored technology for object augmentation to bring mobile devices and physical objects together to enable a user to interact with the augmented objects for information and/or data communication. In this regard, NFC is a short range high frequency wireless communication technology that enables the exchange of data between devices over a relatively short distance.

[0007] A key feature of NFC devices is that the NFC chip that is integrated into the NFC device can read out an RFID tag's information (reader/writer mode), emulate a smart card so that a reader can access its data (card emulation mode), or communicate directly with another NFC device when the two NFC devices are brought in close proximity or together with each other (peer-to-peer mode).

[0008] NFC technology may be incorporated into most any electronic device; however vast business opportunities potentially exist in the use of NFC technology in a mobile device such a cell phone, PDA, or similar device. As such, in one context mobile NFC may be defined as a combination of contactless services and mobile telephony.

[0009] NFC in mobile devices may provide for contactless payment; information gathering; loyalty, promotional, and other value-added programs; and other services. More specifically, mobile NFC enables product and/or service purchases including tickets to a theater performance or a sporting event, access to smart posters that provide on the spot wait times and neighborhood maps, download and redeeming of electronic coupons and vouchers, electronic fund transfer between accounts, and other related applications.

[0010] As shown in FIG. 1, any number of involved parties may comprise an NFC electronic communications ecosystem. Such involved parties may include a customer or user, a merchant, a mobile network operator (MNO), a service provider (SP), a trusted service manager (TSM), a mobile phone

manufacturer, an integrated chip (IC) manufacturer, and application (software) developers to name a few. The duties or roles of one or more involved parties may be combined and preformed by a single entity.

[0011] For example, as shown in FIG. 2, service providers, banks, or other financial institutions are those entities that typically issue credit and provide authorization for conducting financial transactions between the customer and the merchant. A payment provider system (PP), such as PayPal, may provide payment processing for online transactions on behalf of the customer so that the customer does not expose payment information directly to the merchant. Instead, the customer may register his account with the payment provider system, map the account to an email address, and then use the payment provider system to make purchases when redirected to the payment provider system from the merchant's site. After the financial transaction is authorized the payment provider system completes the transaction.

[0012] In online financial transactions, the role of the payment provider system may be expanded to include or share duties generally associated with the service provider such that customers may use the payment provider system as a credit issuer, and for services such as electronic bank transfers from one account to another account, and/or provide access to other related financial activities through electronic communications over electronic networks operated by the MNO, such as the Internet. The payment provider system may provide an infrastructure, software, and services that enable customers and merchants to make and receive payments.

[0013] A central issue with mobile NFC or other wireless technology is the need for cooperation between the many involved parties to meet the needs of the customer via secure over-the-air (OTA) link. As shown in FIGS. 2 and 3, the payment provider system may further act as a TSM to provide a single point of contact for the service provider to access their customer base through the MNOs. More specifically, with the ever changing electronic communications environment including the emergence of NFC, service providers may not be ready or willing to change their working methods or the functions they provide, but they may still want to participate in the new mode of service operation by enhancing the services they offer while maintaining existing core processes. This conflict is solved by the TSM who can help service providers securely distribute and manage contactless services for their customers using the MNOs. In this regard, the TSM may manage the secure download and life-cycle management of the mobile NFC applications on behalf of the service providers.

[0014] Mobile devices generally associated with NFC include, for example, radio frequency-enabled credit and debit cards, key fobs, and NFC-enabled cell phones and PDAs. When registering a mobile device or conducting a financial transaction, or for that matter any transaction, security is generally an issue in that data transferred wirelessly will typically include credit card/financial instrument information, a user name, a password, etc., that is susceptible to theft and/or malicious attack. A user may at various times use any of several different payment applications for different service providers. To the extent that each payment application has its own separate security registration and verification procedures, the user experience may be cumbersome in that a user must separately load and run separate dedicated applications each of which must be separately registered and verified for making secure financial transactions. Moreover, the

security of each of these applications may be compromised by viruses, Trojans, key loggers and the like since the applications and their security information may reside on the same data storage element. Accordingly, a secure, user-friendly method and system may be desirable for enabling secure registration of a mobile device OTA and for conducting a financial transaction at a point-of-sale (POS).

SUMMARY

[0015] For purposes of summarizing the disclosure, exemplary embodiments of systems and methods for enabling secure registration of a mobile device OTA and conducting a financial transaction at a POS have been described herein.

