

**In the United States Patent and Trademark Office**

**US Utility Patent Application for**

**Method and apparatus for providing electronic purse**

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

Futong Cho  
397 Sandhurst Drive  
Milpitas, CA 95035, USA  
Citizenship: U.S.A.

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

Fuliang Cho  
5812 McKellar Drive  
San Jose, CA 95129, USA  
Citizenship: U.S.A.

Assignees:

RFCyber Corp.  
4160 Technology Drive, Suite A  
Fremont, CA 94538  
USA

Express Mail Label # **E-filing**

Date of Deposit: **Sep 23 , 2006**

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

# Method and apparatus for providing electronic purse

## BACKGROUND

### Technical Field

**[0001]** The present invention is generally related to commerce over networks. Particularly, the present invention is related to electronic purses 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

**[0002]** Single functional cards have been successfully used in enclosed environments such as transportation systems. One example of such single functional cards is MIFARE that is the most widely installed contactless smart card technology in the world. With more than 500 million smart card ICs and 5 million reader components sold, MIFARE 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.

**[0003]** It is noticed that such enclosed systems 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 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 cellular networks for m-commerce as the key delivery over a public domain network causes security concerns.

**[0004]** There is, thus, a need for a mechanism in devices, especially portable devices, functioning as an electronic purse (e-purse) to be able to conduct transactions over an open network with a payment server without compromising security.

### **SUMMARY**

**[0005]** 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.

**[0006]** Broadly speaking, the invention is related to a mechanism provided to devices, especially portable devices, functioning as an electronic purse (e-purse) to be able to conduct transactions over an open network with a payment server without compromising security. According to one aspect of the present invention, a device is loaded with an e-purse manager. The e-purse manager is configured to manage various transactions and functions as a mechanism to access an emulator therein. The transactions may be conducted over a wired network or a wireless network.

**[0007]** According to another aspect of the present invention, a three-tier security model is proposed, based on which the present invention is contemplated to operate. The three-tier security model includes a physical security, an e-purse security

and a card manager security, concentrically encapsulating one with another. Security keys (either symmetric or asymmetric) are personalized within the three-tier security model so as to personalize an e-purse and perform 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 backend server.

**[0008]** The invention may be implemented in numerous ways, including a method, system, and device. In one embodiment, the present invention is a method for providing an e-purse, the method comprises providing a portable device embedded with a smart card module pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate communication between an e-purse applet therein and a payment server over a wireless network, wherein the portable device further includes a contactless interface that facilitates communication between the e-purse applet therein and the payment server, and personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys that are subsequently used to establish a secured channel between the e-purse and a SAM or a payment server.

**[0009]** According to another embodiment, the present invention is a system for providing an e-purse, the system comprises a portable device embedded with a smart card module pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate wireless communication between an e-purse applet therein and a payment server over a wireless network, the portable device further including a contactless interface that

facilitates communication between the e-purse applet therein and the payment server, the payment server associated with an issuer of the e-purse, and a SAM module configured to enable the e-purse, wherein the SAM module is behind the payment server when the e-purse is caused to communicate with the payment server via the midlet over a wireless network (M-commerce in FIG.2) or via the agent on a PC over a wired network (E-commerce in FIG.2).

**[0010]** Accordingly one of the objects of the present inventions is to provide a mechanism to be embedded in devices, especially portable devices, to function as an electronic purse (e-purse) to be able to conduct transactions over an open network with a payment server without compromising security.

**[0011]** Other objects, features, and advantages of the present invention 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**

**[0012]** 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:

**[0013]** FIG. 1A shows a three-tier security model based on which the present invention is contemplated to operate according to one embodiment thereof;

**[0014]** FIG. 1B shows a data flow in accordance with the three-tier security model among three entities;

**[0015]** FIG. 2 shows an exemplary architecture diagram according to one embodiment of the present invention;

**[0016]** FIG. 3A a block diagram of related modules interacting with each other to achieve what is referred to herein as e-purse personalization by an authorized person as shown in FIG. 2;

**[0017]** 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 as shown in FIG. 2;

**[0018]** FIG. 3C shows a flowchart or process of personalizing an e-purse according to one embodiment of the present invention;

**[0019]** FIG. 4A and FIG. 4B show together a flowchart or process of financing an e-purse according to one embodiment of the present invention; and

**[0020]** FIG. 4C shows an exemplary block diagram of related blocks interacting with each other to achieve the process FIG. 4A.

### **DETAILED DESCRIPTION OF THE INVENTION**

**[0021]** 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.

**[0022]** 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.

**[0023]** Embodiments of the present invention are discussed herein with reference to FIGS. 1A – 4C. 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.

**[0024]** FIG. 1A shows a three-tier security model **100** based on which the present invention is contemplated to operate according to one embodiment thereof. The three-tier security model **100** includes physical security **102**, e-purse security **104** and card manager security **106**.

**[0025]** Physical security **102** refers to a security mechanism provided by a single functional card to protect data stored on the card. The card may be hardware implemented or software emulated running on a type of media. Data on a single function card is protected by a set of access keys. These keys are configured onto the card when the card is issued. To avoid obscuring aspects of the present invention, the

process of how the keys are configured onto the cards is to be omitted. For accessing the data, related keys are delivered to a reader for authentication.

**[0026]** E-purse security **104** 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 purse when the purse is being issued. During a transaction, the purse uses a set of respective keys for encryption and MAC computation in order to secure the message channel between the purse and the SAM or backend servers. For a single functional card, the e-purse security **104** will 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 purse with the purse transaction keys.

**[0027]** Card Manager Security **106**, referring to a general security framework of a preload operating system in a smart card, provides a platform for PIN management and security channels (security domains) for card personalization. This platform via a card manager can be used to personalize a purse in one embodiment. One example of the card manager security **106** is what is referred to as a Global Platform (GP) that is a cross-industry membership organization created to advance standards for smart card growth. A GP combines the interests of smart card issuers, vendors, industry groups, public entities and technology companies to define requirements and technology standards for multiple application smart cards. In one embodiment, a global platform security is used to personalize a smart card. As a result, both e-purse keys and card access keys are personalized into the target tag.

**[0028]** FIG. 1B shows a data flow in accordance with the three-tier security model among three entities a land-based SAM or a network e-purse server **112**, e-



purse **114** acting as a gate keeper, and a single function tag **116**. According to one embodiment of the present invention, communications between the land-based SAM or the network e-purse server **112** and the e-purse **114** are conducted in sequence of a type of commands (e.g., APDU) while communications between the e-purse **114** and the single function tag **116** are conducted in sequence of another type of commands, wherein the e-purse **114** acts as the gate keeper to ensure only secured and authorized data transactions could happen.

**[0029]** In reference to FIG. 1A, the physical security 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 a payment server. The card manager security (e.g., global platform security) is realized via a card manager to update security keys to establish appropriate channels for interactions between the server and the applets, wherein the e-purse applet(s) acts as a gatekeeper to regulate or control the data exchange.

**[0030]** According to one embodiment, a smart card has a preloaded smart card operation system that provides security framework to control the access to the smart card (e.g., an installation of external applications into the smart card). In order to manage the life cycle of an external application, a card manager module is configured by using the smart card security framework. For instance, a Java based smart card, SmartMX, is preloaded with an operating system JCOP 4.1. The Global Platform 2.1 installed on the SmartMX performs the card manager functionality.

**[0031]** Referring now to FIG. 2, there shows an exemplary architecture diagram **200** according to one embodiment of the present invention. The diagram **200** includes a cellphone **202** 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. The SMX is pre-loaded with a Mifare emulator **208** (which is a single functional card) for storing values. The cellphone is equipped with a RFID interface (e.g., ISO 14443) that allows the cellphone 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 on top of the global platform and implemented 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.

