

In the United States Patent and Trademark Office

US Utility Patent Application for

**Mobile devices for commerce over unsecured networks**

Inventor(s): Liang Seng Koh  
41291 Carmen Street  
Fremont, CA 94539, USA  
Citizenship: USA.

Hsin Pan  
2374 Olive Avenue  
Fremont, CA 94539, USA  
Citizenship: USA.

Xiangzhen Xie  
C505, Long Tai Xuan, Nanguang Village  
Nanshang District  
Shenzhen, Guangdong Province, 518051, China  
Citizenship: P. R. China

Assignees: RFCyber Corp.

Express Mail Label # E-filing Date of Deposit: January 16, 2012  
I hereby certify that this paper or fee is being deposited with the United States Postal Service using  
"Express Mail Post Office To Addressee" service under 37 CFR 1.10 on the date indicated above and is  
addressed to "Mail Stop: New Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA  
22313"

Signed:  / joe zheng /  
Joe Zheng

# Mobile devices for commerce over unsecured networks

## Cross-Reference to Related Applications

**[0001]** This application is a continuation-in-part of co-pending US Pat. App. Serial No.: 11/534,653 filed on 9/24/2006, now US Pat. No.: X,XXX,XXX, and also a continuation-in-part of US Pat. App. Serial No.: 11/739,044 filed on 04/23/2007, which is a continuation-in-part of co-pending US Pat. App. Serial No.:11/534,653 filed on 9/24/2006, now US Pat. No.: X,XXX,XXX.

## BACKGROUND

### Technical Field

**[0002]** The present invention is generally related to commerce over networks. Particularly, the present invention is related to techniques for personalizing a secure element and provisioning an application such as an electronic purse that can be advantageously used in portable devices configured for both electronic commerce (a.k.a., e-commerce) and mobile commerce (a.k.a., m-commerce).

### Description of the Related Art

**[0003]** Single functional cards have been successfully used in enclosed environments such as transportation systems. One example of such single functional cards is MIFARE that has been selected as the most successful contactless smart card technology. MIFARE is the perfect solution for applications like loyalty and vending cards, road tolling, city cards, access control and gaming.

**[0004]** However, single functional card applications are deployed in enclosed systems, which are difficult to be expanded into other areas such as e-commerce and m-commerce because stored values and transaction information are stored in data storage of each tag that is protected by a set of keys. The nature of the tag is that the keys need to be delivered to the card for authentication before any data can be accessed during a transaction. This constraint makes systems using such technology

difficult to be expanded to an open environment such as the Internet for e-commerce and/or wireless networks for m-commerce as the delivery of keys over a public domain network causes security concerns.

**[0005]** In general, a smart card, chip card, or integrated circuit card (ICC), is any pocket-sized card with embedded integrated circuits. A smart card or microprocessor cards contain volatile memory and microprocessor components. Smart cards may also provide strong security authentication for single sign-on (SSO) within large organizations. The benefits of smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contactless smart card can be programmed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card.

**[0006]** Contactless smart cards that do not require physical contact between card and reader are becoming increasingly popular for payment and ticketing applications such as mass transit and highway tolls. Such Near Field Communication (NFC) between a contactless smart card and a reader presents significant business opportunities when used in NFC-enabled mobile phones for applications such as payment, transport ticketing, loyalty, physical access control, and other exciting new services.

**[0007]** To support this fast evolving business environment, several entities including financial institutions, manufactures of various NFC-enabled mobile phones and software developers, in addition to mobile network operators (MNO), become involved in the NFC mobile ecosystem. By nature of their individual roles, these players need to communicate with each other and exchange messages in a reliable and interoperable way.

**[0008]** One of the concerns in the NFC mobile ecosystem is its security in an open network. Thus there is a need to provide techniques to personalize a secure element in a contactless smart card or an NFC-enabled mobile device so that such a

device is so secured and personalized when it comes to financial applications or secure transactions. With a personalized secure element in an NFC-enabled mobile device, various applications or services, such as electronic purse or payments, can be realized. Accordingly, there is another need for techniques to provision or manage an application or service in connection with a personalized secure element.

## SUMMARY

**[0009]** This section is for the purpose of summarizing some aspects of embodiments of the present invention and to briefly introduce some preferred embodiments. Simplifications or omissions in this section as well as the title and the abstract of this disclosure may be made to avoid obscuring the purpose of the section, the title and the abstract. Such simplifications or omissions are not intended to limit the scope of the present invention.

**[0010]** Broadly speaking, the invention is related to techniques for personalizing secure elements in NFC devices to enable various secure transactions over a network (wired and/or wireless network). With a personalized secure element (hence secured element), techniques for provisioning various applications or services are also provided. Interactions among different parties are managed to effectuate a personalization or provisioning process flawlessly to enable an NFC device for a user thereof to start enjoying the convenience of commerce over a data network with minimum effort.

**[0011]** As an example of application to be provided over a secured element, a mechanism is provided to enable devices, especially portable devices, to function as an electronic purse (e-purse) to conduct transactions over an open network with a payment server without compromising security. According to one embodiment, a device is installed with an e-purse manager (i.e., an application). The e-purse manager is configured to manage various transactions and functions as a mechanism to access an emulator therein. Secured financial transactions can then be conducted over a wired network, a wireless network or a combination of both wired and wireless network.



**[0012]** According to another aspect of the present invention, security keys (either symmetric or asymmetric) are personalized so as to personalize an e-purse and perform a secured transaction with a payment server. In one embodiment, the essential data to be personalized into an e-purse include one or more operation keys (e.g., a load key and a purchase key), default PINs, administration keys (e.g., an unblock PIN key and a reload PIN key), and passwords (e.g., from Mifare). During a transaction, the security keys are used to establish a secured channel between an embedded e-purse and an SAM (Security Authentication Module) or a backend server.

**[0013]** The present invention may be implemented in various forms including a method, a system, an apparatus, a part of a system or a computer readable medium. According to one embodiment, the present invention is a method for personalizing a secure element associated with a computing device. The method comprises initiating data communication with a server, sending device information of the secure element in responding to a request from the server after the server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command causing the computing device to retrieve the device information from the secure element, receiving at least a set of keys from the server, wherein the keys are generated in the server in accordance with the device information of the secure element, and storing the set of keys in the secure element to facilitate a subsequent transaction by the computing device.

**[0014]** According to another embodiment, the present invention is a method for personalizing a secure element associated with a computing device. The method comprises receiving an inquiry to establish data communication between a server and the computing device, sending a request from the server to the computing device to request device information of the secure element after the server determines that the computing device is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command that subsequently causes the computing device to retrieve the device information from the secure element therein, generating at least a set of keys in accordance with the device information received, delivering the set of keys through a secured channel over

a data network to the computing device, wherein the set of keys is caused to be stored in the secure element with the computing device, and notifying at least a related party that the secure element is now personalized for subsequent trusted transactions.

**[0015]** According to still another embodiment, the present invention is a method for provisioning an application installed in a mobile device, the method comprises sending to a server an identifier identifying the application together with device information of a secure element associated with a mobile device on which the application has been installed, establishing a secured channel between the secure element and the server using a set of key set installed in the secure element, receiving data prepared by the server to enable the application to function as designed on the mobile device; and sending out an acknowledgement to a provider of the application about a status of the application now being active with the secure element on the mobile device. The data received in the mobile device includes a user interface of the application per the mobile device and a generated application key set.

**[0016]** According to still another embodiment, the present invention is a method for provisioning an application, the method comprises receiving from a mobile device an identifier identifying the application together with device information of a secure element associated with the mobile device on which the application has been installed, establishing a secured channel between the secure element and the server using a set of key set installed on the secure element, preparing data necessary for the application to function as designed on the mobile device, transporting the data from the server to enable the application via the secured channel; and notifying a provider of the application about a status of the application now active with the secure element on the mobile device.

**[0017]** According to yet another embodiment, the present invention is a mobile device for conducting a transaction over a network, the mobile device comprises a network interface, a secure element, a memory space for storing at least a module and an application downloaded from the network, a processor coupled to the memory space and configured to execute the module to cause operations including verifying whether the application has been provisioned. When it is verified that the application

has not been provisioned, the operations further comprise sending to a server via the network interface an identifier identifying the application together with device information of a secure element, establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device, receiving the data from the server to associate the application with the secure element, and sending out an acknowledgement to a provider of the application about a status of the application that is now active with the secure element. The processor is further configured to determine if the secure element has been personalized before performing a provisioning process of the application. If the secure element has not been personalized, the mobile device is caused to personalize the secure element with a designed server.

**[0018]** One of the objects, features, and advantages of the present invention is to enable a mobile device that can be used to perform a secured transaction with a party (e.g., at a point of sale, with a commercial server or accessing remotely) over an unsecured network (e.g., the Internet).

**[0019]** Other objects, features, and advantages of the present invention, which will become apparent upon examining the following detailed description of an embodiment thereof, taken in conjunction with the attached drawings.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0020]** The invention will be readily understood by the following detailed description in conjunction with the accompanying drawings, wherein like reference numerals designate like structural elements, and in which:

**[0021]** FIG. 1A shows a simplified architecture of an NFC-enabled mobile device with a secure element (SE);

**[0022]** FIG. 1B shows a flowchart or process of personalizing an SE according to one embodiment of the present invention;

**[0023]** FIG. 1C shows relationships among an SE manufacturer, a TSM admin and the TSM system for both offline and online modes;

**[0024]** FIG. 1D illustrates data flows among a user for an NFC device (e.g., an NFC mobile phone), the NFC device itself, a TSM server, a corresponding SE manufacturer and an SE issuer;

**[0025]** FIG. 1E shows a data flowchart or process of personalizing data flow among three entities: a land-based SAM or a network e-purse server, an e-purse acting as a gatekeeper, and a single function tag, according to one embodiment;

**[0026]** FIG. 2A shows a mobile payment ecosystem in which related parties are shown in order for the mobile payment ecosystem successful;

**[0027]** FIG. 2B shows a flowchart or process of provisioning one or more applications according to one embodiment;

**[0028]** FIG. 2C shows a data flow illustrating various interactions among different parties when an application is being provisioned in one embodiment;

**[0029]** FIG. 2D shows a data flow among different entities when preparing the application data in provisioning an application;

**[0030]** FIG. 2E shows a flowchart or process for locking or disabling an installed application;

**[0031]** FIG. 2F shows an exemplary architecture diagram of a portable device enabled as an e-purse conducting e-commerce and m-commerce, according to one embodiment of the present invention;

**[0032]** FIG. 3A is a block diagram of related modules interacting with each other to achieve what is referred to herein as e-purse personalization by an authorized personnel (a.k.a., personalizing a mobile device or a secure element therein while provisioning an application);

**[0033]** FIG. 3B shows a block diagram of related modules interacting with each other to achieve what is referred to herein as e-purse personalization by a user of the e-purse;

- [0034]** FIG. 3C shows a flowchart or process of personalizing an e-purse according to one embodiment of the present invention;
- [0035]** FIG. 4A and FIG. 4B show together a flowchart or process of financing, funding, load or top-up an e-purse according to one embodiment of the present invention;
- [0036]** FIG. 4C shows an exemplary block diagram of related blocks interacting with each other to achieve the process FIG. 4A and FIG. 4B;
- [0037]** FIG. 5A is a diagram showing a first exemplary architecture of a portable device for enabling e-commerce and m-commerce functionalities over a cellular communications network (i.e., 3G, LTE or GPRS network), according an embodiment of the present invention;
- [0038]** FIG. 5B is a diagram showing a second exemplary architecture of a portable device for enabling e-commerce and m-commerce functionalities over a wired and/or wireless data network (e.g., Internet), according another embodiment of the present invention;
- [0039]** FIG. 5C is a flowchart illustrating an exemplary process of enabling the portable device of FIG. 5A for services/applications provided by one or more service providers in accordance with one embodiment of the present invention;
- [0040]** FIG. 6A is a diagram showing an exemplary architecture, in which a portable device is enabled as a mobile POS conducting e-commerce and m-commerce, according to one embodiment of the present invention;
- [0041]** FIG. 6B is a diagram showing an exemplary architecture, in which a portable device is enabled as a mobile POS conducting a transaction upload operation over a network, according to an embodiment of the present invention;
- [0042]** FIG. 6C is a flowchart illustrating an exemplary process of conducting m-commerce using the portable device enabled as a mobile POS with an e-token enabled device as a single functional card in accordance with one embodiment of the present invention;

**[0043]** FIG. 6D is a flowchart illustrating an exemplary process of conducting m-commerce using the portable device enabled as a mobile POS against a an e-token enabled device as a multi-functional card; and

**[0044]** FIG. 7 is a diagram depicting an exemplary configuration in which a portable device used for an e-ticking application.

#### DETAILED DESCRIPTION OF THE INVENTION

**[0045]** In the following description, numerous specific details are set forth to provide a thorough understanding of the present invention. The present invention may be practiced without these specific details. The description and representation herein are the means used by those experienced or skilled in the art to effectively convey the substance of their work to others skilled in the art. In other instances, well-known methods, procedures, components, and circuitry have not been described in detail since they are already well understood and to avoid unnecessarily obscuring aspects of the present invention.

**[0046]** Reference herein to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with the embodiment can be included in at least one implementation of the invention. The appearances of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Further, the order of blocks in process, flowcharts or functional diagrams representing one or more embodiments do not inherently indicate any particular order nor imply limitations in the invention.

**[0047]** Embodiments of the present invention are discussed herein with reference to FIGS. 1A – 7. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes only as the invention extends beyond these limited embodiments.

**[0048]** Near Field Communication (NFC) presents significant business opportunities when used in mobile phones for applications such as payment, transport ticketing, loyalty, physical access control, and other exciting new services. To support this fast evolving business environment, several entities including financial institutions, manufactures of various NFC-enabled mobile phones and software developers, in addition to Mobile Network Operators (MNO), become involved in the NFC mobile ecosystem. By nature of their individual roles, these players need to communicate with each other and exchange messages in a reliable and interoperable way.

**[0049]** Equally important to these entities or players, is the need for ongoing security and confidentiality of sensitive applications and data downloaded to and stored on an NFC enabled handset for performing contactless transactions. The component in a mobile phone providing the security and confidentiality required to support various business models in this environment, is referred to as a Secure Element (SE).

**[0050]** FIG. 1A shows a simplified architecture of a computing device 100. Unless otherwise explicitly indicated, the term of “computing device”, “mobile device” or “handset” will be interchangeably used herein, but those skilled in the art will understand the description herein shall be equally applicable to other devices such as a smart phone, a tablet, a laptop computer, a contactless smart card and other portable device.

**[0051]** The mobile device 100 includes a near field communication (NFC) controller 101 that enables the device 100 to interact with another device wirelessly to exchange data with. For example, a user may use the mobile device 100 as an e-purse or a wallet to pay for a purchase or an admission. In operation, the e-purse is controlled by a secure element (SE) 102. Essentially, the SE 102 enables such a mobile device 100 to perform financial transaction, transport ticketing, loyalty, physical access control, and other exciting new services in a secured manner. To offer such services, the SE 102 is configured to support various applets, applications or modules (only two samples 104 and 106 are shown in FIG. 1A). Depending on implementation, these modules may be hardware modules embedded or inserted thereon, or software modules downloadable from one or more servers via a data network.

**[0052]** When a mobile device is first purchased by or delivered to a customer, the SE 102 in the mobile device is installed with a set of default keys (e.g., an Issuer Security Domain (ISD) key set by the SE manufacturer). Depending on implementation, the SE 102 may be in form of a smart card, an integrated circuit (IC) or a software module upgradable by overwriting some of all of the components therein. In one embodiment, the SE 102 is a tamper proof Smart Card chip capable to embed smart card-grade applications (e.g., payment, transport ...) with the required level of security and features. In FIG. 1A, the SE 102 embeds or associates with contactless and NFC-related applications and is connected to the NFC controller 101 to act as the contactless front end.

**[0053]** Typically, a standard-compliant secure element comes with one issuer security domain (ISD) and an option for one or more supplemental security domains (SSD). Each of these domains includes a set of keys. In one embodiment, the SE 102 is a chip embedded in the mobile device 100 or in a miniature card inserted into the mobile device 100 via a card interface 109. In another embodiment, the SE 102 is or includes a software module loaded in a secured memory space 107 in the mobile device 100. The software module may be updated by downloading updating components from a designated server using a network interface 103 (e.g., a 3G network or an LTE network) in the mobile device 100.

**[0054]** The SE 102 needs to go through a personalization process before it can be used. In one embodiment, the personalization process is to load the SE 102 with or update a key set with a derived personalized key set of a chosen card issuer (i.e., a so-called SE issuer). Such a personalization process may be also referred to as a provisioning process. According to one embodiment, the provisioning is performed over the air (OTA) to cause the SE to be personalized while installing an application or enabling a service (i.e., application installation and personalization). The personalization of an SE is only done once to associate the SE to an SE issuer. The application installation and provisioning shall be done for each application when a user subscribes or installs an application.



**[0055]** In one embodiment, when updating or upgrading the SE 102, only one or some components pertaining to the SE 102 are replaced by newer updates to avoid personalizing the SE 102 from beginning. Depending on implementation, such newer updates may be automatically or manually obtained to be loaded into the mobile device 100.

**[0056]** In one embodiment, applications are available for an NFC-enabled mobile device to download from a server or a TSM portal depending on the corresponding SE issuer and the TSM thereof. TSM, standing for Trusted Service Management, is a collection of services. One main role envisaged for the TSM is to help service providers securely distribute and manage contactless services for their customers using the networks of mobile operators. The TSM or its server(s) does not necessarily participate in actual contactless transactions using NFC devices. These transactions are processed normally in whatever system the service provider and its merchant partners have already put in place. Another role of the TSM is to accelerate the successful deployment and ramp-up of mobile NFC applications by acting as a commercial intermediary that facilitates contractual arrangements and other aspects of ongoing business relationships among different parties that make the commerce via the mobile networks possible.

**[0057]** The personalization process can be done either physically in a service center or remotely via a web portal by a TSM server. In the first scenario, the customer may physically go to a service center to let a service representative to personalize the SE in a mobile device. With a computer connected to a NFC reader at a designated place (e.g., a service center), a provisioning manager can be either an installed application or a web-based application connecting to a backend TSM. The provisioning manager is configured to communicate with the SE of the mobile device (e.g., via a reader). Such a personalization process is referred to as a process Over the Internet (OTI).

**[0058]** In the second scenario, the customer registers his/her mobile phone via a server (often a TSM web portal). The TSM server is configured to push a universal resource identifier (URI) of a provisioning manager to the registered mobile phone. Depending on a type of the device, the push can be either an SMS (Short Message

Service) Push or a Google Android Push. The customer can download the provisioning manager into the mobile device and start the personalization process. Such a personalization process is referred to as a process Over the Air (OTA).

**[0059]** In either one of the scenarios, the provisioning manager acts as a proxy between the SE in the mobile device and the TSM server. Referring now to FIG. 1B, it shows a flowchart or process 110 of personalizing an SE according to one embodiment of the present invention. Depending on implementation, the process 110 may be implemented in software or a combination of software and hardware. When a user receives a new NFC device (e.g., a part of a mobile device), the SE therein needs to be personalized.

**[0060]** At 112, the new NFC device is determined if it is a genuine NFC device. One example is to check a serial number associated with the NFC device. The serial number may be verified with a database associated with a TSM server. In the example of a NFC mobile device, the device serial number of the mobile device may be used for verification. It is now assumed that the NFC device is a genuine device (recognizable by a mobile operator). The process 110 goes to 114 to have the NFC device communicated with a dedicated server. In one embodiment, the server is a part of the Trusted Service Management (TSM) system and accessible by a wireless network, the Internet or a combination of wireless and wired networks (herein referred to as a data network or simply a network).

**[0061]** At 116, the NFC device is registered with the server. Once the NFC device becomes part of the system, various services or data may be communicated to the device via the network. As part of the personalization process, the server requests device information of the SE at 118. In one embodiment, the server is configured to send a data request (e.g., a WAP PUSH) to the device. In responding to the request, the device sends back CPLC (card product life cycle) information retrieved from the SE. The CPLC includes the SE product information (e.g., the smart card ID, manufacturer information and a batch number and etc.). Based on the CPLC info, the server is able to retrieve corresponding default Issuer Security Domain (ISD) information of this SE from its manufacturer, an authorized distributor or a service provider (referred to as a manufacturer, a distributor or

a provider of the SE). Depending on implementation, there are two ways that the server may communicate with a SE manufacturer, which will be fully discussed herein later when deemed appropriate.

**[0062]** At 120, it is up to the manufacturer whether to update the device information. In general, when an SE is shipped from the manufacturer, the SE is embedded with some default device information. If it is decided that the default information such as the CPLC data is to be updated with the manufacturer, the process 110 goes to 122 where the manufacturer uploads corresponding updated device information to the server. The updated device information is transported to the device and stored in the SE at 124. If it is decided that the default information in the SE is not to be updated with the manufacturer, the process 110 goes to 124 to store the retrieved default device information in a database with the TSM server. In one embodiment, the server is configured to include an interface to retrieve a derived SE key set. In one embodiment, the derived key set is generated with the device information (e.g., ISD) of the SE. When the derived ISD key set is successfully installed on the SE, the corresponding SE issuer is notified of the use of the derived ISD key set.

**[0063]** According to one embodiment, the device information (default or updated) is used to facilitate the generation of a set of keys at 126. In one embodiment, the server is configured to establish a secured channel using the default ISD between its hardware security module (HSM) and the SE. The server is also configured to compute a derived key set for the SE. Depending on a business agreement, a master ISD key of an issuer for the SE may be housed in a hardware security module (HSM) associated with the server or in a local HSM of the SE issuer. An HSM is a type of secure crypto-processor targeted at managing digital keys, accelerating crypto-processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications. If it is housed in the HSM of the server, the server is configured to instruct the HSM to compute the derived key set. Then, the server prepares a mechanism (e.g., PUT KEY APDU) and uses the default channel to replace the default key set in the SE with the derived key set. If the master ISD key of the SE issuer is in a local HSM of the SE issuer, the server is configured to interact with the remote HSM to retrieve the keys.

**[0064]** At 128, the set of keys is securely delivered to the SE. The set of keys is thus personalized to the SE and will be used for various secured subsequent operations or services with the NFC device. The server at 130 is configured to synchronize the SE with the issuer or provider (e.g., sending a notification thereto about the status of the SE).

**[0065]** After the personalization, the SE can only be accessed using the personalized ISD key of the SE issuer. Depending on the security requirement of each service provider, the TSM can create additional SSDs for the various providers to personalize their respective applications (e.g., the modules 104 or 106 of FIG. 1A).

**[0066]** As mentioned above, there are two ways that may be used to retrieve the corresponding default Issuer Security Domain (ISD) information from the SE in interfacing with the manufacturer thereof. Depending on the infrastructure, a manufacturer can choose to use a real-time approach or a batch approach.

**[0067]** In the real-time approach, the server is configured to communicate with the manufacturer (i.e., its server thereof) when an SE by the manufacturer is being personalized by the TSM server. The default key set is, thus, retrieved on demand from the server of the manufacturer. In one embodiment, the TSM server includes a plugin module for each of the manufacturers to communicate therewith.

**[0068]** In the batch approach, it can be done either offline mode or online mode. In the offline mode, the SE manufacturer delivers the default ISD information for all SEs being supported via an encrypted physical media. An administrator for the TSM may or a computing device may be configured to import the information in the media to a computing device. The default ISDs are then decrypted and retrieved, and stored in a database. In the online mode, the SE manufacturer uploads the default ISD information for the SEs it supports via a network. The default ISDs are then decrypted and retrieved, and stored in a database. Afterwards, the TSM only needs to access its own HSM or the database during an SE personalization process. FIG. 1C shows relationships among the SE manufacturer, the TSM admin and the TSM system for both offline and online modes.

**[0069]** According to one embodiment of the present invention, FIG. 1D illustrates data flows among a user for an NFC device (e.g., an NFC mobile phone),

the NFC device itself, a TSM server, a corresponding SE manufacturer and an SE issuer.

**[0070]** In one perspective, the SE 102 of FIG. 1A may be perceived as a preload operating system in a smart card, providing a platform for PIN management and security channels (security domains) for card personalization. The SE 102 combines the interests of smart card issuers, vendors, industry groups, public entities and technology companies to define requirements and technology standards for multiple applications running in the smart cards.

**[0071]** As an example, one module 104 referred to as an e-purse security defines a set of protocols that enable micro payment transactions to be carried out in both wired and wireless environments. With an electronic purse (a.k.a., e-purse) stored on a smart card, a set of keys (either symmetric or asymmetric) is personalized into the e-purse after the e-purse is issued. During a transaction, the e-purse uses a set of respective keys for encryption and MAC computation in order to secure the message channel between the e-purse and an SAM (Security Authentication Module) or backend servers. For a single functional card, the e-purse security 104 is configured to act as gates to protect actual operations performed on a single functional card. During personalization, the single functional card access keys (or its transformation) are personalized into the e-purse with the e-purse transaction keys.

**[0072]** FIG. 1E shows a flowchart or process 150 of personalizing data flow among three entities: a land-based SAM or a network e-purse server 152, an e-purse 154 acting as a gatekeeper, and a single function tag 156. Communications between the land-based SAM or the network e-purse server 152 and the e-purse 154 are conducted in sequence of a type of commands (e.g., APDU) while communications between the e-purse 154 and the single function tag 156 are conducted in sequence of another type of commands, wherein the e-purse 154 acts as the gate keeper to ensure only secured and authorized data transactions could happen.

**[0073]** In one embodiment, the physical security for the e-purse is realized in an emulator. As used herein, an emulator means a hardware device or a program that pretends to be another particular device or program that other components expect to

interact with. The e-purse security is realized between one or more applets configured to provide e-purse functioning and communication with a payment server. An SE supporting the e-purse is responsible for updating security keys to establish appropriate channels for interactions between a payment server and the applets, wherein the e-purse applet(s) acts as a gatekeeper to regulate or control the data exchange.

**[0074]** Referring now to FIG. 2A, it shows a mobile payment ecosystem 200 in which related parties are involved in order for the mobile payment ecosystem successful. According to one embodiment, an NFC device is allowed to install or download one or more applications from respective designated servers 202 (i.e., application management providers), where the applications are originally developed by developers 204 and distributed by service providers 210, application management providers 202 or others. It is assumed that the secure element 206 provided by a secure element provider 208 has already been personalized via a TSM or a trusted third party (e.g., a financial institution 212).

**[0075]** Once an application is installed in the NFC device, the next step is to provision the application with the secure element. An application provisioning process can be started in several ways. One of the ways is that an SE holder selects an application from a TSM portal on the mobile device and initiates the provisioning process. Another one is that the SE holder receives an application provisioning notification on the mobile device from the TSM on behalf of an application (service) provider.

**[0076]** The TSM or application providers can publish their applications on a TSM portal to be downloaded to a mobile device with the SE and/or subscribed at a request of a user (a.k.a., an SE holder). In one embodiment, the TSM is a cloud service to serve many SE issuers. Thus, many applications from various service providers are available on the TSM portal. However, when getting onto the TSM portal, SE holders can only see those applications approved by its SE issuer. Depending on the arrangement between an SE and a service provider, an application can either be downloaded/installed/personalized using the ISD keyset of the SE or a specific SSD

keyset of the service provider. If a SSD keyset has not been installed on the SE, it can be installed during an application installation.

**[0077]** The TSM knows the memory state of an SE for various SSDs. Based on the state of the SE and the memory allocation policy of the SSDs, the available applications for the various SSD in the application store may be marked with different indicators, for example, “OK to install”, or “Insufficient memory to install”. This will prevent unnecessary failure for users.

**[0078]** Once an application is installed on an NFC device, the application initiates a provisioning process by itself, or the TSM can push a provisioning notification to the NFC device via a cellular network or a wireless data network. Depending on the type of the devices, there are many different types of push messages to cause the NFC device to initial the provision process. An example of the push methods includes an SMS push or an Android Google Push. Once user accepts the notification, the provisioning process starts. The details of the provisioning process will be described below whenever deemed appropriate.

**[0079]** As part of the application provisioning, a TSM server implements some protective mechanism. One is to prevent an SE from being accidentally locked. Another is to disable application download if there is no sufficient memory on SE.

**[0080]** An SE may permanently lock itself if there are too many failed mutual authentications during secure channel establishment. In order to prevent the SE from being accidentally locked, the TSM keeps the track of the number of failed authentications between an SE and the TSM when establishing a secured channel between the two entities. In one embodiment, the TSM is configured to reject any further request if a preset limit is reached. The TSM can continue to process the SE request if the SE is reset at the service center manually.

**[0081]** The TSM also keeps track of the memory usage of each SE. The TSM decides whether an application can be installed on an SE based on the memory allocation assigned by the SE issuer to each service provider. According one embodiment, there are three types of policies:

- Pre-assigned a fixed memory. This is the guaranteed space.

- Pre-assigned a minimum memory. This is the guaranteed minimum space.
- Best efforts.

**[0082]** The SE issuer uses the TSM web portal to make this assignment.

1. For a batch of SE, the SE issuer can pre-assign a memory policy for a service provider to install its applications via the TSM web portal;
2. The TSM server verifies whether the space of the respective service provider conforms to its policy when a Mobile Device requests to install one of its applications. If not conformed, this request is rejected;
3. Otherwise, the TSM server will proceed to handle the provisioning request;
4. If the provisioning succeeds, the TSM will accumulate the memory size of this application service.

**[0083]** When a mobile user subscribes to a mobile application (assuming it has been installed), the application has to be provisioned with the SE in the mobile device before it can be used. According to one embodiment, the provisioning process includes four major stages:

- Create an supplemental security domain (SSD) on the SE, if needed;
- Download and install an application cap on the SE;
- Personalize the application on the SE; and
- Download a UI component on mobile phone.

**[0084]** FIG. 2B shows a flowchart or process 220 of provisioning one or more applications according to one embodiment. The process 220 may be implemented in software or a combination of software and hardware. In one embodiment, the application provisioning process 220 needs to go through a provisioning manager (i.e., proxy) on the mobile phone to interact with the SE therein.

**[0085]** As shown in FIG. 2B, at 222, the application provisioning process 220 may be started manually or automatically. For example, a user may initiate the process 220 by selecting an installed application to subscribe related services or the installed application, when activated, initiates the provisioning process, provided it has



not been provisioned. In another embodiment, a provider of an application pushes a message (e.g., SMS) to the mobile phone to initiate the provisioning process.

**[0086]** In any case, the process 220 goes to 224 to establish a communication with a dedicated server (e.g., a TSM server or a server operated by an application distributor) after the device information (e.g., CPLC) is retrieved from the SE in the mobile device. The device information along with an identifier identifying the application is transmitted to the server at 226. Based on the device information, the server identifies the issuer for the SE first at 228 to determine if the SE has been personalized at 230. If the SE has not been personalized, the process 220 goes to 232 to personalize the SE, where one embodiment of the function 232 may be implemented in accordance with the process 110 of FIG. 1B.

**[0087]** It is now assumed that the SE in the mobile device has been personalized. The process 220 now goes to 234 to establish a secure channel with the SE using the derived ISD. Depending on who houses the HSM (TSM or SE issuer) for the ISD, the server will contact the HSM to compute the derived ISD for the SE and establish a secure channel with the SE using this derived ISD. The server is then configured to check to see whether there is an SSD associated with this application at 236. If there is not an SSD associated with the application, the server is configured to check a database to see whether it has been installed with this SE. If the SSD installation is needed, then the process 220 goes to install the SSD. In one embodiment, the user is alerted of the installation of the SSD (keys). Should the user refuse to install the SSD at 238, the process 220 stops and goes to 222 to restart the provisioning process 220.

**[0088]** It is now assumed that the process of installing the SSD proceeds at 240. Installing the SSD is similar to installing the ISD. The TSM server is configured to contact the HSM that houses the SSD master key to compute the derived SSD key set for the SE. The master SSD key set can be either in the TSM or with the service provider or the SE issuer, largely depending on how the arrangement is made with all parties involved.

**[0089]** To download/install the application cap to the SE, the server is configured to establish a secure channel with the SE using this derived SSD at 242. In one embodiment, this is similar to how the ISD-based secure channel is established. At 244, the data for the application is prepared, the detail of which will be further discussed below. According to one embodiment, the server is configured to contact the service provider to prepare STORE DATA APDUs. Depending on an application installed in a mobile device, the server may be caused to repeatedly issue STORE DATA to personalize the application with the SE. Additional data including an appropriate interface (e.g., a user interface of the application per the mobile device) may be downloaded provided that the provisioning process is successfully done. At 246, the server will notify the application provider the status of the application that has been provisioned.

**[0090]** FIG. 2C shows a data flow 250 illustrating various interactions among different parties when an application is being provisioned in one embodiment.

**[0091]** As shown in 244 of FIG. 2B, one of the important functions in provisioning an application is to prepare customized application data for the targeted SE. For example, for an e-purse application, the personalized data for the application includes various personalized transaction keys generated based on the device information (e.g., CPLC info) of the SE. For transit e-purse, part of the personalized data includes the Mifare access keys derived from an identifier (ID) of the Mifare card, the server is configured to personalize both Java Card applications and Mifare4Mobile service objects. In general, there are at least two different ways to prepare the data to facilitate subsequent transactions.

**[0092]** For data preparation, one embodiment of the present invention supports two operation modes to interact with service providers for computing the personalized application data. For the first mode, a TSM server does not have direct access to the HSM associated with a service provider. The service provider may have a server interacting with its HSM to generate the application keys (e.g., Transit, e-purse, or Mifare Key). The TSM data preparation implementation is to make use of application program interfaces (API) or a protocol provided by the server to request for derived

application keys. The second mode is that data preparation implementation can directly access the HSM associated with the service provider to generate the application keys.

**[0093]** According to one embodiment, FIG. 2D shows a data flow 255 among different entities when preparing the application data in provisioning an application. FIG. 2D is provided for the first mode in which a TSM server does not have direct access to the HSM associated with a service provide. The second mode has the similar flow except that the application data preparation implementation will interact directly with the HSM of a service provider.

**[0094]** Besides supporting a provisioning process, one embodiment of the present invention also supports the life cycle management of an SE. The life cycle management includes, but may not be limited to, SE lock, SE unlock, Application Delete (disabling). The initiation of these activities may be through a TSM push notification. In actual use of mobile devices, FIG. 2E shows a flowchart or process 260 of locking an installed application. An NFC device may have been installed with a number of applications in connection with or running on top of the secured element therein. For some reason (e.g., no activity for a prolonged period or expiration), an application needs to be disabled or locked by its distributor or provider.

**[0095]** The operation or process 260 to disable an installed application is initiated at 262. In one embodiment, the process 260 is initiated by an operator manually via a TSM web portal. In another embodiment, the process 260 is automatically initiated by a service provider internal workflow (e.g., using TSM web service API). Once the process 260 is initiated, a message is pushed to a NFC device (e.g., within a mobile device) in which an application is to be disabled. Depending on application, such a message may come in different forms. In one embodiment, the message is a PUSH command. In another embodiment, the message is a TCP/IP request delivered to the device via a network. The message may be sent from a server (e.g., a TSM server) at 264. Depending on implementation, such a message may include an identifier identifying an application to be locked or disabled. Upon receiving such a message, a card manager proxy on the device is caused to verify whether such

a message is indeed from its original distributor or provider by returning a message at 266. According to one embodiment, the message is sent to a TSM server for verification. If the verification fails, namely there is no acknowledgement to such an inquiry, the process 260 is abandoned.

**[0096]** It is now assumed that the verification is successful, namely the inquiry from the device to a provider of the application returns an acknowledgement that the original request is authenticated. In general, such an acknowledgement includes an identifier confirming the application to be locked at 268. The TSM server is configured to establish a secure channel with the SE as described previously. Then, the TSM server is to prepare appropriate APDUs (such as SET STATUS, or/and DELETE) for the SE for execution via the card manager proxy.

**[0097]** In any case, in responding to the command, the SE proceeds by locking the application at 272. According to one embodiment, the SE is caused to disassociate with the application, thus making the installed application no longer usable with the SE. At 274, the SE is configured to send out an acknowledgement to notify related parties that this application is no longer operating in the device. In one embodiment, the acknowledgement is sent over to the TSM server where there is a database recording what applications have been installed in what device, and a corresponding status of each. The database is updated with the acknowledgement from the SE.

**[0098]** FIG. 2E shows a flowchart or process for locking or disabling an installed application. It is known to those skilled in the art that other operations, such as unlocking or enabling an installed application, extending expiration of an installed application, are similar to those shown in FIG. 2E.

**[0099]** Referring now to FIG. 2F, there shows an exemplary architecture diagram 280 of a portable device enabled as an electronic wallet or e-purse to facilitate e-commerce and m-commerce, according to one embodiment of the present invention. The diagram 280 includes a cell phone 282 embedded with a smart card module. An example of such a cell phone is a near field communication (NFC) enabled cellphone that includes a Smart MX (SMX) module. It shall be noted that a secure element and an application may be integrated. Unless explicitly stated, the following description will

not call out which part is performing the function of a secure element and which part is performing as an application. Those skilled in the art shall appreciate the proper parts or functions being performed given the detailed description herein.

**[00100]** The SMX is pre-loaded with a Mifare emulator 288 (which is a single functional card) for storing values. The cell phone is equipped with a contactless interface (e.g., ISO 14443 RFID) that allows the cell phone to act as a tag. In addition, the SMX is a JavaCard that can run Java applets. According to one embodiment, an e-purse is built as an applet in SMX. The e-purse is configured to be able to access the Mifare data structures with appropriate transformed passwords based on the access keys.

**[00101]** In the cell phone 282, an e-purse manager MIDlet 204 is provided. For m-commerce, the MIDlet 284 acts as an agent to facilitate communications between an e-purse applet 286 and one or more payment network and servers 290 to conduct transactions therebetween. As used herein, a MIDlet is a software component suitable for being executed on a portable device. The e-purse manager MIDlet 284 is implemented as a "MIDlet" on a Java cell phone, or an "executable application" on a PDA device. One of the functions of the e-purse manager MIDlet 284 is to connect to a wireless network and communicate with an e-purse applet which can reside on either the same device or an external smart card. In addition, it is configured to provide administrative functions such as changing a PIN, viewing an e-purse balance and a transaction history log. In one application in which a card issuer provides a SAM 292 that is used to enable and authenticate any transactions between a card and a corresponding server (also referred to as a payment server). As shown in FIG. 2F, APDU commands are constructed by the servers 290 having access to a SAM 292, where the APDU is a communication unit between a reader and a card. The structure of an APDU is defined by the ISO 7816 standards. Typically, an APDU command is embedded in network messages and delivered to the server 290 or the e-purse applet 286 for processing.

**[00102]** For e-commerce, a web agent 294 on a computer (not shown) is responsible for interacting with a contactless reader (e.g., an ISO 14443 RFID reader) and the network server 290. In operation, the agent 294 sends the APDU commands

or receives responses thereto through the contactless reader 296 to/from the e-purse applet 286 residing in the cell phone 282. On the other hand, the agent 294 composes network requests (such as HTTP) and receives responses thereto from the payment server 280.

**[00103]** To personalize the cell phone 282, FIG. 3A shows a block diagram 300 of related modules interacting with each other to achieve what is referred to herein as e-purse personalization (or provisioning) by an authorized person. FIG. 3B shows a block diagram 320 of related modules interacting with each other to achieve what is referred to herein as e-purse personalization by a user of the e-purse as shown in FIG. 2F.

**[00104]** FIG. 3C shows a flowchart or process 350 of personalizing an e-purse applet according to one embodiment of the present invention. FIG. 3C is suggested to be understood in conjunction with FIG. 3A and FIG. 3B. The process 350 may be implemented in software, hardware or a combination of both.

**[00105]** As described above, an e-purse manager is built on top of a global platform to provide a security mechanism necessary to personalize e-purse applets designed therefor. In operation, a security domain is used for establishing a secured channel between a personalization application server and the e-purse applet. According to one embodiment, the essential data to be personalized into the e-purse applet include one or more operation keys (e.g., a load or top-up key and a purchase key), default PINs, administration keys (e.g., an unblock PIN key and a reload PIN key), and passwords (e.g., from Mifare).