[0016] In one embodiment, a method of mobile device registration OTA comprises enabling a pre-loaded payment application having payment account information; enabling a certificate request; receiving payment credentials; associating the payment credentials with the payment account information; transmitting the payment account information and the certificate request OTA; and receiving a certificate of registration of the mobile device OTA.

[0017] In another embodiment, an apparatus for registration OTA comprises a mobile device adapted to enable a pre-loaded payment application having payment account information; enable a certificate request; receive payment credentials; associate the payment credentials with the payment account information; transmit the payment account information and the certificate request OTA; and receive a certificate of registration for the mobile device.

[0018] In still another embodiment, a method of payment instrument deployment to a mobile device for payment at a point-of-sale comprises transmitting a payment instrument request from a mobile device; receiving data including a payment instrument and a card verification value (CVV) by the mobile device; and storing the payment instrument and card verification value in a secure element of the mobile device for payment at a POS.

[0019] These and other features and advantages of the present invention will be more readily apparent from the detailed description of the embodiments set forth below taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE FIGURES

[0020] FIG. 1 illustrates an example of a mobile device ecosystem including involved parties.

[0021] FIG. 2 shows one example of the relationship between involved parties of FIG. 1 including the role of a trusted service manager.

[0022] FIG. 3 shows one example of a portion of the network connectivity between involved parties in the mobile device ecosystem of FIG. 1.

[0023] FIG. 4 shows one embodiment of a mobile device architecture including the physical separation of secure elements within the mobile device.

[0024] FIG. 5 shows various architectural schemes for a secure element within a mobile device.

[0025] FIG. 6 is a flow chart showing one embodiment of secure customer registration of a mobile device for financial transactions at a point-of-sale over a network.

[0026] FIG. 7 is a flow chart showing one embodiment of payment instrument deployment to a mobile device for payment at a point-of-sale.

[0027] Exemplary embodiments and their advantages are best understood by referring to the detailed description that follows. It should be appreciated that like reference numerals are used to identify like elements illustrated in one or more of the figures, wherein showings therein are for purposes of illustrating exemplary embodiments and not for purposes of limiting the same.

DETAILED DESCRIPTION

[0028] Embodiments of the present disclosure related to systems and methods of secure customer registration of a mobile device for financial transactions at a POS over a network. As indicated above, mobile devices may provide for contactless payment; information gathering; loyalty, promotional, and other value-added programs; and other services.

[0029] As shown in FIGS. 2 and 3, in one embodiment a mobile device 100 may be used to communicate over a network 105 via a MNO 110, e.g., Sprint, Verizon, or other mobile network operators, to purchase products and/or services from a merchant 115. In one embodiment, a TSM 120 may provide a single point of contact between the mobile device 100, merchant 115, and service provider 125 through any of the various MNOs 110. In this regard, the TSM 120, or payment provider acting as the TSM, may manage the secure download and life-cycle management of the mobile applications, e.g., payment applications, on behalf of the service provider 125. Although an NFC is illustrated generally discussed herein with regard to various embodiments, the TSM's role or the role of other entities discussed herein is not limited to NFC and can be applied to other types of electronic communication including technologies such as Bluetooth, infrared, SMS (Short Message Service), and similar wireless technologies.

[0030] FIG. 4 shows an example of mobile device architecture 130. The major components of the mobile device include an antenna (not shown) built into the mobile device's case, an NFC or communication (COMM) chip 135, secure elements (SEs) 140, 145, and other associated elements. The communication chip may support one or more modes of communication, including, for example, NFC, GSM (Global System for Mobile Communication), UMTS (Universal Mobile Telecommunications System) and CDMA (Code Division Multiple Access) cellular phone protocols, SMS and internet access via a mobile network or local network, e.g., WAP (Wireless Application Protocol).

[0031] Within NFC or other mobile standards, security is typically managed by the SE. By one definition, a SE is a platform where applications can be installed, personalized and managed preferably OTA. It is a combination of hardware, software, interfaces and protocols that enable secure storage and the use of credentials for payments, authentication and other services. The SE may be pre-loaded with applications and/or may be capable of downloading various applications, for example, applications for facilitating financial transactions over a network. As shown in FIG. 5, a subscriber identification module (SIM) card 150, a secure flash card, or an embedded security controller could all act as a SE. A UICC (Universal Integrated Circuit Card) is a smart card that may be embedded in the mobile device and contains account information and memory that is used to enable GSM (Global System for Mobile communication) cellular telephones. One of the applications running on the smart card may be the SIM 150. As explained in more detail below, the SE hosts the fire walled applications and user credentials, and controls secu-

curity and cryptography using an onboard microprocessor and software. The SE shares mobile functionality with the NFC chipset 135, which manages network communications.