**[0032]** In the cellphone **202**, a purse manager midlet **204** is provided. For M-commerce, the midlet **204** acts as an agent to facilitate communications between an e-purse applet **206** and one or more payment network and servers **210** to conduct transactions therebetween. As used herein, a midlet is a software component suitable for being executed on a portable device. The purse manager midlet **204** is implemented as a “midlet” on a Java cellphone, or an “executable application” on a PDA device. One of the functions this software component provides 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 a purse balance and a history log. In one application in which a card issuer provides a SA module **212** 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. 2, APDU commands are constructed by the servers **210** having access to a SA module **212**, where the APDU stands for Application Protocol Data Unit that 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 **210** or the e-purse applet **206** for processing.

**[0033]** For e-commerce, a web agent **214** on a computing device (not shown) is responsible for interacting with a RFID reader and the network server **210**. In operation, the agent **214** sends the APDU commands or receives responses thereto through the RFID reader **216** to/from the e-purse applet **206** residing in the cellphone **202**. On the other hand, the agent **214** composes network requests (such as HTTP) and receives responses thereto from the payment server **210**.

**[0034]** To personalize the cellphone **202**, 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 by an authorized person as shown in FIG. 2. 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 an user of the e-purse as shown in FIG. 2.

**[0035]** FIG. 3C shows a flowchart or process **350** of personalizing an e-purse 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.

**[0036]** As described above, an e-purse is built on top of a global platform to provide a security mechanism necessary to personalize applets designed therefor. In operation, a security domain is used for establishing a secured channel between a personalization application and the e-purse. According to one embodiment, the essential data to be personalized into the 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).

**[0037]** It is assumed that a user desires to personalize an e-purse embedded in a device (e.g., a cellphone). At **352** of FIG. 3C, a personalization process is initiated.

Depending on implementation, the personalization process may be implemented in a module in the 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 for a user thereof via an existing new e-purse SA module **306** and a SA module **308** with the RFID 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 **304**, the e-purse applet **312** and the emulator **314** are personalized.

**[0038]** Similarly, as shown in FIG. 3B, a user of an e-purse desires to initiate a personalization process to personalize the e-purse 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 cellphone 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** in a device acts as an agent to facilitate the communication between a payment server **324** and the e-purse **312** as well as the emulator **314**, wherein the payment server **324** has the access to the existing new e-purse SA module **306** and a SA module **308**. As a result of the personalization process, the e-purse applet **312** and the emulator **314** are personalized.

**[0039]** Referring now back to FIG. 3C, after the personalization process is started, in view of FIG. 3A, the RFID reader **310** is activated to read the tag ID and essential data from a 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 device.

**[0040]** Each application security domain of a global platform includes three 3DES keys. For example:

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

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

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

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.

**[0041]** 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.

**[0042]** With the security channel is established using the application provider's application security domain, the first set of data can be personalized to the 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.

**[0043]** Via the new 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**.

**[0044]** 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 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”.

**[0045]** FIG. 4A and FIG. 4B show together a flowchart or process **400** of financing 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.

**[0046]** A user is assumed to have obtained a portable device (e.g., a cellphone) 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, a purse manger in the device is activated and initiates a request (also referred to an OTA top off request) at **404**. The midlet in the 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**.

**[0047]** 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 wireless 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 can not 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).

**[0048]** 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 forward the commands the e-purse at **418**. The e-purse verifies the commands at **420** and, provided they are authorized, send 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 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**.

**[0049]** As shown in FIG. 4C, the payment network and server **440** receives a response from the purse manager midlet **434** and verifies that the response is from an authorized e-purse originally issued therefrom with a SAM module **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 bank, the server **440** will either reject the request or form a network response to be sent to the midlet **434**.

**[0050]** The e-purse 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 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**.

**[0051]** 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.

**[0052]** 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.

**[0053]** 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 method for providing an e-purse, the method comprising:  
providing a portable device including or communicating with a smart card module pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate communication between an e-purse applet therein and a payment server over a wireless network, wherein the portable device further includes a contactless interface that facilitates communication between the e-purse applet therein and the payment server over a wired network;  
personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys that are subsequently used to establish a secured channel between the e-purse and a SAM or a payment server.
2. The method as recited in claim 1, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.
3. The method as recited in claim 2, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and an existing SAM originally used to issue the e-purse as well as between the emulator and the existing SAM.

4. The method as recited in claim 2, wherein said personalizing the e-purse applet is done over a wireless network or a wired network.
5. The method as recited in claim 4, wherein, when said personalizing the e-purse applet is done over a wireless network, the midlet in the portable device is configured to facilitate communications between the e-purse and the payment server.
6. The method as recited in claim 5, wherein both of the e-purse applet and the emulator are personalized as a result of said personalizing the e-purse applet.
7. The method as recited in claim 1, further comprising:
  - initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;
  - sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;
  - transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and
  - sending a response from the payment server to the midlet that is configured to process the response before releasing the response to the e-purse applet.
8. The method as recited in claim 7, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.

9. The method as recited in claim 8, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.
  
10. The method as recited in claim 1, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device, and the e-purse supports transactions in either e-commerce or m-commerce.
  
11. A system for providing an e-purse, the system comprising:
  - a portable device including or communicating with a smart card module pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate wireless communication between an e-purse applet therein and a payment server over a wireless network, the portable device further including a contactless interface that facilitates communication between the e-purse applet therein and the payment server over a wired network;
  - the payment server associated with an issuer of the e-purse; and
  - an SAM configured to enable the e-purse, wherein the SAM is behind the payment server when the e-purse is caused to communicate with the payment server via the midlet over a wireless network, the SAM is communicated with the e-purse via the contactless interface when the e-purse is caused to communicate with the payment server over a wired network.
  
12. The system as recited in claim 11, wherein both of the e-purse applet and emulator are personalized by reading off data from the smart card, the data is then used to generate operation keys for the e-purse applet.

13. The system as recited in claim 12, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.
14. The system as recited in claim 13, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and an existing SAM originally used to issue the e-purse as well as between the emulator and the existing SAM.
15. The system as recited in claim 11, wherein, when the portable device is used to have a transaction, there are operations of:
- initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;
  - sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;
  - transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and
  - sending a response from the payment server to the midlet that is configured to process the response before releasing the response to the e-purse applet.

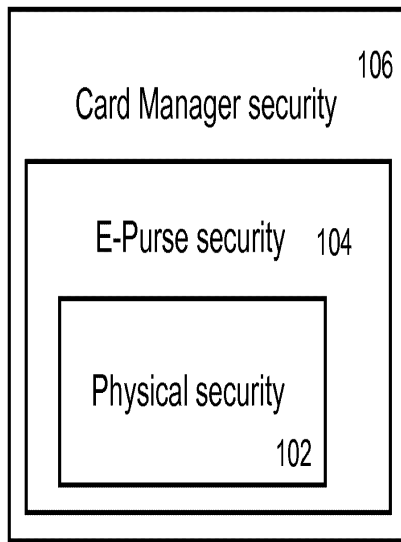
16. The system as recited in claim 15, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.
17. The system as recited in claim 16, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.
18. The system as recited in claim 11, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device.

## **Method and apparatus for providing electronic purse**

### **Abstract**

Techniques for portable devices functioning as an electronic purse (e-purse) are disclosed. According to one aspect of the invention, a mechanism is provided to enable a portable device to conduct transactions over an open network with a payment server without compromising security. In one embodiment, a device is loaded with an e-purse manager. The e-purse manager is configured to manage various transactions and functions as a mechanism to access an emulator therein. The transactions may be conducted over a wired network or a wireless network. A three-tier security model is contemplated to support the security of the transactions from the e-purse. The three-tier security model includes a physical security, an e-purse security and a card manager security, concentrically encapsulating one with another. Security keys (either symmetric or asymmetric) are personalized within the three-tier security model.