**[00106]** It is assumed that a user desires to personalize an e-purse applet embedded in a portable device (e.g., a cell phone). At 352 of FIG. 3C, a personalization process is initiated. Depending on implementation, the personalization process may be implemented in a module in the portable device and activated manually or automatically, or a physical process initiated by an authorized person (typically associated with a card issuer). As shown in FIG. 3A, an authorized person initiates a personalization process 304 to personalize the e-purse applet for a user thereof via an existing new e-purse SAM 306 and an existing SAM 308 with the contactless reader 310 as the interface. The card manager 311 performs at least two

functions: 1) establishing a security channel, via a security domain, to install and personalize an external application (e.g., e-purse applet) in the card personalization; and 2) creating security means (e.g., PINs) to protect the application during subsequent operations. As a result of the personalization process using the personalization application server 304, the e-purse applet 312 and the emulator 314 are personalized.

**[00107]** Similarly, as shown in FIG. 3B, a user of an e-purse desires to initiate a personalization process to personalize the e-purse applet wirelessly (e.g., via the m-commerce path of FIG. 2). Different from FIG. 3A, FIG. 3B allows the personalization process to be activated manually or automatically. For example, there is a mechanism on a cell phone that, if pressed, activates the personalization process. Alternatively, a status of “non-personalized” may prompt to the user to start the personalization process. As described above, a MIDlet 322 (i.e., a provisioning manager or a service manager) in a portable device acts as an agent to facilitate the communication between a payment server 324 and the e-purse applet 312 as well as the emulator 314, wherein the payment server 324 has the access to the existing new e-purse SAM 306 and an existing SAM 308. As a result of the personalization process, the e-purse applet 312 and the emulator 314 are personalized.

**[00108]** Referring now back to FIG. 3C, after the personalization process is started, in view of FIG. 3A, the contactless reader 310 is activated to read the tag ID (i.e., RFID tag ID) and essential data from a smart card in the device at 354. With an application security domain (e.g., a default security setting by a card issuer), a security channel is then established at 356 between a new e-purse SAM (e.g., the SAM 306 of FIG. 3A) and an e-purse applet (e.g., the e-purse applet 312 of FIG. 3A) in the portable device.

**[00109]** Each application security domain key set includes at least three (3) DES keys. For example:

Key1: 255/1/DES-ECB/404142434445464748494a4b4c4d4e4f

Key2: 255/2/DES-ECB/404142434445464748494a4b4c4d4e4f

Key3: 255/3/DES-ECB/404142434445464748494a4b4c4d4e4f

**[00110]** A security domain is used to generate session keys for a secured session between two entities, such as the card manager applet and a host application, in which case the host application may be either a desktop personalization application or a networked personalization service provided by a backend server.

**[00111]** A default application domain can be installed by a card issuer and assigned to various application/service providers. The respective application owner can change the value of the key sets before the personalization process (or at the initial of the process). Then the application can use the new set to create a security channel for performing the personalization process.

**[00112]** With the security channel is established using the application provider's application security domain, the first set of data can be personalized to the e-purse applet. The second set of data can also be personalized with the same channel, too. However, if the data are in separate SAM, then a new security channel with the same key set (or different key sets) can be used to personalize the second set of data.

**[00113]** Via the new e-purse SAM 306, a set of e-purse operation keys and PINs are generated for data transactions between the new e-purse SAM and the e-purse applet to essentially personalize the e-purse applet at 358.

**[00114]** A second security channel is then established at 360 between an existing SAM (e.g., the SAM 308 of FIG, 3A) and the e-purse applet (e.g., the e-purse applet 312 of FIG, 3A) in the portable device. At 362, a set of transformed keys is generated using the existing SAM and the tag ID. The generated keys are stored in the emulator for subsequent data access authentication. At 358, a set of MF passwords is generated using the existing SAM and the tag ID, then is stored into the e-purse applet for future data access authentication. After it is done, the e-purse including the e-purse applet and the corresponding emulator is set to a state of "personalized".

**[00115]** FIG. 4A and FIG. 4B show together a flowchart or process 400 of financing or funding an e-purse according to one embodiment of the present invention. The process 400 is conducted via the m-commerce path of FIG. 2. To better understand the process 400, FIG. 4C shows an exemplary block diagram 450 of related blocks interacting with each other to achieve the process 400. Depending on



an actual application of the present invention, the process 400 may be implemented in software, hardware or a combination of both.

**[00116]** A user is assumed to have obtained a portable device (e.g., a cell phone) that is configured to include an e-purse. The user desires to fund the e-purse from an account associated with a bank. At 402, the user enters a set of personal identification numbers (PIN). Assuming the PIN is valid, an e-purse manager in the portable device is activated and initiates a request (also referred to an over-the-air (OTA) top-up request) at 404. The MIDlet in the portable device sends a request to the e-purse applet at 406, which is illustrated in FIG. 4C where the e-purse manager MIDlet 434 communicates with the e-purse applet 436.

**[00117]** At 408, the e-purse applet composes a response in responding to the request from the MIDlet. Upon receiving the response, the MIDlet sends the response to a payment network and server over a cellular communications network. As shown in FIG. 4C, the e-purse manager MIDlet 434 communicates with the e-purse applet 436 for a response that is then sent to the payment network and server 440. At 410, the process 400 needs to verify the validity of the response. If the response cannot be verified, the process 400 stops. If the response can be verified, the process 400 moves to 412 where a corresponding account at a bank is verified. If the account does exist, a fund transfer request is initiated. At 414, the bank receives the request and responds to the request by returning a response. In general, the messages exchanged between the payment network and server and the bank are compliant with a network protocol (e.g., HTTP for the Internet).

**[00118]** At 416, the response from the bank is transported to the payment network and server. The MIDlet strips and extracts the APDU commands from the response and forwards the commands to the e-purse applet at 418. The e-purse applet verifies the commands at 420 and, provided they are authorized, sends the commands to the emulator at 420 and, meanwhile updating a transaction log. At 422, a ticket is generated to formulate a response (e.g., in APDU format) for the payment server. As a result, the payment server is updated with a successful status message for the MIDlet, where the APDU response is retained for subsequent verification at 424.

**[00119]** As shown in FIG. 4C, the payment network and server 440 receives a response from the e-purse manager MIDlet 434 and verifies that the response is from an authorized e-purse applet 436 originally issued therefrom with a SAM 444. After the response is verified, the payment network and server 440 sends a request to the financing bank 442 with which the user 432 is assumed to maintain an account. The bank will verify the request, authorize the request, and return an authorization number in some pre-arranged message format. Upon receiving the response from the bank 442, the payment server 440 will either reject the request or accept the request by forming a network response sent to the MIDlet 434.

**[00120]** The e-purse manager 434 verifies the authenticity (e.g., in APDU format) and sends commands to the emulator 438 and updates the transaction logs. By now, the e-purse applet 436 finishes the necessary steps and returns a response to the MIDlet 434 that forwards an (APDU) response in a network request to the payment server 440.

**[00121]** Although the process 400 is described as funding the e-purse. Those skilled in the art can appreciate that the process of making purchasing over a network with the e-purse is substantially similar to the process 400, accordingly no separate discussion on the process of making purchasing is provided.

**[00122]** Referring to FIG. 5A, there is shown a first exemplary architecture 500 of enabling a portable device 530 for e-commerce and m-commerce over a cellular communications network 520 (e.g., a GPRS network) in accordance with one embodiment of the present invention. The portable device 530 comprises a baseband 524 and a secured element 529 (e.g., a smart card). One example of such portable device is a Near Field Communication (NFC) enabled portable device (e.g., a cell mobile phone or a PDA). The baseband 524 provides an electronic platform or environment (e.g., a Java Micro Edition (JME), or Mobile Information Device Profile (MIDP)), on which an application MIDlet 523 and a service manager 522 can be executed or run. The secured element 529 contains a Global Platform (GP) card manager 526, an emulator 528 and other components such as PIN manager (not shown).

**[00123]** To enable the portable device 530 to conduct e-commerce and m-commerce, one or more services/applications need to be pre-installed and pre-configured thereon. An instance of a service manager 522 (e.g., a MIDlet with GUI) needs to be activated. In one embodiment, the service manager 522 is downloaded and installed. In another embodiment, the service manager 522 is preloaded. In any case, once the service manager 522 is activated, a list of directories for various services is shown. The items in the list may be related to the subscription by a user, and may also include items in promotion independent of the subscription by the user. The directory list may be received from a directory repository 502 of a directory server 512. The directory server 512 acts as a central hub (i.e., yellow page functions) for different service providers (e.g., an installation server, a personalization server) that may choose to offer products and/or services to subscribers. The yellow page functions of the directory server 512 may include service plan information (e.g., service charge, start date, end date, etc.), installation, personalization and/or MIDlet download locations (e.g., Internet addresses). The installation and personalization may be provided by two different business entities. For example, the installation is provided by an issuer of a secured element 529, while the personalization may be provided by a service provider who holds application transaction keys for a particular application.

**[00124]** According to one embodiment, the service manager 522 is configured to connect to one or more servers 514 (e.g., a TSM server) from a service provider(s) over the cellular communications network 520. It is assumed that the user has chosen one of the applications from the displayed directory. A secured channel 518 is established between the one or more servers 514 and the GP manager 526 to install/download an application applet 527 selected by the user and then to personalize the application applet 527 and optionally emulator 528, and finally to download an application MIDlet 523. The applet repository 504 and MIDlet repository 506 are the sources of generic application applets and application MIDlets, respectively. GP SAM 516 and application SAM 517 are used for creating the secured channel 518 for the personalization operations.

**[00125]** FIG. 5B is a diagram showing a second exemplary architecture 540 of enabling a portable device 530 for e-commerce and m-commerce over a public

network 521, according to another embodiment of the present invention. Most of the components of the second architecture 540 are substantially similar to those of the first architecture 500 of FIG. 5A. While the first architecture 500 is based on operations over a cellular communications network 520, the public network 521 (e.g., Internet) is used in the second architecture 540. The public network 521 may include a local area network (LAN), a wide area network (WAN), a Wi-Fi (IEEE 802.11) wireless link, a Wi-Max (IEEE 802.16) wireless link, etc. In order to conduct service operations over the public network 521, an instance of the service manager 532 (i.e., same or similar functionality of the service manager MIDlet 522) is installed on a computer 538, which is coupled to the public network 521. The computer 538 may be a desktop personal computer (PC), a laptop PC, or other computing devices that can execute the instance of the service manager 532 and be connected to the public network 521. The connection between the computer 538 and the portable device 530 is through a contactless reader 534. The service manager 532 acts as an agent to facilitate the installation and personalization between one or more servers 514 of a service provider and a GP card manager 526 via a secured channel 519.

**[00126]** FIG. 5C is a flowchart illustrating a process 550 of enabling a portable device for e-commerce and m-commerce functionalities in accordance with one embodiment of the present invention. The process 550 may be implemented in software, hardware or a combination of both depending on implementation. To better understand the process 500, previous figures especially FIG. 5A and FIG. 5B are referred to in the following description.

**[00127]** Before the process 550 starts, an instance of a service manager 522 or 532 has been downloaded or pre-installed on either the portable device 530 or a computer 538. At 552, the service manager is activated and sends a service request to the server 514 at a service provider. Next after the authentication of a user and the portable device has been verified, at 554, the process 550 provides a directory list of services/applications based on subscription of the user of the portable device 530. For example, the list may contain a mobile POS application, an e-purse application, an e-ticketing application, and other commercially offered services. Then one of the services/applications is chosen from the directory list. For example, an e-purse or a

mobile-POS may be chosen to configure the portable device 530. Responding to the user selection, the process 550 downloads and installs the selected services/applications at 556. For example, e-purse applet (i.e., application applet 527) is downloaded from the applet repository 504 and installed onto a secured element 529. The path for downloading or installation may be either via a secured channel 518 or 519. At 558, the process 550 personalizes the downloaded application applet and the emulator 528 if needed. Some of the downloaded application applets do not need to be personalized and some do. In one embodiment, a mobile POS application applet (“POS SAM”) needs to be personalized, and the following information or data array has to be provided:

- a unique SAM ID based on the unique identifier of the underlying secured element;
- a set of debit master keys;
- a transformed message encryption key;
- a transformed message authentication key;
- a maximum length of remark for each offline transaction;
- a transformed batch transaction key; and
- a GP PIN.

**[00128]** In another embodiment, personalization of an e-purse applet for a single functional card not only needs to configure specific data (i.e., PINs, transformed keys, start date, end date, etc.) onto the e-purse, but also needs to configure the emulator to be operable in an open system. Finally, at 560, the process 550 downloads and optionally launches the application MIDlet 523. Some of the personalized data from the application applet may be accessed and displayed or provided from the user. The process 550 ends when all of the components of services/applications have been installed, personalized and downloaded.

**[00129]** According to one embodiment, an exemplary process of enabling a portable device 530 as a mobile POS is listed as follows:

- connecting to an installation server (i.e., one of the service provider server 514) to request the server to establish a first security channel (e.g., the secured

channel 518) from an issuer domain (i.e., applet repository 504) to the GP card manager 526 residing in a secured element 529;

receiving one or more network messages including APDU requests that envelop a POS SAM applet (e.g., a Java Cap file from the applet repository 504);

extracting the APDU requests from the received network messages;

sending the extracted APDU requests to the GP card manager 526 in a correct order for installation of the POS SAM (i.e., application applet 527) onto the secured element 529;

connecting to a personalization server (i.e., one of the service provider servers 514) for a second security channel (may or may not be the secured channel 518 depending on the server and/or the path) between the personalization server and the newly downloaded applet (i.e., POS SAM);

receiving one or more network messages for one or more separated 'STORE DATA APDU'; and

extracting and sending the 'STORE DATA APDU' to personalize POS SAM; and

downloading and launching POS manager (i.e., application MIDlet 523).

**[00130]** Referring to FIG. 6A, there is shown an exemplary architecture 600, in which a portable device 630 is enabled as a mobile POS to conduct e-commerce and m-commerce, according to one embodiment of the present invention. The portable device 630 comprises a baseband 624 and a secured element 629. A POS manager 623 is downloaded and installed in the baseband 623 and a POS SAM 628 is installed and personalized in the secured element 629 to enable the portable device 630 to act as a mobile POS. Then a real time transaction 639 can be conducted between the mobile POS enabled portable device 630 and an e-token enabled device 636 (e.g., a single functional card or a portable device enabled with an e-purse). The e-token may represent e-money, e-coupon, e-ticket, e-voucher or any other forms of payment tokens in a device.

**[00131]** The real time transaction 639 can be conducted offline (i.e., without the portable device connecting to a backend POS transaction server 613). However, the portable device 630 may connect to the backend POS transaction servers 613 over the cellular network 520 in certain instances, for example, the amount of the

transaction is over a pre-defined threshold or limit, the e-token enabled device 636 needs a top-up or virtual top-up, transactional upload (single or in batch).

**[00132]** Records of accumulated offline transactions need to be uploaded to the backend POS transaction server 613 for settlement. The upload operations are conducted with the portable device 630 connecting to the POS transaction server 613 via a secured channel 618. Similar to the installation and personalization procedures, the upload operations can be conducted in two different routes: the cellular communications network 520; or the public network 521. The first route has been described and illustrated in FIG. 6A.

**[00133]** The second route is illustrated in FIG. 6B showing an exemplary architecture 640, in which a portable device 630 is enabled as a mobile POS conducting a transaction upload in batch operation over a public network 521, according to an embodiment of the present invention. Records of offline transactions in the mobile POS are generally kept and accumulated in a transaction log in the POS SAM 628. The transaction log are read by a contactless reader 634 into a POS agent 633 installed on a computer 638. The POS agent 633 then connects to a POS transaction server 613 over the public network 521 via a secured channel 619. Each of the upload operations is marked as a different batch, which includes one or more transaction records. Data communication between the POS SAM 628, the contactless reader 634 and the POS agent 632 in APDU containing the transaction records. Network messages that envelop the APDU (e.g., HTTP) are used between the POS agent 632 and the POS transaction server 613.

**[00134]** In one embodiment, an exemplary batch upload process from the POS manager 623 or the POS agent 633 includes:

- sending a request to the POS SAM 628 to initiate a batch upload operation;
- retrieving accumulated transaction records in form of APDU commands from a marked "batch" or "group" in the POS SAM 628 when the POS SAM 628 accepts the batch upload request;
- forming one or more network messages containing the retrieved APDU commands;

sending the one or more network messages to the POS transaction server 613 via a secured channel 619;  
receiving a acknowledgement signature from the POS transaction server 613;  
forwarding the acknowledgement signature in form APDU to the POS SAM 628 for verification and then deletion of the confirmed uploaded transaction records;  
and  
repeating the step b) to step f) if there are additional un-uploaded transaction records still in the same “batch” or “group”.

**[00135]** Referring to FIG. 6C, there is shown a flowchart illustrating a process 650 of conducting m-commerce using the portable device 630 enabled to act as a mobile POS with an e-token enabled device 636 as a single functional card in accordance with one embodiment of the present invention. The process 650, which is preferably understood in conjunction with the previous figures especially FIG. 6A and FIG. 6B, may be implemented in software, hardware or a combination of both.

**[00136]** The process 650 (e.g., a process performed by the POS manager 623 of FIG. 6A) starts when a holder of an e-token enabled device (e.g., a Mifare card or an e-purse enabled cell phone emulating single functional card) desires to make a purchase or order a service with the mobile POS (i.e., the portable device 630). At 652, the portable device 630 retrieving an e-token (e.g., tag ID of Mifare card) by reading the e-token enabled device. Next, the process 650 verifies whether the retrieved e-token is valid at 654. If the e-token enabled device 636 of FIG. 6A is a single functional card (e.g., Mifare), the verification procedure performed by the POS manager 623 includes: i) reading the card identity (ID) of the card stored on an area that is unprotected or protected by a well-known key; ii) sending an APDU request containing the card ID to the POS SAM 628; iii) and receiving one or more transformed keys (e.g., for transaction counter, an issuer data, etc.) generated by the POS SAM 628. If the one or more received transformed keys are not valid, that is, the retrieved e-token being not valid, then the process 650 ends. Otherwise, the process 650 following the “yes” branch to 656, in which it is determined whether there is enough balance in the retrieved e-token to cover the cost of the current transaction. If the result is “no” at 656, the process 650 may optionally offer the holder to top-up (i.e.,



load, fund, finance) the e-token at 657. If “no”, the process 650 ends. Otherwise if the holder agrees to a real time top-up of the e-token enabled device, the process 650 performs either a top-up or a virtual top-up operation at 658. Then the process 650 goes back to 656. Whereas there is enough balance in the e-token, the process 650 deducts or debits the purchase amount from the e-token of the e-token enabled device 636 at 660. In the single functional card case, the one or more transformed keys are used to authorize the deduction. Finally at 662, records of one or more offline transactions accumulated in the POS SAM 628 are uploaded to the POS transaction server 613 for settlement. The upload operations may be conducted for each transaction or in batch over either the cellular communications network 520 or the public domain network 521.

**[00137]** The top-up operations have been described and shown in the process 400 of FIG. 4A. A virtual top-up operation is a special operation of the top-up operation and typically is used to credit an e-token by a sponsor or donor. To enable a virtual top-up operation, the sponsor needs to set up an account that ties to an e-token enabled device (e.g., a single functional card, a multi-functional card, an e-token enable cell phone, etc.). For example, an online account is offered by a commercial entity (e.g., business, bank, etc.). Once the sponsor has funded the e-token to the online account, the holder of the e-token enabled device is able to receive an e-token from the online account when connecting to the mobile POS. Various security measures are implemented to ensure the virtual top-up operation is secure and reliable. One exemplary usage of the virtual top-up is that a parent (i.e., a sponsor) can fund an e-token via an online account, which is linked to a cell phone (i.e., an e-token enabled device) of a child (i.e., the holder), such that the child may receive the funded e-token while the child makes a purchase at a mobile POS. In addition to various e-commerce and m-commerce functionalities described herein, the POS manager 623 is configured to provide various query operations, for example, a) checking the un-batched (i.e., not uploaded) balance accumulated in the POS SAM, b) listing the un-batched transaction log in the POS SAM, c) viewing details of a particular transaction stored in the POS SAM, d) checking the current balance of an e-token

enabled device, e) listing a transaction log of the e-token enabled device, and f) viewing details of a particular transaction of the e-token enabled device.

**[00138]** Referring to FIG. 6D, there is shown a flowchart illustrating an exemplary process 670 of conducting m-commerce using the portable device 630 enabled to act as a mobile POS with an e-token enabled device 636 as a multi-functional card in accordance with one embodiment of the present invention. The process 670, which is preferably understood in conjunction with the previous figures especially FIG. 6A and FIG. 6B, may be implemented in software, hardware or a combination of both.

**[00139]** The process 670 (e.g., a process performed by the POS manager 623 of FIG. 6A) starts when a holder of an e-token enabled device 636 (e.g., a multi-functional card or an e-purse enabled cell phone emulating a multi-functional card) desires to make a purchase or order a service with the mobile POS (i.e., the portable device 630). At 672, the process 670 sends an initial purchase request to the e-token enabled device 636. The purchase amount is sent along with the initial request (e.g., APDU commands). Next the process 670 moves to decision 674. When there is not enough balance in the e-token enabled device 636. The initial purchase request will be turned down as a return message received at the POS manager 623. As a result, the process 670 ends with the purchase request being denied. If there is enough balance in the e-token enabled device 636, the result of the decision 674 is “yes” and the process 670 follows the “yes” branch to 676. The received response (e.g., APDU commands) from the e-token enabled device 636 is forwarded to the POS SAM 628. The response comprises information such as the version of the e-token key and a random number to be used for establishing a secured channel between the applet (e.g., e-purse applet) resided on the e-token enabled device 636 and the POS SAM 628 installed on the portable device 630. Then, at 678, the process 670 receives a debit request (e.g., APDU commands) generated by the POS SAM 628 in response to the forwarded response (i.e., the response at 676). The debit request contains a Message Authentication Code (MAC) for the applet (i.e., e-purse applet) to verify the upcoming debit operation, which is performed in response to the debit request sent at 680. The process 670 moves to 682 in which a confirmation message for the debit operation is received. In the confirmation message, there are additional MACs, which

are used for verification and settlement by the POS SAM 628 and the POS transaction server 613, respectively. Next at 684, the debit confirmation message is forwarded to the POS SAM 628 for verification. Once the MAC is verified and the purchase transaction is recorded in the POS SAM 628, the recorded transaction is displayed at 686 before the process 670 ends. It is noted that the e-commerce transaction described may be carried out offline or online with the POS transaction server 613. Also when there is not enough balance in the e-token enabled device, a top-up or funding operation may be performed using the process 400 illustrated in FIG. 4A and FIG. 4B.

**[00140]** FIG. 7 shows an exemplary configuration in which a portable device is used for an e-ticketing application. A portable device 730 is configured to include an e-purse 724. When an owner or holder of the portable device 730 desires to purchase a ticket for a particular event (e.g., a concert ticket, a ballgame ticket, etc.), the owner can use e-purse 724 to purchase a ticket through an e-ticket service provider 720. The e-ticket service provider 720 may contact a traditional box office reservation system 716 or an online ticketing application 710 for ticket reservation and purchase. Then e-token (e.g., e-money) is deducted from the e-purse 724 of the portable device 730 to pay the ticket purchase to a credit/debit system 714 (e.g., a financial institute, a bank). A SAM 718 is connected to the e-ticket service provider 720 so that the authentication of e-purse 724 in the portable device 730 can be assured. Upon a confirmation of the payment is received, the e-ticket is delivered to the portable device 730 over the air (e.g., a cellular communications network) and stored onto a secured element 726 electronically, for example, an e-ticket code or key or password. Later on, when the owner of the portable device 730, the ticket holder, attends the particular event, the owner needs only to let a gate check-in reader 734 to read the stored e-ticket code or key in the portable device 730. In one embodiment, the gate check-in reader 734 is a contactless reader (e.g., an ISO 14443 complied proximity coupling device). The portable device 730 is a NFC capable mobile phone.

**[00141]** The invention is preferably implemented by software, but can also be implemented in hardware or a combination of hardware and software. The invention can also be embodied as computer readable code on a computer readable medium.

The computer readable medium is any data storage device that can store data which can thereafter be read by a computer system. Examples of the computer readable medium include read-only memory, random-access memory, CD-ROMs, DVDs, magnetic tape, optical data storage devices, and carrier waves. The computer readable medium can also be distributed over network-coupled computer systems so that the computer readable code is stored and executed in a distributed fashion.

**[00142]** The present invention has been described in sufficient details with a certain degree of particularity. It is understood to those skilled in the art that the present disclosure of embodiments has been made by way of examples only and that numerous changes in the arrangement and combination of parts may be resorted without departing from the spirit and scope of the invention as claimed. Accordingly, the scope of the present invention is defined by the appended claims rather than the foregoing description of embodiment.

## Claims

We claim:

1. A mobile device for conducting a secured transaction over a network, the mobile device comprising:
  - a network interface;
  - an interface to receive a secure element;
  - a memory space for storing at least a module and an application downloaded from the network;
  - a processor coupled to the memory space and configured to execute the module to perform operations including:
    - verifying whether the application has been provisioned;
    - when said verifying indicates that the application has not been provisioned, sending to a server via the network interface an identifier identifying the application together with device information of a secure element;
    - establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device;
    - receiving the data from the server to associate the application with the secure element; and
    - sending out an acknowledgement to a provider of the application about a status of the application that is now active with the secure element.
2. The mobile device as recited in claim 1, wherein the data received in the mobile device includes an application key set for the application, and a user interface specifically designed for the mobile device.
3. The mobile device as recited in claim 2, wherein the mobile device is a near field communication (NFC) enabled mobile phone, and the application is an electronic purse (e-purse), the mobile device is used to exchange secured data with another device within a near distance to conduct a transaction.

4. The mobile device as recited in claim 3, wherein the secured data is being exchanged over a secured channel between the mobile device and the another device established by the application key set.
5. The mobile device as recited in claim 4, wherein the transaction is conducted without the mobile communicating with a transaction server.
6. The mobile device as recited in claim 1, wherein said sending to a server via the network interface an identifier identifying the application together with device information of a secure element comprises:
  - determining whether the secure element has been personalized with a Trusted Service Management (TSM) system, wherein the TSM system is a collection of services configured to distribute and manage contactless services for customers signed up with the TSM, and provide data exchanges among different parties to make electronic commerce possible over a wireless network; and
  - performing a personalization process for the secure element when above said determining determines that the secure element has not been personalized with the Trusted Service Management (TSM) system, wherein the secure element when personalized establishes a security platform for the application to run on the mobile device.
7. The mobile device as recited in claim 6, wherein the personalization process comprises:
  - causing the mobile device to initiate data communication with a server in the TSM system;
  - retrieving device information of the secure element in responding to a request from the TSM server after the TSM server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element;

receiving at least a set of keys from the TSM server, wherein the keys are generated in the TSM server in accordance with the device information of the secure element; and  
storing the set of keys in the secure element to facilitate a subsequent transaction with the secure element in the computing device.

8. The mobile device as recited in claim 7, wherein the device information includes an identifier of the secure element, manufacturer information and a batch number.
9. The mobile device as recited in claim 7, wherein the secure element is embedded in the mobile device and integrated with the mobile device via the interface.
10. The mobile device as recited in claim 7, wherein the secure element is a software module installed in a secure memory space only accessible by a distributor of the secure element.
11. The mobile device as recited in claim 10, wherein some components are updated when the secure element is upgraded by the distributor.
12. The mobile device as recited in claim 1, wherein the operations further comprises:
  - receiving a message from a distributor of the application, the message including an identifier identifying the application;
  - verifying that the message is indeed from the distributor;
  - disassociating the application with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and
  - notifying the distributor that the application installed in the mobile device is no longer active.
13. The method as recited in claim 8, wherein part of the data is used to facilitate the server to remotely manage the application.

14. A mobile device for conducting a secured transaction over a network, the mobile device comprising:
- a network interface;
  - a secure element;
  - a memory space for storing various modules downloaded from the network, each of the modules configured to provide an application or a service to a user of the mobile device;
  - a processor coupled to the memory space and configured to execute an embedded module to perform operations including:
    - provisioning each of the modules with a provider that publishes the each of the modules, wherein said provisioning each of the modules with a distributor comprises:
      - sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element;
      - establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the each of the modules to function as designed on the mobile device;
      - receiving the data from the server to associate the each of the modules with the secure element, wherein the data includes a set of keys generated for the each of the modules; and
      - sending out an acknowledgement to the provider of the each of the modules about a status thereof that is now active with the secure element.
15. The mobile device as recited claim 14, wherein the operations further comprise:
- receiving a message from a distributor of one of the modules, the message including an identifier identifying the one of the modules;
  - verifying that the message is authenticated;



disassociating the one of the modules with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and notifying the distributor that the one of the modules installed in the mobile device is no longer active.

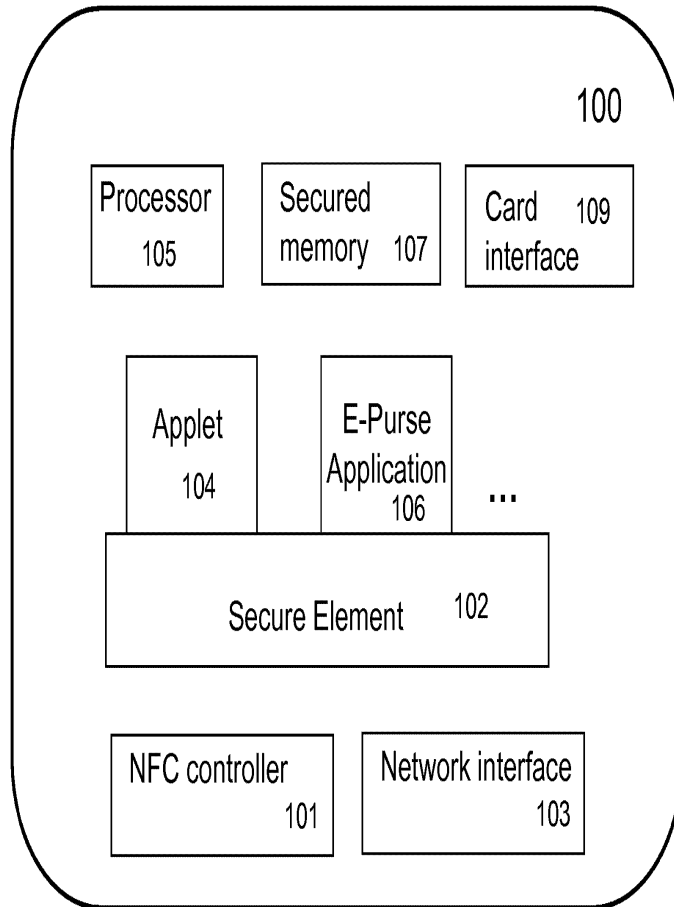
16. The mobile device as recited claim 14, wherein the mobile device includes a display configured to display a user interface showing some of the modules that are still provisioned and active, each of the modules is configured to show another user interface particularly designed for the display of the mobile device when the each of the modules is activated by a user.

17. The mobile device as recited claim 16, wherein the secure element must be personalized before each of the modules is provisioned, each of the provisioned modules is associated with the personalized secure element and a key set generated in accordance with a key set of the secure element.

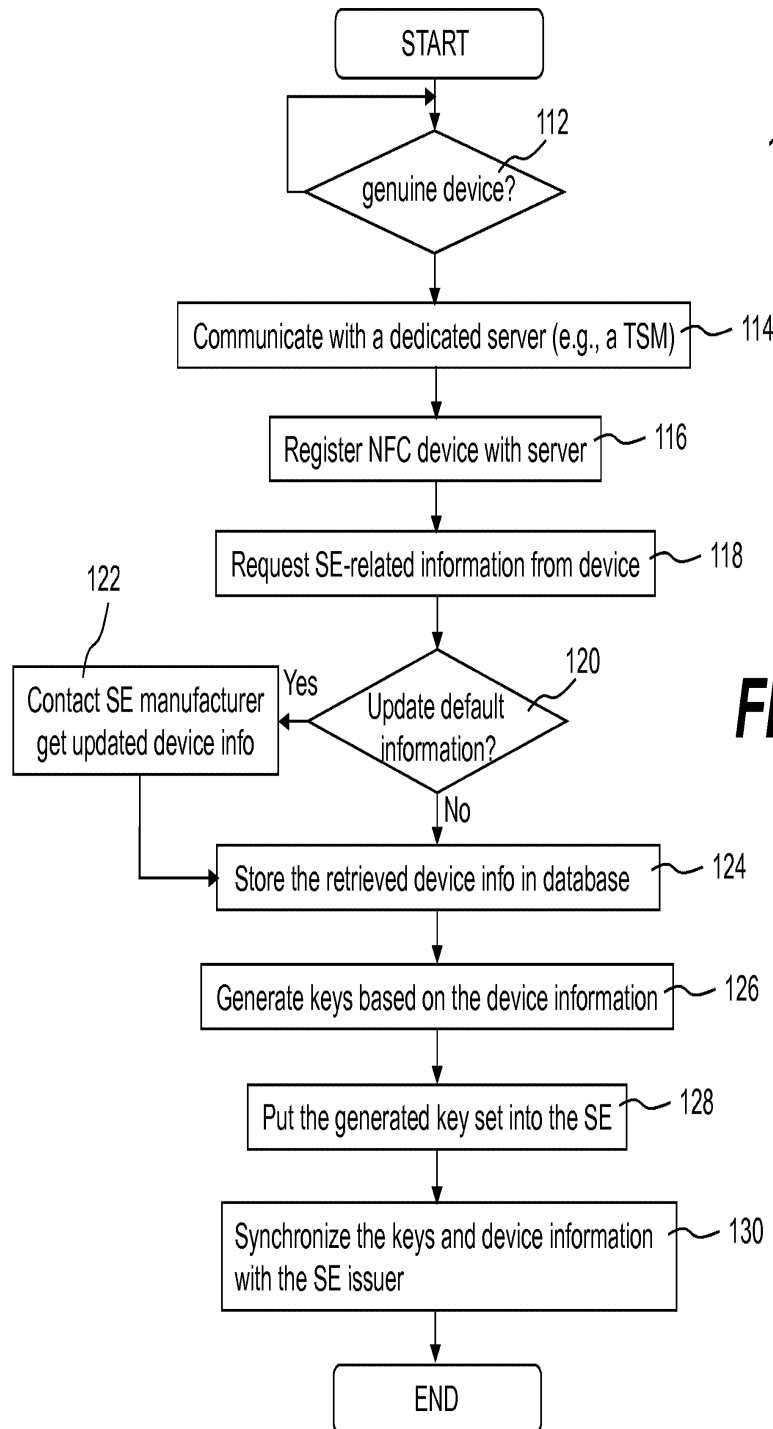
## **Mobile devices for commerce over unsecured networks**

### Abstract

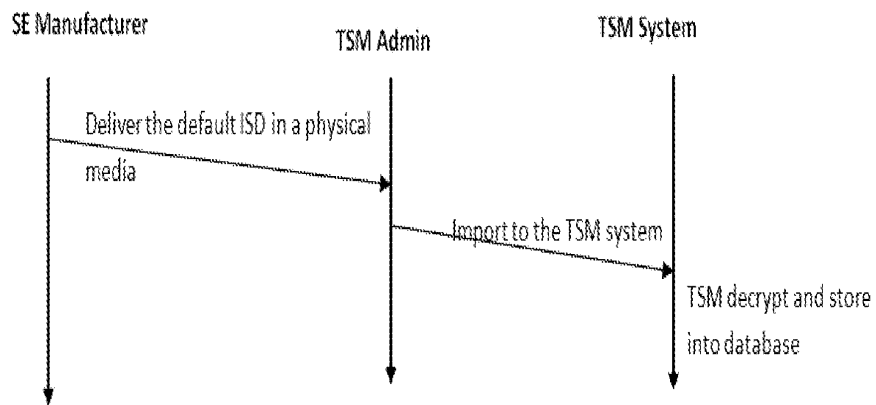
Techniques for managing modules or applications installed in a mobile device are described. To provide authentic and secured transactions with another device, each of the installed applications is provisioned with a server through data communication capability in a mobile device. A provisioned application is associated with the personalized secure element in the mobile device and works with a set of keys that are generated in accordance with a set of keys from the personalized secure element. Further management of controlling an installed application is also described.