[0032] In one embodiment, the architecture of the mobile device may include separate secure elements (SEs), one SE dedicated to running various service provider applications (App SE) 145 and another SE dedicated to providing security for the applications and financial transactions (Crypto SE) 140.

[0033] In this regard, software on the device may consist of a number of applications from credit card companies that require different types of encryption. The number of applications that reside on the mobile device may be numerous as individual retailers may also provide applications to promote and support loyalty programs such as coupons and vouchers, or, provide access to their services. In other words, the customer may shop for ticket(s) remotely OTA using an application supported by a company such as Ticketmaster, pay for the tickets using a credit or debit card application by a company such as PayPal, and then download the electronic ticket to the phone using an application by a company such as Verizon.

[0034] The SE may have logical and end-to-end security. For example, there may be an authenticated and encrypted channel for communication with the SE. In one embodiment, the SE may have physical security. For example, the SE may adhere to certain security standards, for example, FIPS 140-2 Level 3 (tamper proof and copy protection) and Common Criteria ISO 15408 EAL 4+, or other standard as required or desired. The SE may be global. In other words, an SE may be compatible with a variety of communications protocols or systems. For example, as indicated above, the mobile device may be compatible with GSM, UMTS and CDMA cellular phone protocols.

[0035] In one embodiment the SE may be portable, capable of dynamic and remote management, and standardization. A portable application may be an application that may be easily transferred from one device to another. This may be achieved, for example, by porting the SE or by having a TSM 120 that can port applications. Portability may enable a user who has registered one mobile device to register any other mobile devices of the user. For example, a user may have one mobile phone for business and another mobile phone for home where transactions from each of the mobile devices are intended for business or personal use respectively.

[0036] In one embodiment, the SE may be compatible with OTA loading or dynamic remote management. For example, applications resident in the App SE 145 may be compatible with OTA management for life cycle management of the applications. For example, resident applications may be managed, updated, or altered. OTA management may be used to fix newly discovered vulnerabilities in the applications or update the application to add features or modify features.

[0037] In one embodiment, an SE may be standardized. For example, the SE may be compatible with standards set out by a known standards or protocols, for example those established by GlobalPlatform.org and/or Bearer Independent Protocol. The SE may work even when the device is turned off. For example, an NFC transaction or purchase may be made even when the phone is turned off, e.g., when on an airplane or other location where electronic devices may be required to be turned off for operational or security reasons.

[0038] As indicated above, in one embodiment the device may include an App SE 145 and a Crypto SE 140. As used herein, unless otherwise specified the term "Crypto SE" 140

is used to refer to any one of payment, credential, or wallet SEs. Splitting the Crypto SE 140 and the App SE 145 may improve the user experience by reducing the necessity of registering and verifying various applications separately for each service provider and/or re-certification after changes are made to any of the applications. In other words, splitting the App SE 145 and Crypto SE 140 may enable a single certification of a particular mobile device through the Crypto SE 140 while permitting changes to be made to the App SE 145 without requiring additional certification(s) or re-certification of the mobile device. Splitting the Crypto SE 140 from the App SE 145 may also reduce the likelihood of security information on the Crypto SE 140 being compromised by viruses, Trojans, key loggers and the like that may find their way onto the App SE.

[0039] The App SE 145 is configured to store various resident financial transaction applications 155, each of which may facilitate financial transactions for a different financial service provider 125. Such applications 155 may include, for example, a PayPal and/or other payment applications provided by alternative service providers and which facilitate financial transactions over a network 105. In one embodiment, the App SE 145 is a dynamic SE configured to permit application(s) to be managed and modified as needed through, for example, OTA management. Typically, the App SE 145 will not include any payment instruments, certificates, keys or credentials, all of which may be stored in the separate Crypto SE 140.

[0040] Although certain credentials or other sensitive data may be dynamic, the Crypto SE 140 is configured primarily as a static SE. The Crypto SE 140 may be configured for loading and storing credentials, payment instruments 191, certificates, crypto keys and other security-related information, including, for example, unique biometric authentication information related to a specific user. The Crypto SE 140 may provide verification and authentication 196, 197 for multiple applications 155 stored in the App SE 145.