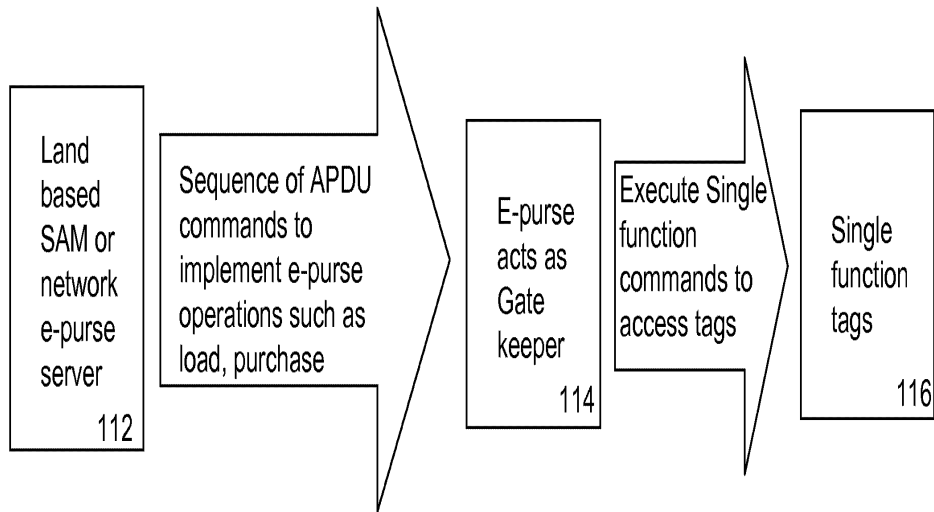
100



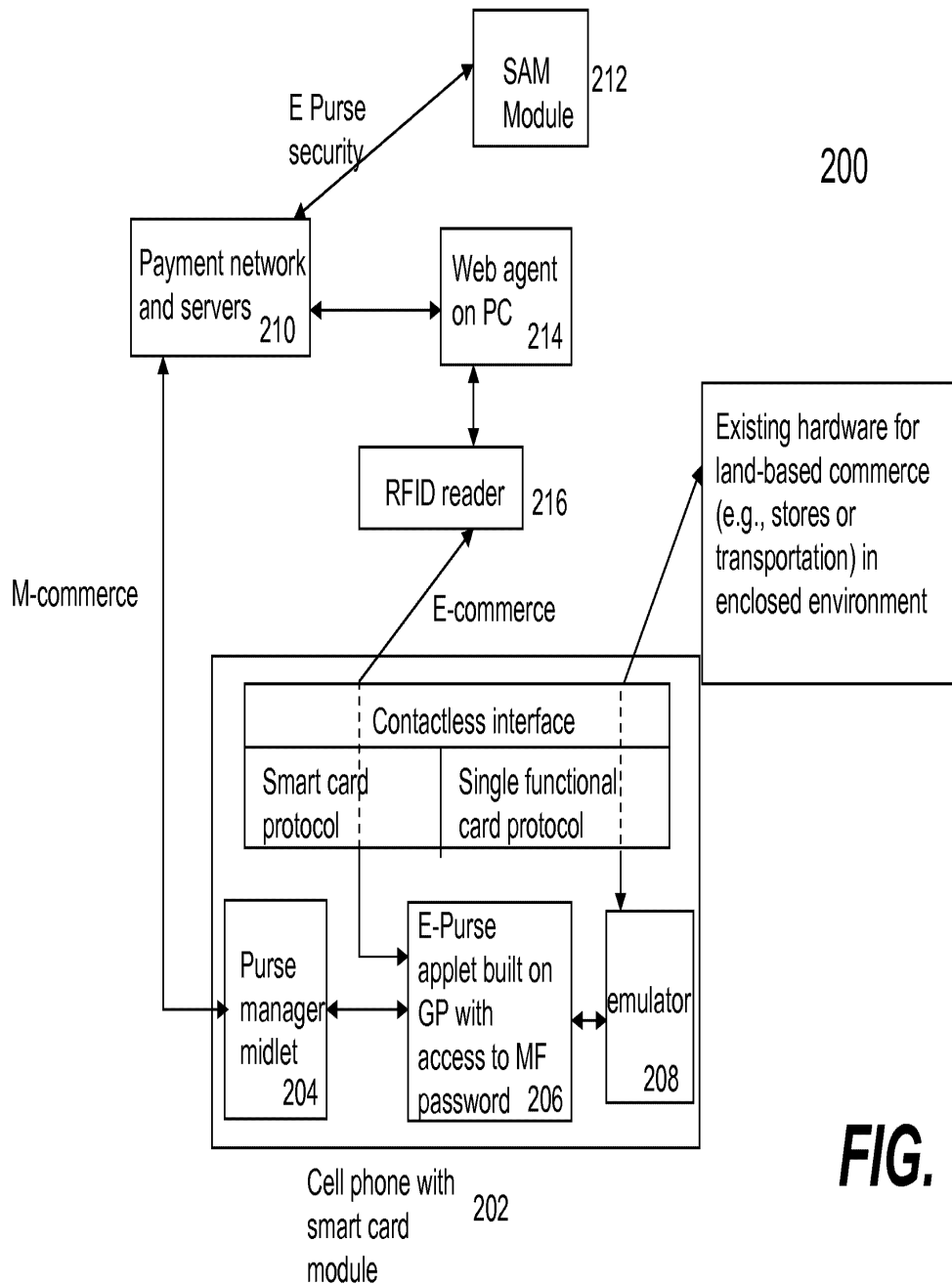
**FIG. 1A**



110

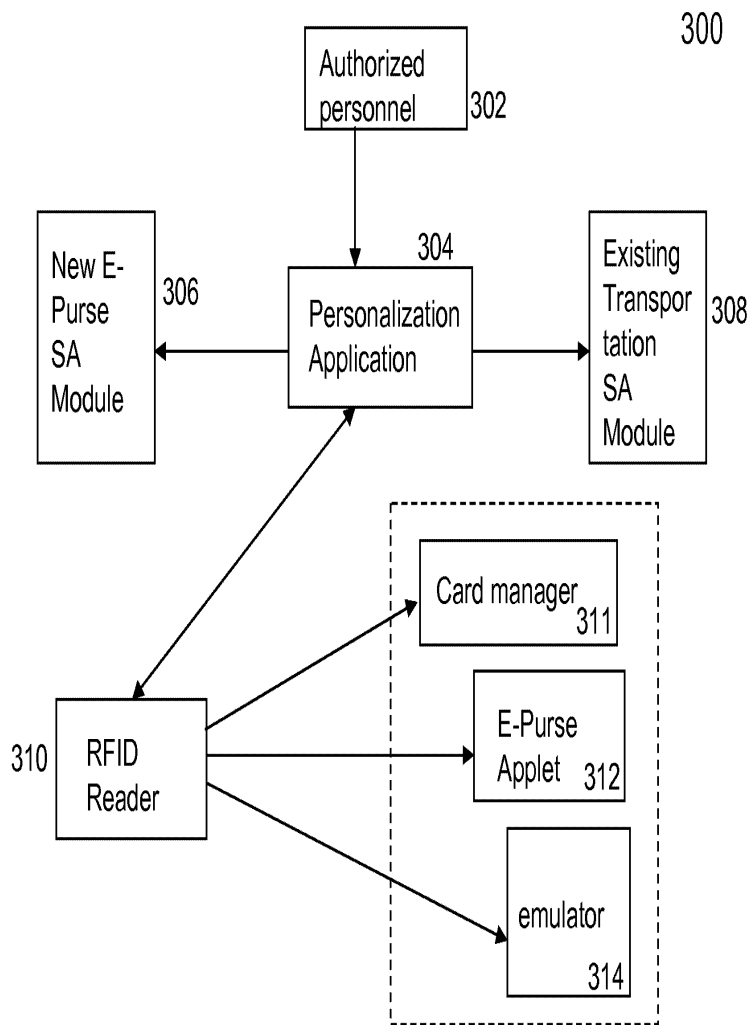


**FIG. 1B**

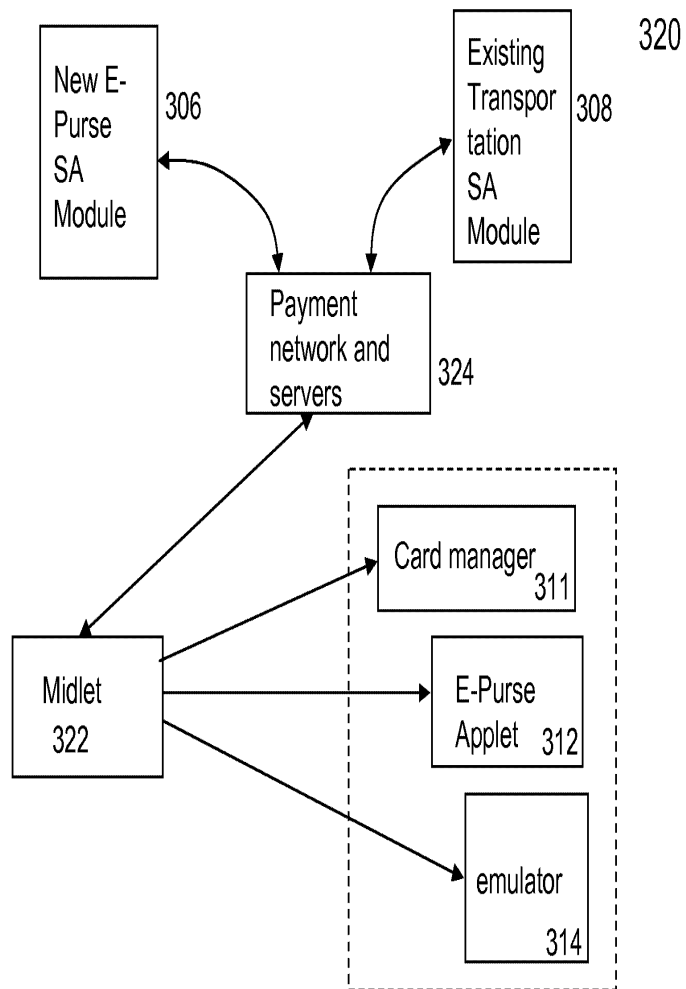


200

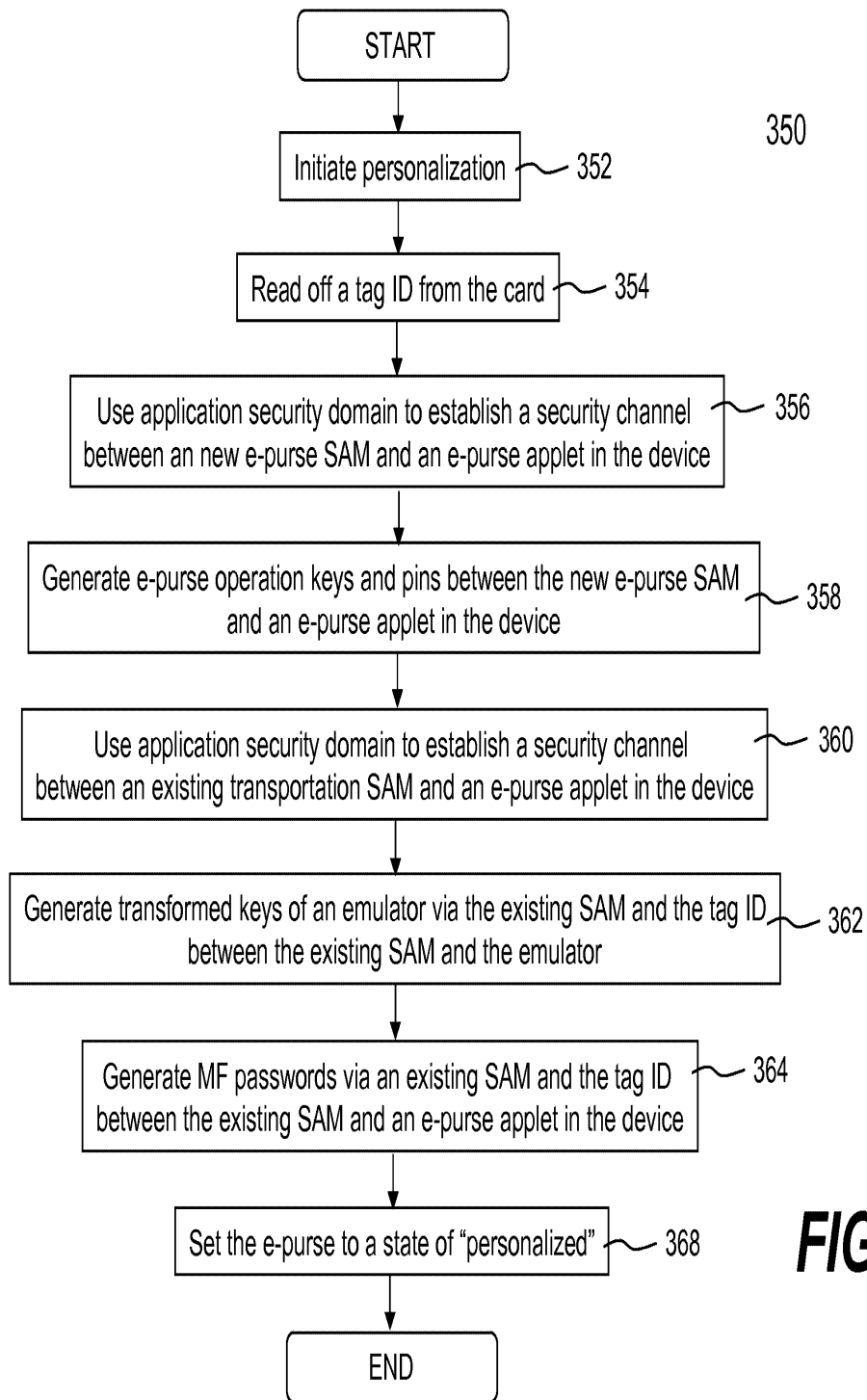
**FIG. 2**



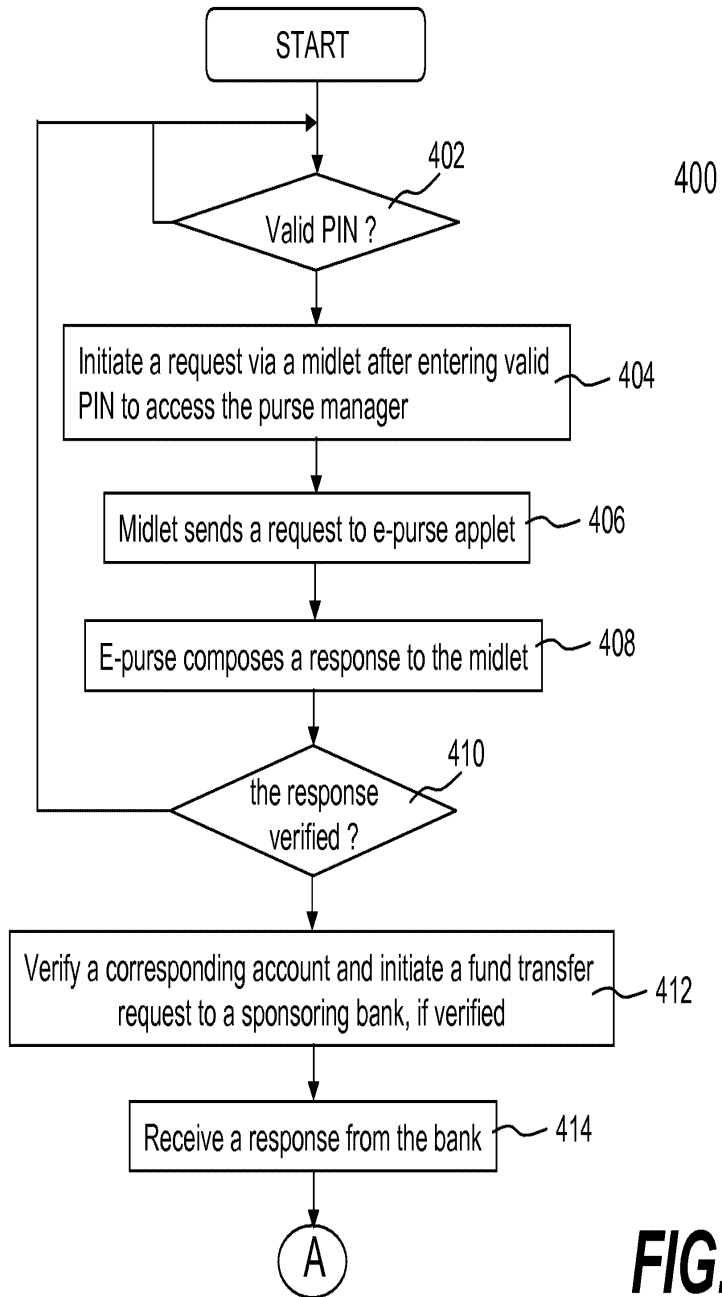
**FIG. 3A**



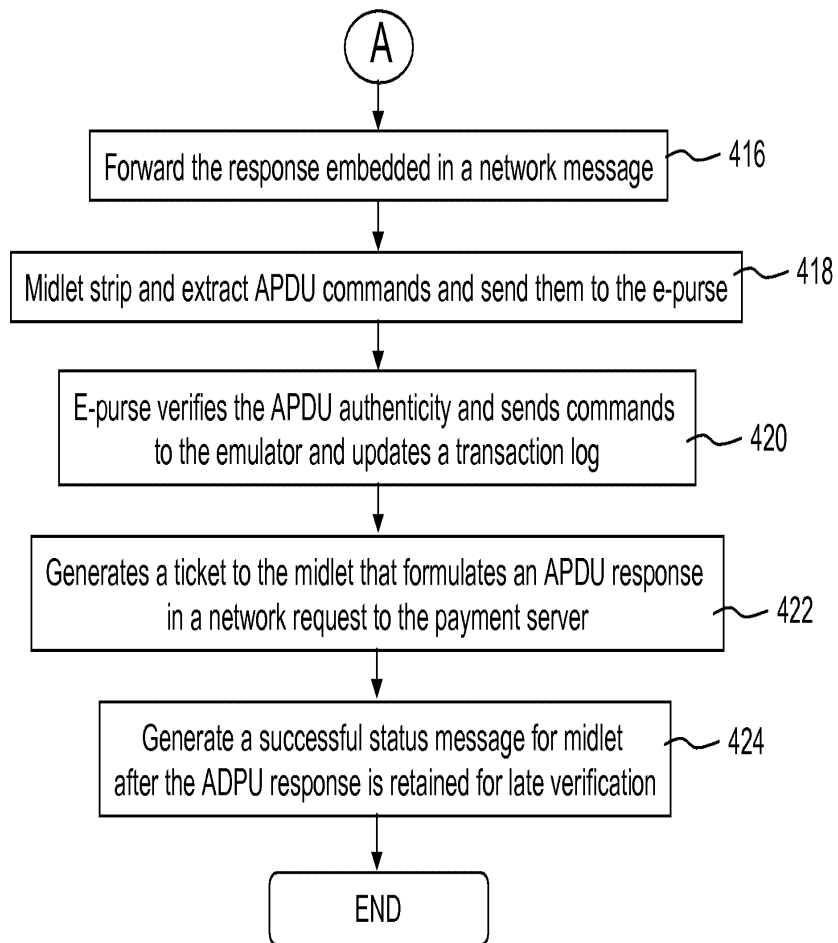
**FIG. 3B**



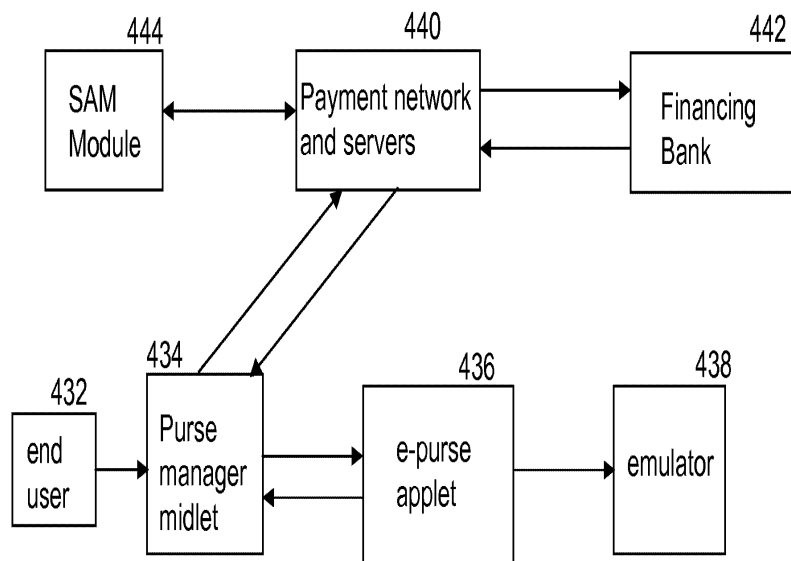
**FIG. 3C**



**FIG. 4A**



**FIG. 4B**



**FIG. 4C**



## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	1216431
<b>Application Number:</b>	11534653
<b>Confirmation Number:</b>	6327
<b>Title of Invention:</b>	Method and apparatus for providing electronic purse
<b>First Named Inventor:</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-081
<b>Receipt Date:</b>	24-SEP-2006
<b>Filing Date:</b>	
<b>Time Stamp:</b>	00:24:33
<b>Application Type:</b>	Utility
<b>International Application Number:</b>	

### Payment information:

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

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Specification	PatentAsFiled.pdf	125409	no	23