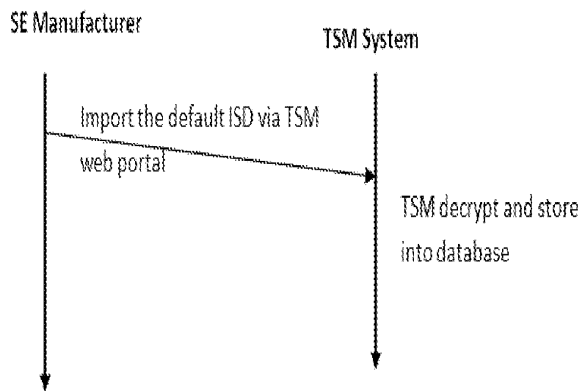
**FIG. 1A**



**FIG. 1B**

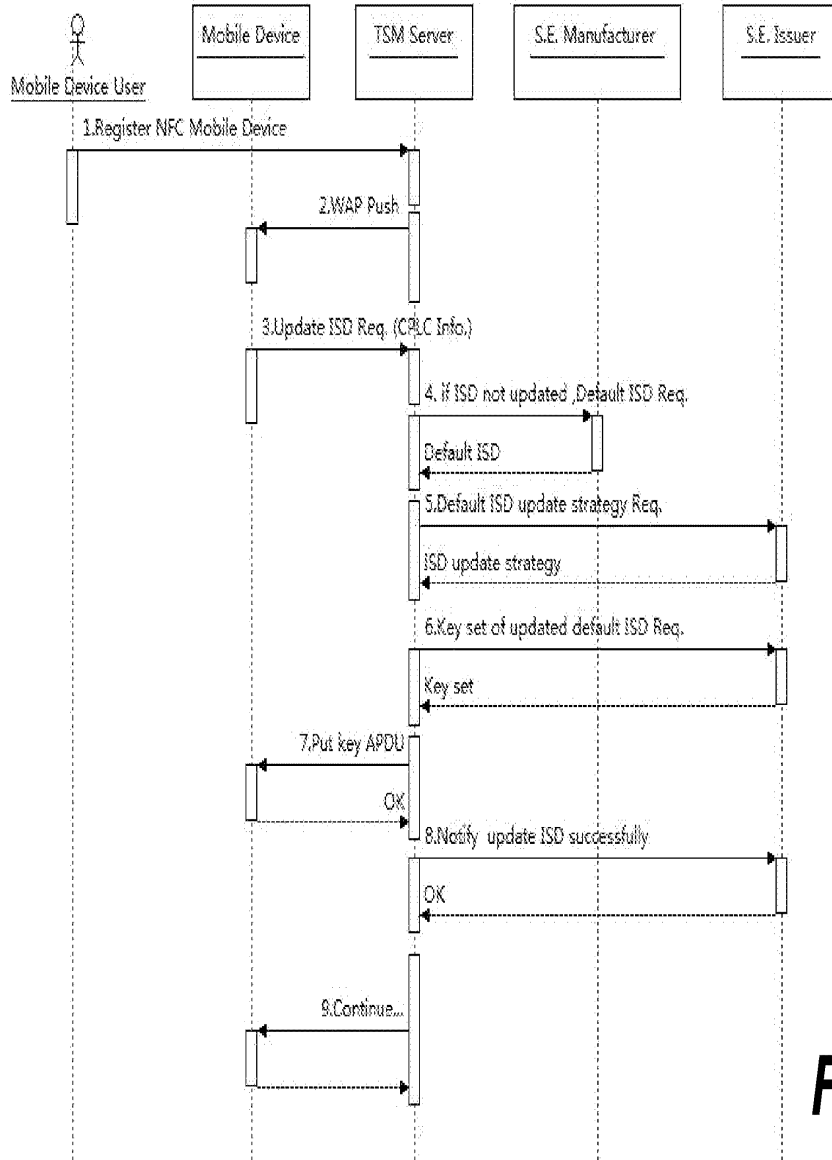


Offline Batch Approach for Default ISD Update



Online Batch Approach for Default ISD Update

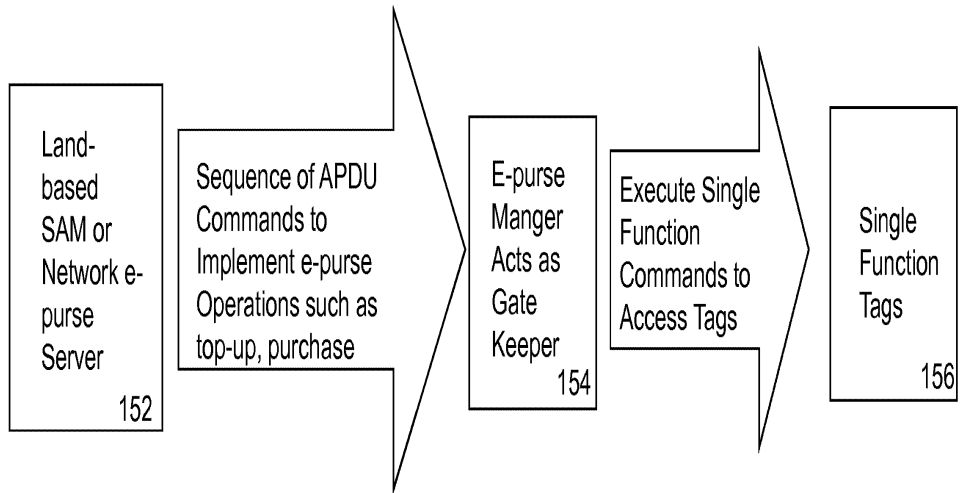
**FIG. 1C**



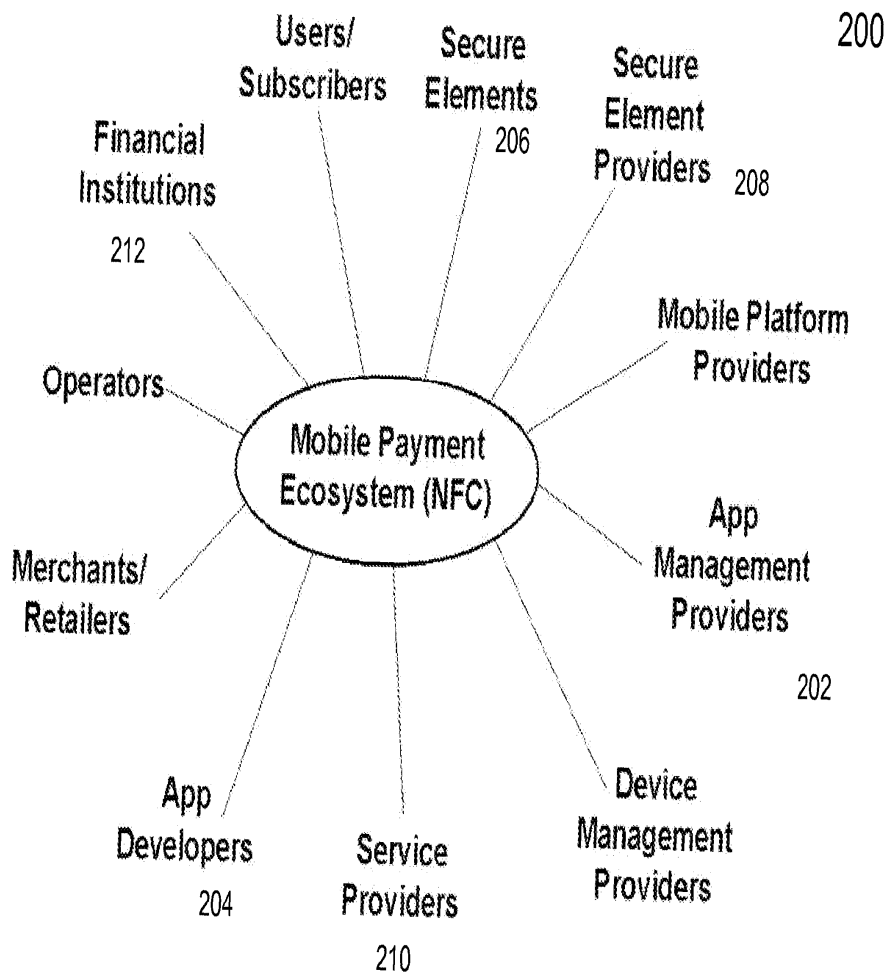
140

**FIG. 1D**

150

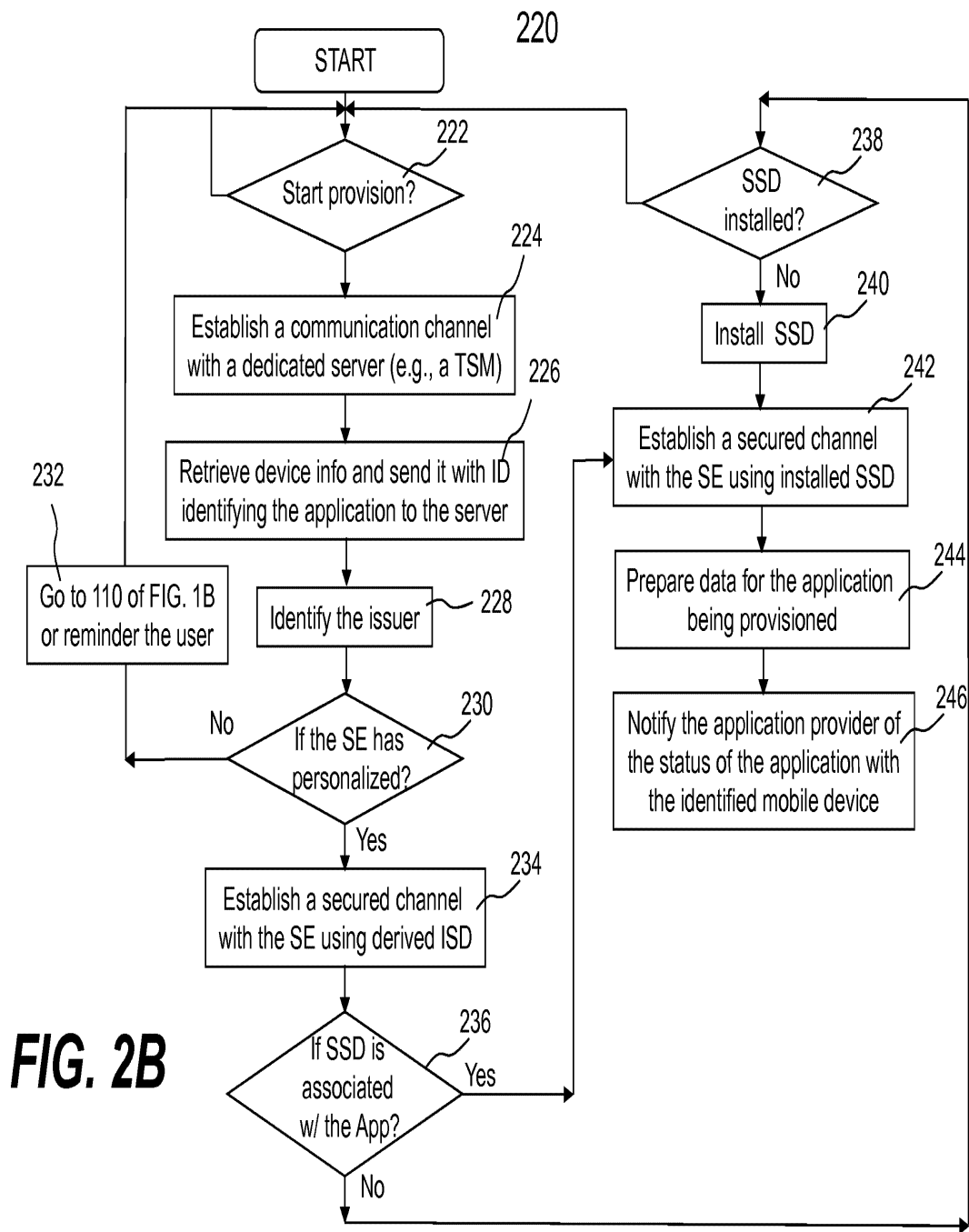


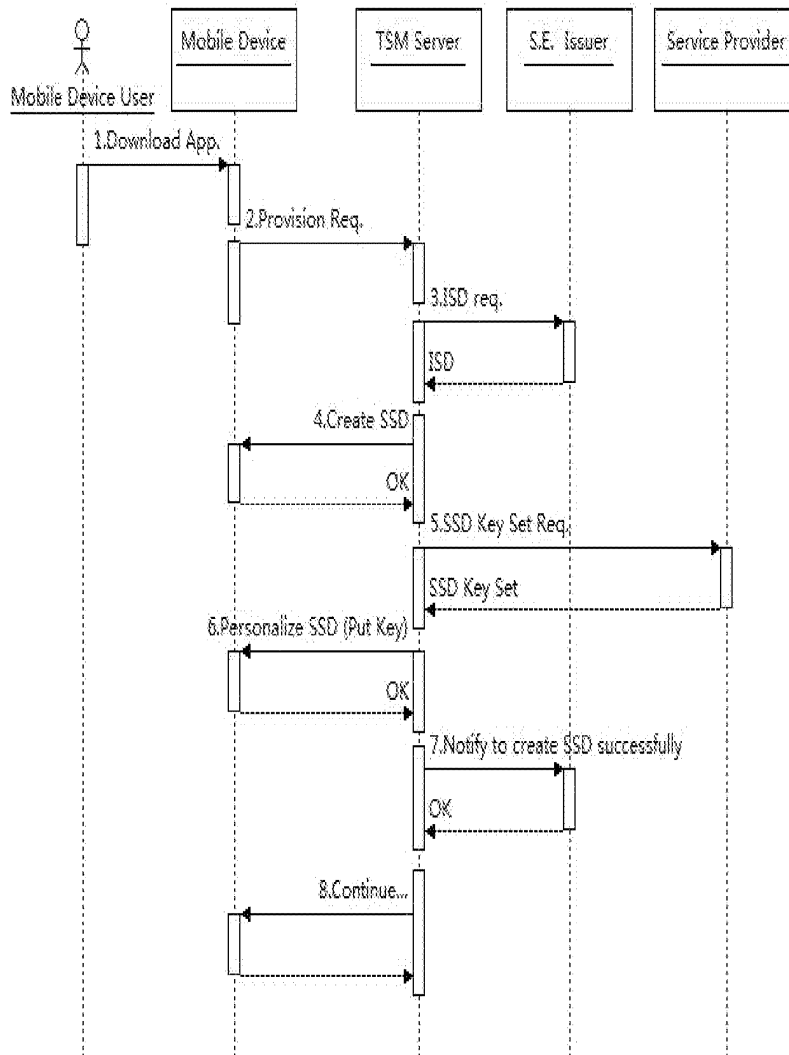
**FIG. 1E**



**FIG. 2A**

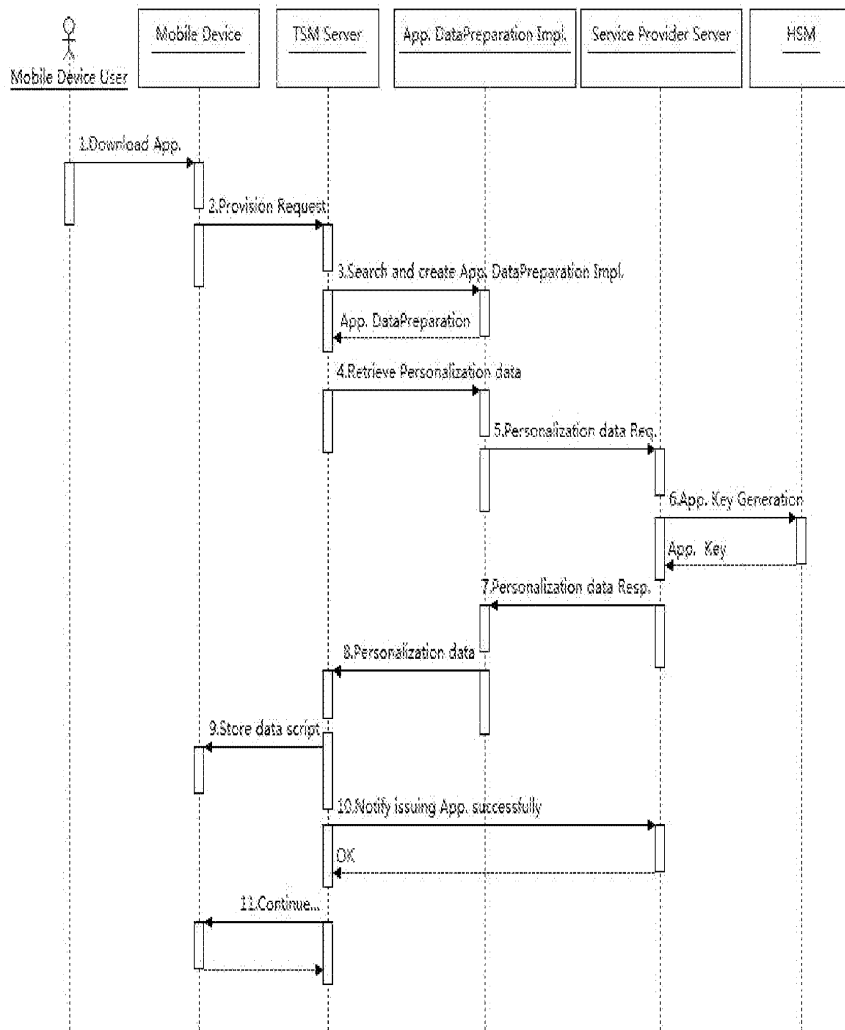






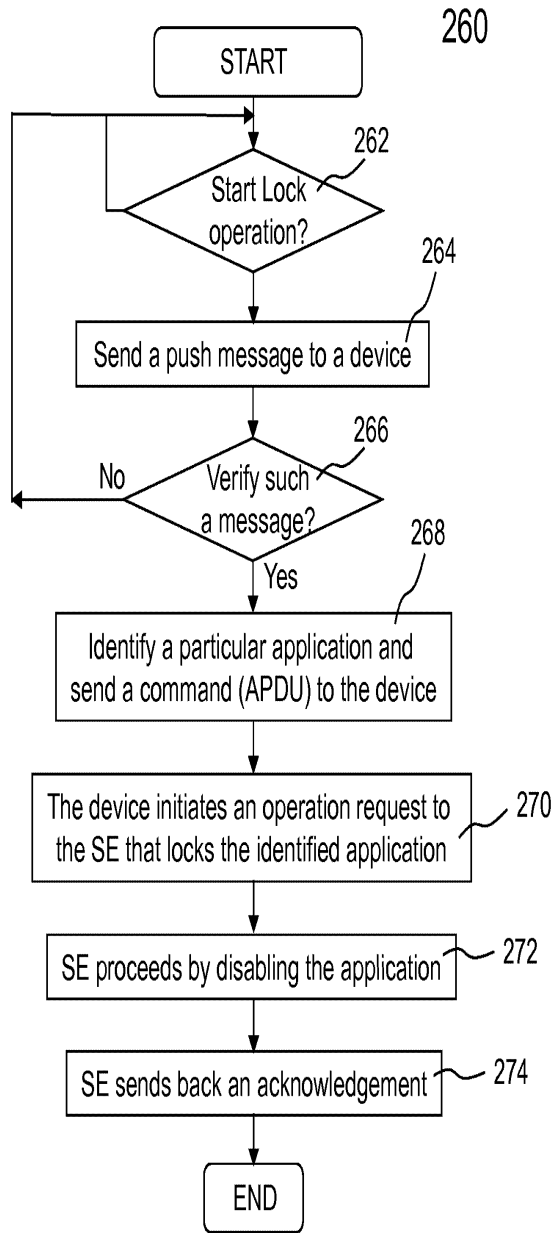
250

**FIG. 2C**

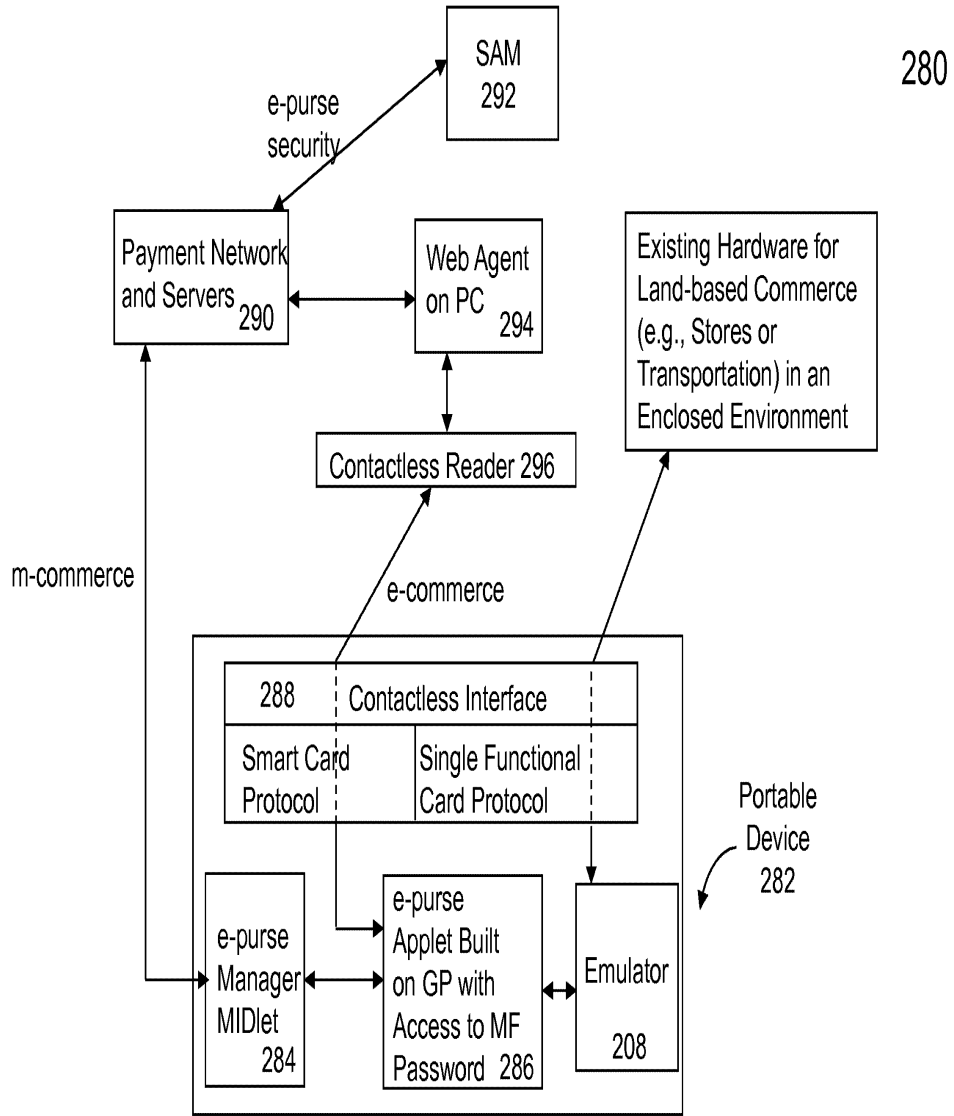


255

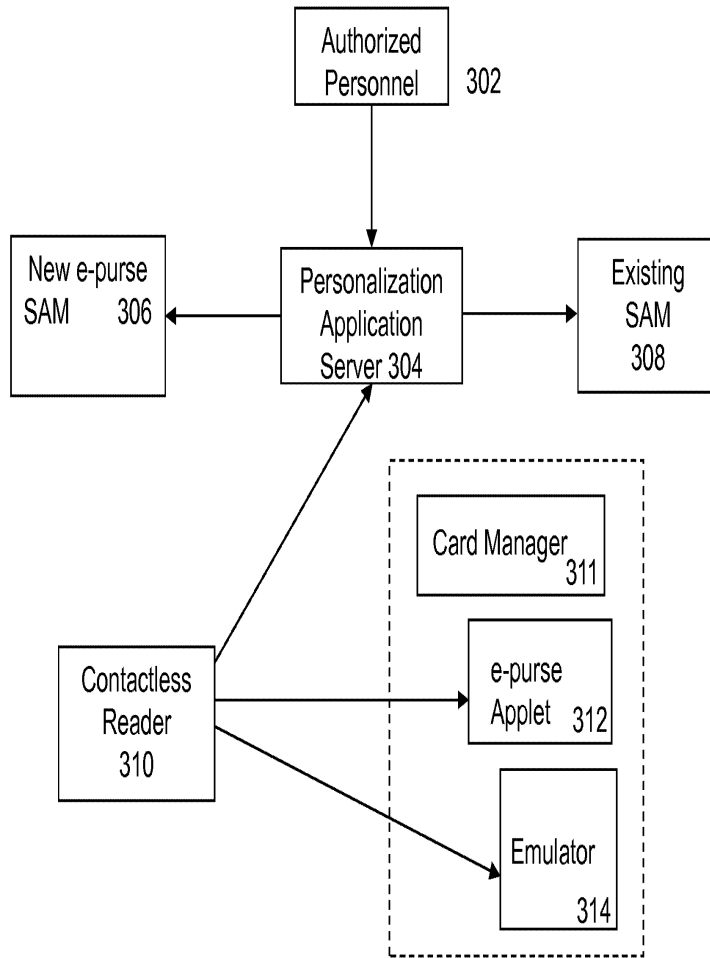
**FIG. 2D**



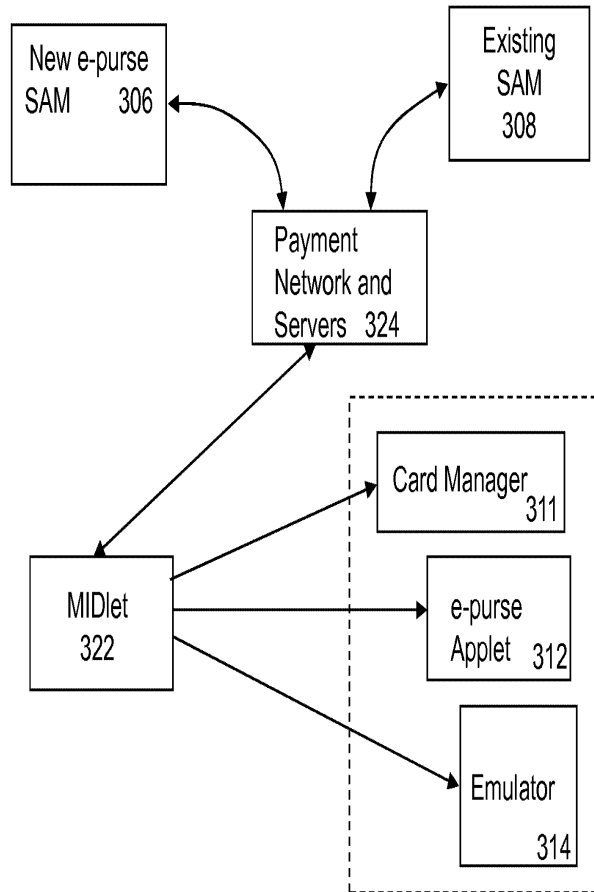
**FIG. 2E**



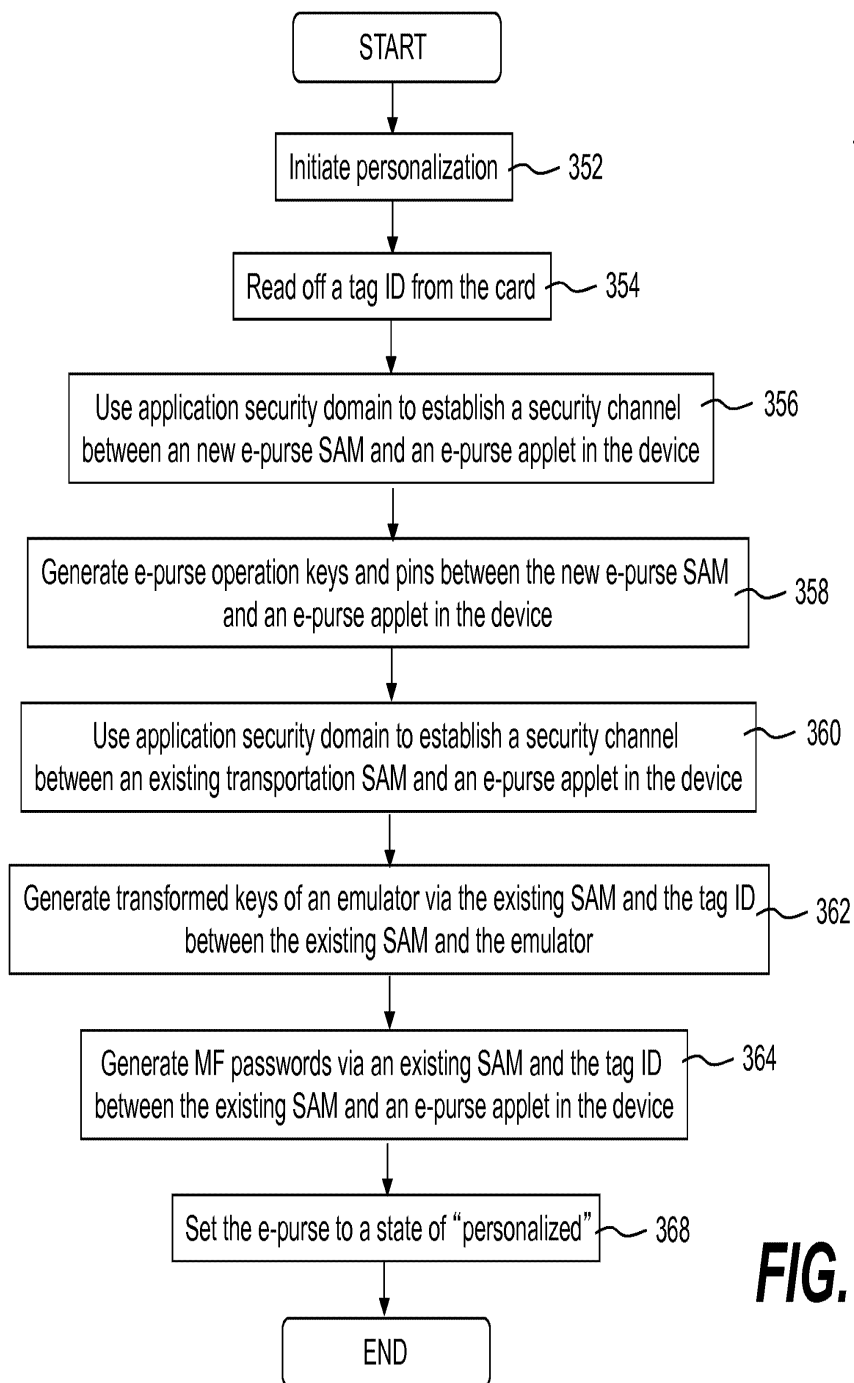
**FIG. 2F**



**FIG. 3A**



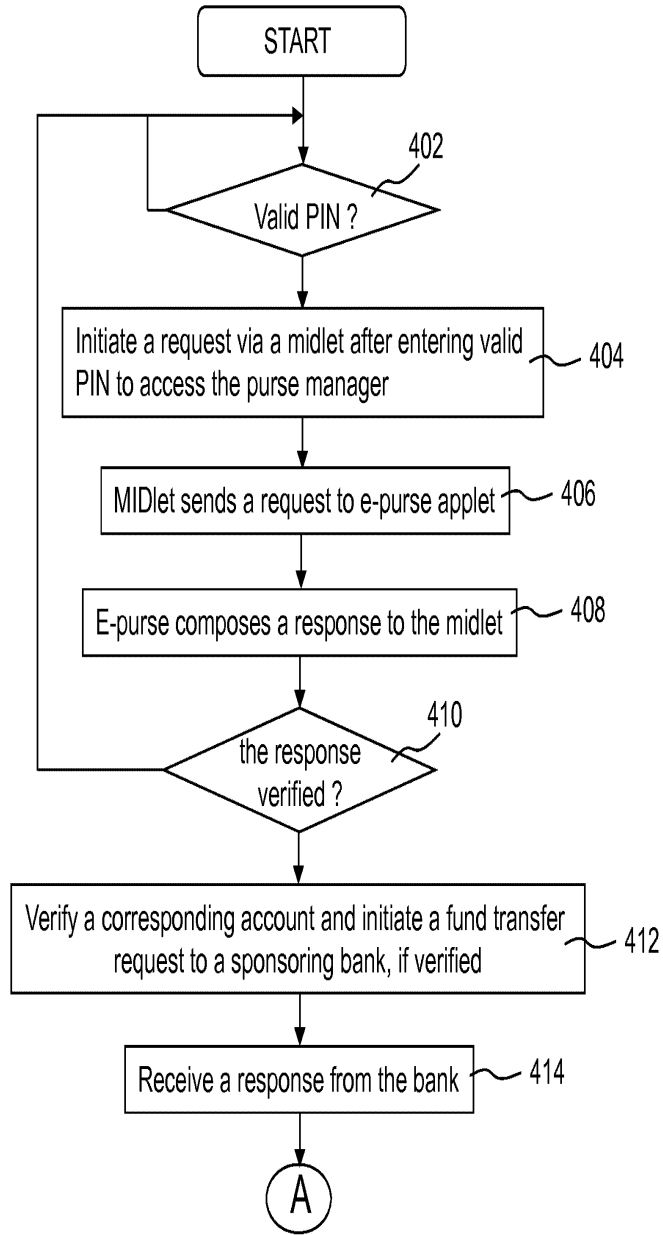
**FIG. 3B**



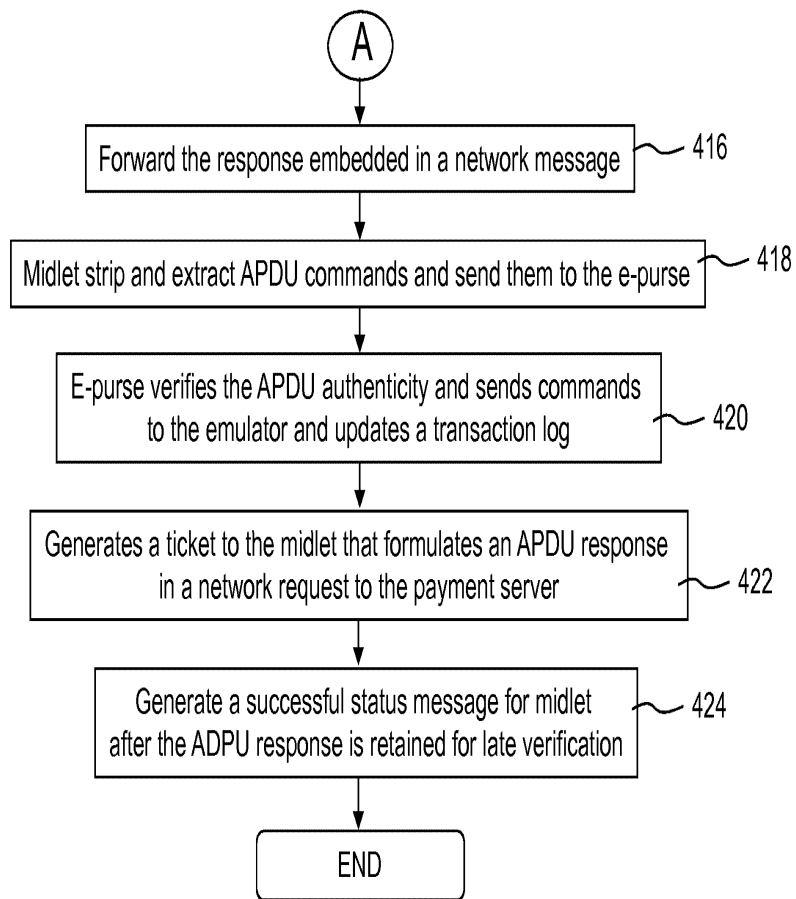
**FIG. 3C**



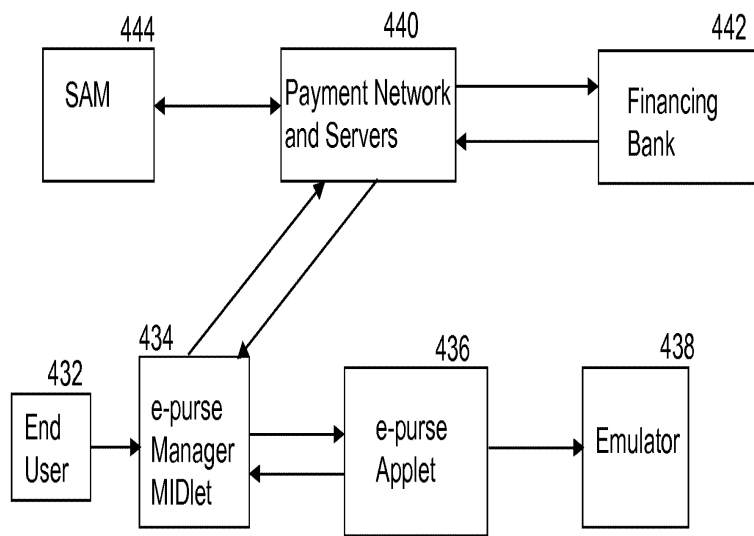
400



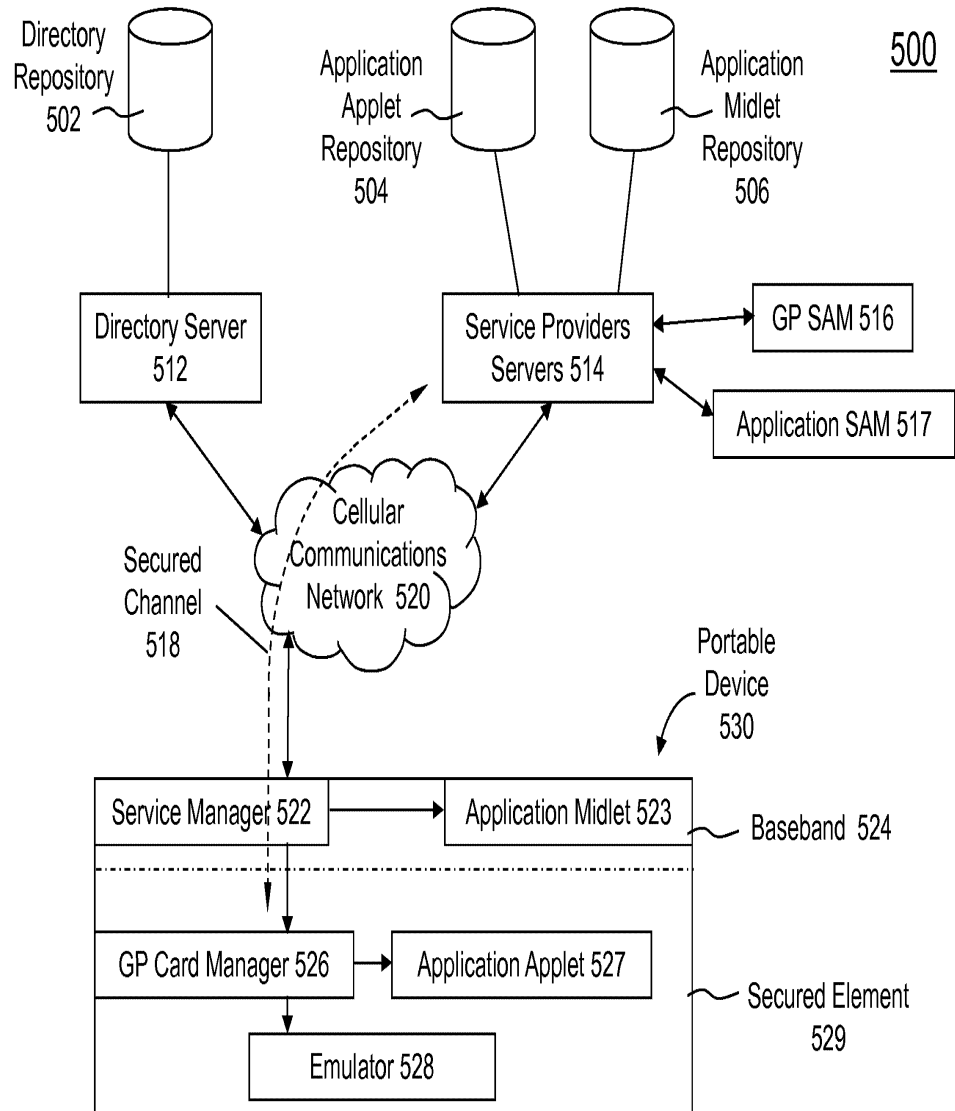
**FIG. 4A**



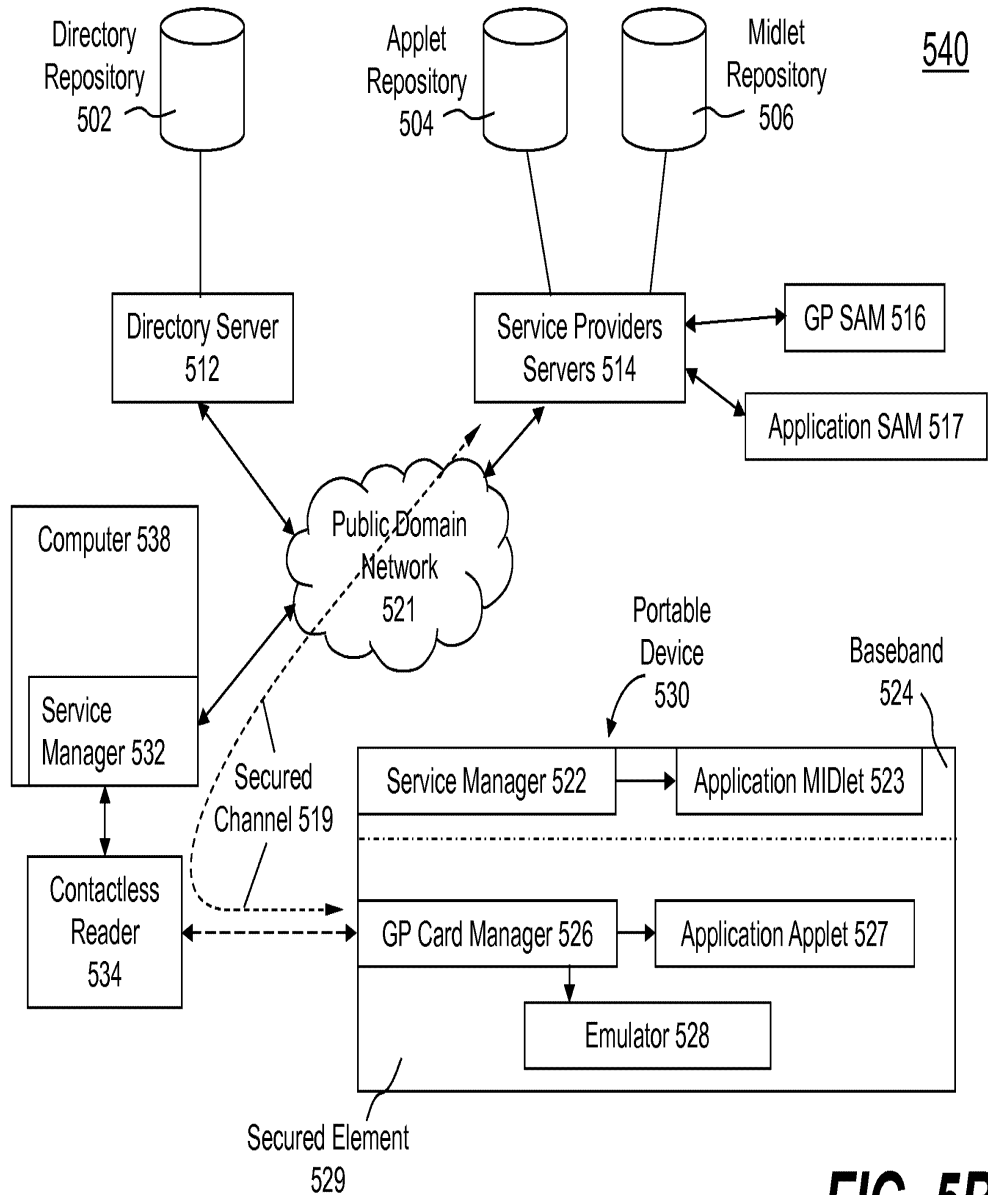
**FIG. 4B**



**FIG. 4C**

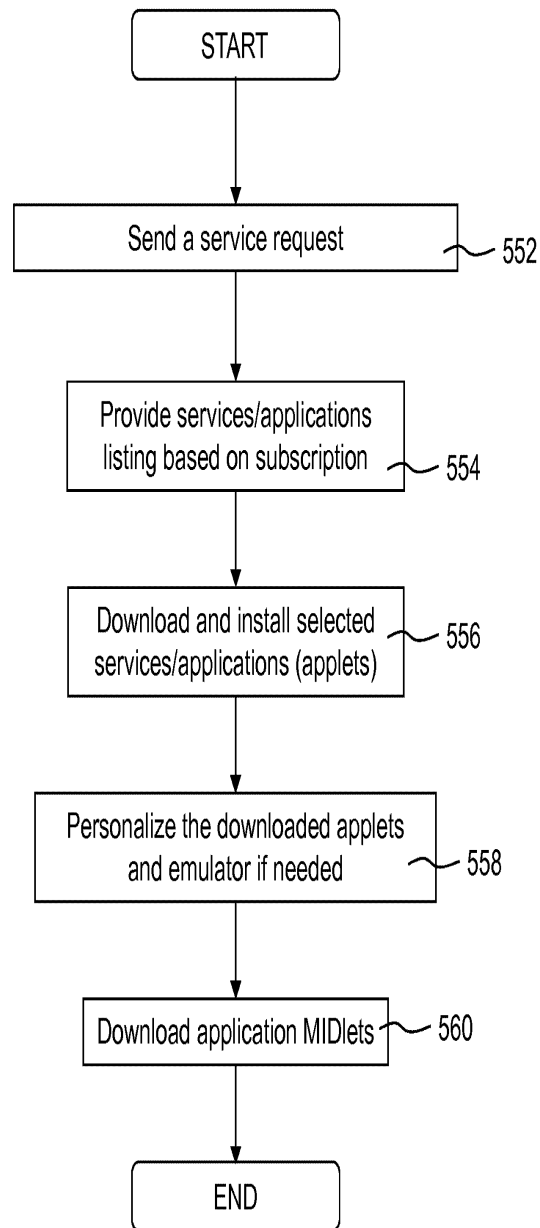


**FIG. 5A**



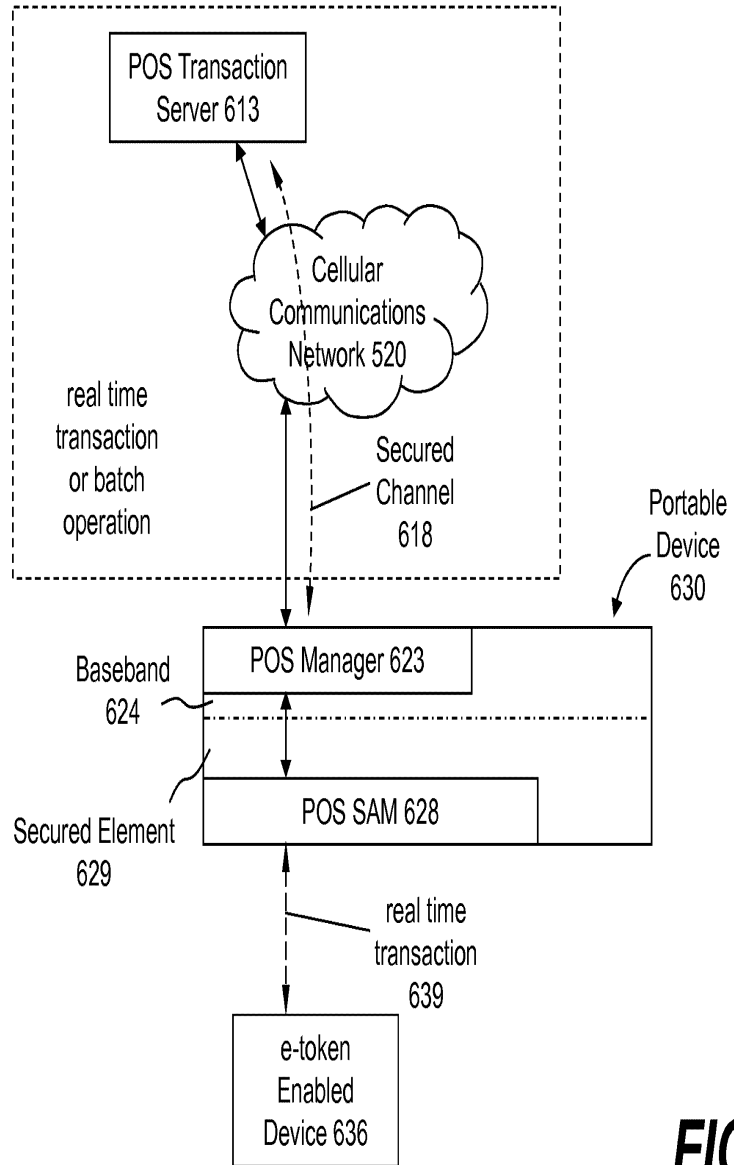
**FIG. 5B**

550

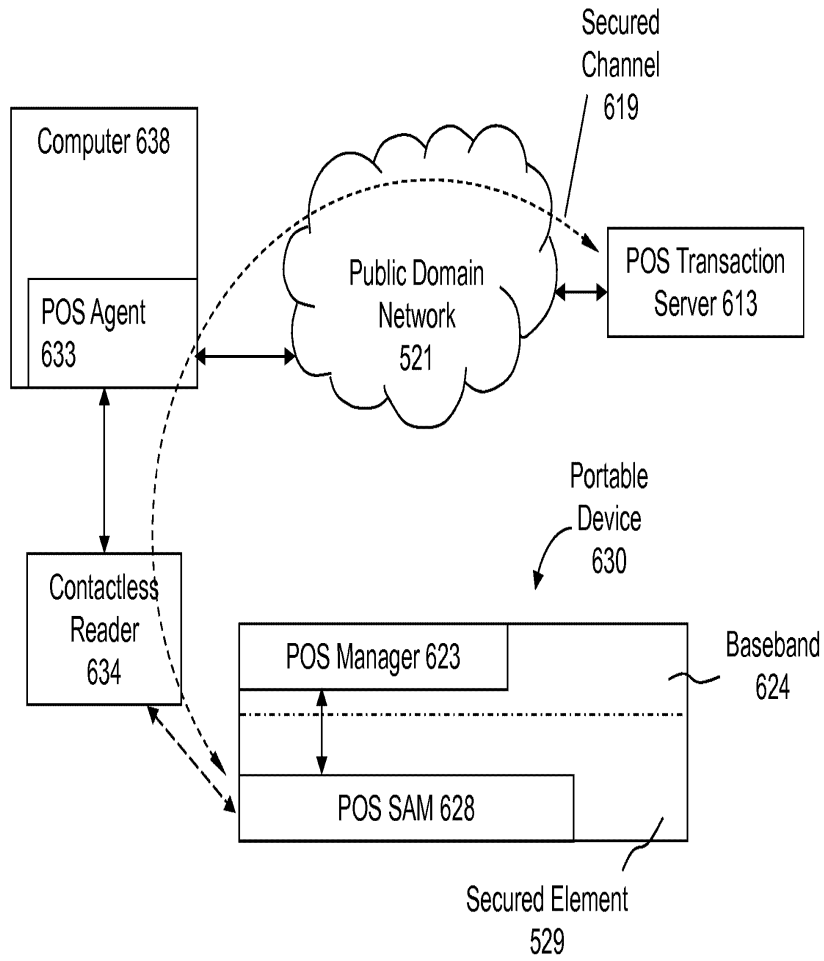


**FIG. 5C**

600



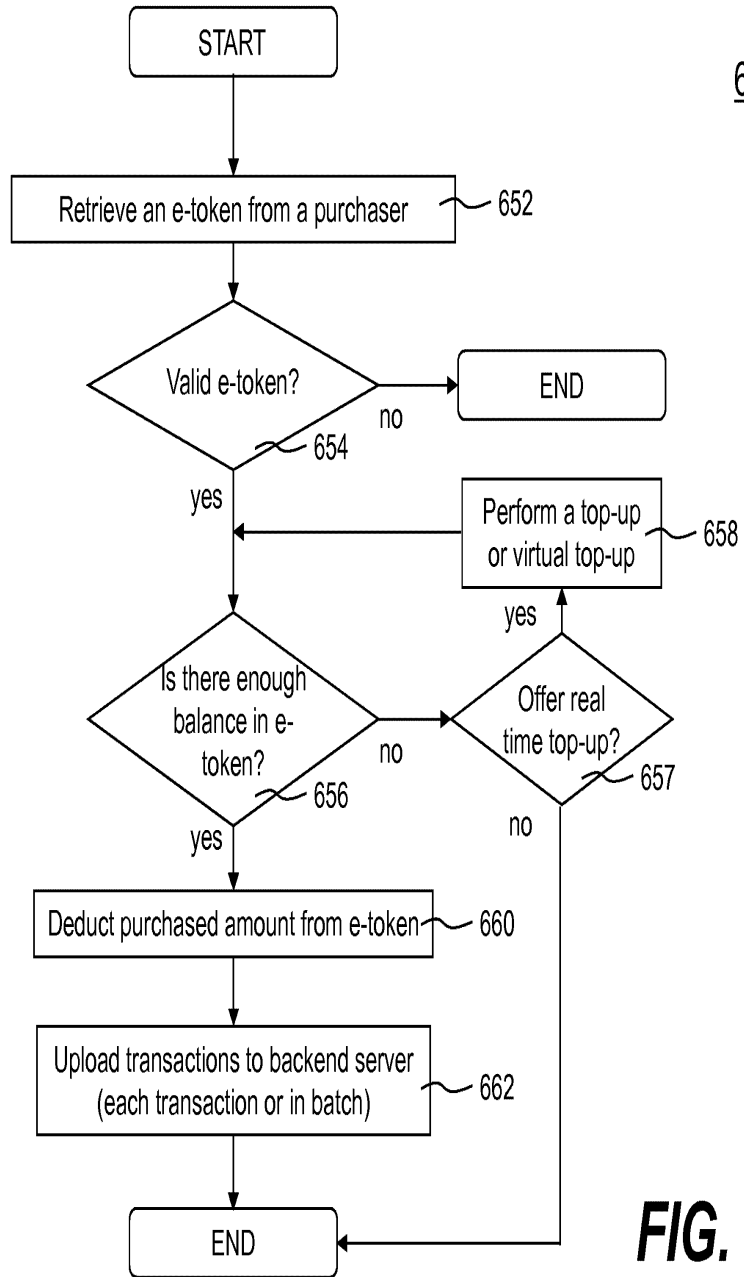
**FIG. 6A**



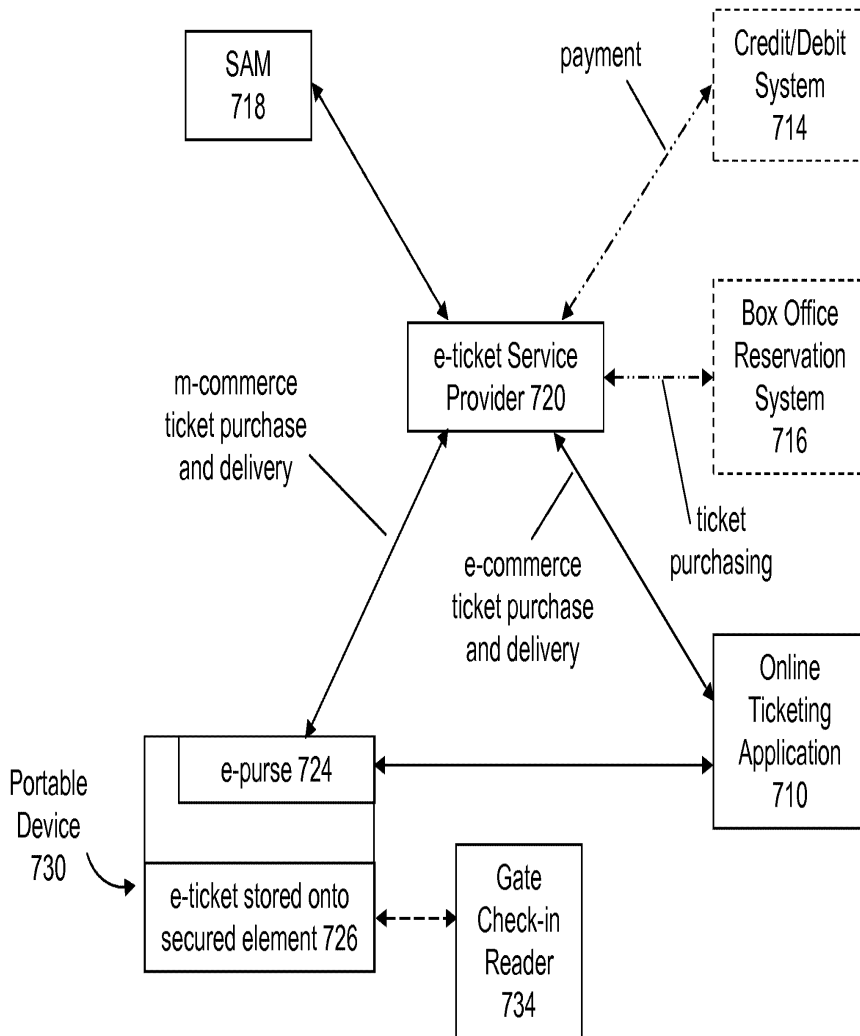
**FIG. 6B**



650



**FIG. 6C**



**FIG. 7**



<u>Prior Foreign Application(s)</u>			<u>Priority Claimed</u>	
_____	_____	_____	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)		
_____	_____	_____	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)		
_____	_____	_____	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)		

I hereby claim the benefit under title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below

_____	_____
(Application Number)	Filing Date
_____	_____
(Application Number)	Filing Date

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

_____	_____	_____
(Application Number)	Filing Date	(Status -- patented, pending, abandoned)
_____	_____	_____
(Application Number)	Filing Date	(Status -- patented, pending, abandoned)

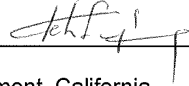
I hereby appoint those associated with:

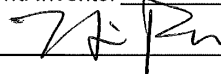
Customer Number:

**26797**

with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Liang Seng Koh  
Inventor's Signature  Date 1/12/2012  
Residence Fremont, California Citizenship United States  
(City, State) (Country)  
Post Office Address 41291 Carmen Street, Fremont, CA 94539, USA

Full Name of Joint/Second Inventor Hsin Pan  
Inventor's Signature  Date 1/12/2012  
Residence Fremont, California Citizenship United States  
(City, State) (Country)  
Post Office Address 2374 Olive Avenue, Fremont, CA 94539, USA

Full Name of Joint/Third Inventor Xiangzhen Xie  
Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_  
Residence Shenzhen, Guangdong, China Citizenship People's Republic of China  
(City, State) (Country)  
Post Office Address C505, Long Tai Xuan, Nanguang Village, Nanshang District,  
Shenzhen, Guangdong Province, 518051, People's Republic of China

I hereby appoint those associated with:

Customer Number:

**26797**

with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Liang Seng Koh

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence Fremont, California Citizenship United States  
(City, State) (Country)

Post Office Address 41291 Carmen Street, Fremont, CA 94539, USA

Full Name of Joint/Second Inventor Hsin Pan

Inventor's Signature \_\_\_\_\_ Date \_\_\_\_\_

Residence Fremont, California Citizenship United States  
(City, State) (Country)

Post Office Address 2374 Olive Avenue, Fremont, CA 94539, USA

Full Name of Joint/Third Inventor Xiangzhen Xie

Inventor's Signature Xiangzhen Xie Date 1/12/2012

Residence Shenzhen, Guangdong, China Citizenship People's Republic of China  
(City, State) (Country)

Post Office Address C505, Long Tai Xuan, Nanguang Village, Nanshang District,  
Shenzhen, Guangdong Province, 518051, People's Republic of China

Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>				
<b>Filing Date:</b>				
<b>Title of Invention:</b>	Mobile devices for commerce over unsecured networks			
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh			
<b>Filer:</b>	Joe Zheng			
<b>Attorney Docket Number:</b>	RFID-081CIPC			
Filed as Small Entity				
<b>Utility under 35 USC 111(a) Filing Fees</b>				
<b>Description</b>	<b>Fee Code</b>	<b>Quantity</b>	<b>Amount</b>	<b>Sub-Total in USD(\$)</b>
<b>Basic Filing:</b>				
Utility filing Fee (Electronic filing)	4011	1	95	95
Utility Search Fee	2111	1	310	310
Utility Examination Fee	2311	1	125	125
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				



Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>530</b>

<b>Electronic Acknowledgement Receipt</b>	
<b>EFS ID:</b>	11840125
<b>Application Number:</b>	13350835
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	1986
<b>Title of Invention:</b>	Mobile devices for commerce over unsecured networks
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh
<b>Customer Number:</b>	26797
<b>Filer:</b>	Joe Zheng
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	RFID-081CIPC
<b>Receipt Date:</b>	16-JAN-2012
<b>Filing Date:</b>	
<b>Time Stamp:</b>	03:20:45
<b>Application Type:</b>	Utility under 35 USC 111(a)

**Payment information:**

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 530
RAM confirmation Number	8349
Deposit Account	
Authorized User	

**File Listing:**

<b>Document Number</b>	<b>Document Description</b>	<b>File Name</b>	<b>File Size(Bytes)/ Message Digest</b>	<b>Multi Part /.zip</b>	<b>Pages (if appl.)</b>
------------------------	-----------------------------	------------------	---	-------------------------	-------------------------

1	Specification	PatentAsFiled.pdf	199465 7ad7f0ecb215d664e13c80333518e6681f2ff27	no	46
<b>Warnings:</b>					
<b>Information:</b>					
2	Drawings-other than black and white line drawings	DrawingsH.pdf	704473 761b5e102cfbd0a65665880cb013eb4177569301	no	24
<b>Warnings:</b>					
<b>Information:</b>					
3	Oath or Declaration filed	SignedDeclaration.pdf	215644 b683ddb360f514edc4f544573082cda6502b4768	no	5
<b>Warnings:</b>					
<b>Information:</b>					
4	Fee Worksheet (SB06)	fee-info.pdf	32768 523cb8913c31c772a3c4f448929bec8087ac6dbf	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>				1152350	
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

## SCORE Placeholder Sheet for IFW Content

Application Number: 13350835

Document Date: 1/16/2012

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface using the Supplemental Content tab.
- Other USPTO employees can bookmark the current SCORE URL (<http://es/ScoreAccessWeb/>).
- External customers may access SCORE content via the Public and Private PAIR interfaces using the Supplemental Content tab.

Form Revision Date: May 1, 2009

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875					Application or Docket Number 13/350,835					
<b>APPLICATION AS FILED - PART I</b>										
(Column 1)		(Column 2)			SMALL ENTITY		OR	OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA			RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)	
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A			N/A	95		N/A		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A			N/A	310		N/A		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A			N/A	125		N/A		
TOTAL CLAIMS (37 CFR 1.16(i))	17	minus 20 =	*		x 30 =	0.00	OR			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2	minus 3 =	*		x 125 =	0.00				
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					0.00				
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))						0.00				
* If the difference in column 1 is less than zero, enter "0" in column 2.					TOTAL	530		TOTAL		
<b>APPLICATION AS AMENDED - PART II</b>										
(Column 1)		(Column 2)		(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY		
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	=	OR	x	=	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	=	OR	x	=	
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	=	OR	x	=	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	=	OR	x	=	
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.</p>										



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 4 columns: APPLICATION NUMBER (13/350,835), FILING OR 371(C) DATE (01/16/2012), FIRST NAMED APPLICANT (Liang Seng Koh), ATTY. DOCKET NO./TITLE (RFID-081CIPC)

26797
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014

CONFIRMATION NO. 1986
FORMALITIES LETTER



Date Mailed: 02/01/2012

NOTICE TO FILE CORRECTED APPLICATION PAPERS

Filing Date Granted

An application number and filing date have been accorded to this application. The application is informal since it does not comply with the regulations for the reason(s) indicated below. Applicant is given TWO MONTHS from the date of this Notice within which to correct the informalities indicated below. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

The required item(s) identified below must be timely submitted to avoid abandonment:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
• Numbers, letters, and reference characters on the drawings must measure at least 0.32 cm (1/8 inch) in height. See Figure(s) 1D and 2D.

The following item(s) appear to have been omitted from the application:

- Figure(s) 6D described in the specification.

Applicant must reply to this notice within the time period set forth in this notice to avoid abandonment of this application. Applicant must select one of the three following options and the reply must comply with the requirements set forth in the selected option and any other requirements set forth in this notice. The reply should also indicate which option applicant has selected.

I. Petition for date of deposit: Should applicant contend that the above-noted omitted item(s) was in fact deposited in the U.S. Patent and Trademark Office (USPTO) with the nonprovisional application papers, a copy of this Notice and a petition (and \$400.00 petition fee (37 CFR 1.17(f))) with evidence of such deposit must be filed within TWO MONTHS of the date of this Notice. The petition fee will be refunded if it is determined that the item(s) was received by the USPTO. THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b).

II. Petition for later filing date: Should applicant desire to supply the omitted item(s) and accept the date that such omitted item(s) was filed in the USPTO as the filing date of the above-identified application, a copy of this Notice, the omitted item(s) (with a supplemental oath or declaration in compliance with 37 CFR 1.63 and 1.64 referring to such items), and a petition under 37 CFR 1.182 (with the \$400.00 petition fee (37 CFR 1.17(f))) requesting the later filing date must be filed within TWO MONTHS of the date of this Notice. THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b).

Applicant is advised that generally the filing fee required for an application is the filing fee in effect on the filing date accorded the application and that payment of the requisite basic filing fee on a date later than the filing date of the application requires payment of a surcharge (37 CFR 1.16(f)). To avoid processing delays and payment

of a surcharge, applicant should submit any balance due for the requisite filing fee based on the later filing date being requested when submitting the omitted item(s) and the petition (and petition fee) requesting the later filing date.

**III. Acceptance of application as deposited:** Applicant may accept the application as deposited in the USPTO by filing an appropriate amendment as set forth in either (A) or (B) below within **TWO MONTHS** of the date of this Notice. **THIS TWO MONTH PERIOD IS EXTENDABLE UNDER 37 CFR 1.136(a) or (b)** . The application will maintain a filing date as of the date of deposit of the application papers in the USPTO, and original application papers (i.e., the original disclosure of the invention) will include only those application papers present in the USPTO on the date of deposit. A petition is not required for this option.

**(A)** If applicant wants to accept the application as deposited without adding the subject matter that was in the omitted item (e.g., a missing page or figure), applicant is required to submit one or more of the following items without adding any new matter (see 35 U.S.C. 132(a)):

1. For a missing page of the specification,
  - a) a substitute specification including claims that amends the specification to renumber the pages consecutively and cancels any incomplete sentences, and
  - b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;
2. For a missing figure of the drawings,
  - a) replacement drawing sheets in compliance with 37 CFR 1.121(d) to renumber the drawing figures consecutively (if necessary),
  - b) a substitute specification excluding claims that amends the specification to cancel any references to any omitted drawing(s) and corrects the references in the specification to the drawing figures to correspond with any relabeled drawing figures, and
  - c) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;
3. For a missing page of the claim listing only, a replacement claim listing with the claims renumbered consecutively or, if amendment to the claims is also necessary, then a complete claim listing in compliance with 37 CFR 1.121(c);
4. For a missing or unreadable compact disc,
  - a) a substitute specification (excluding the claims) deleting the reference to the compact disc and the files contained on the compact disc, and
  - b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125; and
5. For a missing or unreadable file submitted on a compact disc,
  - a) a substitute specification (excluding the claims) deleting the reference to the missing or unreadable file, and a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125; and
  - b) a replacement transmittal letter listing all of the files except the missing or unreadable file in compliance with 37 CFR 1.52(e)(3)(ii).

**(B)** Alternatively, if applicant wants to accept the application as deposited but wishes to add the subject matter in the omitted item (e.g., a missing page or figure) by relying on an incorporation by reference under 37 CFR 1.57 or other portions of the original disclosure, applicant is required to submit one or more of the following items without adding any new matter (see 35 U.S.C. 132(a)):

1. To add the subject matter in a missing page of specification,
  - a) a substitute specification excluding claims and
  - b) a statement that the substitute specification includes no new matter, in compliance with 37 CFR 1.121(b)(3) and 1.125;
2. To add a missing figure of the drawings, new and replacement drawing sheets in compliance with 37 CFR 1.121(d);

3. To add the subject matter in a missing page of the claim listing, a complete claim listing in compliance with 37 CFR 1.121(c) (e.g., a claim in the missing page should be submitted as a new claim);
4. To add the subject matter in a missing or unreadable compact disc,
  - a) a replacement compact disc and a duplicate copy of the compact disc, in compliance with 37 CFR 1.52(e); and
  - b) a statement that the replacement compact disc contains no new matter in compliance with 37 CFR 1.52(e)(4); and,
5. To add the subject matter in a missing or unreadable file submitted on a compact disc,
  - a) a replacement compact disc that contains all of the files listed in the specification including the missing or unreadable file and a duplicate copy of the compact disc, in compliance with 37 CFR 1.52(e); and
  - b) a statement that the replacement compact disc contains no new matter in compliance with 37 CFR 1.52(e)(4).

If applicant is relying on an incorporation by reference under 37 CFR 1.57 to add the omitted subject matter, then applicant must also comply with the requirements of 37 CFR 1.57.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