[0041] In one embodiment, the mobile device 100 may include a biometric sensor 160, e.g., a thumbprint sensor, to provide biometric information to the Crypto SE 140 for transactional security. In alternative embodiments, the biometric sensor 160 may be any sensor that provides unique user identification by biometric means, including for example, retina scan, voice identification, etc. As used herein, the term biometric sensor refers not just to the physical sensor that senses biometric data, but to the arrangement of the sensor, logic, algorithms, and the like that collectively sense and generate a data signal or signals representative of the user being biometrically sensed.

[0042] The sensed biometric data from the biometric sensor may be tunneled through a biometric tunnel 165 and may be received by the Crypto SE 140. A biometric authorization application 170 may reside on the Crypto SE 140 to evaluate the biometric data and compare the data to data from a registered user, or may register the data where the data is being collected as part of a registration or certification procedure.

[0043] In one embodiment, the Crypto SE may be certified, for example by a credit processing company such as MasterCard or VISA. The Crypto SE 140 may be certified, for example, using the biometric sensor and biometric authorization application 170. Once the Crypto SE portion is certified, the mobile device 100 is certified for use.

[0044] In cryptography, a public key infrastructure (PKI) is an arrangement that binds public keys with respective user

identities by means of a certificate authority (CA). A TSM 120 may act as the CA. The user identity must be unique for each CA. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at the CA. A Registration Authority (RA) assures this binding. For each user, the user identity, the public key, binding, validity conditions and other attributes are stored on the certificates issued by the CA.

[0045] As shown in FIG. 4, a cryptographic key-pair may be pre-loaded on a Crypto SE 140 of the mobile device 100. For example, an X509 key-pair 175, EMV (Europay, MasterCard, VISA) 180, or ECC 185 may be pre-loaded on the Crypto SE 140. A TSM Root CA certificate 190 may also be pre-loaded in a Crypto SE 140 of the mobile device 100. In addition, a financial transaction application 155 such as a PayPal application or other payment application may be pre-loaded on the App SE 145. In one embodiment, all applications may be registered and deployed using a TSM public key. An application may include instructions for periodically checking whether an update to the application is available. If the update is available and customer verification is approved, applications are downloaded and the signature is verified. Once the signature is matched the new application is activated.

[0046] In one embodiment, a user may unlock a payment credential pre-loaded on the mobile device 100 by registering the user's unique biometric profile using the biometric sensor 160. In this regard, the credential may be unlocked, for example, by registering a thumb-print twice using a thumb-print/finger print biometric sensor.

[0047] FIG. 6 is a flow chart showing one embodiment of secure customer registration 600 of a mobile device for financial transactions at a POS over a network. As illustrated in FIG. 6, when registering a mobile device 100, payment credentials (account number, credit card number, etc.) are first unlocked, such as with a thumbprint or other biometric technique, to enable a pre-loaded payment application (step 605). The pre-loaded payment application may be associated with a payment provider such as PayPal. Enablement of the pre-loaded payment application causes a SCEP/CRMF (Simple Certificate Enrollment Protocol/Certificate Request Message Format) or similar certificate request protocol to be invoked (step 610). A user's TSM credential(s) such as user name and password is entered and associated with the payment provider's user account information stored in the payment application (step 620 and step 630). A random counter 195 or timestamp 200 may be generated and stored in the Crypto SE 140 for counter based replay protection (step 660). The timestamp, user's credentials or associated account information, and phone information, e.g., IMEI number, as well as the certificate request protocol is sent to the TSM OTA and a phone certificate may be issued to the mobile device for registration of the phone (step 640 and step 650).

[0048] FIG. 7 is a flow chart showing one embodiment of payment instrument 191 deployment to a mobile device for payment at a point-of-sale 700. Payment account numbers such as associated with credit or debit cards may be deployed to a mobile device OTA for payment to an offline merchant using the payment/service provider account. For example, a payment account number may be generated by the payment/service provider along with a CVV (card verification value). In one embodiment, a payment instrument request is transmitted from the mobile device 100 to the TSM 120 (step 705).

In response, a payment account number 710, a CVV 711, and a counter/timestamp (to prevent replay attacks) 712 may be SMS encrypted using the public key 713 of the mobile phone, signed using the TSM's private key 714, and sent to the mobile device 100 (step 720). The counter/timestamp may be checked and the payment account number 710 and the CVV 711 (payment instruments 191) may be stored in the Crypto SE 140 of the mobile device 100 (step 725). The mobile device 100 is now able to make payments (step 730). The payment account number 710 may also be obtained from the service provider 125, such as from a representative, either by phone, e-mail, or other method of inquiry as may be required for entry of the account number when making a payment (step 730). In this regard, a customer may manually enter an account number, obtain as indicated above, using a keypad on the mobile device. This may be done after activating the biometric credential and registering the mobile device. The application may then load the Crypto SE 140 with a payment instrument identified by its account number.