<b>Warnings:</b>					
<b>Information:</b>					
2	Drawings	DrawingH.pdf	61465	no	9
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			186874		
<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>  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>					

Please type a plus sign (+) inside this box →

PTO/SB/01 (12-97)

Approved for use through 9/30/00. OMB 0651-0032  
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

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

<b>DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)</b>  <input checked="" type="checkbox"/> Declaration Submitted with Initial Filing <input type="checkbox"/> Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)	Attorney Docket Number	RFID-081
	First Named Inventor	Liang Seng Koh
	<i>COMPLETE IF KNOWN</i>	
	Application Number	/
	Filing Date	
	Group Art Unit	
Examiner Name		

**As a below named inventor, I hereby declare that:**

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

**Method and apparatus for providing electronic purse**

the specification of which (Title of the Invention)

is attached hereto  
OR  
 was filed on (MM/DD/YYYY)  as United States Application Number or PCT International Application Number  and was amended on (MM/DD/YYYY)  (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

---

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	
		<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 0.4 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, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box →

PTO/SB/01 (12-97)  
Approved for use through 9/30/00. OMB 0651-0032  
Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

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

## DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Customer Number **26797** → Place Customer Number Bar Code Label here  
OR  
 Registered practitioner(s) name/registration number listed below

Name	Registration Number	Name	Registration Number

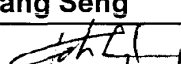
Additional registered practitioner(s) named on supplemental Registered Practitioner Information sheet PTO/SB/02C attached hereto.