Replies should be mailed to:

Mail Stop Missing Parts  
Commissioner for Patents  
P.O. Box 1450  
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.  
<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/rerry/

---

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101





UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 6 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/350,835, 01/16/2012, 2617, 530, RFID-081CIPC, 17, 2

CONFIRMATION NO. 1986

FILING RECEIPT

26797
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014



Date Mailed: 02/01/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

Liang Seng Koh, Fremont, CA;
Hsin Pan, Fremont, CA;
Xiangzhen Xie, Shenzhen, CHINA;

Assignment For Published Patent Application

RFCyber Corp.

Power of Attorney: The patent practitioners associated with Customer Number 26797

Domestic Priority data as claimed by applicant

This application is a CIP of 11/534,653 09/24/2006
and is a CIP of 11/739,044 04/23/2007
which is a CIP of 11/534,653 09/24/2006

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 01/27/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is US 13/350,835

Projected Publication Date: To Be Determined - pending completion of Corrected Papers

Non-Publication Request: No

Early Publication Request: No

\*\* SMALL ENTITY \*\*

**Title**

Mobile devices for commerce over unsecured networks

**Preliminary Class**

455

**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER****Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

page 2 of 3

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

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

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**Applicant(s):** Liang Seng Koh et al  
**Title:** Mobile devices for commerce over unsecured networks  
**Serial No.:** 13/350,835  
**Filing Date:** 01/16/2012  
**Examiner:** Unknown  
**Group Art Unit:** Unknown  
**Docket No.:** RFID-081CIPB

---

February 2, 2000

Mail Stop: Petition Office  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Response to**  
**NOTICE TO FILE CORRECTED APPLICATION PAPERS**  
***Filing Date Granted***

Dear Sir:

In response to NOTICE TO FILE CORRECTED APPLICATION PAPERS– Filing Date Granted, (hereinafter “NOTICE”), mailed by the United States Patent and Trademark Office on February 1, 2012, FIG. 6D is enclosed to complete the filing of the above-identified patent application.

The Applicant hereby states no new matter is introduced with the inclusion of FIG. 6D. The full description of FIG. 6D is given in paragraphs [00138]-[00139]. Further, FIG. 6D is a replication of FIG. 6D of co-pending US App. Serial No.: 11/739,044 a priority of which is being claimed.

It is hereby respectfully submitted that the enclosed document completes the filing of the above patent application and justifies the US filing date of 01/16/2012.

Please telephone the undersigned at (408)777-8873, if there are any questions.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", on February 2, 2012.

Name: Joe Zheng

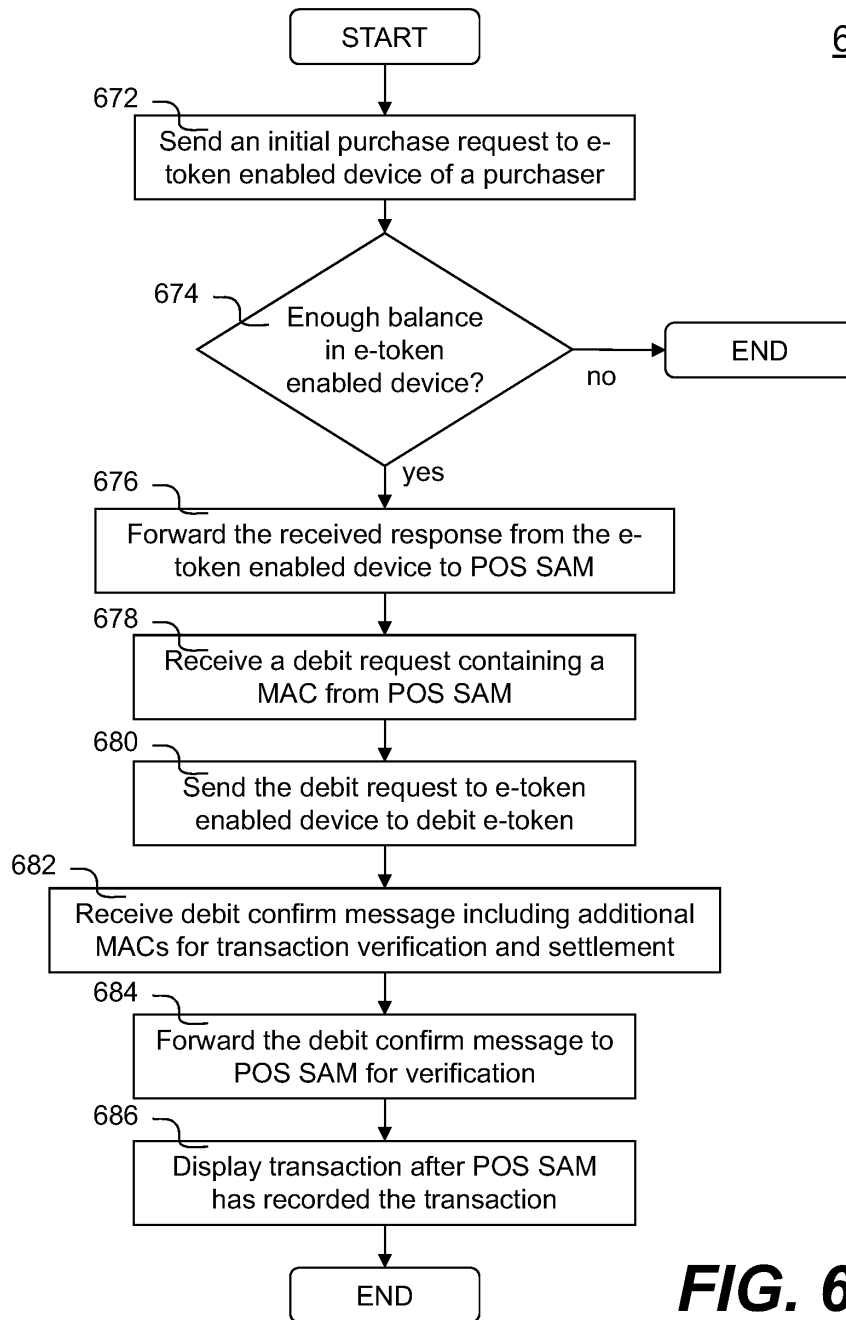
Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng  
Reg.: No. 39,450

670



**FIG. 6D**

<b>Electronic Acknowledgement Receipt</b>	
<b>EFS ID:</b>	11989928
<b>Application Number:</b>	13350835
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	1986
<b>Title of Invention:</b>	Mobile devices for commerce over unsecured networks
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh
<b>Customer Number:</b>	26797
<b>Filer:</b>	Joe Zheng
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	RFID-081CIPC
<b>Receipt Date:</b>	02-FEB-2012
<b>Filing Date:</b>	16-JAN-2012
<b>Time Stamp:</b>	19:30:44
<b>Application Type:</b>	Utility under 35 USC 111(a)

**Payment information:**

Submitted with Payment	no
------------------------	----

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Response to Pre-Exam Sequence Notice	ResponseToMissingParts.pdf	79444 <small>48571ca0c19e41575528fcaefc1547fb4ba b975</small>	no	2

**Warnings:**

**Information:**

2	Drawings-only black and white line drawings	FIG6D.pdf	21641 baa1814aef1e5bdefeadc91e953c57d939a73ec4	no	1
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>				101085	
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p>					



<b>PATENT APPLICATION FEE DETERMINATION RECORD</b>					Application or Docket Number 13/350,835					
Substitute for Form PTO-875										
<b>APPLICATION AS FILED - PART I</b>										
(Column 1)		(Column 2)			SMALL ENTITY		OR	OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA			RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)	
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A			N/A	95		N/A		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A			N/A	310		N/A		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A			N/A	125		N/A		
TOTAL CLAIMS (37 CFR 1.16(i))	17	minus 20 =	*		x 30 =	0.00	OR			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2	minus 3 =	*		x 125 =	0.00				
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					0.00				
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))						0.00				
* If the difference in column 1 is less than zero, enter "0" in column 2.					TOTAL	530		TOTAL		
<b>APPLICATION AS AMENDED - PART II</b>										
(Column 1)		(Column 2)		(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY		
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	**	=	x =		OR	x =		
	Independent (37 CFR 1.16(h))	*	**	=	x =		OR	x =		
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)	
	Total (37 CFR 1.16(i))	*	**	=	x =		OR	x =		
	Independent (37 CFR 1.16(h))	*	**	=	x =		OR	x =		
	Application Size Fee (37 CFR 1.16(s))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.</p>										



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 6 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Row 1: 13/350,835, 01/16/2012, 2617, 530, RFID-081CIPB, 17, 2

26797
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014

CONFIRMATION NO. 1986
UPDATED FILING RECEIPT



Date Mailed: 02/13/2012

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

Liang Seng Koh, Fremont, CA;
Hsin Pan, Fremont, CA;
Xiangzhen Xie, Shenzhen, CHINA;

Assignment For Published Patent Application

RFCyber Corp.

Power of Attorney: The patent practitioners associated with Customer Number 26797

Domestic Priority data as claimed by applicant

This application is a CIP of 11/534,653 09/24/2006 PAT 8118218
and is a CIP of 11/739,044 04/23/2007
which is a CIP of 11/534,653 09/24/2006 PAT 8118218

Foreign Applications (You may be eligible to benefit from the Patent Prosecution Highway program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 01/27/2012

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is US 13/350,835

Projected Publication Date: 05/24/2012

Non-Publication Request: No

Early Publication Request: No

\*\* SMALL ENTITY \*\*

**Title**

Mobile devices for commerce over unsecured networks

**Preliminary Class**

455

**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

**LICENSE FOR FOREIGN FILING UNDER****Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

page 2 of 3

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

**NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

---

***SelectUSA***

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 4 columns: APPLICATION NUMBER (13/350,835), FILING OR 371(C) DATE (01/16/2012), FIRST NAMED APPLICANT (Liang Seng Koh), ATTY. DOCKET NO./TITLE (RFID-081CIPB)

26797
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014

CONFIRMATION NO. 1986
PUBLICATION NOTICE



Title: Mobile devices for commerce over unsecured networks

Publication No. US-2012-0130839-A1

Publication Date: 05/24/2012

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Row 1: 13/350,835, 01/16/2012, INV001Liang Seng Koh, RFID-081CIPB, 1986
Row 2: 26797, 7590, 03/21/2013, (Empty), (Empty)
Row 3: SILICON VALLEY PATENT AGENCY, 7394 WILDFLOWER WAY, CUPERTINO, CA 95014, EXAMINER STANFORD, CHRISTOPHER J, (Empty)
Row 4: (Empty), (Empty), (Empty), ART UNIT 2887, PAPER NUMBER (Empty)
Row 5: (Empty), (Empty), (Empty), NOTIFICATION DATE 03/21/2013, DELIVERY MODE ELECTRONIC

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

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

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

uspatents@sbcglobal.net

<b>Office Action Summary</b>	<b>Application No.</b> 13/350,835	<b>Applicant(s)</b> KOH ET AL.	
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887	

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

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 16 January 2012.
- 2a)  This action is **FINAL**.                      2b)  This action is non-final.
- 3)  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 4)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 5)  Claim(s) 1-17 is/are pending in the application.  
5a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 6)  Claim(s) \_\_\_\_\_ is/are allowed.
- 7)  Claim(s) 1-17 is/are rejected.
- 8)  Claim(s) \_\_\_\_\_ is/are objected to.
- 9)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

\* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).

**Application Papers**

- 10)  The specification is objected to by the Examiner.
- 11)  The drawing(s) filed on 16 January 2012 is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

**Priority under 35 U.S.C. § 119**

- 12)  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a)  All    b)  Some \*    c)  None of:  
1.  Certified copies of the priority documents have been received.  
2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3.  Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 3)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4)  Other: \_\_\_\_\_.

**DETAILED ACTION**

***Priority***

1. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 120 as follows:

The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of 35 U.S.C. 112(a) or the first paragraph of 35 U.S.C. 112 (pre-AIA). See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).

The disclosures of the prior-filed applications, Application No.11/534,653 and 11/739,044, fail to provide adequate support or enablement in the manner provided by 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph for one or more claims of this application. The language used in the at least claims 1 and 14 are not supported by the disclosures of Applications '653 and '044. Specifically the recitations regarding how the processor coupled to the mobile device's memory space is configured. Claims 1 and 14 recited the following limitations that are not wholly supported by the patent applications:



- verifying whether the application has been provisioned; when said verifying indicates that the application has not been provisioned, sending to a server via the network interface an identifier identifying the application together with device information of a secure element; and sending out an acknowledgement to a provider of the application about a status of the application that is now active with the secure element (claim 1)
- provisioning each of the modules with a provider that publishes the each of the modules, wherein said provisioning each of the modules with a distributor comprises: sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element; and sending out an acknowledgement to the provider of the each of the modules about a status thereof that is now active with the secure element (claim 14).

The instant application will be not receive the priority filing dates of the prior-filed parent applications. For prior art purposes, the effective filing date of the instant application will coincide with the actual filing date of 1/16/2012.

#### ***Claim Objections***

2. Claim 6 is objected to because of the following informalities: there appears to be a typographical omission in “without the mobile communicating”. It is believed that the claim language should recite “without the mobile device communicating”. Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

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

A person shall be entitled to a patent unless –

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

4. **Claims 1-9, 13-14, and 16-17** are rejected under 35 U.S.C. 102(b) as being anticipated by Musfeldt et al. (US PG Pub. 2010/0291904; hereinafter Musfeldt).

**Regarding claim 1**, Musfeldt teaches a mobile device (mobile device 150a, Fig. 1) for conducting a secured transaction (para [0017]) over a network (carrier network 180a/b & network 170, Fig. 1), the mobile device comprising: a network interface (network interface 159a, Fig. 1); an interface (interfaces for secure element embodiments such as SIM cards; para [0025]) to receive a secure element (secure element 155a, Fig. 1); a memory space (memory 152a, Fig. 1) for storing at least a module (provisioning module 154a, Fig. 1) and an application downloaded from the network (“memory and data storage device, can store data and information for subsequent retrieval; para [0031]); a processor (processor 156a, Fig. 1) coupled to the memory space and configured to execute the module to perform operations (“TSM provisioning module 154a, 154b may comprise computer-executable program instructions or software, including a dedicated program, for facilitating mobile device application provisioning on secure elements 155a, 155b as carried out by the TSM computer 110”; para [0025, 0053-0066]) including: verifying whether the application has

been provisioned (“a provisioning request can come from any of the mobile devices 150 or associated end users”; para [0054]); when said verifying indicates that the application has not been provisioned (“a provisioning request can come from any of the mobile devices 150 or associated end users”; para [0054]), sending to a server via the network interface an identifier identifying the application (“it can be determined whether the mobile device is technically capable of receiving an OTA provisioned application or capable of operating the specific application requested”; para [0056]) together with device information of a secure element (“the identity of the mobile device end user can be verified as the correct end user for receiving the mobile device application and/or associated personalization data, and/or that the mobile device is in the correct end user's possession”; para [0057]); establishing a secured channel between the secure element and the server using a key set installed on the secure element (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]), wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device (“the requested application can be installed on the secure element of the mobile device 150 para [0062]); receiving the data from the server to associate the application with the secure element (“a service provider computer 160 regarding a specific end user (e.g., as identified by name, account, or other unique identifier), the TSM computer 110 is operable to identify the end user as

having a TSM-provisioned application installed”; para [0062-0065]); and sending out an acknowledgement to a provider of the application about a status of the application that is now active with the secure element (“the TSM computer 110 can be operable to record application installation status, including successes and failures, as may be provided by the lifecycle management module 127”; para [0064]).

**Regarding claim 2**, Musfeldt teaches the data received in the mobile device includes an application key set for the application (“facilitate management of secured keys used to securely load and delete mobile device applications on mobile device secure elements”; para [0044]), and a user interface specifically designed for the mobile device (“provide a mobile device user interface for accessing provisioned mobile device applications on each mobile device (e.g., a mobile wallet)”; para [0044]).