[0049] In one embodiment, instead of entering a PIN on a POS keypad or making a signature at a POS electronic signature screen as is currently done, a customer may enter a POS PIN directly onto a keyboard 198 on their mobile device 100. In this regard, a user may authenticate their mobile device 100 for secure keyboard PIN entry using the biometric sensor 160 and biometric authentication application 170 on their mobile device 100. Biometric authentication of the mobile device 100 may create a secure tunnel 165 from the keyboard to the Crypto SE 140 on the mobile device 100. The user may then enter a PIN on a keyboard on the mobile device 100.

[0050] Banking regulations do not allow entering a PIN in a non-encrypted PIN pad. As such, in one embodiment, the mobile device PIN pad has an encrypted PIN pad mode where PIN is tunneled directly to Crypto SE. The SE will behave as Chip and PIN Authentication and/or as ARQC-ARPC.

[0051] In one method of conducting a NFC transaction at a point of sale POS a customer may prepare a mobile device for use, for example by opening the mobile phone. The user may select a "Payment" function on the mobile device by selecting a corresponding payment button, utilizing voice recognition technology, or any other appropriate method of selection as appropriate for a particular mobile device.

[0052] Selecting "Payment" may prompt a payment application 155 on the mobile device 100 to check the biometric sensor 160 for biometric input. For example, a user may place their thumb on a thumb/finger print sensor or swipe their thumb on a biometric input. The biometric input may be directly linked to the Crypto SE 140 via tunnel circuitry 165. The tunnel circuitry 165 may be FIPS 140-2 level 3 compliant and may be arranged so that biometric data, for example thumbprint data, is input directly into the Crypto SE 140 for authentication/unlocking. Using the tunnelling circuitry 165 to input biometric data directly into a Crypto SE 140 may improve the security of a transaction over devices without such a tunnel circuitry, e.g., where the architecture is such that biometric data may be captured by any application on the mobile device 100. In this regard, tunnelling the biometric data to a separate Crypto SE 140 may improve security of a transaction and prevent compromising a user's unique identifying information. The App SE 145 may then send a request to the Crypto SE 140 for payment information.

[0053] Once a user's biometric identity is authenticated properly, the Crypto SE 140 may then send payment or other

information to the App SE 145. The payment information may then be sent to Comm/NFC chip 135 and POS by NFC technology when customer taps on POS. The payment information may include payment information and the CVV.

[0054] In implementation of the various embodiments, the mobile device may comprise a personal computing device, such as a personal computer, laptop, PDA, cellular phone or other personal computing or communication devices. The payment provider system may comprise a network computing device, such as a server or a plurality of servers, computers, or processors, combined to define a computer system or network to provide the payment services provided by a payment provider system.

[0055] In this regard, a computer system may include a bus or other communication mechanism for communicating information, which interconnects subsystems and components, such as processing component (e.g., processor, microcontroller, digital signal processor (DSP), etc.), system memory component (e.g., RAM), static storage component (e.g., ROM), disk drive component (e.g., magnetic or optical), network interface component (e.g., modem or Ethernet card), display component (e.g., CRT or LCD), input component (e.g., keyboard or keypad), and/or cursor control component (e.g., mouse or trackball). In one embodiment, disk drive component may comprise a database having one or more disk drive components.

[0056] The computer system may perform specific operations by processor and executing one or more sequences of one or more instructions contained in a system memory component. Such instructions may be read into the system memory component from another computer readable medium, such as static storage component or disk drive component. In other embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention.

[0057] Logic may be encoded in a computer readable medium, which may refer to any medium that participates in providing instructions to the processor for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. In various implementations, non-volatile media includes optical or magnetic disks, such as disk drive component, volatile media includes dynamic memory, such as system memory component, and transmission media includes coaxial cables, copper wire, and fiber optics, including wires that comprise bus. In one example, transmission media may take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications.

[0058] Some common forms of computer readable media includes, for example, floppy disk, flexible disk, hard disk, magnetic tape, any other magnetic medium, CD-ROM, any other optical medium, punch cards, paper tape, any other physical medium with patterns of holes, RAM, PROM, EPROM, FLASH-EPROM, any other memory chip or cartridge, carrier wave, or any other medium from which a computer is adapted.