Direct all correspondence to:  Customer Number or Bar Code Label **26797** OR  Correspondence address below

Name						
Address						
Address						
City		State		ZIP		
Country		Telephone	<b>(408)777-8873</b>	Fax	<b>(408)873-9249</b>	

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 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**Name of Sole or First Inventor:**  A petition has been filed for this unsigned inventor

Given Name (first and middle (if any))			Family Name or Surname				
<b>Liang Seng</b>			<b>Koh</b>				
Inventor's Signature				Date	<b>9-23-06</b>		
Residence: City	<b>Fremont</b>	State	<b>CA</b>	Country	<b>USA</b>	Citizenship	<b>USA</b>
Post Office Address	<b>41291 Carmen Street</b>						
Post Office Address							
City	<b>Fremont</b>	State	<b>CA</b>	ZIP	<b>94539</b>	Country	<b>USA</b>

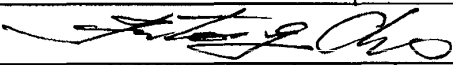
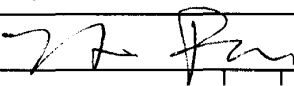

Additional inventors are being named on the **1** supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto

Please type a plus sign (+) inside this box →

PTO/SB/02A (3-97)  
 Approved for use through 9/30/98. OMB 0651-0032  
 Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

<b>DECLARATION</b>	<b>ADDITIONAL INVENTOR(S) Supplemental Sheet</b> Page <u>1</u> of <u>2</u>
--------------------	---

<b>Name of Additional Joint Inventor, if any:</b>		<input type="checkbox"/> A petition has been filed for this unsigned inventor					
Given Name (first and middle [if any])				Family Name or Surname			
<b>Futong</b>				<b>Cho</b>			
Inventor's Signature						Date	1/23/06
Residence: City	<b>Milpitas</b>	State	<b>CA</b>	Country	<b>USA</b>	Citizenship	<b>USA</b>
Post Office Address	<b>397 Sandhurst Drive</b>						
Post Office Address							
City	<b>Milpitas</b>	State	<b>CA</b>	ZIP	<b>95035</b>	Country	<b>USA</b>
<b>Name of Additional Joint Inventor, if any:</b>		<input type="checkbox"/> A petition has been filed for this unsigned inventor					
Given Name (first and middle [if any])				Family Name or Surname			
<b>Hsin</b>				<b>Pan</b>			
Inventor's Signature						Date	1/23/06
Residence: City	<b>Fremont</b>	State	<b>CA</b>	Country	<b>US</b>	Citizenship	<b>USA</b>
Post Office Address	<b>2374 Olive Avenue</b>						
Post Office Address							
City	<b>Fremont</b>	State	<b>CA</b>	ZIP	<b>94539</b>	Country	<b>US</b>
<b>Name of Additional Joint Inventor, if any:</b>		<input type="checkbox"/> A petition has been filed for this unsigned inventor					
Given Name (first and middle [if any])				Family Name or Surname			
<b>Fuliang</b>				<b>Cho</b>			
Inventor's Signature						Date	1/23/06
Residence: City	<b>San Jose</b>	State	<b>CA</b>	Country	<b>US</b>	Citizenship	<b>USA</b>
Post Office Address	<b>5812 McKellar Drive</b>						
Post Office Address							
City	<b>San Jose</b>	State	<b>CA</b>	ZIP	<b>95129</b>	Country	<b>US</b>

Burden Hour Statement: This form is estimated to take 0.4 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, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Electronic Patent Application Fee Transmittal				
<b>Application Number:</b>	11534653			
<b>Filing Date:</b>				
<b>Title of Invention:</b>				
<b>First Named Inventor:</b>	Liang Seng Koh			
<b>Filer:</b>	Joe Zheng			
<b>Attorney Docket Number:</b>				
Filed as Small Entity				
<b>Utility Filing Fees</b>				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
Utility filing Fee (Electronic filing)	4011	1	75	75
Utility Search Fee	2111	1	250	250
Utility Examination Fee	2311	1	100	100
<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(\$)
Post-Allowance-and-Post-Issuance:				
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>425</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	1229393
<b>Application Number:</b>	11534653
<b>Confirmation Number:</b>	6327
<b>Title of Invention:</b>	
<b>First Named Inventor:</b>	Liang Seng Koh
<b>Correspondence Address:</b>	- - - - - - -
<b>Filer:</b>	Joe Zheng
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	
<b>Receipt Date:</b>	30-SEP-2006
<b>Filing Date:</b>	
<b>Time Stamp:</b>	00:34:10
<b>Application Type:</b>	Utility
<b>International Application Number:</b>	

### Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$425



RAM confirmation Number	1692
Deposit Account	

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Oath or Declaration filed	Declaration.pdf	255461	no	3

**Warnings:**

**Information:**

2	Fee Worksheet (PTO-875)	fee-info.pdf	8287	no	2
---	-------------------------	--------------	------	----	---

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>			263748		
-------------------------------------	--	--	--------	--	--

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.



## UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/534,653	09/24/2006	Liang Seng Koh	RFID-081

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

**CONFIRMATION NO. 6327**  
**FORMALITIES**  
**LETTER**

Date Mailed: 10/23/2006

### NOTICE OF INCOMPLETE REPLY (NONPROVISIONAL)

#### *Filing Date Granted*

The U.S. Patent and Trademark Office has received your reply on 09/30/2006 to the Notice to File Missing Parts (Notice) mailed 10/23/2006 and it has been entered into the nonprovisional application. The reply, however, does not include the following items required in the Notice.

The period of reply remains as set forth in the Notice. You may, however, obtain EXTENSIONS OF TIME under the provisions of 37 CFR 1.136 (a) accompanied by the appropriate fee (37 CFR 1.17(a)).

A complete reply must be timely filed to prevent ABANDONMENT of the above-identified application. Replies should be mailed to: Mail Stop Missing Parts, Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

- Surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$65 was not received.

The applicant needs to satisfy supplemental fees problems indicated below.

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

#### **SUMMARY OF FEES DUE:**

Total additional fee(s) required for this application is **\$65** for a small entity

- **\$65** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria VA 22313-1450

***A copy of this notice MUST be returned with the reply.***

A handwritten signature in black ink, appearing to read "Symantec" followed by a stylized flourish.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382

PART 3 - OFFICE COPY



## UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/534,653	09/24/2006	Liang Seng Koh	RFID-081

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

**CONFIRMATION NO. 6327**  
**FORMALITIES**  
**LETTER**

Date Mailed: 10/23/2006

## NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

*Filing Date Granted*

### Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. 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 oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*  
*Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.*

The applicant needs to satisfy supplemental fees problems indicated below.

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

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.

### SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **\$65** for a small entity

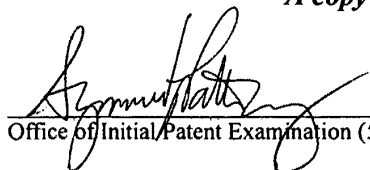
- **\$65** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts  
 Commissioner for Patents

P.O. Box 1450  
Alexandria VA 22313-1450

---

*A copy of this notice **MUST** be returned with the reply.*

A handwritten signature in black ink, appearing to be "S. M. Patten", is written over a horizontal line.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382  
PART 3 - OFFICE COPY



## UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
11/534,653	09/24/2006	Liang Seng Koh	RFID-081

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

**CONFIRMATION NO. 6327**  
**FORMALITIES**  
**LETTER**

Date Mailed: 10/23/2006

## NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

*Filing Date Granted*

### Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. 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 oath or declaration is missing. *A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.*  
*Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.*

The applicant needs to satisfy supplemental fees problems indicated below.

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

- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.

### SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **\$65** for a small entity

- **\$65** Surcharge.

Replies should be mailed to: Mail Stop Missing Parts  
 Commissioner for Patents

P.O. Box 1450  
Alexandria VA 22313-1450

---

*A copy of this notice **MUST** be returned with the reply.*

A handwritten signature in black ink, appearing to be "Symon P. [unclear]", written over a horizontal line.

Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382  
PART 3 - OFFICE COPY

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

**Applicant(s):** Liang Seng Koh  
**Title:** Method and apparatus for providing electronic purse  
**Serial No.:** 11/534,653  
**Filing Date:** 9/24/2006  
**Examiner:** Unknown  
**Group Art Unit:** N/A  
**Docket No.:** RFID-081

---

November 19, 2006

Commissioner of Patents and Trademarks  
Box Missing Parts  
Washington, DC 20231

Response to Notice to File Missing Parts of Application  
*Filing Date Granted*

Dear Sir:

In response to the "Notice To Missing parts of Application – Filing Date Granted" mailed by the United States Patent and Trademark Office on 10/23/2006, the following document is enclosed to complete the filing of the above-identified patent application:

1. \$65 payment is enclosed

It is hereby respectfully submitted that the enclosed documents complete the filing of the above patent application and justify the US filing date of 9/24/2006. 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", November 19, 2006.