**Regarding claim 3**, Musfeldt teaches the mobile device is a near field communication (NFC) enabled mobile phone (“multiple service providers (e.g., card issuing banks, retailers, transit operators, etc.) need to load and manage applications (e.g., NFC-based applications, etc.) onto mobile devices supported by multiple mobile network operators”; para [0002]), and the application is an electronic purse (e-purse) (“provide a mobile device user interface for accessing provisioned mobile device applications on each mobile device (e.g., a mobile wallet)”; para [0044]), the mobile device is used to exchange secured data with another device within a near distance to conduct a transaction (para [0046,0053,0065]).

Regarding claim 4, Musfeldt teaches the secured data is being exchanged over a secured channel (para [0046,0053,0065]) between the mobile device and the another device established by the application key set (para [0046,0053,0065]).

Regarding claim 5, Musfeldt teaches the transaction is conducted without the mobile communicating with a transaction server (off-line; para [0029]).

Regarding claim 6, Musfeldt teaches said sending to a server via the network interface an identifier identifying the application together with device information of a secure element comprises: determining whether the secure element has been personalized with a Trusted Service Management (TSM) system (“it is determined whether the mobile device and/or end user associated with the mobile device has previously received a mobile device application via the TSM computer 110”; para [0060]), wherein the TSM system (TSM service manager 110, Fig. 1) is a collection of services configured to distribute and manage contactless services for customers signed up with the TSM (each stored in memories 112, Fig. 1; para [0021,0043]), and provide data exchanges among different parties to make electronic commerce possible over a wireless network (para [0021,0043]); and performing a personalization process for the secure element when above said determining determines that the secure element has not been personalized with the Trusted Service Management (TSM) system (“If it is determined at decision block 330 that the mobile device and/or the end user has not previously received a mobile device application via the TSM computer, then block 335 follows, in which the TSM computer 110 installs TSM administration software on the mobile device 150 that may be utilized to provide secured access to secure elements

and further facilitate installing, accessing, and operating TSM-provisioned applications”; para [0061]), wherein the secure element when personalized establishes a security platform for the application to run on the mobile device (para [0061]).

Regarding claim 7, Musfeldt teaches the personalization process comprises: causing the mobile device to initiate data communication with a server in the TSM system (para [0061]); retrieving device information of the secure element in responding to a request from the TSM server (“the identity of the mobile device end user can be verified as the correct end user for receiving the mobile device application and/or associated personalization data, and/or that the mobile device is in the correct end user's possession”; para [0057]) after the TSM server determines that the secure element is registered therewith (“as part of the registration process, the TSM computer 110 can be configured to store unique identifiers of the mobile device, its secure element, and/or the end users for subsequent processing”; para [0057-0058]), wherein the device information is a sequence of characters uniquely identifying the secure element (“TSM computer 110 can identify the end user by the secure element identifier (e.g., the ICCID, IMSI, etc. associated with the secure element)”; para [0065]); receiving at least a set of keys from the TSM server, wherein the keys are generated in the TSM server in accordance with the device information of the secure element (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]); and

storing the set of keys in the secure element to facilitate a subsequent transaction with the secure element in the computing device (para [0035,0042,0044,0059]).

**Regarding claim 8**, Musfeldt discloses the device information includes an identifier of the secure element (“the secure element identifier (e.g., the ICCID, IMSI, etc. associated with the secure element)”; para [0065]), manufacturer information (para [0065]), and batch number. The ICCID standard is laid out in ISO/IEC 7812 and includes the issuer identification number, the individual account identification, and the international mobile subscriber identity which identified the operator networks within which the communication is designed to occur.

**Regarding claim 9**, Musfeldt teaches the secure element is embedded in the mobile device and integrated with the mobile device via the interface (Fig. 1; para [0025]).

**Regarding claim 13**, Musfeldt teaches part of the data is used to facilitate the server to remotely manage the application (para [0065]).

**Regarding claim 14**, Musfeldt teaches a mobile device (mobile device 150a, Fig. 1) for conducting a secured transaction (para [0017]) over a network (carrier network 180a/b & network 170, Fig. 1), the mobile device comprising: a network interface (network interface 159a, Fig. 1); a secure element (secure element 155a, Fig. 1); a memory space (memory 152a, Fig. 1) for storing various modules (provisioning module 154a used for many provisioning processes, Fig. 1; para [0025]) each of the modules configured to provide an application of service to a user of the mobile device (“memory and data storage device, can store data and information for subsequent retrieval; para

[0031]); a processor (processor 156a, Fig. 1) coupled to the memory space and configured to execute the module to perform operations (“TSM provisioning module 154a, 154b may comprise computer-executable program instructions or software, including a dedicated program, for facilitating mobile device application provisioning on secure elements 155a, 155b as carried out by the TSM computer 110”; para [0025]) including: provisioning each of the modules with a provider (service providers 160a, Fig. 1) that publishes the each of the modules (para [0053-0066]), wherein said provisioning each of the modules with a distributor comprises sending to a server via the network interface an identifier identifying the application (“it can be determined whether the mobile device is technically capable of receiving an OTA provisioned application or capable of operating the specific application requested”; para [0056]) together with device information of a secure element (“the identity of the mobile device end user can be verified as the correct end user for receiving the mobile device application and/or associated personalization data, and/or that the mobile device is in the correct end user's possession”; para [0057]); establishing a secured channel between the secure element and the server using a key set installed on the secure element (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]), wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device (“the requested application can be installed



on the secure element of the mobile device 150 para [0062]); receiving the data from the server to associate the each of the modules with the secure element (“a service provider computer 160 regarding a specific end user (e.g., as identified by name, account, or other unique identifier), the TSM computer 110 is operable to identify the end user as having a TSM-provisioned application installed”; para [0062-0065]) wherein the data includes a set of keys generated for the each of the modules (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]); and sending out an acknowledgement to the provider of the each of the modules about a status of the application that is now active with the secure element (“the TSM computer 110 can be operable to record application installation status, including successes and failures, as may be provided by the lifecycle management module 127”; para [0064]).

Regarding claim 16, Musfeldt teaches the mobile device includes a display configured to display (para [0026]) a user interface showing some of the modules that are still provisioned and active, each of the modules is configured to show another user interface particularly designed for the display of the mobile device when the each of the modules is activated by a user (para [0044]).

Regarding claim 17, Musfeldt teaches the secure element must be personalized before each of the modules is provisioned (step 330-345, Fig. 3), each of the

provisioned modules is associated with the personalized secure element and a key set generated in accordance with a key set of the secure element (para [0053-0066]).

***Claim Rejections - 35 USC § 103***

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

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 10 and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over Musfeldt as applied to claim 7, and further in view of Jain et al. (US PG Pub. 2009/0069051; hereinafter Jain).

**Regarding claim 10**, Musfeldt discloses the secure element is a software module installed in a secure memory space ("the secure elements 155a, 155b may refer to any computer-readable storage in the memory 152"; para [0025]).

Musfeldt discloses the claimed invention as cited above though does not explicitly disclose: the secure element is a software module installed in a secure memory space only accessible by a distributor of the secure element.

Jain discloses "the memory 612 may include secure portions designed to be accessible only by the service provider" (para [0066]).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to provide portions of memory only accessible by a service provider as taught by Jain with the system as disclosed by Musfeldt. The motivation would have

been to maintain data within a memory that may only be accessed by trusted entities (para [0066]).

Regarding claim 11, Musfeldt discloses some components are updated when the secure element is upgraded by the distributor (para [0065]).

7. Claims 12 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Musfeldt, as applied to claims 1 and 14, and further in view of Shenfield et al. (US PG Pub. 2006/0168355; hereinafter Shenfield).

Regarding claims 12 and 15, Musfeldt teaches receiving a message from a distributor of the application (para [0065]), the message including an identifier identifying the application (para [0035-0044]); verifying that the message is indeed from the distributor (“provide a communications gateway via a respective carrier network for OTA provisioning of mobile device applications; provide a mobile device user interface for accessing provisioned mobile device applications on each mobile device (e.g., a mobile wallet); facilitate management of secured keys used to securely load and delete mobile device applications on mobile device secure elements”; para [0044]); disassociating the application with the secure element (remove an application; para [0065]); and notifying the distributor that the application installed in the mobile device is no longer active lifecycle management module 127 can be configured to facilitate tracking the status of users' mobile devices and the status of previously provisioned applications. For example, the lifecycle management module 127 can be configured to maintain inventories of various types of mobile devices, associated secure elements and the

state of the secure elements and applications (active, locked, unlocked, terminated), which may be used to track the status of applications and mobile devices and to communicate with MNOs and/or service providers regarding the provisioned applications"; para [0038,0064]).

Musfeldt discloses the claimed invention as cited above though does not explicitly disclose disassociating the application with the secure element in responding to a confirmation.

Shenfield discloses lifecycle maintenance by service providers including removing applications at the request of the service provider (para [0067]).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to provide portions of memory only accessible by a service provider as taught by Shenfield with the system as disclosed by Musfeldt. The motivation would have been to allow the service providers to remove provisioned applications (para [0067]).

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER STANFORD whose telephone number is (571)270-3337. The examiner can normally be reached on Monday through Fridays, 8am-5pm PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHRISTOPHER STANFORD/  
Examiner, Art Unit 2887

<b>Notice of References Cited</b>	Application/Control No. 13/350,835	Applicant(s)/Patent Under Reexamination KOH ET AL.	
	Examiner CHRISTOPHER STANFORD	Art Unit 2887	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-2006/0168355 A1	07-2006	Shenfield et al.	709/250
*	B US-2009/0069051 A1	03-2009	Jain et al.	455/558
*	C US-2010/0291904 A1	11-2010	Musfeldt et al.	455/414.1
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**


*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

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

<b><i>Index of Claims</i></b> 	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

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

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant			<input type="checkbox"/> CPA			<input type="checkbox"/> T.D.			<input type="checkbox"/> R.1.47		
CLAIM			DATE								
Final	Original	03/15/2013									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									

<b>Search Notes</b>  	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	379,380,451,492	3/14/13	CS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor, Assignee Search	3/14/13	CS
Parent Case Search	3/14/13	CS
Text search (see search history report)	3/14/13	CS
NPL Search	3/14/13	CS

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

/CHRISTOPHER STANFORD/ Examiner.Art Unit 2887	
--	--



## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S49	5	S48 and (remov\$3 or uninstall\$3 or un install\$3 or (revers\$3 or un) provision\$3) with (application or applet or program or (digital or electronic or e) (wallet or purse)) same (service provider or distributor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:58
S48	10	(US-20120130839-\$ or US-20120129452-\$ or US-20050137981-\$ or US-20060168355-\$ or US-20100291904-\$ or US-20120300938-\$ or US-20090069051-\$ or US-20080082646-\$).did. or (US-8118218-\$ or US-7729363-\$).did.	US-PGPUB; USPAT	ADJ	ON	2013/03/14 15:58
S47	78	S46 not S45	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:44
S46	90	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or (mobile or smart or cell) phone) and (remov\$3 or uninstall\$3 or un install\$3 or (revers\$3 or un) provision\$3) with (application or applet or program or (digital or electronic or e) (wallet or purse)) same (service provider or distributor) and (notify\$3 or notif\$3 or verif\$3 or verifying or verification or authenticat\$3 or confirm\$3 or confirmation) near3 (service provider or distributor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:44
S45	12	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or (mobile or smart or cell) phone) and (remov\$3 or uninstall\$3 or un install\$3 or (revers\$3 or un) provision\$3) with (application or applet or program or (digital or electronic or e) (wallet or purse)) same (notify\$3 or notif\$3 or verif\$3 or verifying or verification or authenticat\$3 or confirm\$3 or confirmation) near3 (service provider or distributor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:42
S44	8	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone	US-PGPUB; USPAT; USOCR;	ADJ	ON	2013/03/14 15:41

		or (mobile or smart or cell) phone) and (remov\$3 or uninstall\$3 or un install\$3 or (revers\$3 or un) provision\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (notify\$3 or motif\$3 or verif\$3 or verifying or verification or authenticat\$3 or confirm\$3 or confirmation) near3 (provider)	FPRS; EPO; JPO			
S43	9	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or (mobile or smart or cell) phone) and (remov\$3 or uninstall\$3 or un install\$3 or (revers\$3 or un) provision\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (notify\$3 or motif\$3 or verif\$3 or verifying or verification or authenticat\$3 or confirm\$3 or confirmation) near3 (service provider or distributor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:41
S42	7	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or cell phone) and (remov\$3 or uninstall\$3 or un install\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (notify\$3 or verif\$3 or verifying or verification or authenticat\$3 or confirm\$3 or confirmation) near3 (service provider or distributor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:38
S41	0	(personaliz\$3 or personalization or provision\$3 not provisional or install\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (remov\$3 or uninstall\$3 or un install\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) and (remov\$3 or uninstall\$3 or un install\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (verif\$3 or verifying or verification or authenticat\$3 or confirm\$3 or confirmation) near3 (service provider or distributor)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:37
S40	0	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or cell phone) and (personaliz\$3 or personalization or provision\$3 not provisional or install\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (remov\$3 or uninstall\$3 or un install\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) and (remov\$3 or uninstall\$3 or un install\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (verif\$3 or verifying or verification or authenticat\$3 or confirm\$3 or confirmation) near3 (service	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:36

		provider or distributor)				
S39	11	S38 and (remov\$3 or uninstall\$3 or un install\$3) with (application or applet or program or (digital or electronic or e) (wallet or purse)) with (service provider or distributor)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:33
S38	69	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or cell phone) and (personaliz\$3 or personalization or provision\$3 not provisional) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (remov\$3 or uninstall\$3 or un install\$3) with (application or applet or program or (digital or electronic or e) (wallet or purse))	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:33
S37	716	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or cell phone) and (personaliz\$3 or personalization or provision\$3 not provisional) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) and (remov\$3 or uninstall\$3 or un install\$3) with (application or applet or program or (digital or electronic or e) (wallet or purse))	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:32
S36	11	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or cell phone) and (personaliz\$3 or personalization or provision\$3 not provisional) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) and (memory or (secure\$1 or security) element) with only near2 (distributor or service provider or issu\$3)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:27
S35	24	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or cell phone) and (personaliz\$3 or personalization or provision\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) and (memory or (secure\$1 or security) element) with only near2 (distributor or service provider or issu\$3)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:26
S33	1	"20100291904" and secure element same software	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:22
S32	35	first data.as. and batch with manufactur\$3	US-	ADJ	ON	2013/03/14

			PGPUB; USPAT; USOCR; FPRS; EPO; JPO			15:17
S31	6	cpic same batch with manufactur\$3	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:16
S30	6	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or cell phone) and (personaliz\$3 or personalization or provision\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) and cpic same batch with manufactur\$3	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:15
S29	6	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or cell phone) and (personaliz\$3 or personalization or provision\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) and (personaliz\$3 or personalization or provision\$3) same (tsm or trusted service) and batch with manufactur\$3	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 15:13
S28	1	"20100291904" and key\$1	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 12:49
S27	7	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse) or cellphone or cell phone) and pull adj2 (personaliz\$3 or personalization or provision\$3) with (application or applet or program or (digital or electronic or e) (wallet or purse)) and (personaliz\$3 or personalization or provision\$3) with (tsm or trusted service)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 12:25
S26	62	(smartphone or smart phone or telephone or phone) and (already or previous\$2 or past) adj3 (personalized or provisioned) same (personaliz\$3 or personalization or provision\$3) near2 (application or applet or program or (digital or electronic or e) (wallet or purse))	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 12:23
S25	14	(smartphone or smart phone or telephone or phone) and (already or previous\$2 or past) adj3 (personalized or provisioned) same (personaliz\$3 or personalization or	US- PGPUB; USPAT; USOCR;	ADJ	ON	2013/03/14 12:22

		provision\$3) near2 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (tsm or trusted service)	FPRS; EPO; JPO			
S24	6	(smartphone or smart phone or telephone or phone) same (personalized or provisioned) with (lifecycl\$3 or life cycl\$3) and (personaliz\$3 or personalization or provision\$3) near2 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (tsm or trusted service)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 12:19
S23	0	(smartphone or smart phone or telephone or phone) same (personaliz\$3 or personalization or provision\$3) near3 (local or locally) and (personaliz\$3 or personalization or provision\$3) near2 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (tsm or trusted service)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 12:17
S22	3	(smartphone or smart phone or telephone or phone) same (personaliz\$3 or personalization or provision\$3) near3 (manager or management) and (personaliz\$3 or personalization or provision\$3) near2 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (tsm or trusted service)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 12:16
S21	40	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse)) and (personaliz\$3 or personalization or provision\$3) near2 (application or applet or program or (digital or electronic or e) (wallet or purse)) same (tsm or trusted service)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 10:02
S20	48	S18 and (personaliz\$3 or personalization or provision\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse))	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 10:01
S19	0	S18 and (personaliz\$3 or personalization or provision\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) and (tsm or trusted service)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 10:00
S18	68	("20020032783"   "20020180789"   "20030235282"   "20040024882"   "20050063335"   "20050086510"   "20050138113"   "6006258"   "6041365"   "6088796"   "6304908"   "6415329"   "6519636"   "6611873"   "6678733"   "6748386"   "7080155"   "7085817"   "7200142"   "7260651"   "7293095"   "7324473").PN. OR ("7729363").URPN.	US- PGPUB; USPAT; USOCR	ADJ	ON	2013/03/14 09:59
S17	87	S16 and (personaliz\$3 or personalization or provision\$3) near3 (application or applet or program or (digital or electronic or e) (wallet or purse)) with (tsm or trusted service or	US- PGPUB; USPAT; USOCR;	ADJ	ON	2013/03/14 09:30

		service provider)	FPRS; EPO; JPO			
S16	18957	(nfc or "near" field communicat\$3 or subscriber identity module or sim card or smartphone or smart phone or google wallet or (digital or electronic or e) (wallet or purse)) and ("235" or "340" or "7"\$2).clas. and (personaliz\$3 or personalization or provision\$3) near2 (application or applet or program or (digital or electronic or e) (wallet or purse))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 09:28
S15	5	(KOH adj2 LIANG).inv. and (personaliz\$3 or personalization or provision\$3) same (id or identifier or identification)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 09:06
S14	21	(KOH adj2 LIANG).inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 09:05
S13	1	"20120130839" and provision\$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 08:39
S12	3	"11739044"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/03/14 08:31
S11	6	"8118218"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 10:33
S10	6	705/64,71.ccls. and (tsm or trusted service).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 10:16
S9	14	713/168,171,172.ccls. and (tsm or trusted service).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 10:16

EAST Search History

S8	121	S7 and (nfc or "near" field or sim or smartphone or smart phone).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 10:04
S7	8141	713/168,171,172.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 10:04
S6	36	"455".clas. and (card or sim or nfc or "near" field) with key with (remote\$2 or server).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 10:00
S5	32	"455".clas. and (card or sim) with key with (remote\$2 or server).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 10:00
S4	5	(secur\$3).clm. and S2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 09:58
S2	21	(KOH adj2 LIANG).inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 09:56
S1	37	("near" field or nfc).clm. and server with key.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/02/25 09:53

**EAST Search History (Interference)**

< This search history is empty >

**3/ 15/ 2013 9:35:38 AM**

**C:\Users\cstanford\Documents\EAST\Workspaces\13350835.wsp**

UNITED STATES PATENT AND TRADEMARK OFFICE  
COMMISSIONER FOR PATENTS  
P.O. BOX 1450  
ALEXANDRIA VA 22313-1451

PRESORTED  
FIRST-CLASS MAIL  
U.S. POSTAGE PAID  
POSTEDIGITAL  
NNNNN

SILICON VALLEY PATENT AGENCY  
7394 WILDFLOWER WAY  
CUPERTINO, CA 95014



**Courtesy Reminder for  
Application Serial No: 13/350,835**

Attorney Docket No: RFID-081CIPB

Customer Number: 26797

Date of Electronic Notification: 03/21/2013

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:  
uspatents@sbcglobal.net

To view your correspondence online or update your email addresses, please visit us anytime at <https://sportal.uspto.gov/secure/myportal/privatepair>. If you have any questions, please email the Electronic Business Center (EBC) at [EBC@uspto.gov](mailto:EBC@uspto.gov) or call 1-866-217-9197.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**Applicant(s):** Liang Seng Koh et al  
**Title:** Mobile devices for commerce over unsecured networks  
**Serial No.:** 13/350,835  
**Filing Date:** 01/16/2012  
**Examiner:** Chris Stanford  
**Group Art Unit:** 2887  
**Docket No.:** RFID-081CIP3

---

June 17, 2013

Mail Stop: No-Fee Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Response to First OA**

Dear Sir:

In response to Office Action dated 03/21/2013, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

**AMENDMENTS TO THE SPECIFICATION** begin on page 2 of this Response.

**AMENDMENTS TO THE CLAIMS** are reflected in the listing of claims which begins on page 3 of this Response.

**REMARKS/ARGUMENTS** begin on page 8 of this Response.

## AMENDMENTS TO THE SPECIFICATION

1. Please amend paragraph [0001] as follows:

**[0001]** This application is a continuation-in-part of co-pending US Pat. App. Serial No.: 11/534,653 filed on 9/24/2006, now US Pat. No.: 8,118,218~~X,XXX,XXX~~, and also a continuation-in-part of US Pat. App. Serial No.: 11/739,044 filed on 04/23/2007, which is a continuation-in-part of co-pending US Pat. App. Serial No.: 11/534,653 filed on 9/24/2006, now US Pat. No.: 8,118,218~~X,XXX,XXX~~.

## AMENDMENTS TO THE CLAIMS

Please amend Claims 1, 6 and 14 as follows:

1. *(Currently amended)* A mobile device for conducting a secured transaction over a network, the mobile device comprising:
  - a network interface;
  - an interface to receive a secure element;
  - a memory space for storing at least a module and an application downloaded from the network;
  - a processor coupled to the memory space and configured to execute the module to perform operations including:
    - ~~verifying whether the application has been provisioned;~~
    - ~~when said verifying indicates that the application has not been provisioned,~~
    - sending to a server via the network interface an identifier identifying the application together with device information of a secure element;
    - establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device; and
    - receiving the data from the server to associate the application with the secure element; ~~and~~
    - ~~sending out an acknowledgement to a provider of the application about a status of the application that is now active with the secure element.~~
2. *(Original)* The mobile device as recited in claim 1, wherein the data received in the mobile device includes an application key set for the application, and a user interface specifically designed for the mobile device.
3. *(Original)* The mobile device as recited in claim 2, wherein the mobile device is a near field communication (NFC) enabled mobile phone, and the application is an

electronic purse (e-purse), the mobile device is used to exchange secured data with another device within a near distance to conduct a transaction.

4. (*Original*) The mobile device as recited in claim 3, wherein the secured data is being exchanged over a secured channel between the mobile device and the another device established by the application key set.
5. (*Original*) The mobile device as recited in claim 4, wherein the transaction is conducted without the mobile device communicating with a transaction server.
6. (*Currently amended*) The mobile device as recited in claim 1, wherein said sending to a server via the network interface an identifier identifying the application together with device information of a secure element comprises:
  - determining whether the secure element has been personalized with a Trusted Service Management (TSM) system, wherein the TSM system is a collection of services configured to distribute and manage contactless services for customers signed up with the TSM, and provide data exchanges among different parties to make electronic commerce possible over a wireless network; and
  - performing a personalization process for the secure element when above said determining determines that the secure element has not been personalized with the Trusted Service Management (TSM) system, wherein the secure element when personalized establishes a security platform for the application to run on the mobile device.
7. (*Original*) The mobile device as recited in claim 6, wherein the personalization process comprises:
  - causing the mobile device to initiate data communication with a server in the TSM system;
  - retrieving device information of the secure element in responding to a request from the TSM server after the TSM server determines that the secure

element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element; receiving at least a set of keys from the TSM server, wherein the keys are generated in the TSM server in accordance with the device information of the secure element; and storing the set of keys in the secure element to facilitate a subsequent transaction with the secure element in the computing device.

8. *(Original)* The mobile device as recited in claim 7, wherein the device information includes an identifier of the secure element, manufacturer information and a batch number.
9. *(Original)* The mobile device as recited in claim 7, wherein the secure element is embedded in the mobile device and integrated with the mobile device via the interface.
10. *(Original)* The mobile device as recited in claim 7, wherein the secure element is a software module installed in a secure memory space only accessible by a distributor of the secure element.
11. *(Original)* The mobile device as recited in claim 10, wherein some components are updated when the secure element is upgraded by the distributor.
12. *(Original)* The mobile device as recited in claim 1, wherein the operations further comprises:
  - receiving a message from a distributor of the application, the message including an identifier identifying the application;
  - verifying that the message is indeed from the distributor;
  - disassociating the application with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and

notifying the distributor that the application installed in the mobile device is no longer active.

13. *(Original)* The method as recited in claim 8, wherein part of the data is used to facilitate the server to remotely manage the application.
14. *(Currently amended)* A mobile device for conducting a secured transaction over a network, the mobile device comprising:
- a network interface;
  - a secure element;
  - a memory space for storing various modules downloaded from the network, each of the modules configured to provide an application or a service to a user of the mobile device;
  - a processor coupled to the memory space and configured to execute an embedded module to perform operations including:
    - ~~provisioning each of the modules with a provider that publishes the each of the modules,~~ wherein said provisioning each of the modules with a distributor comprises:
      - sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element;
      - establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the each of the modules to function as designed on the mobile device; and
      - receiving the data from the server to associate the each of the modules with the secure element, wherein the data includes a set of keys generated for the each of the modules; ~~and~~
      - ~~sending out an acknowledgement to the provider of the each of the modules about a status thereof that is now active with the secure element.~~

15. *(Original)* The mobile device as recited claim 14, wherein the operations further comprise:

receiving a message from a distributor of one of the modules, the message including an identifier identifying the one of the modules;  
verifying that the message is authenticated;  
disassociating the one of the modules with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and  
notifying the distributor that the one of the modules installed in the mobile device is no longer active.

16. *(Original)* The mobile device as recited claim 14, wherein the mobile device includes a display configured to display a user interface showing some of the modules that are still provisioned and active, each of the modules is configured to show another user interface particularly designed for the display of the mobile device when the each of the modules is activated by a user.

17. *(Original)* The mobile device as recited claim 16, wherein the secure element must be personalized before each of the modules is provisioned, each of the provisioned modules is associated with the personalized secure element and a key set generated in accordance with a key set of the secure element.

## REMARKS

Claims 1 - 17 are submitted for examination. In the Office Action dated 03/21/2013, Claims 1-9, 13-14, and 16-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Musfeldt et al. (US PG Pub. 2010/0291904, hereinafter Musfeldt), Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Musfeldt as applied to claim 7, and further in view of Jain et al. (US PG Pub. 2009/0069051, hereinafter Jain).

The Applicants appreciate the Examiner for providing detailed comments in the Office Action. In the foregoing amendments, Claims 1, 6 and 14 have been amended. No new matters have been introduced. Reconsideration of pending claims 1-17 is respectfully requested.

On page 2 of this Office Action, the Examiner alleges that Claims 1 and 14 are not supported by the disclosures of prior Application No: 11/534,653 and No.: 11/739,044. With the entry of the foregoing amendments, the Applicant respectfully disagrees with the Examiner. As amended, Claim 1 is fully supported in prior applications '653 and '044 as follows:

### Showing of Support under 35 USC 112, First Paragraph

Claim 1	Prior applications No: 11/534,653 and No.: 11/739,044
A mobile device for conducting a secured transaction over a network, the mobile device comprising: a network interface;	Described at least in para [0007] of '653.  shown at least in FIG. 2 and described in paragraph [0009] of '653, a network interface must be present for the wireless communication.  Indicated in '044, an example of



<p>an interface to receive a secure element;</p> <p>a memory space for storing at least a module and an application downloaded from the network;</p> <p>a processor coupled to the memory space and configured to execute the module to perform operations including:</p> <p style="padding-left: 40px;">sending to a server via the network interface an identifier identifying the application together with device information of a secure element;</p> <p style="padding-left: 40px;">establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device;</p> <p style="padding-left: 40px;">receiving the data from the server to associate the application with the secure element.</p>	<p>secure element is a smart card, it is well known that there must be an interface for a smart card as described in [0002] of '653. Described at least in [0009] of '653, and [0071] of '044.</p> <p>It is well known that a mobile device must have a processor to execute various modules. Described at least in [0039] and FIG. 3C of '653, the Tag ID (i.e., the identifier is used, when the secure element (e.g., the smart card) or the mobile device having the secure element is used as a tag. Described at least in [0028] and [0036] of '653, a secured channel is used to send a key to the secure element (e.g., the smart card) or the mobile device. Described at least in [0036] of '653,</p>
--	---

Thus Claim 1 satisfies the requirement of 35 USC 112 in '653 and '044. Accordingly, the Applicant submits these two cited references Musfeldt and Jain as cited by the Examiner in the Office Action cannot be used as qualified references to

reject Claims 1 -13 as the filing dates of these two references are AFTER the priority dates of this instant application.

Claim 14 has been amended similarly to Claim 1. The support of Claim 14 under 35 USC 112 First Paragraph is not going to be repeated as the support can be referenced in the table above for Claim 1. Accordingly, the Applicant submits these two cited references Musfeldt and Jain cannot be used as qualified references to reject Claims 14 - 17 as the filing dates of these two references are AFTER the priority dates of this instant application.

In view of the above amendments and remark, the Applicant believes that Claims 1 - 17 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)777-8873.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", June 17, 2013. e-filed.

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng  
Reg.: No. 39,450

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	16061729
<b>Application Number:</b>	13350835
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	1986
<b>Title of Invention:</b>	Mobile devices for commerce over unsecured networks
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh
<b>Customer Number:</b>	26797
<b>Filer:</b>	Joe Zheng
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	RFID-082CIP3
<b>Receipt Date:</b>	17-JUN-2013
<b>Filing Date:</b>	16-JAN-2012
<b>Time Stamp:</b>	17:00:41
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	no
------------------------	----

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	ResponseTo1stOA.pdf	110325 <small>9d0b39464603c35f771ad36d098d8e9d3ae1f261</small>	no	10

### Warnings:

### Information:

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

**New Applications Under 35 U.S.C. 111**

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

**National Stage of an International Application under 35 U.S.C. 371**

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

**New International Application Filed with the USPTO as a Receiving Office**

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

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

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875	Application or Docket Number <b>13/350,835</b>	Filing Date <b>01/16/2012</b>	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

ENTITY:  LARGE  SMALL  MICRO

**APPLICATION AS FILED – PART I**

FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

**APPLICATION AS AMENDED – PART II**

	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
<b>AMENDMENT</b>	<b>06/17/2013</b>	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		
	Total (37 CFR 1.16(i))	+ 17	Minus	** 20	= 0	X \$40 = 0
	Independent (37 CFR 1.16(h))	+ 2	Minus	***3	= 0	X \$210 = 0
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
					TOTAL ADD'L FEE	<b>0</b>

	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
<b>AMENDMENT</b>		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		
	Total (37 CFR 1.16(i))	+	Minus	**	=	X \$ =
	Independent (37 CFR 1.16(h))	+	Minus	***	=	X \$ =
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
					TOTAL ADD'L FEE	

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".  
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE  
 /JOSEPH BROOKS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**  
 If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
13/350,835 01/16/2012 Liang Seng Koh RFID-082CIP3 1986
26797 7590 08/22/2013
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014
EXAMINER
STANFORD, CHRISTOPHER J
ART UNIT PAPER NUMBER
2887
NOTIFICATION DATE DELIVERY MODE
08/22/2013 ELECTRONIC

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

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

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

uspatents@sbcglobal.net

<b>Office Action Summary</b>	<b>Application No.</b> 13/350,835	<b>Applicant(s)</b> KOH ET AL.	
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887	<b>AIA (First Inventor to File) Status</b> No

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

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 17 June 2013.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
- 2a)  This action is **FINAL**.                      2b)  This action is non-final.
- 3)  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 4)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 5)  Claim(s) 1-17 is/are pending in the application.  
5a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 6)  Claim(s) \_\_\_\_\_ is/are allowed.
- 7)  Claim(s) 1-17 is/are rejected.
- 8)  Claim(s) \_\_\_\_\_ is/are objected to.
- 9)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

\* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).

**Application Papers**

- 10)  The specification is objected to by the Examiner.
- 11)  The drawing(s) filed on \_\_\_\_\_ is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

**Priority under 35 U.S.C. § 119**

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

**Certified copies:**

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

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 3)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 4)  Other: \_\_\_\_\_

**DETAILED ACTION**

***Response to Amendment***

1. Receipt is acknowledged of the amendment filed 6/17/2013. Claims 1, 5, and 14 are amended and claims 1-17 are currently pending. The status identifiers for claims 5 and 6 are incorrect. Claim 5 should be identified as "Currently Amended" and claim 6 should be identified as "Original".

***Priority***

2. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 120 as follows:

The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of 35 U.S.C. 112(a) or the first paragraph of 35 U.S.C. 112 (pre-AIA). See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).

The disclosures of the prior-filed applications, Application No.11/534,653 and 11/739,044, fail to provide adequate support or enablement in the manner provided by 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph for one or more claims of



this application. The language used in the at least claims 1 and 14 are not supported by the disclosures of Applications '653 and '044. Specifically the recitations regarding how the processor coupled to the mobile device's memory space is configured. Claims 1 and 14 recited the following limitations that are not wholly supported by the patent applications:

- sending to a server via the network interface an identifier identifying the application together with device information of a secure element (claim 1 & 6)
- provisioning each of the modules with a provider that publishes the each of the modules, wherein said provisioning each of the modules with a distributor comprises: sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element (claim 14).

Applicant contends that the claim limitations above are supported in "at least [0039] and Fig. 3C of '653. Upon reviewing the full context of the disclosure, Examiner points specifically to [0034-0044] as encompassing most of what could be considered the context of Applicant's alleged support. In para [0039] the RFID reader reads the "tag ID" which is would have been interpreted by one of ordinary skill in the art as supporting the claimed "device information of a secure element". However there is no disclosure that the tag ID is send to a server via a network interface together with an application identifier. It is clear that a security domain is established after the tag ID is read and it is further clarified that keys may be generated by a server in [0040]. In

[0044], “a set of transformed keys is generated using ... the tag ID”. This disclosure and the context around it does not support a claim limitation requiring the device information of a secure element to be sent “to a server via the network interface” together with an application identifier.

Furthermore, in the context noted above, Applicant does not disclose sending “an identifier identifying the application” to a server via a network interface. In [0044], “a set of transformed keys is generated using the existing SAM”. Neither this disclosure nor any other in the originally filed ‘653 application supports sending an application identifier to a server.

The claims of instant application will be not receive the priority filing dates of the prior-filed parent applications. For prior art purposes, the effective filing date of the claims of the instant application will coincide with the actual filing date of 1/16/2012.

***Claim Rejections - 35 USC § 102***

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

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

4. **Claims 1-9, 13-14, and 16-17** are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Musfeldt et al. (US PG Pub. 2010/0291904; hereinafter Musfeldt; previously cited).

**Regarding claim 1**, Musfeldt teaches a mobile device (mobile device 150a, Fig. 1) for conducting a secured transaction (para [0017]) over a network (carrier network

Art Unit: 2887

180a/b & network 170, Fig. 1) , the mobile device comprising: a network interface (network interface 159a, Fig. 1); an interface (interfaces for secure element embodiments such as SIM cards; para [0025]) to receive a secure element (secure element 155a, Fig. 1); a memory space (memory 152a, Fig. 1) for storing at least a module (provisioning module 154a, Fig. 1) and an application downloaded from the network (“memory and data storage device, can store data and information for subsequent retrieval; para [0031]); a processor (processor 156a, Fig. 1) coupled to the memory space and configured to execute the module to perform operations (“TSM provisioning module 154a, 154b may comprise computer-executable program instructions or software, including a dedicated program, for facilitating mobile device application provisioning on secure elements 155a, 155b as carried out by the TSM computer 110”; para [0025, 0053-0066]) including: verifying whether the application has been provisioned (“a provisioning request can come from any of the mobile devices 150 or associated end users”; para [0054]); when said verifying indicates that the application has not been provisioned (“a provisioning request can come from any of the mobile devices 150 or associated end users”; para [0054]), sending to a server via the network interface an identifier identifying the application (“it can be determined whether the mobile device is technically capable of receiving an OTA provisioned application or capable of operating the specific application requested”; para [0056]) together with device information of a secure element (“the identity of the mobile device end user can be verified as the correct end user for receiving the mobile device application and/or associated personalization data, and/or that the mobile device is in the correct end

user's possession"; para [0057]); establishing a secured channel between the secure element and the server using a key set installed on the secure element ("additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.); para [0035,0042,0059]), wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device ("the requested application can be installed on the secure element of the mobile device 150 para [0062]); receiving the data from the server to associate the application with the secure element ("a service provider computer 160 regarding a specific end user (e.g., as identified by name, account, or other unique identifier), the TSM computer 110 is operable to identify the end user as having a TSM-provisioned application installed"; para [0062-0065]).

**Regarding claim 2**, Musfeldt teaches the data received in the mobile device includes an application key set for the application ("facilitate management of secured keys used to securely load and delete mobile device applications on mobile device secure elements"; para [0044]), and a user interface specifically designed for the mobile device ("provide a mobile device user interface for accessing provisioned mobile device applications on each mobile device (e.g., a mobile wallet)"; para [0044]).

**Regarding claim 3**, Musfeldt teaches the mobile device is a near field communication (NFC) enabled mobile phone ("multiple service providers (e.g., card issuing banks, retailers, transit operators, etc.) need to load and manage applications

(e.g., NFC-based applications, etc.) onto mobile devices supported by multiple mobile network operators”; para [0002]), and the application is an electronic purse (e-purse) (“provide a mobile device user interface for accessing provisioned mobile device applications on each mobile device (e.g., a mobile wallet)”); para [0044]), the mobile device is used to exchange secured data with another device within a near distance to conduct a transaction (para [0046,0053,0065]).

**Regarding claim 4**, Musfeldt teaches the secured data is being exchanged over a secured channel (para [0046,0053,0065]) between the mobile device and the another device established by the application key set (para [0046,0053,0065]).

**Regarding claim 5**, Musfeldt teaches the transaction is conducted without the mobile communicating with a transaction server (off-line; para [0029]).

**Regarding claim 6**, Musfeldt teaches said sending to a server via the network interface an identifier identifying the application together with device information of a secure element comprises: determining whether the secure element has been personalized with a Trusted Service Management (TSM) system (“it is determined whether the mobile device and/or end user associated with the mobile device has previously received a mobile device application via the TSM computer 110”; para [0060]), wherein the TSM system (TSM service manager 110, Fig. 1) is a collection of services configured to distribute and manage contactless services for customers signed up with the TSM (each stored in memories 112, Fig. 1; para [0021,0043]), and provide data exchanges among different parties to make electronic commerce possible over a wireless network (para [0021,0043]); and performing a personalization process for the

secure element when above said determining determines that the secure element has not been personalized with the Trusted Service Management (TSM) system (“If it is determined at decision block 330 that the mobile device and/or the end user has not previously received a mobile device application via the TSM computer, then block 335 follows, in which the TSM computer 110 installs TSM administration software on the mobile device 150 that may be utilized to provide secured access to secure elements and further facilitate installing, accessing, and operating TSM-provisioned applications”; para [0061]), wherein the secure element when personalized establishes a security platform for the application to run on the mobile device (para [0061]).

Regarding claim 7, Musfeldt teaches the personalization process comprises: causing the mobile device to initiate data communication with a server in the TSM system (para [0061]); retrieving device information of the secure element in responding to a request from the TSM server (“the identity of the mobile device end user can be verified as the correct end user for receiving the mobile device application and/or associated personalization data, and/or that the mobile device is in the correct end user's possession”; para [0057]) after the TSM server determines that the secure element is registered therewith (“as part of the registration process, the TSM computer 110 can be configured to store unique identifiers of the mobile device, its secure element, and/or the end users for subsequent processing”; para [0057-0058]), wherein the device information is a sequence of characters uniquely identifying the secure element (“TSM computer 110 can identify the end user by the secure element identifier (e.g., the ICCID, IMSI, etc. associated with the secure element)”; para [0065]); receiving

at least a set of keys from the TSM server, wherein the keys are generated in the TSM server in accordance with the device information of the secure element (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]); and storing the set of keys in the secure element to facilitate a subsequent transaction with the secure element in the computing device (para [0035,0042,0044,0059]).