[0059] In various embodiments, execution of instruction sequences for practicing the invention may be performed by a computer system. In various other embodiments, a plurality of computer systems coupled by communication link (e.g., LAN, WLAN, PTSN, or various other wired or wireless networks) may perform instruction sequences to practice the invention in coordination with one another.

[0060] Computer system may transmit and receive messages, data, information and instructions, including one or more programs (i.e., application code) through communication link and communication interface. Received program code may be executed by processor as received and/or stored in disk drive component or some other non-volatile storage component for execution.

[0061] Where applicable, various embodiments provided by the present disclosure may be implemented using hardware, software, or combinations of hardware and software. Also, where applicable, the various hardware components and/or software components set forth herein may be combined into composite components comprising software, hardware, and/or both without departing from the spirit of the present disclosure. Where applicable, the various hardware components and/or software components set forth herein may be separated into sub-components comprising software, hardware, or both without departing from the scope of the present disclosure. In addition, where applicable, it is contemplated that software components may be implemented as hardware components and vice-versa.

[0062] Software, in accordance with the present disclosure, such as program code and/or data, may be stored on one or more computer readable mediums. It is also contemplated that software identified herein may be implemented using one or more general purpose or specific purpose computers and/or computer systems, networked and/or otherwise. Where applicable, the ordering of various steps described herein may be changed, combined into composite steps, and/or separated into sub-steps to provide features described herein.

[0063] The foregoing disclosure is not intended to limit the present invention to the precise forms or particular fields of use disclosed. It is contemplated that various alternate embodiments and/or modifications to the present invention, whether explicitly described or implied herein, are possible in light of the disclosure.

What is claimed is:

1. Method of mobile device registration over-the-air (OTA) comprising:
 - enabling a pre-loaded payment application having payment account information;
 - enabling a certificate request;
 - receiving payment credentials;
 - associating the payment credentials with the payment account information;
 - transmitting the payment account information and the certificate request OTA; and
 - receiving a certificate of registration by the mobile device OTA.
2. The method of claim 1, further comprising unlocking the payment credentials prior to receiving the payment credentials.
3. The method of claim 2, wherein unlocking the payment credentials further comprising receiving a biometric input.
4. The method of claim 3, wherein the biometric input includes one of a fingerprint, a retinal scan, or voice recognition.
5. The method of claim 1, wherein enabling the certificate request includes one of invoking a simple certificate enrollment protocol (SCEP) or a certificate request message format (CRMF).
6. The method of claim 1, wherein the payment credentials are one of a user name or a password.

7. The method of claim 1, further comprising transmitting a counter or a timestamp along with the payment account information and the certificate request.

8. The method of claim 1, wherein at least a portion of the OTA is via near field communication.

9. An apparatus for registration over-the-air (OTA) comprising:

a mobile device adapted to enable a pre-loaded payment application having payment account information; enable a certificate request; receive payment credentials; associate the payment credentials with the payment account information and the certificate request OTA; and receive a certificate of registration for the mobile device.

10. The apparatus of claim 9, wherein the mobile device is adapted to unlock the payment credentials prior to receipt of the payment credentials.

11. The apparatus of claim 10, wherein the mobile device is adapted to unlock the payment credentials upon receipt of a biometric input.

12. The apparatus of claim 11, wherein the biometric input includes one of a fingerprint, a retina scan, or voice recognition.

13. The apparatus of claim 9, wherein the certificate request includes one of a simple certificate enrollment protocol (SCEP) or a certificate request message format (CRMF).

14. The apparatus of claim 9, wherein the payment credentials are one of a user name or a password.

15. The apparatus of claim 9, wherein the mobile device is adapted to transmit a counter or a timestamp along with the payment account information and the certificate request.

16. The apparatus of claim 9, wherein at least a portion of the OTA is via near field communication.

17. A method of payment instrument deployment to a mobile device for payment at a point-of-sale (POS) comprising:

transmitting a payment instrument request from a mobile device;

receiving data including a payment instrument and a card verification value (CVV) by the mobile device; and storing the payment instrument and card verification value in a secure element of the mobile device for payment at a POS.

18. The method of claim 17, wherein the payment instrument is a payment account number.

19. The method of claim 17, wherein the payment instrument and the CVV is encrypted using a public key of the mobile device and signed using a private key of a payment/provider system.

20. The method of claim 17, wherein the data further includes counter or timestamp information to prevent replay attacks.

* * * * *