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>	11534653			
<b>Filing Date:</b>	24-Sep-2006			
<b>Title of Invention:</b>	Method and apparatus for providing electronic purse			
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh			
<b>Filer:</b>	Joe Zheng			
<b>Attorney Docket Number:</b>	RFID-081			
Filed as Small Entity				
<b>Utility 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>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
Late filing fee for oath or declaration	2051	1	65	65
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
Post-Allowance-and-Post-Issuance:				
<b>Extension-of-Time:</b>				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>65</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	1322713
<b>Application Number:</b>	11534653
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	6327
<b>Title of Invention:</b>	Method and apparatus for providing electronic purse
<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-081
<b>Receipt Date:</b>	19-NOV-2006
<b>Filing Date:</b>	24-SEP-2006
<b>Time Stamp:</b>	17:59:53
<b>Application Type:</b>	Utility

### Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$65
RAM confirmation Number	1129
Deposit Account	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	------------------	------------------	------------------

1	Response to Pre-Exam Sequence Notice	MissingNotice.pdf	55167	no	2
<b>Warnings:</b>					
<b>Information:</b>					
2	Response to Pre-Exam Sequence Notice	ResponseToMissingParts.pdf	83600	no	1
<b>Warnings:</b>					
<b>Information:</b>					
3	Fee Worksheet (PTO-875)	fee-info.pdf	8140	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			146907		
<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>  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>					



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 8 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, DRAWINGS, TOT CLAIMS, IND CLAIMS. Row 1: 11/534,653, 09/24/2006, 2876, 490, RFID-081, 9, 18, 2

CONFIRMATION NO. 6327

26797
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA95014

UPDATED FILING RECEIPT

Date Mailed: 11/21/2006

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. 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 mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. 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 (if appropriate).

Applicant(s)

Liang Seng Koh, Fremont, CA;
Futong Cho, Milpitas, CA;
Hsin Pan, Fremont, CA;
Fuliang Cho, San Jose, CA;

Assignment For Published Patent Application

RFCyber Corp., Fremont, CA

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

Domestic Priority data as claimed by applicant

Foreign Applications

If Required, Foreign Filing License Granted: 10/17/2006

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is US11/534,653

Projected Publication Date: 03/27/2008

Non-Publication Request: No

Early Publication Request: No

\*\* SMALL ENTITY \*\*

Title

Method and apparatus for providing electronic purse

**Preliminary Class**

235

**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 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 application(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).



APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/534,653	09/24/2006	Liang Seng Koh	RFID-081

**CONFIRMATION NO. 6327**

26797  
SILICON VALLEY PATENT AGENCY  
7394 WILDFLOWER WAY  
CUPERTINO, CA95014

**Title:** Method and apparatus for providing electronic purse

**Publication No.** US-2008-0073426-A1

**Publication Date:** 03/27/2008

### 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 publicly available Searchable Databases via the Internet at [www.uspto.gov](http://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](http://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.

---

Pre-Grant Publication Division, 703-605-4283





UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/534,653	09/24/2006	Liang Seng Koh	RFID-081	6327
26797                      7590                      02/03/2010 SILICON VALLEY PATENT AGENCY 7394 WILDFLOWER WAY CUPERTINO, CA 95014			EXAMINER STANFORD, CHRISTOPHER J	
			ART UNIT	PAPER NUMBER
			2887	
			NOTIFICATION DATE	DELIVERY MODE
			02/03/2010	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> 11/534,653	<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 24 September 2006.
- 2a)  This action is **FINAL**.                      2b)  This action is non-final.
- 3)  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**

- 4)  Claim(s) 1-18 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5)  Claim(s) \_\_\_\_\_ is/are allowed.
- 6)  Claim(s) 1-18 is/are rejected.
- 7)  Claim(s) \_\_\_\_\_ is/are objected to.
- 8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9)  The specification is objected to by the Examiner.
- 10)  The drawing(s) filed on 24 September 2006 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).
- 11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**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)  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4)  Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_\_.

## DETAILED ACTION

### *Claim Objections*

1. Claims 1, 3, 11, and 14 are objected to because of the following informalities: the abbreviate "SAM" should be defined prior to the use of the acronym. Appropriate correction is required. For the purposes of examination, "SAM" will be interpreted to mean **security authentication module**.
2. Claims 11 is objected to because of the following informalities: there appears to be a typographical error in claim 11 wherein "the SAM **is communicated** with the e-purse". Appropriate correction is required. The SAM as depicted in the specifications and Figures 2 and 3A, for example, appears to be either an externally run program/applet or remote hardware that is not capable or **being** communicated. For the purposes of examination, this limitation will be interpreted to mean "the SAM is **in communication** with the e-purse".

### *Claim Rejections - 35 USC § 112*

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:  

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
4. Claims 7-9 and 15-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 7 and 15 recite the limitation "the response" in the final lines of each claim. There is insufficient antecedent basis for this limitation in the claim. Claims 7 and 15 recite at least two responses (line 5 and 10 for

claim 7, lines 6 and 11 for claim 15) and thus “the response” does not clearly point out to which response applicant refers. Claims 8-9 and 16-17 are rejected due to their dependence on claims 7 and 15 respectively.

***Claim Rejections - 35 USC § 102***

5. 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.

6. Claims 1-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Shmueli et al. (US 2002/0145632 A1; hereinafter Shmueli).

Regarding claim 1, Shmueli teaches providing an e-purse (e-wallet 82, Fig. 6; para [0053]), the method comprising: providing a portable device (host system 12 embodied as a cell phone, Fig. 1; para [0029]) including or communicating with a smart card module (key 10 embodied as smart card 10B, Figs. 1 & 2B; para [0033]) pre-loaded with an emulator (para [0027-0028]), the portable device including a memory space (memory 28, Fig. 1; para [0029]) loaded with a midlet (keylets such as web keylet 56, Fig. 4) that is configured to facilitate communication between an e-purse applet (key manager application 58, Fig. 4; para [0041-0044]) therein and a payment server (server 14 running web servlet 66, Figs. 1 & 4) over a wireless network (mobile phone network is partially wireless), wherein the portable device further includes a contactless interface (mobile phone network interface 38, Fig. 1) that facilitates communication between the

e-purse applet therein and the payment server over a wired network (host 12 embodied as a mobile phone accessing network 16 via the internet would include a partially wired network, i.e. the internet); personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys (Figs. 3A-3B) that are subsequently used to establish a secured channel between the e-purse and a SAM or a payment server (para [0037-0042]).

Regarding claims 2 and 13, Shmueli teaches the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords (Figs. 3A-3B; para [0037-0042]).

Regarding claims 3 and 14, Shmueli teaches at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server (Figs. 3A-3B; para [0037-0042]), and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and an existing SAM (e.g. VISA) originally used to issue the e-purse as well as between the emulator and the existing SAM (para [0044-0047, 0063-0064]).

Regarding claim 4, Shmueli teaches the personalizing the e-purse applet is done over a wireless network or a wired network (via network 16 which is embodied as a mobile phone network and the internet, Figs. 3A-3B; para [0037-0042]).

Regarding claim 5, Shmueli teaches when the personalizing the e-purse applet is done over a wireless network, the midlet in the portable device is configured to facilitate

communications between the e-purse and the payment server (keylets such as web keylet 56, Fig. 4; para [0037-0042]).

Regarding claim 6, Shmueli teaches both of the e-purse applet and the emulator are personalized as a result of said personalizing the e-purse applet (key 10 and host 12 contain applet and emulator and all are personalized via authentication, Figs. 3A, 3B, & 4; para [0037-0042]).

Regarding claims 7 and 15, Shmueli teaches initiating a request (para [0042-0045]) from the e-purse after valid personal identification numbers are entered and accepted on the portable device (steps 114-120, Fig. 3A); sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet (data from files 60, 62, 64 sent from key manager application to web keylets in the interaction with web servlets 66, Fig. 4; para [0042-0045,0057,0064]); transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse (authenticated prior to running keylet, Fig. 3A-B), wherein the payment server further communicates with a financial institution (business partners of third party services 70, para [0044,0063-0064]) to authorize a transaction therewith; and sending a response (update key automatically, step 124 of Fig. 3B) from the payment server to the midlet that is configured to process the response before releasing the response to the e-purse applet (para [0039]).