**Regarding claim 8**, Musfeldt discloses the device information includes an identifier of the secure element (“the secure element identifier (e.g., the ICCID, IMSI, etc. associated with the secure element)”; para [0065]), manufacturer information (para [0065]), and batch number. The ICCID standard is laid out in ISO/IEC 7812 and includes the issuer identification number, the individual account identification, and the international mobile subscriber identity which identified the operator networks within which the communication is designed to occur.

**Regarding claim 9**, Musfeldt teaches the secure element is embedded in the mobile device and integrated with the mobile device via the interface (Fig. 1; para [0025]).

**Regarding claim 13**, Musfeldt teaches part of the data is used to facilitate the server to remotely manage the application (para [0065]).

**Regarding claim 14**, Musfeldt teaches a mobile device (mobile device 150a, Fig. 1) for conducting a secured transaction (para [0017]) over a network (carrier network

180a/b & network 170, Fig. 1) , the mobile device comprising: a network interface (network interface 159a, Fig. 1); a secure element (secure element 155a, Fig. 1); a memory space (memory 152a, Fig. 1) for storing various modules (provisioning module 154a used for many provisioning processes, Fig. 1; para [0025]) each of the modules configured to provide an application of service to a user of the mobile device (“memory and data storage device, can store data and information for subsequent retrieval; para [0031]); a processor (processor 156a, Fig. 1) coupled to the memory space and configured to execute the module to perform operations (“TSM provisioning module 154a, 154b may comprise computer-executable program instructions or software, including a dedicated program, for facilitating mobile device application provisioning on secure elements 155a, 155b as carried out by the TSM computer 110”; para [0025]) including: provisioning each of the modules with a provider (service providers 160a, Fig. 1) that publishes the each of the modules (para [0053-0066]), wherein said provisioning each of the modules with a distributor comprises sending to a server via the network interface an identifier identifying the application (“it can be determined whether the mobile device is technically capable of receiving an OTA provisioned application or capable of operating the specific application requested”; para [0056]) together with device information of a secure element (“the identity of the mobile device end user can be verified as the correct end user for receiving the mobile device application and/or associated personalization data, and/or that the mobile device is in the correct end user's possession”; para [0057]); establishing a secured channel between the secure element and the server using a key set installed on the secure element (“additional



space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.); para [0035,0042,0059]), wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device (“the requested application can be installed on the secure element of the mobile device 150 para [0062]); receiving the data from the server to associate the each of the modules with the secure element (“a service provider computer 160 regarding a specific end user (e.g., as identified by name, account, or other unique identifier), the TSM computer 110 is operable to identify the end user as having a TSM-provisioned application installed”; para [0062-0065]) wherein the data includes a set of keys generated for the each of the modules (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]).

**Regarding claim 16**, Musfeldt teaches the mobile device includes a display configured to display (para [0026]) a user interface showing some of the modules that are still provisioned and active, each of the modules is configured to show another user interface particularly designed for the display of the mobile device when the each of the modules is activated by a user (para [0044]).

Regarding claim 17, Musfeldt teaches the secure element must be personalized before each of the modules is provisioned (step 330-345, Fig. 3), each of the provisioned modules is associated with the personalized secure element and a key set generated in accordance with a key set of the secure element (para [0053-0066]).

***Claim Rejections - 35 USC § 103***

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

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Musfeldt as applied to claim 7, and further in view of Jain et al. (US PG Pub. 2009/0069051; hereinafter Jain; previously cited).

Regarding claim 10, Musfeldt discloses the secure element is a software module installed in a secure memory space ("the secure elements 155a, 155b may refer to any computer-readable storage in the memory 152"; para [0025]).

Musfeldt discloses the claimed invention as cited above though does not explicitly disclose: the secure element is a software module installed in a secure memory space only accessible by a distributor of the secure element.

Jain discloses "the memory 612 may include secure portions designed to be accessible only by the service provider" (para [0066]).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to provide portions of memory only accessible by a service provider as taught by Jain with the system as disclosed by Musfeldt. The motivation would have been to maintain data within a memory that may only be accessed by trusted entities (para [0066]).

Regarding claim 11, Musfeldt discloses some components are updated when the secure element is upgraded by the distributor (para [0065]).

7. Claims 12 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Musfeldt, as applied to claims 1 and 14, and further in view of Shenfield et al. (US PG Pub. 2006/0168355; hereinafter Shenfield; previously cited).

Regarding claims 12 and 15, Musfeldt teaches receiving a message from a distributor of the application (para [0065]), the message including an identifier identifying the application (para [0035-0044]); verifying that the message is indeed from the distributor (“provide a communications gateway via a respective carrier network for OTA provisioning of mobile device applications; provide a mobile device user interface for accessing provisioned mobile device applications on each mobile device (e.g., a mobile wallet); facilitate management of secured keys used to securely load and delete mobile device applications on mobile device secure elements”; para [0044]); disassociating the application with the secure element (remove an application; para [0065]); and notifying the distributor that the application installed in the mobile device is no longer active lifecycle management module 127 can be configured to facilitate tracking the status of

users' mobile devices and the status of previously provisioned applications. For example, the lifecycle management module 127 can be configured to maintain inventories of various types of mobile devices, associated secure elements and the state of the secure elements and applications (active, locked, unlocked, terminated), which may be used to track the status of applications and mobile devices and to communicate with MNOs and/or service providers regarding the provisioned applications"; para [0038,0064]).

Musfeldt discloses the claimed invention as cited above though does not explicitly disclose disassociating the application with the secure element in responding to a confirmation.

Shenfield discloses lifecycle maintenance by service providers including removing applications at the request of the service provider (para [0067]).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to provide portions of memory only accessible by a service provider as taught by Shenfield with the system as disclosed by Musfeldt. The motivation would have been to allow the service providers to remove provisioned applications (para [0067]).

### ***Response to Arguments***

8. Applicant's arguments filed 6/17/2013 have been fully considered but they are not persuasive.

9. Applicant's arguments focus on the support for the currently presented claim language such that the effective filing date that should be given to the claims would

precede the filing dates of applied prior art. Examiner contends that a portion of the claim is not supported in the '653 application, as noted in the Priority section above, and therefore the rejections stand. An explanation of the missing support can be found in the Priority section above.

***Conclusion***

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER STANFORD whose telephone number is (571)270-3337. The examiner can normally be reached on Monday through Fridays, 8am-5pm PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHRISTOPHER STANFORD/  
Examiner, Art Unit 2887

<b>Search Notes</b>  	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	379,380,451,492	3/14/13	CS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor, Assignee Search	3/14/13	CS
Parent Case Search	3/14/13	CS
Text search (see search history report)	3/14/13	CS
NPL Search	3/14/13	CS
Text search (see search history report)	8/13/13	CS

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

/CHRISTOPHER STANFORD/ Examiner.Art Unit 2887	
--	--

**EAST Search History**

**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L13	4	L11 and (purse or wallet or epurse or ewallet or (transaction or financial or credit or debit) near3 (application or applet or midlet or program)) same (key or encrypt\$3 or cryptograph\$2 or decrypt\$3) with (install\$3 or installation or personaliz\$3 or personalization or download\$3 or upload\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/08/13 11:35
L11	512	(("3573747"   "3609697"   "3790700"   "3796830"   "3798359"   "3798360"   "3798605"   "3806874"   "3806882"   "3829833"   "3845391"   "3906448"   "3911397"   "3924065"   "3931504"   "3946200"   "3946220"   "3956615"   "3958081"   "3970992"   "3996449"   "4020326"   "4048619"   "4071911"   "4104721"   "4112421"   "4120030"   "4162483"   "4163280"   "4168396"   "4183085"   "4196310"   "4200913"   "4209787"   "4217588"   "4220991"   "4232193"   "4232317"   "4236217"   "4246638"   "4253157"   "4259720"   "4262329"   "4265371"   "4270182"   "4278837"   "4305131"   "4306289"   "4309569"   "4319079"   "4321672"   "4323921"   "4328544"   "4337483"   "4361877"   "4375579"   "4405829"   "4433207"   "4434464"   "4442484"   "4442486"   "4446519"   "4454594"   "4458315"   "4462076"   "4462078"   "4465901"   "4471163"   "4471216"   "4484217"   "4494156"   "4513174"   "4523271"   "4525599"   "4528588"   "4528643"   "4529870"   "4553252"   "4558176"   "4558413"   "4562305"   "4562306"   "4562495"   "4573119"   "4577289"   "4578530"   "4584639"   "4584641"   "4588991"   "4589064"   "4590552"   "4593183"   "4593353"   "4593376"   "4595950"   "4597058"   "4598288"   "4599489"   "4609777"   "4609985"   "4621321"   "4621334"   "4622222"   "4634807"   "4644493"   "4646234"   "4652990"   "4658093"   "4670857"   "4672572"   "4672605"   "4677434"   "4677552"   "4680731"   "4683553"   "4683968"   "4685056"   "4688169"   "4691350"   "4696034"   "4700296"   "4701846"   "4712238"   "4713753"   "4727550").PN. OR ("4740890"   "4747139"   "4748561"   "4757533"   "4757534"   "4768087"   "4780821"   "4791565"   "4796181"   "4796220"   "4798209"   "4799156"   "4807288"	US-PGPUB; USPAT; USOCR	ADJ	ON	2013/08/13 11:30



"4816655"	"4817140"	"4823264"
"4827508"	"4858121"	"4864494"
"4864616"	"4866769"	"4868736"
"4868877"	"4888798"	"4893248"
"4893332"	"4903296"	"4919545"
"4924378"	"4926480"	"4930073"
"4937863"	"4941175"	"4949187"
"4953209"	"4962533"	"4975647"
"4975878"	"4977594"	"4995082"
"4999806"	"5001752"	"5005122"
"5005200"	"5010571"	"5014234"
"5022080"	"5023907"	"5027397"
"5032979"	"5047928"	"5048085"
"5050213"	"5058162"	"5065429"
"5079648"	"5091966"	"5103392"
"5103459"	"5103476"	"5109413"
"5111390"	"5113518"	"5119493"
"5126936"	"5128525"	"5129084"
"5136643"	"5136646"	"5136647"
"5136716"	"5138712"	"5146575"
"5148481"	"5150407"	"5155680"
"5163091"	"5164988"	"5168147"
"5185717"	"5187787"	"5191573"
"5199066"	"5199074"	"5201046"
"5201047"	"5204897"	"5206951"
"5208748"	"5214702"	"5216603"
"5218605"	"5221833"	"5222134"
"5224160"	"5224163"	"5227797"
"5235642"	"5241671"	"5245165"
"5247575"	"5251294"	"5257369"
"5260999"	"5263157"	"5263158"
"5263165"	"5265164"	"5276735"
"5276901"	"5280479"	"5283830"
"5285494"	"5287407"	"5291598"
"5301231"	"5301326"	"5311591"
"5319705"	"5319735"	"5319785"
"5325524"	"5335169"	"5335346"
"5337357".PN. OR ("5337360"   "5341429"		
"5343526"	"5343527"	"5347579"
"5349642"	"5351293"	"5355474"
"5359721"	"5361359"	"5365587"
"5367621"	"5369702"	"5369707"
"5371792"	"5373440"	"5373561"
"5383113"	"5388211"	"5390247"
"5390297"	"5390330"	"5392220"
"5392390"	"5394469"	"5410598"
"5412717"	"5418713"	"5420927"
"5421006"	"5422953"	"5428606"
"5432851"	"5432928"	"5432950"
"5438508"	"5440634"	"5442645"
"5444779"	"5449895"	"5449896"
"5450490"	"5450493"	"5453601"
"5453605"	"5455407"	"5455861"
"5455953"	"5457746"	"5457747"
"5458494"	"5463565"	"5473687"
"5473692"	"5479509"	"5485622"
"5490216"	"5491800"	"5497479"
"5497491"	"5499298"	"5504757"
"5504818"	"5504837"	"5508913"
"5509070"	"5513261"	"5524933"
"5530235"	"5530752"	"5533123"
"5534855"	"5534975"	"5535322"
"5537526"	"5539735"	"5539828"
"5550971"	"5553282"	"5557518"

		"5557798"   "5563946"   "5568552"   "5572673"   "5574962"   "5577209"   "5581800"   "5592549"   "5603031"   "5606609"   "5613004"   "5621797"   "5625693"   "5629770"   "5629980"   "5633932"   "5634012"   "5636276"   "5636292"   "5638443"   "5638504"   "5640546"   "5649099"   "5655077"   "5671279"   "5678170"   "5687236"   "5689565"   "5689566"   "5689587"   "5692047"   "5692180"   "5699427"   "5710834"   "5715314"   "5715403"   "5717923"   "5721788"   "5724424"   "5724425"   "5732398"   "5740549"   "5745569"   "5745604"   "5745678").PN. OR ("5748763"   "5748783"   "5748960"   "5754849"   "5757914"   "5758152"   "5765152"   "5768426"   "5774872"   "5787334"   "5802590"   "5819263"   "5842173"   "5845281"   "5892899"   "5892900"   "5896454"   "5910987"   "5915019"   "5917912"   "5920861"   "5940504"   "5940505"   "5943422"   "5949876"   "5956408"   "5966440"   "5978484"   "5982891"   "5999949"   "6009170"   "6016393"   "6102965"   "6112181"   "6135646"   "6138119"   "6157721"   "6185683"   "6237786"   "6240185"   "6253193"   "6292569"   "6363488"   "6389402"   "6427140"   "6449367"   "6618484"   "6640304"   "6658568"   "6668325").PN. OR ("7076652").URPN.				
L5	3	"20020112171"	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/08/13 11:28
L4	27	L3 and @ay<"2007"	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/08/13 10:57
L3	128	(smartphone or (mobile or cell or cellular or portable or handheld or hand held or wireless or smart) adj2 (phone or telephone or device or apparatus) same (purse or wallet or epurse or ewallet) and (purse or wallet or epurse or ewallet or (transaction or financial or credit or debit) near3 (application or applet or midlet or program)) same (key or encrypt\$3 or cryptohraph\$2 or decrypt\$3) with (install\$3 or installation or personaliz\$3 or personalization or download\$3 or upload\$3)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/08/13 10:56
L2	2	"20080073426" and server and sam	US- PGPUB; USPAT; USOCR; FPRS;	ADJ	ON	2013/08/13 10:14

EAST Search History


			EPO; JPO			
L1	9	"11534653"	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2013/08/13: 09:37

**EAST Search History (Interference)**

<This search history is empty>

**8/ 13/ 2013 11:35:45 AM**

**C:\Users\cstanford\Documents\EAST\Workspaces\13350835.wsp**

<b>Index of Claims</b> 	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

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

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant		<input type="checkbox"/> CPA		<input type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47			
CLAIM		DATE							
Final	Original	03/15/2013	08/13/2013						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						
	15	✓	✓						
	16	✓	✓						
	17	✓	✓						

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

<b>REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL</b>  Subsection (b) of 35 U.S.C. § 132, effective on May 29, 2000, provides for continued examination of an utility or plant application filed on or after June 8, 1995. See The American Inventors Protection Act of 1999 (AIPA).	Application Number	<b>13/350,835</b>
	Filing Date	<b>01/16/2012</b>
	First Named Inventor	<b>Liang Seng Koh</b>
	Group Art Unit	<b>2887</b>
	Examiner Name	<b>Chris Stanford</b>
	Attorney Docket Number	<b>RFID-081CIP3</b>

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application.

**NOTE:** 37 C.F.R. § 1.114 is effective on May 29, 2000. If the above-identified application was filed prior to May 29, 2000, applicant may wish to consider filing a continued prosecution application (CPA) under 37 C.F.R. § 1.53 (d) (PTO/SB/29) instead of a RCE to be eligible for the patent term adjustment provisions of the AIPA. See Changes to Application Examination and Provisional Application Practice, Final Rule, 65 Fed. Reg. 50092 (Aug. 16, 2000); Interim Rule, 65 Fed. Reg. 14865 (Mar. 20, 2000), 1233 Off. Gaz. Pat. Office 47 (Apr. 11, 2000), which established RCE practice.

1. **Submission required under 37 C.F.R. § 1.114**

a.  Previously submitted

i.  Consider the amendment(s)/reply under 37 C.F.R. § 1.116 previously filed on \_\_\_\_\_  
(Any unentered amendment(s) referred to above will be entered).

ii.  Consider the arguments in the Appeal Brief or Reply Brief previously filed on \_\_\_\_\_

iii.  Other \_\_\_\_\_

b.  Enclosed

i.  Amendment/Reply

ii.  Affidavit(s)/Declaration(s)

iii.  Information Disclosure Statement (IDS)

iv.  Other \_\_\_\_\_

2. **Miscellaneous**

a.  Suspension of action on the above-identified application is requested under 37 C.F.R. § 1.103(c) for a period of \_\_\_\_\_ months. (Period of suspension shall not exceed 3 months; Fee under 37 C.F.R. § 1.17(i) required)

b.  Other \_\_\_\_\_

3. **Fees** The RCE fee under 37 C.F.R. § 1.17(e) is required by 37 C.F.R. § 1.114 when the RCE is filed.

a.  The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. \_\_\_\_\_

i.  RCE fee required under 37 C.F.R. § 1.17(e) **Small Entity**

ii.  Extension of time fee (37 C.F.R. §§ 1.136 and 1.17)

iii.  Other \_\_\_\_\_

b.  Check in the amount of \$\_\_\_\_\_ enclosed

c.  Payment by credit card (Form PTO-2038 enclosed) paid via PAIR

**SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED**

Name (Print/Type)	<b>Joe Zheng</b>	Registration No. (Attorney/Agent)	<b>39,450</b>
Signature	<b>/ joe zheng /</b>	Date	<b>11/22/2013</b>

**CERTIFICATE OF MAILING OR TRANSMISSION**

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner For Patents, Box RCE, Washington, DC 20231, or facsimile transmitted to the U.S. Patent and Trademark Office on:

Name (Print/Type)	<b>Joe Zheng</b>
Signature	<b>/ joe zheng /</b>
Date	<b>11/22/2013</b>

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND Fees and Completed Forms to the following address: Assistant Commissioner for Patents, Box RCE, Washington, DC 20231.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**Applicant(s):** Liang Seng Koh et al  
**Title:** Mobile devices for commerce over unsecured networks  
**Serial No.:** 13/350,835  
**Filing Date:** 01/16/2012  
**Examiner:** Chris Stanford  
**Group Art Unit:** 2887  
**Docket No.:** RFID-081CIP3

---

Nov. 22, 2013

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

**Response to Final OA**

Dear Sir:

In response to Office Action dated 08/22/2013, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

**AMENDMENTS TO THE CLAIMS** are reflected in the listing of claims which begins on page 2 of this Response.

**REMARKS/ARGUMENTS** begin on page 7 of this Response.

## AMENDMENTS TO THE CLAIMS

Please amend Claim 6 as follows:

1. *(Previously amended)* A mobile device for conducting a secured transaction over a network, the mobile device comprising:
  - a network interface;
  - an interface to receive a secure element;
  - a memory space for storing at least a module and an application downloaded from the network;
  - a processor coupled to the memory space and configured to execute the module to perform operations including:
    - sending to a server via the network interface an identifier identifying the application together with device information of a secure element;
    - establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device; and
    - receiving the data from the server to associate the application with the secure element.
2. *(Original)* The mobile device as recited in claim 1, wherein the data received in the mobile device includes an application key set for the application, and a user interface specifically designed for the mobile device.
3. *(Original)* The mobile device as recited in claim 2, wherein the mobile device is a near field communication (NFC) enabled mobile phone, and the application is an electronic purse (e-purse), the mobile device is used to exchange secured data with another device within a near distance to conduct a transaction.

4. (*Original*) The mobile device as recited in claim 3, wherein the secured data is being exchanged over a secured channel between the mobile device and the another device established by the application key set.
5. (*Original*) The mobile device as recited in claim 4, wherein the transaction is conducted without the mobile device communicating with a transaction server.
6. (*Currently amended*) The mobile device as recited in claim 1, wherein said sending to a server via the network interface an identifier identifying the application together with device information of a secure element comprises:
  - determining whether the secure element has been personalized with a Trusted Service Management (TSM) system, wherein the TSM system is a collection of services configured to distribute and manage contactless services for customers signed up with the TSM, and provide data exchanges among different parties to make electronic commerce possible over a wireless network; and
  - performing a personalization process for the secure element when ~~above said determining determines that~~ the secure element has not been personalized with the Trusted Service Management (TSM) system, wherein the secure element when personalized establishes a security platform for the application to run on the mobile device.
7. (*Original*) The mobile device as recited in claim 6, wherein the personalization process comprises:
  - causing the mobile device to initiate data communication with a server in the TSM system;
  - retrieving device information of the secure element in responding to a request from the TSM server after the TSM server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element;



receiving at least a set of keys from the TSM server, wherein the keys are generated in the TSM server in accordance with the device information of the secure element; and  
storing the set of keys in the secure element to facilitate a subsequent transaction with the secure element in the computing device.

8. (*Original*) The mobile device as recited in claim 7, wherein the device information includes an identifier of the secure element, manufacturer information and a batch number.
9. (*Original*) The mobile device as recited in claim 7, wherein the secure element is embedded in the mobile device and integrated with the mobile device via the interface.
10. (*Original*) The mobile device as recited in claim 7, wherein the secure element is a software module installed in a secure memory space only accessible by a distributor of the secure element.
11. (*Original*) The mobile device as recited in claim 10, wherein some components are updated when the secure element is upgraded by the distributor.
12. (*Original*) The mobile device as recited in claim 1, wherein the operations further comprises:
  - receiving a message from a distributor of the application, the message including an identifier identifying the application;
  - verifying that the message is indeed from the distributor;
  - disassociating the application with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and
  - notifying the distributor that the application installed in the mobile device is no longer active.

13. *(Original)* The method as recited in claim 8, wherein part of the data is used to facilitate the server to remotely manage the application.
14. *(Currently amended)* A mobile device for conducting a secured transaction over a network, the mobile device comprising:
- a network interface;
  - a secure element;
  - a memory space for storing various modules downloaded from the network, each of the modules configured to provide an application or a service to a user of the mobile device;
  - a processor coupled to the memory space and configured to execute an embedded module to perform operations including:
    - provisioning each of the modules, wherein said provisioning each of the modules with a distributor comprises:
      - sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element;
      - establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the each of the modules to function as designed on the mobile device; and
      - receiving the data from the server to associate the each of the modules with the secure element, wherein the data includes a set of keys generated for the each of the modules.
15. *(Original)* The mobile device as recited claim 14, wherein the operations further comprise:
- receiving a message from a distributor of one of the modules, the message including an identifier identifying the one of the modules;
  - verifying that the message is authenticated;

disassociating the one of the modules with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and notifying the distributor that the one of the modules installed in the mobile device is no longer active.

16. *(Original)* The mobile device as recited claim 14, wherein the mobile device includes a display configured to display a user interface showing some of the modules that are still provisioned and active, each of the modules is configured to show another user interface particularly designed for the display of the mobile device when the each of the modules is activated by a user.

17. *(Original)* The mobile device as recited claim 16, wherein the secure element must be personalized before each of the modules is provisioned, each of the provisioned modules is associated with the personalized secure element and a key set generated in accordance with a key set of the secure element.

## REMARKS

Claims 1 - 17 are submitted for examination. In the Office Action dated 08/22/2013, Claims 1-9, 13-14, and 16-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Musfeldt et al. (US PG Pub. 2010/0291904, hereinafter Musfeldt), Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Musfeldt as applied to claim 7, and further in view of Jain et al. (US PG Pub. 2009/0069051, hereinafter Jain).

The Applicants appreciate the Examiner for providing detailed comments in the Office Action. In the foregoing amendments, Claim 6 has been amended to correct some informalities. No new matters have been introduced. Reconsideration of pending claims 1-17 is respectfully requested.

On page 2, section 2 of this Office Action, the Examiner alleges Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 USC 120. In particular, the Examiner states:

The language used in the at least claims 1 and 14 are not supported by the disclosures of Applications '653 and '044. Specifically the recitations regarding how the processor coupled to the mobile device's memory space is configured. Claims 1 and 14 recited the following limitations that are not wholly supported by the patent applications:

- sending to a server via the network interface an identifier identifying the application together with device information of a secure element (claim 1 & 6)
- provisioning each of the modules with a provider that publishes the each of the modules, wherein said provisioning each of the modules with a distributor comprises: sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element (claim 14).

The Applicant wishes to point out that, per MPEP 2164.01, a patent application does not need to teach, and preferably omits, what is well known in the art. *In re Buchner*, 929 F.2d 660, 661, 18 USPQ2d 1331, 1332 (Fed. Cir. 1991); *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1463, 221 USPQ 481, 489 (Fed. Cir. 1984). It is a common knowledge (well known to those skilled in the art) that a microprocessor or processor is often

coupled to a memory space to execute software code (e.g., firmware) therein to perform certain functions. Specifically, a mobile device such as the computing device 100 of FIG. 1A has to have a processor and a memory space to store necessary code for the processor to execute as such the mobile device can function as described. In fact, US Application 11/739,044 describes in paragraph [0009] a memory space associated with microprocessor circuitry. Accordingly, the Applicant submits the recitation of “*a processor coupled to the memory space and configured to execute the module to perform operations*” in Claim 1 is not a unique feature to the invention being claimed but makes the claim technically understandable.

Regarding the 2nd allegation that “*• sending to a server via the network interface an identifier identifying the application together with device information of a secure element (claim 1 & 6)*” is not supportive in the two parent applications this instant application depends upon, the Applicant wishes to refer the Examiner to US App. Ser. No.: 11/739,044, paragraph [0071] and FIG. 5A and FIG. 5C, where it describes a list of directories for various services (i.e., applications) is shown so that a user may choose one therefrom. When one of the items is chosen, an identifier identifying the chosen item together with device information of a secure element must be provided to the server providing the list, where the device information is needed to identify the mobile device choosing the identified application. Based on the identifier, an applet corresponding to the chosen item can be downloaded to the mobile device as described as 556 of FIG. 5C. Accordingly, the Applicant submits the recitation identified by the Examiner is fully supported in US App. Ser. No.: 11/739,044.

Claim 1 satisfies the requirement of 35 USC 112 in '653 and '044. Accordingly, the Applicant submits these two cited references Musfeldt and Jain as cited by the Examiner in the Office Action cannot be used as qualified references to reject Claims 1 -13 as the filing dates of these two references are AFTER the priority dates of this instant application.

Regarding the 3rd allegation that “*•provisioning each of the modules with a provider that publishes the each of the modules, wherein said provisioning each of*

*the modules with a distributor comprises: sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element (claim 14)*" is not supportive in the two parent applications this instant application depends upon, the Applicant wishes to refer the Examiner to US App. Ser. No.: 11/739,044, paragraphs [0071], [0072] and [0073] and further in FIG. 5C. As explicitly described in [0072], the chosen item, namely, an application applet by the identifier is downloaded. The downloaded applet must be personalized or provisioned before it can be used as graphically shown as 558 of FIG. 5C in US App. Ser. No.: 11/739,044. The second part of this particular recitation is substantially similar to the 2<sup>nd</sup> allegation which has been shown above the full support in US App. Ser. No.: 11/739,044.

Accordingly, Claim 14 satisfies the requirement of 35 USC 112 in '653 and '044. Accordingly, the Applicant submits these two cited references Musfeldt and Jain as cited by the Examiner in the Office Action cannot be used as qualified references to reject Claims 14 -17 as the filing dates of these two references are AFTER the priority dates of this instant application.

In view of the above amendments and remark, the Applicant believes that Claims 1 - 17 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)777-8873.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", Nov 22, 2013. e-filed.

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng  
Reg.: No. 39,450

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13350835			
<b>Filing Date:</b>	16-Jan-2012			
<b>Title of Invention:</b>	Mobile devices for commerce over unsecured networks			
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh			
<b>Filer:</b>	Joe Zheng			
<b>Attorney Docket Number:</b>	RFID-082CIP3			
Filed as Small Entity				
<b>Utility under 35 USC 111(a) Filing Fees</b>				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
Request for Continued Examination	2801	1	600	600
<b>Total in USD (\$)</b>				<b>600</b>



## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	17474053
<b>Application Number:</b>	13350835
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	1986
<b>Title of Invention:</b>	Mobile devices for commerce over unsecured networks
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh
<b>Customer Number:</b>	26797
<b>Filer:</b>	Joe Zheng
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	RFID-082CIP3
<b>Receipt Date:</b>	22-NOV-2013
<b>Filing Date:</b>	16-JAN-2012
<b>Time Stamp:</b>	03:11:29
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 600
RAM confirmation Number	8111
Deposit Account	502436
Authorized User	ZHENG, JOE
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)  
 Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)  
 Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	RCEReqTrnsAsFiled.pdf	113663 b2ee7b2926b149ff8c39003373b2fbc37684ac39	no	1

**Warnings:**

This is not a USPTO supplied RCE SB30 form.

**Information:**

2	Amendment Submitted/Entered with Filing of CPA/RCE	ResponseToFinalOA.pdf	113793 9f394bf96812cf4eca06914eafda29f1e4049624	no	9
---	--	-----------------------	--	----	---

**Warnings:**

**Information:**

3	Fee Worksheet (SB06)	fee-info.pdf	30022 cd920a8ab76a2843392f63038b493f469196d691	no	2
---	----------------------	--------------	---	----	---

**Warnings:**

**Information:**

**Total Files Size (in bytes):** 257478

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

**New Applications Under 35 U.S.C. 111**

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

**National Stage of an International Application under 35 U.S.C. 371**

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

**New International Application Filed with the USPTO as a Receiving Office**

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

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

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875			Application or Docket Number 13/350,835	Filing Date 01/16/2012	<input type="checkbox"/> To be Mailed		
ENTITY: <input type="checkbox"/> LARGE <input checked="" type="checkbox"/> SMALL <input type="checkbox"/> MICRO							
<b>APPLICATION AS FILED – PART I</b>							
(Column 1)		(Column 2)					
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)			
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A				
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A				
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A				
TOTAL CLAIMS (37 CFR 1.16(i))	17 minus 20 =	* 0	x \$30 =	0			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	* 0	x \$125 =	0			
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	0			
<b>APPLICATION AS AMENDED – PART II</b>							
(Column 1)		(Column 2)		(Column 3)			
AMENDMENT	11/22/2013	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	+ 17	Minus ** 20	= 0	x \$40 =	0	
	Independent (37 CFR 1.16(h))	+ 2	Minus *** 3	= 0	x \$210 =	0	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0	
(Column 1)		(Column 2)		(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	+	Minus **	=	x \$	=	
	Independent (37 CFR 1.16(h))	+	Minus ***	=	x \$	=	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))						
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE		
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.							
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".							
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".							
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.							
LIE /GERALDINE STANLEY/							

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**  
 If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Row 1: 13/350,835, 01/16/2012, Liang Seng Koh, RFID-082CIP3, 1986
Row 2: 26797, 7590, 11/28/2014, [EXAMINER: STANFORD, CHRISTOPHER J]
Row 3: [ART UNIT: 2887], [PAPER NUMBER]
Row 4: [NOTIFICATION DATE: 11/28/2014], [DELIVERY MODE: ELECTRONIC]

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

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

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

uspatents@sbcglobal.net

<b>Office Action Summary</b>	<b>Application No.</b> 13/350,835	<b>Applicant(s)</b> KOH ET AL.	
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887	<b>AIA (First Inventor to File) Status</b> No

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

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 11/22/2013.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_.
- 2a)  This action is **FINAL**.                      2b)  This action is non-final.
- 3)  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 4)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims\***

- 5)  Claim(s) 1-17 is/are pending in the application.  
5a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 6)  Claim(s) \_\_\_\_ is/are allowed.
- 7)  Claim(s) 1-17 is/are rejected.
- 8)  Claim(s) \_\_\_\_ is/are objected to.
- 9)  Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

\* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).

**Application Papers**

- 10)  The specification is objected to by the Examiner.
- 11)  The drawing(s) filed on \_\_\_\_ is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

**Priority under 35 U.S.C. § 119**

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

**Certified copies:**

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

\*\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)  
Paper No(s)/Mail Date \_\_\_\_.
- 3)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 4)  Other: \_\_\_\_.

**DETAILED ACTION**

***Notice of Pre-AIA or AIA Status***

1. The present application is being examined under the pre-AIA first to invent provisions.

***Priority***

2. Applicant's claim for the benefit of a prior-filed application under 35 U.S.C. 119(e) or under 35 U.S.C. 120, 121, or 365(c) is acknowledged. Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. 120 as follows:

The later-filed application must be an application for a patent for an invention which is also disclosed in the prior application (the parent or original nonprovisional application or provisional application). The disclosure of the invention in the parent application and in the later-filed application must be sufficient to comply with the requirements of 35 U.S.C. 112(a) or the first paragraph of 35 U.S.C. 112 (pre-AIA). See *Transco Products, Inc. v. Performance Contracting, Inc.*, 38 F.3d 551, 32 USPQ2d 1077 (Fed. Cir. 1994).

The disclosures of the prior-filed applications, Application No.11/534,653 and 11/739,044, fail to provide adequate support or enablement in the manner provided by 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph for one or more claims of this application. The language used in the at least claims 1 and 14 are not supported by the disclosures of Applications '653 and '044. Specifically the recitations regarding how

the processor coupled to the mobile device's memory space is configured – not the mere presence of a connection and interoperability between a processor and memory. Claims 1 and 14 recited the following limitations that are not wholly supported by the patent applications:

- a processor coupled to the memory space and configured to execute the module to perform operations including: sending to a server via the network interface an identifier identifying the application together with device information of a secure element (claim 1)
- a processor coupled to the memory space and configured to execute an embedded module to perform operations including: provisioning each of the modules with a provider that publishes the each of the modules, wherein said provisioning each of the modules with a distributor comprises: sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element (claim 14).

Firstly, Examiner acknowledges that it is known and unnecessary to disclose a processor executing instructions stored in a memory space (as argued by Applicant on pages 7-8). This claim feature is not the heart of the matter being raised here.

On page 8 of the Response dated 11/22/2013, Applicant points to application serial number 11/739,044 para [0071] and Figs. 5A & 5C as providing support for the claimed material. Examiner wishes to additionally point to para [0070-0077] and Fig. 5B as well. Applicant specifically argues “[w]hen one of the items is chosen, an identifier

identifying the chosen item together with device information of a secure element must be provided to the server providing the list, where the device information is needed to identify the mobile device choosing the identified application. Based on the identifier, an applet corresponding to the chosen item can be downloaded to the mobile device as described as 556 of Fig. 5C". Examiner acknowledges that in order for data stored within a server (such as directory server 512 or service providers servers 514 of Fig. 5A) to reach the secure element 529, and specifically the GP card manager 526, that addressing is required. Examiner contends, however that the data transmitted by one of the servers must only go in the general direction of a secure element and not specifically and/or directly to the secure element. A person of ordinary skill in the art at the time of the invention would have been aware and capable of implementing many possible addressing schemes for the system shown in Fig. 5A and the method conducted in the cited figures and paragraphs of Applicant's written disclosure. The servers need not have the address of the mobile device or the secure element, for that matter. One possible addressing scheme would mask the identity of the portable device from the third party servers and the phone address/identifier would only be known to an element of the cellular communications network. An additional scheme could be characterized by an entity within the cellular communications network 520 (Fig. 5A) sending the portable device identifier to the server as opposed to a processor within the claimed mobile device. Another scheme could be characterized by the portable device being identified to the remote servers, possibly by the mobile device's processor, but the "device identifier of a secure element" is never transmitted to the remote server as



the mobile device's processor directs any received data messages to the secure element once received from the remote servers. In this last example, the identifying device information is not "of a secure element" but rather identifying device information of the mobile device itself. These possible addressing schemes are not described within the original disclosure but would have been known, familiar, and obvious schemes to implement the claimed application provisioning. As an artisan at the time of the invention would have had many options for implementing the invention, the written description requirement necessitates that the Applicant evidence possession of the specific solution that is claimed. There is no disclosure that the processor of the mobile devices sends identifying device information of a secure element to a server together with an application identifier. Applicant clearly disclosed, in Application '044, that the mobile device is verified (para [0075]) but not the mechanism by which the device is verified. Additionally, based on the arguments presented in the Response dated 11/22/2013, Examiner acknowledges that a mobile device must identify an application for provisioning but does not necessarily identify itself to the remote server(s) as explained above. Applicant clearly establishes support for this claim language in the instant application in para [0060-0061] of the originally-filed Specifications: "At 116, the NFC device is registered with the server. Once the NFC device becomes part of the system, various services or data may be communicated to the device via the network. As part of the personalization process, the server requests device information of the SE at 118. In one embodiment, the server is configured to send a data request (e.g., a WAP PUSH) to the device." This disclosure clearly describes an addressing scheme in

which a remote server is trusted to know device identifying information directly and communicate directly with the mobile device. The priority applications lack such description and therefore lack support for the claim language.

The claims of instant application will be not receive the priority filing dates of the prior-filed parent applications. For prior art purposes, the effective filing date of the claims of the instant application will coincide with the actual filing date of 1/16/2012.

***Claim Rejections - 35 USC § 102***

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

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

4. **Claims 1-9, 13-14, and 16-17** are rejected under pre-AIA 35 U.S.C. 102(b) as being anticipated by Musfeldt et al. (US PG Pub. 2010/0291904; hereinafter Musfeldt; previously cited).

**Regarding claim 1**, Musfeldt teaches a mobile device (mobile device 150a, Fig. 1) for conducting a secured transaction (para [0017]) over a network (carrier network 180a/b & network 170, Fig. 1), the mobile device comprising: a network interface (network interface 159a, Fig. 1); an interface (interfaces for secure element embodiments such as SIM cards; para [0025]) to receive a secure element (secure element 155a, Fig. 1); a memory space (memory 152a, Fig. 1) for storing at least a module (provisioning module 154a, Fig. 1) and an application downloaded from the network ("memory and data storage device, can store data and information for

subsequent retrieval; para [0031]); a processor (processor 156a, Fig. 1) coupled to the memory space and configured to execute the module to perform operations (“TSM provisioning module 154a, 154b may comprise computer-executable program instructions or software, including a dedicated program, for facilitating mobile device application provisioning on secure elements 155a, 155b as carried out by the TSM computer 110”; para [0025, 0053-0066]) including: verifying whether the application has been provisioned (“a provisioning request can come from any of the mobile devices 150 or associated end users”; para [0054]); when said verifying indicates that the application has not been provisioned (“a provisioning request can come from any of the mobile devices 150 or associated end users”; para [0054]), sending to a server via the network interface an identifier identifying the application (“it can be determined whether the mobile device is technically capable of receiving an OTA provisioned application or capable of operating the specific application requested”; para [0056]) together with device information of a secure element (“the identity of the mobile device end user can be verified as the correct end user for receiving the mobile device application and/or associated personalization data, and/or that the mobile device is in the correct end user's possession”; para [0057]); establishing a secured channel between the secure element and the server using a key set installed on the secure element (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]),

wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device (“the requested application can be installed on the secure element of the mobile device 150para [0062]); receiving the data from the server to associate the application with the secure element (“a service provider computer 160 regarding a specific end user (e.g., as identified by name, account, or other unique identifier), the TSM computer 110 is operable to identify the end user as having a TSM-provisioned application installed”; para [0062-0065]).

**Regarding claim 2**, Musfeldt teaches the data received in the mobile device includes an application key set for the application (“facilitate management of secured keys used to securely load and delete mobile device applications on mobile device secure elements”; para [0044]), and a user interface specifically designed for the mobile device (“provide a mobile device user interface for accessing provisioned mobile device applications on each mobile device (e.g., a mobile wallet)”; para [0044]).

**Regarding claim 3**, Musfeldt teaches the mobile device is a near field communication (NFC) enabled mobile phone (“multiple service providers (e.g., card issuing banks, retailers, transit operators, etc.) need to load and manage applications (e.g., NFC-based applications, etc.) onto mobile devices supported by multiple mobile network operators”; para [0002]), and the application is an electronic purse (e-purse) (“provide a mobile device user interface for accessing provisioned mobile device applications on each mobile device (e.g., a mobile wallet)”; para [0044]), the mobile device is used to exchange secured data with another device within a near distance to conduct a transaction (para [0046,0053,0065]).

Regarding claim 4, Musfeldt teaches the secured data is being exchanged over a secured channel (para [0046,0053,0065]) between the mobile device and the another device established by the application key set (para [0046,0053,0065]).

Regarding claim 5, Musfeldt teaches the transaction is conducted without the mobile communicating with a transaction server (off-line; para [0029]).

Regarding claim 6, Musfeldt teaches said sending to a server via the network interface an identifier identifying the application together with device information of a secure element comprises: determining whether the secure element has been personalized with a Trusted Service Management (TSM) system (“it is determined whether the mobile device and/or end user associated with the mobile device has previously received a mobile device application via the TSM computer 110”; para [0060]), wherein the TSM system (TSM service manager 110, Fig. 1) is a collection of services configured to distribute and manage contactless services for customers signed up with the TSM (each stored in memories 112, Fig. 1; para [0021,0043]), and provide data exchanges among different parties to make electronic commerce possible over a wireless network (para [0021,0043]); and performing a personalization process for the secure element when above said determining determines that the secure element has not been personalized with the Trusted Service Management (TSM) system (“If it is determined at decision block 330 that the mobile device and/or the end user has not previously received a mobile device application via the TSM computer, then block 335 follows, in which the TSM computer 110 installs TSM administration software on the mobile device 150 that may be utilized to provide secured access to secure elements

and further facilitate installing, accessing, and operating TSM-provisioned applications”; para [0061]), wherein the secure element when personalized establishes a security platform for the application to run on the mobile device (para [0061]).

Regarding claim 7, Musfeldt teaches the personalization process comprises: causing the mobile device to initiate data communication with a server in the TSM system (para [0061]); retrieving device information of the secure element in responding to a request from the TSM server (“the identity of the mobile device end user can be verified as the correct end user for receiving the mobile device application and/or associated personalization data, and/or that the mobile device is in the correct end user's possession”; para [0057]) after the TSM server determines that the secure element is registered therewith (“as part of the registration process, the TSM computer 110 can be configured to store unique identifiers of the mobile device, its secure element, and/or the end users for subsequent processing”; para [0057-0058]), wherein the device information is a sequence of characters uniquely identifying the secure element (“TSM computer 110 can identify the end user by the secure element identifier (e.g., the ICCID, IMSI, etc. associated with the secure element)”; para [0065]); receiving at least a set of keys from the TSM server, wherein the keys are generated in the TSM server in accordance with the device information of the secure element (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]); and

storing the set of keys in the secure element to facilitate a subsequent transaction with the secure element in the computing device (para [0035,0042,0044,0059]).

**Regarding claim 8**, Musfeldt discloses the device information includes an identifier of the secure element (“the secure element identifier (e.g., the ICCID, IMSI, etc. associated with the secure element)”; para [0065]), manufacturer information (para [0065]), and batch number. The ICCID standard is laid out in ISO/IEC 7812 and includes the issuer identification number, the individual account identification, and the international mobile subscriber identity which identified the operator networks within which the communication is designed to occur.

**Regarding claim 9**, Musfeldt teaches the secure element is embedded in the mobile device and integrated with the mobile device via the interface (Fig. 1; para [0025]).

**Regarding claim 13**, Musfeldt teaches part of the data is used to facilitate the server to remotely manage the application (para [0065]).

**Regarding claim 14**, Musfeldt teaches a mobile device (mobile device 150a, Fig. 1) for conducting a secured transaction (para [0017]) over a network (carrier network 180a/b & network 170, Fig. 1), the mobile device comprising: a network interface (network interface 159a, Fig. 1); a secure element (secure element 155a, Fig. 1); a memory space (memory 152a, Fig. 1) for storing various modules (provisioning module 154a used for many provisioning processes, Fig. 1; para [0025]) each of the modules configured to provide an application of service to a user of the mobile device (“memory and data storage device, can store data and information for subsequent retrieval; para

[0031]); a processor (processor 156a, Fig. 1) coupled to the memory space and configured to execute the module to perform operations (“TSM provisioning module 154a, 154b may comprise computer-executable program instructions or software, including a dedicated program, for facilitating mobile device application provisioning on secure elements 155a, 155b as carried out by the TSM computer 110”; para [0025]) including: provisioning each of the modules with a provider (service providers 160a, Fig. 1) that publishes the each of the modules (para [0053-0066]), wherein said provisioning each of the modules with a distributor comprises sending to a server via the network interface an identifier identifying the application (“it can be determined whether the mobile device is technically capable of receiving an OTA provisioned application or capable of operating the specific application requested”; para [0056]) together with device information of a secure element (“the identity of the mobile device end user can be verified as the correct end user for receiving the mobile device application and/or associated personalization data, and/or that the mobile device is in the correct end user's possession”; para [0057]); establishing a secured channel between the secure element and the server using a key set installed on the secure element (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]), wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device (“the requested application can be installed



on the secure element of the mobile device 150 para [0062]); receiving the data from the server to associate the each of the modules with the secure element (“a service provider computer 160 regarding a specific end user (e.g., as identified by name, account, or other unique identifier), the TSM computer 110 is operable to identify the end user as having a TSM-provisioned application installed”; para [0062-0065]) wherein the data includes a set of keys generated for the each of the modules (“additional space may be provisioned via the MNO, secured keys may be provided (e.g., by the TSM or by the MNO), privileges associated with the secure element may be added or changed, and/or the mobile device may be initialized for utilizing the mobile device application (e.g., initialized for NFC transactions, etc.)”; para [0035,0042,0059]).

Regarding claim 16, Musfeldt teaches the mobile device includes a display configured to display (para [0026]) a user interface showing some of the modules that are still provisioned and active, each of the modules is configured to show another user interface particularly designed for the display of the mobile device when the each of the modules is activated by a user (para [0044]).

Regarding claim 17, Musfeldt teaches the secure element must be personalized before each of the modules is provisioned (step 330-345, Fig. 3), each of the provisioned modules is associated with the personalized secure element and a key set generated in accordance with a key set of the secure element (para [0053-0066]).

***Claim Rejections - 35 USC § 103***

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

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 10 and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over Musfeldt as applied to claim 7, and further in view of Jain et al. (US PG Pub. 2009/0069051; hereinafter Jain; previously cited).

**Regarding claim 10**, Musfeldt discloses the secure element is a software module installed in a secure memory space ("the secure elements 155a, 155b may refer to any computer-readable storage in the memory 152"; para [0025]).

Musfeldt discloses the claimed invention as cited above though does not explicitly disclose: the secure element is a software module installed in a secure memory space only accessible by a distributor of the secure element.

Jain discloses "the memory 612 may include secure portions designed to be accessible only by the service provider" (para [0066]).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to provide portions of memory only accessible by a service provider as taught by Jain with the system as disclosed by Musfeldt. The motivation would have been to maintain data within a memory that may only be accessed by trusted entities (para [0066]).

Regarding claim 11, Musfeldt discloses some components are updated when the secure element is upgraded by the distributor (para [0065]).

7. Claims 12 and 15 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Musfeldt, as applied to claims 1 and 14, and further in view of Shenfield et al. (US PG Pub. 2006/0168355; hereinafter Shenfield; previously cited).

Regarding claims 12 and 15, Musfeldt teaches receiving a message from a distributor of the application (para [0065]), the message including an identifier identifying the application (para [0035-0044]); verifying that the message is indeed from the distributor (“provide a communications gateway via a respective carrier network for OTA provisioning of mobile device applications; provide a mobile device user interface for accessing provisioned mobile device applications on each mobile device (e.g., a mobile wallet); facilitate management of secured keys used to securely load and delete mobile device applications on mobile device secure elements”; para [0044]); disassociating the application with the secure element (remove an application; para [0065]); and notifying the distributor that the application installed in the mobile device is no longer active lifecycle management module 127 can be configured to facilitate tracking the status of users' mobile devices and the status of previously provisioned applications. For example, the lifecycle management module 127 can be configured to maintain inventories of various types of mobile devices, associated secure elements and the state of the secure elements and applications (active, locked, unlocked, terminated), which may be used to track the status of applications and mobile devices and to

communicate with MNOs and/or service providers regarding the provisioned applications”; para [0038,0064]).

Musfeldt discloses the claimed invention as cited above though does not explicitly disclose disassociating the application with the secure element in responding to a confirmation.

Shenfield discloses lifecycle maintenance by service providers including removing applications at the request of the service provider (para [0067]).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to provide portions of memory only accessible by a service provider as taught by Shenfield with the system as disclosed by Musfeldt. The motivation would have been to allow the service providers to remove provisioned applications (para [0067]).

### ***Response to Arguments***

8. Applicant's arguments filed 11/22/2013 have been fully considered but they are not persuasive.

9. The arguments do not address the art-based rejections but rather focus on the issues concerning priority claims. The Priority section above addresses the arguments presented in the Response.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER STANFORD whose telephone number

Art Unit: 2887

is (571)270-3337. The examiner can normally be reached on Monday through Fridays, 8am-5pm PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHRISTOPHER STANFORD/  
Primary Examiner, Art Unit 2887

**EAST Search History**

**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S72	2	"13158456"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 15:20
S71	2	"20100304819" and (wag\$3 or credit or transfer or transferr\$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 15:03
S70	2	"20100304819"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 14:57
S69	119	S67 and (card or memory or storage or (security or secure) element or smartcard) same (download\$3 or upload\$3 or install\$3 or installation or personaliz\$3 or personalization) near3 (application or applet) same (cryptograph\$2 or encrypt\$3 or decrypt\$3 or private near2 key or public near2 key) with (server or service provider)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 11:00
S68	52	S67 and("near" field communicat\$3 or nfc or "18093") with (application or applet) and (card or memory or storage or (security or secure) element or smartcard) same (download\$3 or upload\$3 or install\$3 or installation or personaliz\$3 or personalization) near3 (application or applet) same (cryptograph\$2 or encrypt\$3 or decrypt\$3 or private near2 key or public near2 key) with (server or service provider)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 11:00
S67	69083	(( G06F21/34 OR G07F7/1008 OR G06Q20/341 OR G06Q20/3674 OR G06Q20/382 OR G06Q20/20 OR G06Q20/32 OR G06Q20/367 or G06Q20/3672).CPC. )	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 11:00
S66	39	(S61 or S62)	US-PGPUB; USPAT; USOCR; FPRS;	ADJ	ON	2014/11/21 10:57

			EPO; JPO			
S65	1	(S61 or S62) and (download\$3 or upload\$3 or install\$3 or installation or personaliz\$3 or personalization) near3 (application or applet) same (cryptograph\$2 or encrypt\$3 or decrypt\$3 or private near2 key or public near2 key)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 10:41
S64	0	(S61 or S62) and (download\$3 or upload\$3 or install\$3 or installation or personaliz\$3 or personalization) near3 (application or applet) same (cryptograph\$2 or encrypt\$3 or decrypt\$3 or private near2 key or public near2 key) with (server or service provider)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 10:41
S63	0	(S61 or S62) and (card or memory or storage or (security or secure) element or smartcard) same (download\$3 or upload\$3 or install\$3 or installation or personaliz\$3 or personalization) near3 (application or applet) same (cryptograph\$2 or encrypt\$3 or decrypt\$3 or private near2 key or public near2 key) with (server or service provider)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 10:40
S62	35	("20010049785"   "20020111918"   "20020152390"   "20040059921"   "20040059923"   "20050171898"   "20050187782"   "20050240778"   "20050273609"   "20060080548"   "20060080549"   "20060136735"   "20060265743"   "20070019622"   "20070022058"   "20070033149"   "20070092112"   "20070219926"   "20080065885"   "20090164799"   "20090191846"   "20100117791"   "20110179284"   "20110238578"   "5355413"   "6269348"   "6581042"   "7206847"   "7392941"   "7512567"   "7543156"   "7844082"   "7877605"   "7917769").PN. OR ("8417643").URPN.	US- PGPUB; USPAT; USOCR	ADJ	ON	2014/11/21 10:39
S61	26	("20040059923"   "20050171898"   "20050240778"   "20050273609"   "20060265743"   "20070019622"   "20070022058"   "20070033149"   "20070092112"   "20070219926"   "20080065885"   "20090164799"   "20090191846"   "20100117791"   "20110179284"   "6269348"   "6581042"   "7512567"   "7543156"   "7844082"   "7877605"   "7917769").PN. OR ("8108318").URPN.	US- PGPUB; USPAT; USOCR	ADJ	ON	2014/11/21 10:39
S60	5	"12339850"	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 10:38
S59	71	("near" field communicat\$3 or nfc or "18093") with (application or applet) and (card or memory or storage or (security or secure) element or smartcard) same	US- PGPUB; USPAT; USOCR;	ADJ	ON	2014/11/21 10:27

EAST Search History


		(download\$3 or upload\$3 or install\$3 or installation or personaliz\$3 or personalization) near3 (application or applet) same (cryptograph\$2 or encrypt\$3 or decrypt\$3 or private near2 key or public near2 key) with (server or service provider)	FPRS; EPO; JPO			
S58	337	("near" field communicat\$3 or nfc or "18093") and (card or memory or storage or (security or secure) element or smartcard) same (download\$3 or upload\$3 or install\$3 or installation or personaliz\$3 or personalization) near3 (application or applet) same (cryptograph\$2 or encrypt\$3 or decrypt\$3 or private near2 key or public near2 key)	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2014/11/21 07:20

**EAST Search History (Interference)**

< This search history is empty >

**11/ 24/ 2014 7:04:02 AM**



<b><i>Index of Claims</i></b> 	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887


✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant		<input type="checkbox"/> CPA		<input type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47			
CLAIM		DATE							
Final	Original	03/15/2013	08/13/2013	11/21/2014					
	1	✓	✓	✓					
	2	✓	✓	✓					
	3	✓	✓	✓					
	4	✓	✓	✓					
	5	✓	✓	✓					
	6	✓	✓	✓					
	7	✓	✓	✓					
	8	✓	✓	✓					
	9	✓	✓	✓					
	10	✓	✓	✓					
	11	✓	✓	✓					
	12	✓	✓	✓					
	13	✓	✓	✓					
	14	✓	✓	✓					
	15	✓	✓	✓					
	16	✓	✓	✓					
	17	✓	✓	✓					

<b>Search Notes</b>  	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/34 G07F7/1008 G06Q20/341 G06Q20/3674 G06Q20/382 G06Q20/20 G06Q20/32 G06Q20/367 G06Q20/3672	11/21/14	CS

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	379,380,451,492	3/14/13	CS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor, Assignee Search	3/14/13	CS
Parent Case Search	3/14/13	CS
Text search (see search history report)	3/14/13	CS
NPL Search	3/14/13	CS
Text search (see search history report)	8/13/13	CS
Text search (see search history report)	11/21/14	CS

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

	/CHRISTOPHER STANFORD/ Primary Examiner.Art Unit 2887
--	--

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**Applicant(s):** Liang Seng Koh et al  
**Title:** Mobile devices for commerce over unsecured networks  
**Serial No.:** 13/350,835  
**Filing Date:** 01/16/2012  
**Examiner:** Chris Stanford  
**Group Art Unit:** 2887  
**Docket No.:** RFID-081CIP3

---

February 23, 2015

Mail Stop: No-Fee Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Response to First OA (RCE)**

Dear Sir:

In response to Office Action dated 11/28/2014, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

**AMENDMENTS TO THE CLAIMS** are reflected in the listing of claims which begins on page 2 of this Response.

**REMARKS/ARGUMENTS** begin on page 7 of this Response.

## AMENDMENTS TO THE CLAIMS

Please amend Claim 1 as follows:

1. *(Currently amended)* A mobile device for conducting a secured transaction over a network, the mobile device comprising:
  - a network interface;
  - an interface to receive a secure element;
  - a memory space for storing at least a module and an application downloaded from the network;
  - a processor coupled to the memory space and configured to execute the module to perform operations including:
    - sending to a server via the network interface an identifier identifying the application together with device information of a secure element;
    - establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device; and
    - receiving the data from the server to associate the application with the secure element, wherein the application functions in conjunction with the secure element in mobile device.
2. *(Original)* The mobile device as recited in claim 1, wherein the data received in the mobile device includes an application key set for the application, and a user interface specifically designed for the mobile device.
3. *(Original)* The mobile device as recited in claim 2, wherein the mobile device is a near field communication (NFC) enabled mobile phone, and the application is an electronic purse (e-purse), the mobile device is used to exchange secured data with another device within a near distance to conduct a transaction.

4. (*Original*) The mobile device as recited in claim 3, wherein the secured data is being exchanged over a secured channel between the mobile device and the another device established by the application key set.
5. (*Original*) The mobile device as recited in claim 4, wherein the transaction is conducted without the mobile device communicating with a transaction server.
6. (*Previously amended*) The mobile device as recited in claim 1, wherein said sending to a server via the network interface an identifier identifying the application together with device information of a secure element comprises:
  - determining whether the secure element has been personalized with a Trusted Service Management (TSM) system, wherein the TSM system is a collection of services configured to distribute and manage contactless services for customers signed up with the TSM, and provide data exchanges among different parties to make electronic commerce possible over a wireless network; and
  - performing a personalization process for the secure element when the secure element has not been personalized with the Trusted Service Management (TSM) system, wherein the secure element when personalized establishes a security platform for the application to run on the mobile device.
7. (*Original*) The mobile device as recited in claim 6, wherein the personalization process comprises:
  - causing the mobile device to initiate data communication with a server in the TSM system;
  - retrieving device information of the secure element in responding to a request from the TSM server after the TSM server determines that the secure element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element;

receiving at least a set of keys from the TSM server, wherein the keys are generated in the TSM server in accordance with the device information of the secure element; and  
storing the set of keys in the secure element to facilitate a subsequent transaction with the secure element in the computing device.

8. *(Original)* The mobile device as recited in claim 7, wherein the device information includes an identifier of the secure element, manufacturer information and a batch number.
9. *(Original)* The mobile device as recited in claim 7, wherein the secure element is embedded in the mobile device and integrated with the mobile device via the interface.
10. *(Original)* The mobile device as recited in claim 7, wherein the secure element is a software module installed in a secure memory space only accessible by a distributor of the secure element.
11. *(Original)* The mobile device as recited in claim 10, wherein some components are updated when the secure element is upgraded by the distributor.
12. *(Original)* The mobile device as recited in claim 1, wherein the operations further comprises:
  - receiving a message from a distributor of the application, the message including an identifier identifying the application;
  - verifying that the message is indeed from the distributor;
  - disassociating the application with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and
  - notifying the distributor that the application installed in the mobile device is no longer active.

13. *(Original)* The method as recited in claim 8, wherein part of the data is used to facilitate the server to remotely manage the application.
14. *(Previously amended)* A mobile device for conducting a secured transaction over a network, the mobile device comprising:
- a network interface;
  - a secure element;
  - a memory space for storing various modules downloaded from the network, each of the modules configured to provide an application or a service to a user of the mobile device;
  - a processor coupled to the memory space and configured to execute an embedded module to perform operations including:
    - provisioning each of the modules, wherein said provisioning each of the modules with a distributor comprises:
      - sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element;
      - establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the each of the modules to function as designed on the mobile device; and
      - receiving the data from the server to associate the each of the modules with the secure element, wherein the data includes a set of keys generated for the each of the modules.
15. *(Original)* The mobile device as recited claim 14, wherein the operations further comprise:
- receiving a message from a distributor of one of the modules, the message including an identifier identifying the one of the modules;
  - verifying that the message is authenticated;

disassociating the one of the modules with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and notifying the distributor that the one of the modules installed in the mobile device is no longer active.

16. *(Original)* The mobile device as recited claim 14, wherein the mobile device includes a display configured to display a user interface showing some of the modules that are still provisioned and active, each of the modules is configured to show another user interface particularly designed for the display of the mobile device when the each of the modules is activated by a user.

17. *(Original)* The mobile device as recited claim 16, wherein the secure element must be personalized before each of the modules is provisioned, each of the provisioned modules is associated with the personalized secure element and a key set generated in accordance with a key set of the secure element.



## REMARKS

Claims 1 - 17 examined again. In the Office Action dated 11/28/2014, Claims 1-9, 13-14, and 16-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Musfeldt et al. (US PG Pub. 2010/0291904, hereinafter Musfeldt), Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Musfeldt as applied to claim 7, and further in view of Jain et al. (US PG Pub. 2009/0069051, hereinafter Jain), Claims 12 and 15 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Musfeldt, as applied to claims 1 and 14, and further in view of Shenfield et al. (US PG Pub. 2006/0168355; hereinafter Shenfield).

In the foregoing amendments, Claim 1 has been amended to clarify what is being claimed. No new matters have been introduced. Reconsideration of pending claims 1-17 is respectfully requested.

### Interview Summary

The Applicant appreciates the Examiner for granting a telephonic interview that took place on 02/17/2015. Mr. Examiner Chris Stanford, Applicant Liang Seng Koh and the undersigned Joe Zheng participated in the interview. No cited references were discussed. The interview was focused on the priority issue whether Claim 1 shall be given the priority dates of the parent applications Application No.11/534,653 and 11 /739,044. Applicant has presented appropriate paragraphs in 11/739,044 to show the full support of Claim 1 in 11/739,044. No agreement was reached. The Examiner will consider the evidences and remarks after a formal response is filed.

### Priority Issue

On page 2, section 2 of this Office Action, the Examiner alleges that the instant application has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 USC 120. In particular, the Examiner states:

Claims 1 and 14 recite the following limitations that are not wholly supported by the patent applications (Application No.11 /534,653 and 11 /739,044,):

- a processor coupled to the memory space and configured to execute the module to perform operations including: sending to a server via the network interface an identifier identifying the application together with device information of a secure element (claim 1)
- a processor coupled to the memory space and configured to execute an embedded module to perform operations including: provisioning each of the modules with a provider that publishes the each of the modules, wherein said provisioning each of the modules with a distributor comprises: sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element (claim 14).

The Applicant wishes to point out that, per MPEP 2164.01, a patent application does not need to teach, and preferably omits, what is well known in the art. *In re Buchner*, 929 F.2d 660, 661, 18 USPQ2d 1331, 1332 (Fed. Cir. 1991); *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1463, 221 USPQ 481, 489 (Fed. Cir. 1984). It is a common knowledge (well known to those skilled in the art) that a microprocessor or processor is often coupled to a memory space (e.g., a RAM) to execute software code (e.g., firmware) therein to perform certain functions. Specifically, a mobile device such as the computing device 100 of FIG. 1A has to have a processor and a memory space to store necessary code for the processor to execute as such the mobile device can function as described. In fact, US Application 11/739,044 describes in paragraph [0009] a memory space associated with microprocessor circuitry. Accordingly, the Applicant submits the recitation of “a processor coupled to the memory space and configured to execute the module to perform operations” in Claim 1 is not a unique feature to the invention being claimed but makes the claim technically and logically understandable.

On Page 3 of the Office Action, the Examiner states "*Examiner acknowledges that it is known and unnecessary to disclose a processor executing instructions stored in a memory space (as argued by Applicant on ages 7-8). This claim feature is not the heart of the matter being raised here*". Accordingly, the Applicant assumes that the Examiner has withdrawn the rejection of receiving the benefit of an earlier

filing date under 35 USC 120 for "a processor coupled to the memory space and configured to execute the module to perform operations" recited in Claim 1.

Regarding the 2nd allegation that "sending to a server via the network interface an identifier identifying the application together with device information of a secure element (claim 1)" is not supportive in the two parent applications this instant application depends upon, the Applicant wishes to refer the Examiner to US App. Ser. No.: 11/739,044, paragraph [0075], where it specifically describes "a unique SAM ID based on the unique identifier of the underlying secured element". The Applicant respectfully points out that the Examiner's statement on Page 5 of the Office Action "There is no disclosure that the processor of the mobile devices sends identifying device information of a secure element to a server together with an application identifier" seems to be unsupported.

Specifically, as described in paragraph [0075], an e-purse applet (i.e., application applet 527) is downloaded from an applet repository 504 and installed onto a secured element 529. The e-purse has to be personalized with the secure element 529 before it can function on a mobile device (e.g., the portable device 202 of FIG. 2). Paragraph [0075] lists some exemplary items a through g that have to be sent to the personalization server, and item a explicitly describes that the unique identifier of the underlying secured element is sent to the server, which supports "sending to a server via the network interface an identifier identifying the application together with device information of a secure element" as recited in Claim 1 of this instant application. To further clarify that the server is indeed to personalize such an e-purse, paragraph [0050] describes "In operation, a security domain is used for establishing a secured channel between a personalization application server and the e-purse applet". Accordingly, the Applicant submits the recitation identified by the Examiner is fully supported in US App. Ser. No.: 11/739,044.

The Above shows that Claim 1 satisfies the requirement of 35 USC 112 in '653 and '044. Accordingly, the Applicant submits the two cited references Musfeldt and Jain as cited by the Examiner in the Office Action cannot be used as qualified

references to reject Claims 1 -13 as the filing dates of these two references are AFTER the priority dates of this instant application.

Regarding the 3rd allegation that “*provisioning each of the modules with a provider that publishes the each of the modules, wherein said provisioning each of the modules with a distributor comprises: sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element (claim 14)*” is not supportive in the two parent applications this instant application depends upon, the Applicant wishes to refer the Examiner to US App. Ser. No.: 11/739,044, paragraph [0071] - [0075] and FIG. 5C. As explicitly described in [0072], the chosen item, namely, an application applet by the identifier is downloaded. The downloaded applet must be personalized or provisioned before it can be used as graphically shown as 558 of FIG. 5C in US App. Ser. No.: 11/739,044. The second part of this particular recitation is substantially similar to the 2<sup>nd</sup> allegation which has been shown above the full support thereof in US App. Ser. No.: 11/739,044.

Accordingly, Claim 14 satisfies the requirement of 35 USC 112 in '653 and '044. Accordingly, the Applicant submits these two cited references Musfeldt and Jain as cited by the Examiner in the Office Action cannot be used as qualified references to reject Claims 14 -17 as the filing dates of these two references are AFTER the priority dates of this instant application.

In view of the above amendments and remark, the Applicant believes that Claims 1 - 17 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)777-8873.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", Feb. 23, 2015. e-filed.

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng

Reg.: No. 39,450

<b>Electronic Acknowledgement Receipt</b>	
<b>EFS ID:</b>	21572066
<b>Application Number:</b>	13350835
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	1986
<b>Title of Invention:</b>	Mobile devices for commerce over unsecured networks
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh
<b>Customer Number:</b>	26797
<b>Filer:</b>	Joe Zheng
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	RFID-082CIP3
<b>Receipt Date:</b>	23-FEB-2015
<b>Filing Date:</b>	16-JAN-2012
<b>Time Stamp:</b>	15:51:14
<b>Application Type:</b>	Utility under 35 USC 111(a)

**Payment information:**

Submitted with Payment	no
------------------------	----

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	ResponseTo1stOARCE.pdf	130968 de10591f510aba82ba6b2f3c67bd1b32f5e8cc7	no	11

**Warnings:**

**Information:**

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

**New Applications Under 35 U.S.C. 111**

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

**National Stage of an International Application under 35 U.S.C. 371**

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

**New International Application Filed with the USPTO as a Receiving Office**

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes application details for LogicPatents, LLC and examination information for STANFORD, CHRISTOPHER J.

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

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

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

uspatents@sbcglobal.net



<b>Office Action Summary</b>	<b>Application No.</b> 13/350,835	<b>Applicant(s)</b> KOH ET AL.	
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887	<b>AIA (First Inventor to File) Status</b> No

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

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1)  Responsive to communication(s) filed on 2/23/2015.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
- 2a)  This action is **FINAL**.                      2b)  This action is non-final.
- 3)  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
- 4)  Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims\***

- 5)  Claim(s) 1-17 is/are pending in the application.  
5a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 6)  Claim(s) \_\_\_\_\_ is/are allowed.
- 7)  Claim(s) 1-17 is/are rejected.
- 8)  Claim(s) \_\_\_\_\_ is/are objected to.
- 9)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

\* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).

**Application Papers**

- 10)  The specification is objected to by the Examiner.
- 11)  The drawing(s) filed on \_\_\_\_\_ is/are: a)  accepted or b)  objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

**Priority under 35 U.S.C. § 119**

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

**Certified copies:**

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

\*\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1)  Notice of References Cited (PTO-892)
- 2)  Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 3)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 4)  Other: \_\_\_\_\_.

**DETAILED ACTION**

***Notice of Pre-AIA or AIA Status***

1. The present application is being examined under the pre-AIA first to invent provisions.

***Priority***

2. The arguments asserting that support for the claims of the instant application is present in SN 11/739,044 are persuasive. The effective filing date of claims 1, 14, and dependents thereof will be 4/23/2007.

3. Examiner is most persuaded by the separate disclosures of sending an identifier identifying an application to a server and sending device information to a secure element to a server within the same general purpose/function of the disclosed mobile device. The disclosure of '044 does not support a particularly narrow interpretation of "sending ... together with" but it can be said that a person of ordinary skill in the art could point to features of the '044 disclosure for evidence of Applicant's possession of broadly sending the application identifier and device information "together". Examiner notes that "sending ... an identifier... together with device information" will be interpreted as having no finite or procedural limits on the proximity of the information being sent. There is no limit, necessarily, on the particular module, program, or hardware device utilized to send the information. There is no limit, necessarily, on whether the two types of information are sent in the same packet as a response or

simply as separate functions of the device. That language will be interpreted as broadly as is permissible by the plain meaning of the constituent terms while still being interpreted in the context of the claim language. As long as a processor of prior art is capable of sensing an application identifier and device information to a server, then it will held that the prior art disclosure anticipates the claimed sending functionality.

***Response to Amendment***

4. Receipt is acknowledged of the amendment filed 2/23/2015. Claim 1 is amended and claims 1-17 are currently pending.

***Claim Rejections - 35 USC § 103***

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

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 1-17** are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over PG Pub. 2005/0187873 to Labrou et al. (hereinafter Labrou) in view of US PG Pub. 2008/0006685 to Rackley et al. (hereinafter Rackley).

**Regarding claims 1 and 14**, Labrou discloses a mobile device for conducting a secured transaction over a network (para [0019,0042]), the mobile device comprising: a network interface ("mobile phone 106 can be an Internet enabled, according to known

techniques, mobile phone”; para [0042]); an interface to receive a secure element (“an authentic mobile payment software 108 can be installed or provided for a mobile phone 106 via mobile phone removable/installable (e.g., smart card) and/or embedded computer readable media, embedded in a mobile phone computing processor, via an emailed download link, emailed attachment, etc.”; para [0046]); a memory space for storing at least a module and an application downloaded from the network (para [0042,0052-0059]); a processor coupled to the memory space and configured to execute the module to perform operations (para [0042,0052-0059]) including: sending to a server via a network interface an identifier identifying the application together with device information of a secure element (“one is asked for a phone number of the mobile phone to be used for mobile phone cashless money payments”; para [0052-0055]); establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device (“the activation code is a number (for easier user entry) and used as a one-time password that encrypts the UPTF-related initialization parameters of the downloaded software 108, so that if a third party attacker intercepts the software while in transit, the attacker cannot have access to the device-specific initialization parameters”; para [0052-0059]); and receiving the data from the server to associate the application with the secure element wherein the application functions in conjunction with the secure element in mobile device (para [0052-0059]).

Labrou discloses the claimed invention as cited above though does not explicitly disclose that the application and the mobile device are identified via a network interface of the mobile device itself. Labrou clearly discloses that the mobile phone to which the mobile wallet application is downloaded may be embodied as an internet-enabled phone. Furthermore, the mobile wallet application is disclosed as, in part, a web browser interface. Labrou, however, only ever explicitly states that a user's "personal computer" is used to submit the mobile device identifier and initiate the mobile wallet download onto the mobile device. It would stand that a person of ordinary skill in the art, in light of Labrou alone, would find the implementation of the mobile wallet download *by* the internet-enabled mobile device itself an obvious variant.

Rackley discloses securely downloading a mobile wallet application with a mobile device itself ("This registration is completed via the user web site interface 154 either through a computer 140 with a internet connection, or through a mobile device 15 that has Internet access capabilities" & "alternatively directly downloaded via the wireless network into the mobile device for situations where a mobile device is capable of direct application download"; para [0194,0254-0262])

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to use a mobile device to register the device for application downloading and personalization as taught by Rackley with the system as disclosed by Labrou. The motivation would have been to eliminate extra steps and devices that are otherwise necessary when a separate personal computer is required to register and download an application to a mobile device.

Regarding claim 14, the mere duplication of the steps for multiple modules would have been obvious to one of ordinary skill in the art. A client device, as disclosed by Labrou and Rackley could have multiple mobile wallet applications and/or accounts requiring more than one module. The motivation for duplicating the download and personalization steps would have been to provide more than one mobile wallet functionality.

**Regarding claim 2**, Labrou discloses the data received in the mobile device includes an application key set for the application (para [0052-0059]), and a user interface specifically designed for the mobile device (applet browser; para [0051-0059]).

**Regarding claim 3**, Labrou discloses the mobile device is a near field communication (NFC) enabled mobile phone (para [0070]), and the application is an electronic purse (e-purse) (abstract & para [0051-0059]), the mobile device is used to exchange secured data with another device within a near distance to conduct a transaction (para [0070]).

**Regarding claim 4**, Labrou discloses the secured data is being exchanged over a secured channel between the mobile device and the another device established by the application key set (para [0042,0061,0066]).

**Regarding claim 5**, Labrou discloses the transaction is conducted without the mobile device communicating with a transaction server (Fig. 3; para [0069-0070]).

**Regarding claim 6**, Labrou discloses said sending to a server via the network interface an identifier identifying the application together with device information of a secure element comprises: determining whether the secure element has been

personalized with a Trusted Service Management (TSM) system (para [0052-0059]), wherein the TSM system is a collection of services configured to distribute and manage contactless services for customers signed up with the TSM (para [0052-0059]), and provide data exchanges among different parties to make electronic commerce possible over a wireless network (para [0042,0052-0061]); and performing a personalization process for the secure element when the secure element has not been personalized with the Trusted Service Management (TSM) system, wherein the secure element when personalized establishes a security platform for the application to run on the mobile device (para [0052-0059]).

**Regarding claim 7**, Labrou discloses the personalization process comprises: causing the mobile device to initiate data communication with a server in the TSM system (para [0052-0059]); retrieving device information of the secure element in responding to a request from the TSM server after the TSM server determines that the secure element is registered therewith (para [0052-0059]), wherein the device information is a sequence of characters uniquely identifying the secure element (phone number; para [0052-0059]) receiving at least a set of keys from the TSM server, wherein the keys are generated in the TSM server in accordance with the device information of the secure element (para [0042,0061,0066]); and storing the set of keys in the secure element to facilitate a subsequent transaction with the secure element in the computing device (para [0042,0061,0066]).

**Regarding claim 8**, Labrou discloses the device information includes an identifier of the secure element, manufacturer information and a batch number (para [0042]).

**Regarding claim 9**, Labrou discloses the secure element is embedded in the mobile device and integrated with the mobile device via the interface (“an authentic mobile payment software 108 can be installed or provided for a mobile phone 106 via mobile phone removable/installable (e.g., smart card) and/or embedded computer readable media, embedded in a mobile phone computing processor, via an emailed download link, emailed attachment, etc.”; para [0046]).

**Regarding claim 10**, Labrou discloses the secure element is a software module installed in a secure memory space only accessible by a distributor of the secure element (accessible via pins, keys, and other encryption means; para [0042,0051-0061]).

**Regarding claim 11**, Labrou discloses some components are updated when the secure element is upgraded by the distributor (para [0042,0051-0061]).

**Regarding claims 12 and 15**, Labrou discloses the claimed invention as cited above though does not explicitly disclose the operations further comprises: receiving a message from a distributor of the application, the message including an identifier identifying the application; verifying that the message is indeed from the distributor; disassociating the application with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the



distributor; and notifying the distributor that the application installed in the mobile device is no longer active.

Rackley discloses receiving a message from a distributor of the application, the message including an identifier identifying the application; verifying that the message is indeed from the distributor; disassociating the application with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and notifying the distributor that the application installed in the mobile device is no longer active (para [0209,0236,0264]). Not only does Rackley disclose disassociating the mobile wallet account from client device, but all demographic information stored can be rendered inaccessible. A person of ordinary skill in the art, in light of Rackley's entire disclosure and the portions specifically disclosing deletion of a mobile wallet application would have found the claimed steps to be an obvious and predictable variant over prior art.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to delete an application as taught by Rackley with the system as disclosed by Labrou. The motivation would have been to prevent misuse of mobile wallet functionality if a client device is stolen or lost (para [0264]).

**Regarding claim 13**, Labrou discloses part of the data is used to facilitate the server to remotely manage the application (keys; para [0042,0051-0061]).

**Regarding claim 16**, Labrou discloses the mobile device includes a display configured to display a user interface showing some of the modules that are still provisioned and active, each of the modules is configured to show another user

interface particularly designed for the display of the mobile device when the each of the modules is activated by a user (Fig. 7A).

**Regarding claim 17**, Labrou discloses the secure element must be personalized before each of the modules is provisioned (para [0042,0051-0061]), each of the provisioned modules is associated with the personalized secure element and a key set generated in accordance with a key set of the secure element (para [0042,0051-0061]).

### ***Response to Arguments***

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

### ***Conclusion***

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US PG Pub. 2004/0039919 to Takayama et al. discloses downloading a mobile wallet and key application through secure communications; US PG Pub. 2007/125838 to Law et al. discloses a wallet token with cryptographic communications and locally stored keys;

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER STANFORD whose telephone number is (571)270-3337. The examiner can normally be reached on Monday through Fridays, 8am-5pm PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHRISTOPHER STANFORD/  
Primary Examiner, Art Unit 2887

<b>Notice of References Cited</b>	Application/Control No. 13/350,835	Applicant(s)/Patent Under Reexamination KOH ET AL.	
	Examiner CHRISTOPHER STANFORD	Art Unit 2887	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-2004/0039919 A1	02-2004	Takayama et al.	713/180
*	B US-2005/0187873 A1	08-2005	Labrou et al.	705/040
*	C US-2007/0125838 A1	06-2007	Law et al.	235/379
*	D US-2008/0006685 A1	01-2008	Rackley III et al.	235/379
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			

**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

**NON-PATENT DOCUMENTS**

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

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

**EAST Search History**

**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S91	1	"13294791"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 13:29
S90	1	"20110290886"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 13:23
S89	1	"20130342887"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 12:42
S88	22	rackley.inv. and @ay<"2007" and wallet	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 12:29
S87	44	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3 or secur\$3 or safe\$2) near3 (session or communicat\$3 or channel) with (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) near3 (applet or application or (e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse or program or software) and (phone or cell or cellular or telephone or communication adj2 (device or apparatus) or pda) with ((e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse) and @ay<"2007"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 10:16
S86	42	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) same (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) with (applet or application or (e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse or program or software) same ((e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse)and (phone or cell or cellular or telephone or communication adj2 (device or apparatus) or pda) with ((e or electronic or digital) adj2 (purse or wallet) or	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 10:10

		ewallet or epurse) and @ay<"2007"				
S85	121	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) same (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) with (applet or application or (e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse or program or software) and (phone or cell or cellular or telephone or communication adj2 (device or apparatus) or pda) with ((e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse) and @ay<"2007"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 10:05
S84	99	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) same (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) with (applet or application or (e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse or program or software) same ((e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse) and @ay<"2007"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 10:04
S83	70	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) same (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) with ((e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse) same (card or smartcard or module or sim or nfc or "near" field or token or chip) and @ay<"2007"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 10:02
S82	92	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) same (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) with ((e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse) and @ay<"2007"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 10:02
S81	9	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) same (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) with (applet or application or (e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse or program) and S78 and @ay<"2007"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 10:01
S80	16	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) same (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) with (applet or application or (e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse or program) and S78	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 09:59
S79	14	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) and (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) with(applet or application or (e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse or program) same (id or identifier or identif\$3 or identifying or identification or name or aid) and S78	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/29 09:50
S78	17	(US-20120130839-\$ or US-20120129452-\$ or US-20050137981-\$ or US-20060168355-\$ or US-20100291904-\$ or US-20120300938-\$ or US-20090069051-\$ or US-20080082646-\$ or	US-PGPUB; USPAT	ADJ	ON	2015/04/29 09:19

		US-20080073426-\$ or US-20040039919-\$ or US-20070125838-\$ or US-20070125840-\$ or US-20020112171-\$ or US-20120089520-\$ or US-20090307142-\$).did. or (US-8118218-\$ or US-7729363-\$).did.				
S77	2	(("20030116635"   "20030173409"   "20040162732"   "20050043997"   "20070114274"   "4720860"   "4797542"   "5237614"   "5856661"   "6130621"   "6681988"   "6811082"   "7357319"   "7360688"   "6163771"   "6776332"   "4529870"   "6308890"   "20010045454"   "20060163353"   "5479512"   "5608203"   "5834756"   "6176430"   "6655585"   "6980969"   "6592044"   "5623552"   "7530495"   "7620606"   "20020082989"   "20050154643"   "4353064"   "5168520"   "5361062"   "5591949"   "5937394"   "7114652"   "7246752"   "7337326"   "20070034700"   "20080148394"   "6961858"   "7090128"   "5524072"   "20040133787"   "20050116026"   "4614861"   "4701601"   "4791283"   "5276311"   "5347580"   "5485519"   "5864623"   "5907142"   "6095416"   "6157920"   "6182894"   "6269163"   "7051929"   "20110028184"   "20050187873"   "20040035942"   "20060085328"   "20080040276"   "4786791"   "6045043"   "6076163"   "6240184"   "6446052"   "6592044"   "20010034702"   "6764005"   "20040230488"   "20020116330"   "7020635"   "20010034702"   "20070192249"   "4394654"   "5038251"   "5434405"   "6189098"   "6873974"   "7100821"   "7140550"   "7380710"   "7398253"   "20050080747"   "7080049"   "20010047335"   "20040172535"   "20060091223"   "20060161435"   "20070241201"   "20080040271"   "4667087"   "5412199"   "5484997"   "5657388"   "6085320"   "6411715"   "6991155"   "7163153"   "7427033"   "7083094"   "7334732"   "7150045"   "20030130955"   "5478994"   "5585787"   "5956699"   "6609654"   "6705520"   "7051929"   "20030105964"   "5834747"   "7828207"   "7107462").PN. and nonce	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/28 14:21
S76	47	(("20030116635"   "20030173409"   "20040162732"   "20050043997"   "20070114274"   "4720860"   "4797542"   "5237614"   "5856661"   "6130621"   "6681988"   "6811082"   "7357319"   "7360688"   "6163771"   "6776332"   "4529870"   "6308890"   "20010045454"   "20060163353"   "5479512"   "5608203"   "5834756"   "6176430"   "6655585"   "6980969"   "6592044"   "5623552"   "7530495"   "7620606"   "20020082989"   "20050154643"   "4353064"   "5168520"   "5361062"   "5591949"   "5937394"   "7114652"   "7246752"   "7337326"   "20070034700"   "20080148394"   "6961858"   "7090128"   "5524072"   "20040133787"   "20050116026"   "4614861"   "4701601"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/28 14:18

		"4791283"   "5276311"   "5347580"   "5485519"   "5864623"   "5907142"   "6095416"   "6157920"   "6182894"   "6269163"   "7051929"   "20110028184"   "20050187873"   "20040035942"   "20060085328"   "20080040276"   "4786791"   "6045043"   "6076163"   "6240184"   "6446052"   "6592044"   "20010034702"   "6764005"   "20040230488"   "20020116330"   "7020635"   "20010034702"   "20070192249"   "4394654"   "5038251"   "5434405"   "6189098"   "6873974"   "7100821"   "7140550"   "7380710"   "7398253"   "20050080747"   "7080049"   "20010047335"   "20040172535"   "20060091223"   "20060161435"   "20070241201"   "20080040271"   "4667087"   "5412199"   "5484997"   "5657388"   "6085320"   "6411715"   "6991155"   "7163153"   "7427033"   "7083094"   "7334732"   "7150045"   "20030130955"   "5478994"   "5585787"   "5956699"   "6609654"   "6705520"   "7051929"   "20030105964"   "5834747"   "7828207"   "7107462").PN. and count\$3				
S75	13	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) same ((secure or security) adj2 (element or module or device) or card or smartcard or sim or subscriber identity or nfc or "near" field) and (download\$3 or upload\$3 or install\$3 or substantiat\$3 or initializ\$3 or load\$3) near3 (applet or application or (e or electronic or digital) adj2 (purse or wallet) or ewallet or epurse or program) and S73	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/28; 13:56
S74	13	(key or crypto or cryptograph\$2 or encrypt\$3 or decrypt\$3) same ((secure or security) adj2 (element or module or device) or sim or subscriber identity or nfc or "near" field) and S73	US- PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2015/04/28; 13:47
S73	17	(US-20120130839-\$ or US-20120129452-\$ or US-20050137981-\$ or US-20060168355-\$ or US-20100291904-\$ or US-20120300938-\$ or US-20090069051-\$ or US-20080082646-\$ or US-20080073426-\$ or US-20040039919-\$ or US-20070125838-\$ or US-20070125840-\$ or US-20020112171-\$ or US-20120089520-\$ or US-20090307142-\$).did. or (US-8118218-\$ or US-7729363-\$).did.	US- PGPUB; USPAT	ADJ	ON	2015/04/28; 13:47


**EAST Search History (Interference)**

<This search history is empty>

**4/ 29/ 2015 2:53:12 PM**

**C:\Users\cstanford\Documents\EAST\Workspaces\13350835\_AOM2.wsp**




<b><i>Index of Claims</i></b> 	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

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

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

CLAIM		DATE							
Final	Original	03/15/2013	08/13/2013	11/21/2014	04/30/2015				
	1	✓	✓	✓	✓				
	2	✓	✓	✓	✓				
	3	✓	✓	✓	✓				
	4	✓	✓	✓	✓				
	5	✓	✓	✓	✓				
	6	✓	✓	✓	✓				
	7	✓	✓	✓	✓				
	8	✓	✓	✓	✓				
	9	✓	✓	✓	✓				
	10	✓	✓	✓	✓				
	11	✓	✓	✓	✓				
	12	✓	✓	✓	✓				
	13	✓	✓	✓	✓				
	14	✓	✓	✓	✓				
	15	✓	✓	✓	✓				
	16	✓	✓	✓	✓				
	17	✓	✓	✓	✓				

<b>Search Notes</b>  	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/34 G07F7/1008 G06Q20/341 G06Q20/3674 G06Q20/382 G06Q20/20 G06Q20/32 G06Q20/367 G06Q20/3672	11/21/14	CS

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	379,380,451,492	3/14/13	CS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor, Assignee Search	3/14/13	CS
Parent Case Search	3/14/13	CS
Text search (see search history report)	3/14/13	CS
NPL Search	3/14/13	CS
Text search (see search history report)	8/13/13	CS
Text search (see search history report)	11/21/14	CS
Text search (see search history report)	4/29/15	CS

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

	/CHRISTOPHER STANFORD/ Primary Examiner.Art Unit 2887
--	--

UNITED STATES PATENT AND TRADEMARK OFFICE  
COMMISSIONER FOR PATENTS  
P.O. BOX 1450  
ALEXANDRIA VA 22313-1451

PRESORTED  
FIRST-CLASS MAIL  
U.S. POSTAGE PAID  
POSTEDIGITAL  
NNNNN

LogicPatents, LLC  
21701 Stevens Creek Boulevard, #284  
CUPERTINO, CA 95015



**Courtesy Reminder for  
Application Serial No: 13/350,835**

Attorney Docket No: RFID-082CIP3

Customer Number: 26797

Date of Electronic Notification: 05/05/2015

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:  
uspatents@sbcglobal.net

To view your correspondence online or update your email addresses, please visit us anytime at <https://sportal.uspto.gov/secure/myportal/privatepair>. If you have any questions, please email the Electronic Business Center (EBC) at [EBC@uspto.gov](mailto:EBC@uspto.gov) or call 1-866-217-9197.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**Applicant(s):** Liang Seng Koh et al  
**Title:** Mobile devices for commerce over unsecured networks  
**Serial No.:** 13/350,835  
**Filing Date:** 01/16/2012  
**Examiner:** Chris Stanford  
**Group Art Unit:** 2887  
**Docket No.:** RFID-081CIP3

---

Sept. 3, 2015

Mail Stop: No-Fee Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Response to Second OA (RCE)**

Dear Sir:

In response to Office Action dated 05/05/2015, the Applicant respectfully requests the Examiner to enter the following amendments before reconsidering the above-referenced application:

**AMENDMENTS TO THE CLAIMS** are reflected in the listing of claims which begins on page 2 of this Response.

**REMARKS/ARGUMENTS** begin on page 7 of this Response.

## AMENDMENTS TO THE CLAIMS

Please amend Claims 1 and 14 as follows:

1. *(Currently amended)* A mobile device for conducting a secured transaction over a network, the mobile device comprising:
  - a network interface;
  - an interface to receive a secure element;
  - a memory space for storing at least a module and an application downloaded from the network;
  - a processor coupled to the memory space and configured to execute the module to perform operations including:
    - sending to a server via the network interface an identifier identifying the application together with device information of a secure element, wherein the application is downloaded from the network in the mobile device;
    - establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device; and
    - receiving the data from the server to associate the application with the secure element, wherein the application subsequently functions in conjunction with the secure element.
2. *(Original)* The mobile device as recited in claim 1, wherein the data received in the mobile device includes an application key set for the application, and a user interface specifically designed for the mobile device.
3. *(Original)* The mobile device as recited in claim 2, wherein the mobile device is a near field communication (NFC) enabled mobile phone, and the application is an

electronic purse (e-purse), the mobile device is used to exchange secured data with another device within a near distance to conduct a transaction.

4. (*Original*) The mobile device as recited in claim 3, wherein the secured data is being exchanged over a secured channel between the mobile device and the another device established by the application key set.
5. (*Original*) The mobile device as recited in claim 4, wherein the transaction is conducted without the mobile device communicating with a transaction server.
6. (*Previously amended*) The mobile device as recited in claim 1, wherein said sending to a server via the network interface an identifier identifying the application together with device information of a secure element comprises:
  - determining whether the secure element has been personalized with a Trusted Service Management (TSM) system, wherein the TSM system is a collection of services configured to distribute and manage contactless services for customers signed up with the TSM, and provide data exchanges among different parties to make electronic commerce possible over a wireless network; and
  - performing a personalization process for the secure element when the secure element has not been personalized with the Trusted Service Management (TSM) system, wherein the secure element when personalized establishes a security platform for the application to run on the mobile device.
7. (*Original*) The mobile device as recited in claim 6, wherein the personalization process comprises:
  - causing the mobile device to initiate data communication with a server in the TSM system;
  - retrieving device information of the secure element in responding to a request from the TSM server after the TSM server determines that the secure

element is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element; receiving at least a set of keys from the TSM server, wherein the keys are generated in the TSM server in accordance with the device information of the secure element; and storing the set of keys in the secure element to facilitate a subsequent transaction with the secure element in the computing device.

8. *(Original)* The mobile device as recited in claim 7, wherein the device information includes an identifier of the secure element, manufacturer information and a batch number.
9. *(Original)* The mobile device as recited in claim 7, wherein the secure element is embedded in the mobile device and integrated with the mobile device via the interface.
10. *(Original)* The mobile device as recited in claim 7, wherein the secure element is a software module installed in a secure memory space only accessible by a distributor of the secure element.
11. *(Original)* The mobile device as recited in claim 10, wherein some components are updated when the secure element is upgraded by the distributor.
12. *(Original)* The mobile device as recited in claim 1, wherein the operations further comprises:
  - receiving a message from a distributor of the application, the message including an identifier identifying the application;
  - verifying that the message is indeed from the distributor;
  - disassociating the application with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and

notifying the distributor that the application installed in the mobile device is no longer active.

13. *(Original)* The method as recited in claim 8, wherein part of the data is used to facilitate the server to remotely manage the application.

14. *(Previously amended)* A mobile device for conducting a secured transaction over a network, the mobile device comprising:

a network interface;

a secure element;

a memory space for storing various modules downloaded from the network, each of the modules configured to provide an application or a service to a user of the mobile device;

a processor coupled to the memory space and configured to execute an embedded module to perform operations including:

provisioning each of the modules, wherein said provisioning each of the modules with a distributor comprises:

sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element, wherein the each of the modules is downloaded from the network in the mobile device;

establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the each of the modules to function as designed on the mobile device; and

receiving the data from the server to associate the each of the modules with the secure element, wherein the data includes a set of keys generated for the each of the modules, wherein the each of the modules subsequently functions in conjunction with the secure element.



15. (*Original*) The mobile device as recited claim 14, wherein the operations further comprise:

receiving a message from a distributor of one of the modules, the message including an identifier identifying the one of the modules;  
verifying that the message is authenticated;  
disassociating the one of the modules with the secure element in responding to a confirmation from the distributor after the message has been verified and was indeed from the distributor; and  
notifying the distributor that the one of the modules installed in the mobile device is no longer active.

16. (*Original*) The mobile device as recited claim 14, wherein the mobile device includes a display configured to display a user interface showing some of the modules that are still provisioned and active, each of the modules is configured to show another user interface particularly designed for the display of the mobile device when the each of the modules is activated by a user.

17. (*Original*) The mobile device as recited claim 16, wherein the secure element must be personalized before each of the modules is provisioned, each of the provisioned modules is associated with the personalized secure element and a key set generated in accordance with a key set of the secure element.

## REMARKS

Claims 1 - 17 examined again. In the Office Action dated 05/05/2015, Claims 1-17 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over PG Pub. No.: 2005/0187873 to Labrou et al. (hereinafter Labrou) in view of US PG Pub. No.: 2008/0006685 to Rackley et al. (hereinafter Rackley).

In the foregoing amendments, Claims 1 and 14 have been amended to further distinguish from cited references. No new matters have been introduced. Reconsideration of pending claims 1-17 is respectfully requested.

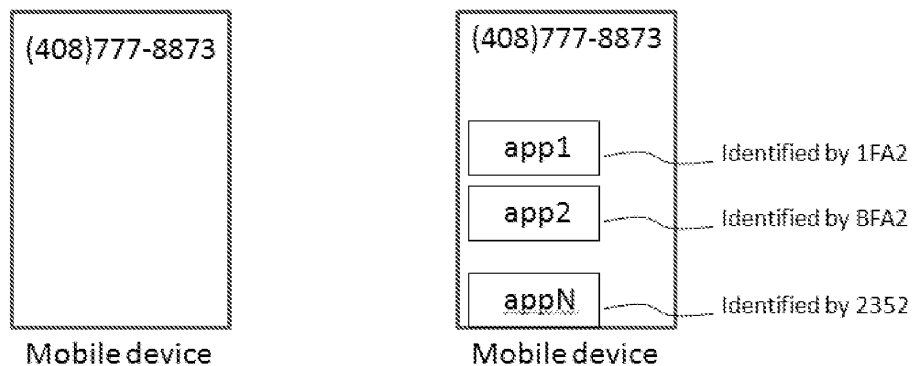
As amended, Claim 1 now recites:

a network interface;  
an interface to receive a secure element;  
a memory space for storing at least a module and an application downloaded from the network;  
a processor coupled to the memory space and configured to execute the module to perform operations including:  
    sending to a server via the network interface an identifier identifying the application together with device information of a secure element, wherein the application is downloaded from the network in the mobile device;  
    establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device; and  
    receiving the data from the server to associate the application with the secure element, wherein the application subsequently functions in conjunction with the secure element.

As stated in paragraph [0010], one embodiment of the present invention is to personalize a secure element in an NFC device to enable various secure

transactions over a network. In other words, a device must be equipped with a secure element. As publically known, a secure element is a tamper-resistant device capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. For an application to be used for financial transaction, the application must be provisioned first with the secure element. Subsequently, the application functions in conjunction with the secure element.

In contrast, Labrou teaches a mobile device for conducting a secured transaction over a network. Labrou explicitly teaches about using a phone number of the mobile device to conduct a secured transaction. The Applicant wishes to point out that a phone number is conceptually different from an identifier identifying an application running in a mobile device. A phone number can only identify one device while multiple identifiers can respectfully identify multiple applications (as it is more explicit in Claim 14) running on the mobile device. The figure below is provided to illustrate the subtle difference between a phone number identifying a mobile device and an identifier identifying an application installed on a mobile device.



It can be appreciated that the phone number (408)777-8873 can uniquely identify a mobile device but an identifier (e.g., 1FA2) is used to identify an application installed and running on the mobile device identified by the phone number (408)777-8873.

Further Labrou is silent about a secure element in a mobile device. As a matter of fact, the concept of a secure element was not even introduced prior to 2003 (the priority of Labrou). Labrou admits in paragraph [0016] that the mobile device is a WAP-enabled phone that did not use a secure element to operate as it is well known in the field. The Applicant respectfully submits Labrou neither teaches nor suggests "*an identifier identifying the application together with device information of a secure element*" when the device communicates with the server.

The Applicant acknowledges that a patent Examiner could interpret the claims in the broadest term. The Examiner could interpret a secure element as a processor. However, Claim 1 of the instant application recites a processor that is configured to provision an installed application with the secure element, which indicates that the secure element is a separate device. Labrou neither teaches nor suggests a second processor to act as a secure element to provision an application that subsequently functions with the secure element. The Applicant respectfully submits Labrou fails to teach "*establishing a secured channel between the secure element*" and "*the application subsequently functions in conjunction with the secure element*". Accordingly, Claim 1 as amended shall be allowable over Labrou. Reconsideration of Claims 1-13 is kindly requested.

On Page 5 of the Office Action, the Examiner admits Labrou discloses the claimed invention as cited above though does not explicitly disclose that the application and the mobile device are identified via a network interface of the mobile device itself and then cites Rackley to show the teachings in combination. However, Rackley teaches about providing real time account balances to users of mobile devices from a mobile financial transaction system (MFTS) that stores user information and transaction information. The MFTS is operative to obtain and provide updated account balances to mobile devices in response to predetermined conditions. Rackley neither teaches nor suggests about provisioning an installed application with a secure element. The Applicant respectfully submits the combination of Labrou and Rackley does not make up the deficiency in Labrou in view of Claim 1 of the instant application. Accordingly, Claim 1 as amended shall be

allowable over Labrou and Rackley. Reconsideration of Claims 1-13 is kindly requested.

Claim 14 has been amended similarly to Claim 1. The Applicant wishes to rely upon the above arguments/reasons supporting Claim 1 to support Claim 14, and further points out that there are multiple modules are installed in a mobile device, each of the modules has an identifier which could not be interpreted as or replaced with a phone number, otherwise all the modules would be identified by the same number. Accordingly, Claim 14 as amended shall be allowable over Labrou and Rackley. Reconsideration of Claims 14-17 is kindly requested.

The patentability of the independent claims has been argued as set forth above and thus Applicant will not take this opportunity to argue the merits of the rejection with regard to each dependent claim. However, Applicant does not concede that the dependent claims are not independently patentable and reserves the right to argue the patentability of the dependent claims at a later date if necessary.

In view of the above amendments and remark, the Applicant believes that Claims 1 - 17 shall be in condition for allowance over the cited references. Early and favorable action is being respectfully solicited.

If there are any issues remaining which the Examiner believes could be resolved through either a Supplementary Response or an Examiner's Amendment, the Examiner is respectfully requested to contact the undersigned at (408)777-8873.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231", Sept. 3 2015. e-filed.

Name: Joe Zheng

Signature: / joe zheng /

Respectfully submitted;

/ joe zheng /

Joe Zheng  
Reg.: No. 39,450

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	13350835			
<b>Filing Date:</b>	16-Jan-2012			
<b>Title of Invention:</b>	Mobile devices for commerce over unsecured networks			
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh			
<b>Filer:</b>	Joe Zheng			
<b>Attorney Docket Number:</b>	RFID-082CIP3			
Filed as Small Entity				
<b>Filing Fees for Utility under 35 USC 111(a)</b>				
<b>Description</b>	<b>Fee Code</b>	<b>Quantity</b>	<b>Amount</b>	<b>Sub-Total in USD(\$)</b>
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 1 month with \$0 paid	2251	1	100	100
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>100</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	23390379
<b>Application Number:</b>	13350835
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	1986
<b>Title of Invention:</b>	Mobile devices for commerce over unsecured networks
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh
<b>Customer Number:</b>	26797
<b>Filer:</b>	Joe Zheng
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	RFID-082CIP3
<b>Receipt Date:</b>	03-SEP-2015
<b>Filing Date:</b>	16-JAN-2012
<b>Time Stamp:</b>	03:59:51
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 100
RAM confirmation Number	7510
Deposit Account	502436
Authorized User	ZHENG, JOE
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	



Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)  
 Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)  
 Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	ResponseTo2ndOARCE.pdf	128606 a37eb2d4926739757b26cd3f7deafcd5f06fd1d	no	10

**Warnings:**

**Information:**

2	Fee Worksheet (SB06)	fee-info.pdf	30351 e32aae98ec17910ae0103fa8159e9d5bb6dcd9e5	no	2
---	----------------------	--------------	---	----	---

**Warnings:**

**Information:**

**Total Files Size (in bytes):** 158957

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

**New Applications Under 35 U.S.C. 111**

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

**National Stage of an International Application under 35 U.S.C. 371**

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

**New International Application Filed with the USPTO as a Receiving Office**

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

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

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875			Application or Docket Number 13/350,835	Filing Date 01/16/2012	<input type="checkbox"/> To be Mailed	
ENTITY: <input type="checkbox"/> LARGE <input checked="" type="checkbox"/> SMALL <input type="checkbox"/> MICRO						
<b>APPLICATION AS FILED – PART I</b>						
(Column 1)		(Column 2)				
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)		
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A			
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X \$ =			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$ =			
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))						
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			
<b>APPLICATION AS AMENDED – PART II</b>						
(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	<b>09/03/2015</b>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	+ 17	Minus ** 20	= 0	X \$40 =	0
	Independent (37 CFR 1.16(h))	+ 2	Minus *** 3	= 0	X \$210 =	0
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
					TOTAL ADD'L FEE	<b>0</b>
(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	+	Minus **	=	X \$ =	
	Independent (37 CFR 1.16(h))	+	Minus ***	=	X \$ =	
	<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					
					TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".						
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.						
LIE /DAWN BREWER/						

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**  
 If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

26797 7590 12/10/2015
LogicPatents, LLC
21701 Stevens Creek Boulevard, #284
CUPERTINO, CA 95015

EXAMINER

STANFORD, CHRISTOPHER J

ART UNIT PAPER NUMBER

2887

DATE MAILED: 12/10/2015

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

13/350,835 01/16/2012 Liang Seng Koh RFID-082CIP3 1986

TITLE OF INVENTION: MOBILE DEVICES FOR COMMERCE OVER UNSECURED NETWORKS

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

nonprovisional SMALL \$480 \$0 \$0 \$480 03/10/2016

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

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

HOW TO REPLY TO THIS NOTICE:

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

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

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

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

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

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

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

**PART B - FEE(S) TRANSMITTAL**

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

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

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

26797 7590 12/10/2015  
 LogicPatents, LLC  
 21701 Stevens Creek Boulevard, #284  
 CUPERTINO, CA 95015

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

**Certificate of Mailing or Transmission**

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

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/350,835	01/16/2012	Liang Seng Koh	RFID-082CIP3	1986

TITLE OF INVENTION: MOBILE DEVICES FOR COMMERCE OVER UNSECURED NETWORKS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	03/10/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
STANFORD, CHRISTOPHER J	2887	235-380000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) The names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1 _____</p> <p>(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2 _____</p> <p>_____ 3 _____</p>
---	---

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

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

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

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

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (<b>Please first reapply any previously paid issue fee shown above</b>)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--

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

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscounted fee status.

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

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

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

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

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_ Registration No. \_\_\_\_\_



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes application details for LogicPatents, LLC and examiner information for STANFORD, CHRISTOPHER J.

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

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

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

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

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

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

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

### Privacy Act Statement

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

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

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

<b>Notice of Allowability</b>	<b>Application No.</b> 13/350,835	<b>Applicant(s)</b> KOH ET AL.	
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887	<b>AIA (First Inventor to File) Status</b> No

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

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

1.  This communication is responsive to amendments filed 9/03/2015.  
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on \_\_\_\_\_.
2.  An election was made by the applicant in response to a restriction requirement set forth during the interview on \_\_\_\_\_; the restriction requirement and election have been incorporated into this action.
3.  The allowed claim(s) is/are 1-17. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see [http://www.uspto.gov/patents/init\\_events/pph/index.jsp](http://www.uspto.gov/patents/init_events/pph/index.jsp) or send an inquiry to [PPHfeedback@uspto.gov](mailto:PPHfeedback@uspto.gov).
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

**Certified copies:**

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

\* Certified copies not received: \_\_\_\_\_.

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

5.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.  
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.  
**Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |   |  |
|---|--|
| <ol style="list-style-type: none"> <li>1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)</li> <li>2. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br/>Paper No./Mail Date _____</li> <li>3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material</li> <li>4. <input type="checkbox"/> Interview Summary (PTO-413),<br/>Paper No./Mail Date _____.</li> </ol> | <ol style="list-style-type: none"> <li>5. <input type="checkbox"/> Examiner's Amendment/Comment</li> <li>6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance</li> <li>7. <input type="checkbox"/> Other _____.</li> </ol> |
|---|--|

/CHRISTOPHER STANFORD/  
Primary Examiner, Art Unit 2887

**DETAILED ACTION**

***Notice of Pre-AIA or AIA Status***

1. The present application is being examined under the pre-AIA first to invent provisions.

***Response to Amendment***

2. Receipt is acknowledged of the amendment filed 9/03/2015. Claims 1 and 14 are amended and claims 1-17 are currently pending.

***Allowable Subject Matter***

3. Claims 1-17 are allowed.

4. The following is an examiner's statement of reasons for allowance: the prior art of record, taken alone or in combination with other references, neither teaches nor suggests:

- A mobile device for conducting a secured transaction over a network, the mobile device comprising: a network interface; an interface to receive a secure element; a memory space for storing at least a module and an application downloaded from the network; a processor coupled to the memory space and configured to execute the module to perform operations including: sending to a server via the network interface an identifier identifying the application together with device information of a secure element, wherein the application is downloaded from the network in the mobile device; establishing a secured



channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the application to function as designed on the mobile device; and receiving the data from the server to associate the application with the secure element, wherein the application subsequently functions in conjunction with the secure element (claim 1)

- A mobile device for conducting a secured transaction over a network, the mobile device comprising: a network interface; a secure element; a memory space for storing various modules downloaded from the network, each of the modules configured to provide an application or a service to a user of the mobile device; a processor coupled to the memory space and configured to execute an embedded module to perform operations including: provisioning each of the modules, wherein said provisioning each of the modules with a distributor comprises: sending to a server via the network interface an identifier identifying the each of the modules together with device information of the secure element, wherein the each of the modules is downloaded from the network in the mobile device; establishing a secured channel between the secure element and the server using a key set installed on the secure element, wherein the server is configured to prepare data necessary for the each of the modules to function as designed on the mobile device; and receiving the data from the server to associate the each of the modules with the secure element, wherein the data includes a set of keys generated for the each of the modules, wherein the each

of the modules subsequently functions in conjunction with the secure element  
(claim 14)

The history of prosecution and language of the claims themselves evidence the distinguishing features of the claimed invention over prior art. Arguments found on Page 9 of the Response filed 9/03/2015 are particularly persuasive in pointing out the deficiencies of the prior art relating to the secure element. Applicant states the claim requires “a processor that is configured to provision an installed application with the secure element, which indicated that the secure element is a separate device”. It is believed that the most compelling evidence in the claim for this is two-fold: “a processor ... configured to execute the module to perform operations including ... establishing a secured channel between the secure element and the server using a key set ... the application subsequently functions in conjunction with the secure element”.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US Pat. 8,725,632 to Tompkins discloses downloading a financial transaction application through a secure channel.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER STANFORD whose telephone number is (571)270-3337. The examiner can normally be reached on Monday through Fridays, 8am-5pm PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Steve Paik can be reached on (571) 272-2404. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/CHRISTOPHER STANFORD/  
Primary Examiner, Art Unit 2887

<b>Notice of References Cited</b>	Application/Control No. 13/350,835	Applicant(s)/Patent Under Reexamination KOH ET AL.	
	Examiner CHRISTOPHER STANFORD	Art Unit 2887	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A US-8,725,632 B2	05-2014	Tompkins; Peter	G06Q20/12	705/39
B	US-				
C	US-				
D	US-				
E	US-				
F	US-				
G	US-				
H	US-				
I	US-				
J	US-				
K	US-				
L	US-				
M	US-				


**FOREIGN PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
N					
O					
P					
Q					
R					
S					
T					

**NON-PATENT DOCUMENTS**

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
*	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
U					
V					
W					
X					

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

<b>Search Notes</b>  	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/34 G07F7/1008 G06Q20/341 G06Q20/3674 G06Q20/382 G06Q20/20 G06Q20/32 G06Q20/367 G06Q20/3672	11/21/14	CS

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
235	379,380,451,492	3/14/13	CS

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor, Assignee Search	3/14/13	CS
Parent Case Search	3/14/13	CS
Text search (see search history report)	3/14/13	CS
NPL Search	3/14/13	CS
Text search (see search history report)	8/13/13	CS
Text search (see search history report)	11/21/14	CS
Text search (see search history report)	4/29/15	CS
Text search (see search history report)	12/4/15	CS

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
All Groups Listed Above		12/4/15	CS

	/CHRISTOPHER STANFORD/ Primary Examiner.Art Unit 2887
--	--



## UNITED STATES PATENT AND TRADEMARK OFFICE

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

## BIB DATA SHEET

CONFIRMATION NO. 1986

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
13/350,835	01/16/2012	235	2887	RFID-082CIP3		
<b>RULE</b>						
<b>APPLICANTS</b>						
<b>INVENTORS</b>						
Liang Seng Koh, Fremont, CA; Hsin Pan, Fremont, CA; Xiangzhen Xie, Shenzhen, CHINA;						
<b>** CONTINUING DATA *****</b>						
This application is a CIP of 11/534,653 09/24/2006 PAT 8118218 and is a CIP of 11/739,044 04/23/2007 which is a CIP of 11/534,653 09/24/2006 PAT 8118218						
<b>** FOREIGN APPLICATIONS *****</b>						
<b>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **</b>						
01/27/2012						
Foreign Priority claimed 35 USC 119(a-d) conditions met	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Met after Allowance	<b>STATE OR COUNTRY</b>	<b>SHEETS DRAWINGS</b>	<b>TOTAL CLAIMS</b>	<b>INDEPENDENT CLAIMS</b>
Verified and Acknowledged	/CHRISTOPHER J STANFORD/ Examiner's Signature	Initials	CA	25	17	2
<b>ADDRESS</b>						
LogicPatents, LLC 21701 Stevens Creek Boulevard, #284 CUPERTINO, CA 95015 UNITED STATES						
<b>TITLE</b>						
Mobile devices for commerce over unsecured networks						
<b>FILING FEE RECEIVED</b>	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		
530						

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	20	(US-20120130839-\$ or US-20120129452-\$ or US-20050137981-\$ or US-20060168355-\$ or US-20100291904-\$ or US-20120300938-\$ or US-20090069051-\$ or US-20080082646-\$ or US-20080073426-\$ or US-20040039919-\$ or US-20070125838-\$ or US-20070125840-\$ or US-20020112171-\$ or US-20120089520-\$ or US-20090307142-\$ or US-20050187873-\$ or US-20080006685-\$).did. or (US-8118218-\$ or US-7729363-\$ or US-7822688-\$).did.	US-PGPUB; USPAT	ADJ	ON	2015/12/04 09:12
L2	32023	(G06Q20/32 OR G06Q20/10 OR G06Q20/367 OR G06Q20/3674 OR G06Q20/40 OR G06Q20/04 OR G06Q20/3227 OR G06Q20/3672 OR G06Q20/382 OR G06Q20/3223 OR G06Q20/3552 OR G06Q20/3278 OR G06Q20/105 OR G07F7/0826).CPC.	US-PGPUB; USPAT	ADJ	ON	2015/12/04 09:14

## EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	12772	(G06Q20/32 OR G06Q20/10 OR G06Q20/367 OR G06Q20/3674 OR G06Q20/40 OR G06Q20/04 OR G06Q20/3227 OR G06Q20/3672 OR G06Q20/382 OR G06Q20/3223 OR G06Q20/3552 OR G06Q20/3278 OR G06Q20/105 OR G07F7/0826).CPC.	USPAT	ADJ	ON	2015/12/04 09:15
L4	7034	L3 and @ay<"2007"	USPAT	ADJ	ON	2015/12/04 09:16
L5	484	L4 and (program or software or app or application or applet or ewallet or (e or electronic or digital) adj2 (purse or wallet) or epurse) with (id or identifier or identification or name or identifying).clm. and (device or apparatus or phone or telephone or mobile or sim or card or smartcard or chipcard or iccard or (secure\$1 or security) adj2 (element or module)) with (id or identifier or identification or name or identifying).clm.	USPAT	ADJ	ON	2015/12/04 09:26
L6	33	L5 and (download\$3 or upload\$3 or load\$3 or send\$3 or receive\$3 or instantiat\$3 or transmit or transmitt\$3 or transmission) near3 (program or software or app or application or applet or ewallet or (e or electronic or digital) adj2 (purse or wallet) or epurse) with (key or keyset or cryptograph\$2 or encrypt\$3 or decrypt\$3).clm.	USPAT	ADJ	ON	2015/12/04 09:33
L7	0	L5 and new adj2 (program or software or app	USPAT	ADJ	ON	2015/12/04

		or application or applet or ewallet or (e or electronic or digital) adj2 (purse or wallet) or epurse) with (key or keyset or cryptograph\$2 or encrypt\$3 or decrypt\$3).dm.				09:38
L8	8	L5 and new adj2 (program or software or app or application or applet or ewallet or (e or electronic or digital) adj2 (purse or wallet) or epurse) with (key or keyset or cryptograph\$2 or encrypt\$3 or decrypt\$3)	USPAT	ADJ	ON	2015/12/04 09:38
L9	10	L5 and (install\$3 or installation) adj2 (program or software or app or application or applet or ewallet or (e or electronic or digital) adj2 (purse or wallet) or epurse) with (key or keyset or cryptograph\$2 or encrypt\$3 or decrypt\$3)	USPAT	ADJ	ON	2015/12/04 09:39
L10	80	("20010041973"   "20010056387"   "20010056401"   "20020035536"   "20020049788"   "20020065752"   "20020065774"   "20020073236"   "20030195797"   "20040006538"   "20040158829"   "20050027610"   "20050176449"   "20060031784"   "20060094411"   "20070060206"   "20080096535"   "20080126986"   "5220501"   "5221838"   "5465206"   "5530438"   "5640002"   "5689565"   "5706211"   "5715020"   "5744787"   "5745689"   "5748737"   "5790677"   "5790790"   "5796832"   "5839052"   "5875302"   "5878141"   "5878337"   "5903652"   "5907547"   "5920847"   "5944786"   "5953670"   "5959543"   "5963925"   "5987303"   "5987439"   "5999624"   "6014636"   "6035104"   "6044362"   "6049698"   "6055513"   "6078820"   "6094643"   "6094681"   "6128603"   "6138158"   "6167253"   "6184878"   "6230970"   "6269393"   "6289324"   "6311058"   "6317885"   "6356752"   "6385652"   "6449638"   "6477579"   "6535726"   "6536661"   "6553412"   "6609106"   "6609113"   "6633910"   "6678518"   "6694316"   "6745229"   "6952645"   "7043230"   "7113801"   "7720742").PN. OR ("8725632").URPN.	US- PGPUB; USPAT	ADJ	ON	2015/12/04 09:50
L11	0	L10 and (install\$3 or installation or download\$3 or new) adj3 (program or software or app or application or applet or ewallet or (e or electronic or digital) adj2 (purse or wallet) or epurse) with (key or keyset or cryptograph\$2 or encrypt\$3 or decrypt\$3)	USPAT	ADJ	ON	2015/12/04 09:51
L12	4	L10 and (install\$3 or installation or download\$3 or new) adj3 (program or software or app or application or applet or ewallet or (e or electronic or digital) adj2 (purse or wallet) or epurse) same (key or keyset or cryptograph\$2 or encrypt\$3 or decrypt\$3)	USPAT	ADJ	ON	2015/12/04 09:51
L13	9	L10 and (install\$3 or installation or download\$3 or new) adj3 (program or	USPAT	ADJ	ON	2015/12/04 09:52



EAST Search History


	software or app or application or applet or ewallet or (e or electronic or digital) adj2 (purse or wallet) or epurse) not L12				
--	---	--	--	--	--

**12/ 4/ 2015 10:31:33 AM**

**C:\Users\cstanford\Documents\EAST\Workspaces\13350835\_AOM2.wsp**





<b>Issue Classification</b> 	<b>Application/Control No.</b> 13350835	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

<input type="checkbox"/> <b>Claims renumbered in the same order as presented by applicant</b>																<input type="checkbox"/> <b>CPA</b>		<input type="checkbox"/> <b>T.D.</b>		<input type="checkbox"/> <b>R.1.47</b>	
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original						
1	1	17	17																		
2	2																				
3	3																				
4	4																				
5	5																				
6	6																				
7	7																				
8	8																				
10	9																				
11	10																				
12	11																				
13	12																				
9	13																				
14	14																				
15	15																				
16	16																				

NONE		<b>Total Claims Allowed:</b>	
(Assistant Examiner)	(Date)	17	
/CHRISTOPHER STANFORD/ Primary Examiner. Art Unit 2887	12/04/2015	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

**PART B - FEE(S) TRANSMITTAL**

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

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

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

26797 7590 12/10/2015  
 LogicPatents, LLC  
 21701 Stevens Creek Boulevard, #284  
 CUPERTINO, CA 95015

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

**Certificate of Mailing or Transmission**

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

Joe Zheng	(Depositor's name)
/ joe zheng /	(Signature)
12/11/2015	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/350,835	01/16/2012	Liang Seng Koh	RFID-082CIP3	1986

TITLE OF INVENTION: MOBILE DEVICES FOR COMMERCE OVER UNSECURED NETWORKS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	03/10/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
STANFORD, CHRISTOPHER J	2887	235-380000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address Form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. <b>Use of a Customer Number is required.</b></p>	<p>2. For printing on the patent front page, list</p> <p>(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,</p> <p>(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.</p> <p>1. <u>Joe Zheng</u></p> <p>2. _____</p> <p>3. _____</p>
---	---

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

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

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

Rich House Global Technology Ltd. (Shenzhen, CN)  
 RFCyber Corp. (Fremont, CA)

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

<p>4a. The following fee(s) are submitted:</p> <p><input checked="" type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input checked="" type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
--	--

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

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscounted fee status.

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

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

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

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

Authorized Signature / joe zheng / Date 12/11/2015

Typed or printed name Joe Zheng Registration No. 39,450

Electronic Patent Application Fee Transmittal				
<b>Application Number:</b>	13350835			
<b>Filing Date:</b>	16-Jan-2012			
<b>Title of Invention:</b>	MOBILE DEVICES FOR COMMERCE OVER UNSECURED NETWORKS			
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh			
<b>Filer:</b>	Joe Zheng			
<b>Attorney Docket Number:</b>	RFID-082CIP3			
Filed as Small Entity				
<b>Filing Fees for Utility under 35 USC 111(a)</b>				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
<b>Post-Allowance-and-Post-Issuance:</b>				
Utility Appl Issue Fee	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>480</b>

<b>Electronic Acknowledgement Receipt</b>	
<b>EFS ID:</b>	24340430
<b>Application Number:</b>	13350835
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	1986
<b>Title of Invention:</b>	MOBILE DEVICES FOR COMMERCE OVER UNSECURED NETWORKS
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh
<b>Customer Number:</b>	26797
<b>Filer:</b>	Joe Zheng
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	RFID-082CIP3
<b>Receipt Date:</b>	11-DEC-2015
<b>Filing Date:</b>	16-JAN-2012
<b>Time Stamp:</b>	16:44:20
<b>Application Type:</b>	Utility under 35 USC 111(a)

**Payment information:**

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 480
RAM confirmation Number	3629
Deposit Account	502436
Authorized User	ZHENG, JOE
<p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <ul style="list-style-type: none"> <li>Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)</li> <li>Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)</li> </ul>	



Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)  
 Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)  
 Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	FeeTransmittal.pdf	103175 <small>85f8b1e2221869e636bb233520babbf0e45dadd2</small>	no	1

**Warnings:**

**Information:**

2	Fee Worksheet (SB06)	fee-info.pdf	30444 <small>84d521dfaf6364f19c71a4572c22aea004fd54f1</small>	no	2
---	----------------------	--------------	--	----	---

**Warnings:**

**Information:**

**Total Files Size (in bytes):** 133619

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

**New Applications Under 35 U.S.C. 111**

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

**National Stage of an International Application under 35 U.S.C. 371**

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

**New International Application Filed with the USPTO as a Receiving Office**

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/350,835	01/19/2016	9240009	RFID-082CIP3	1986

26797 7590 12/29/2015  
LogicPatents, LLC  
21701 Stevens Creek Boulevard, #284  
CUPERTINO, CA 95015

**ISSUE NOTIFICATION**

The projected patent number and issue date are specified above.

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

The Patent Term Adjustment is 227 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Liang Seng Koh, Fremont, CA;  
Hsin Pan, Fremont, CA;  
Xiangzhen Xie, Shenzhen, CHINA;

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