Regarding claims 8 and 16, Shmueli teaches messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages (files sent via network; para [0027-0028,0041-0042]).

Regarding claims 9 and 17, Shmueli teaches the commands are applicable for Application Protocol Data Unit (APDU) (data files system; para [0027-0028,0041-0042,0096-0098]). Shmueli teaches commands for authentication, access, and data transfer just as is evident in APDU and therefore the commands **are applicable** for APDU. The prior art need not teach the specific format of APDU commands in order to teach the applicability of the commands.

Regarding claims 10 and 18, Shmueli teaches the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device (para [0063-0064]), and the e-purse supports transactions in either e-commerce or m-commerce (para [0063-0064]).

Regarding claim 11, Shmueli teaches a system for providing an e-purse (e-wallet 82, Fig. 6; para [0053]), the system comprising: a portable device (host system 12 embodied as a cell phone, Fig. 1; para [0029]) including or communicating with a smart card module (key 10 embodied as smart card 10B, Figs. 1 & 2B; para [0033]) pre-loaded with an emulator (para [0027-0028]), the portable device including a memory space (memory 28, Fig. 1; para [0029]) loaded with a midlet (keylets such as web keylet 56, Fig. 4) that is configured to facilitate wireless communication between an e-purse applet (key manager application 58, Fig. 4; para [0041-0044]) therein and a payment server (server 14 running web servlet 66, Figs. 1 & 4) over a wireless network (mobile phone network is partially wireless), the portable device further including a contactless interface (mobile phone network interface 38, Fig. 1) that facilitates communication between the e-purse applet therein and the payment server over a wired network (host

12 embodied as a mobile phone accessing network 16 via the internet would include a partially wired network, i.e. the internet); the payment server associated with an issuer of the e-purse (para [0044-0047, 0063-0064]); and an SAM (third party services behind extended application program interface 74 of server 14, Figs. 1 and 3-4) configured to enable the e-purse, wherein the SAM is behind the payment server when the e-purse is caused to communicate with the payment server via the midlet over a wireless network (Figs. 3A-3B; para [0037-0047,0063-0064]), the SAM is communicated with the e-purse via the contactless interface when the e-purse is caused to communicate with the payment server over a wired network (mobile phones connecting to business partners, VISA, and/or credit card management companies over the internet communicate over a partially wired and partially wireless network 16).

Regarding claim 12, Shmueli teaches both of the e-purse applet and emulator are personalized (Figs. 3A-3B) by reading off data from the smart card (para [0037-0042]), the data is then used to generate operation keys for the e-purse applet (para [0037-0042]).

### ***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 , 7:30am-4:30pm.



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.

/Thien M. Le/  
Primary Examiner, Art Unit 2887

/CHRISTOPHER STANFORD/  
Examiner, Art Unit 2887

<b>Notice of References Cited</b>	Application/Control No. 11/534,653	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-2002/0145632 A1	10-2002	Shmueli et al.	345/835
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	Classification
N					
O					
P					
Q					
R					
S					
T					

**NON-PATENT DOCUMENTS**

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

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

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	"11534653"	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/08 14:04
S2	6	"7349871"	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/08 14:21
S3	184769	(ic or integrated circuit or smart or sim or subscriber near2 module or chip or rf or radio frequeuncy or rfid) (tag or card) or rfid or icc	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 11:26
S4	222	(emulate or emulator) same (midlet or mid let or applet)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:17
S5	68	S3 and S4	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:17
S6	4315	(e or electronic or digital) (purse or wallet) or epurse or ewallet	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:18
S7	11	S5 and S6	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:18
S8	127	(rfcyber).as. or (koh near2 (liang or l) or cho near2 futong or pan near2 hsin or cho near2 fuilang). inv.	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:52

S9	2	S8 and (midlet or applet or emmulator)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:53
S10	57	S3 and S4 and (transaction or (credit or debit) card)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:56
S11	10803	(emulate or emulator) same (midlet or mid let or applet or application)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:57
S12	5095	(emulate or emulator) with (midlet or mid let or applet or application)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:57
S13	284	S3 and S12 and (transaction or (credit or debit) card)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:57
S14	233	S13 and ("235". clas. or "7"\$3. clas.)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 12:57
S15	46	S6 same (emulate or emulator or simulator)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 14:18
S16	33	S6 same (emulate or emulator or simulator) not (magnetic with emulator)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 14:24
S17	13	S6 and midlet	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/01/25 14:29

**EAST Search History (I nterference)**

&lt; This search history is empty &gt;

**1/ 25/ 2010 4:22:14 PM****C:\ Documents and Settings\ cstanford\ My Documents\ EAST\ Workspaces\ 11534653.wsp**




## UNITED STATES PATENT AND TRADEMARK OFFICE

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

## BIB DATA SHEET

CONFIRMATION NO. 6327

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
11/534,653	09/24/2006	235	2887	RFID-081		
<b>APPLICANTS</b> Liang Seng Koh, Fremont, CA; Futong Cho, Milpitas, CA; Hsin Pan, Fremont, CA; Fuliang Cho, San Jose, CA;						
** CONTINUING DATA *****						
** FOREIGN APPLICATIONS *****						
** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** * SMALL ENTITY ** 10/17/2006						
Foreign Priority claimed 35 USC 119(a-d) conditions met Verified and Acknowledged	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No /CHRISTOPHER J STANFORD/ Examiner's Signature	<input type="checkbox"/> Met after Allowance Initials	<b>STATE OR COUNTRY</b> CA	<b>SHEETS DRAWINGS</b> 9	<b>TOTAL CLAIMS</b> 18	<b>INDEPENDENT CLAIMS</b> 2
<b>ADDRESS</b> SILICON VALLEY PATENT AGENCY 7394 WILDFLOWER WAY CUPERTINO, CA 95014 UNITED STATES						
<b>TITLE</b> Method and apparatus for providing electronic purse						
<b>FILING FEE RECEIVED</b> 490	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			

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 11534653	<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>

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

CLAIM		DATE									
Final	Original	01/25/2010									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	✓									

<b>Search Notes</b>  	<b>Application/Control No.</b>  11534653	<b>Applicant(s)/Patent Under Reexamination</b>  KOH ET AL.
	<b>Examiner</b>  CHRISTOPHER STANFORD	<b>Art Unit</b>  2887

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
235	379,380,492	1/22-25/10	CS

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>
Inventor, Assignee Search	1/22-25/10	CS
NPL Search	1/22-25/10	CS
Text Search (see search history report print out)	1/22-25/10	CS

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

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

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

**Applicant(s):** Liang Seng Koh et al  
**Title:** Method and apparatus for providing electronic purse  
**Serial No.:** 11/534,653  
**Confirmation No.:** 6327  
**Filing Date:** 09/24/2006  
**Examiner:** Chris Stanford  
**Group Art Unit:** 2887  
**Docket No:** RFID-081

---

May 3, 2010

Mail Stop: Non-fee amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Response to 1<sup>st</sup> OA**

Dear Sir:

In response to Office Action dated 02/03/2010, 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 [0027] as follows:

**[0027]** Card Manager Security **106**, referring to a general security framework of a preload operating system in a smart card, provides a platform for PIN management and security channels (security domains) for card personalization. This platform via a card manager can be used to personalize a purse in one embodiment. One example of the card manager security **106** is what is referred to as a Global Platform (GP) that is created by a cross-industry membership organization ~~created~~ to advance standards for smart card growth. A GP combines the interests of smart card issuers, vendors, industry groups, public entities and technology companies to define requirements and technology standards for multiple application smart cards. In one embodiment, a global platform security is used to personalize a smart card. As a result, both e-purse keys and card access keys are personalized into the target tag.

2. Please amend paragraph [0029] as follows:

**[0029]** In reference to FIG. 1A, the physical security is realized in an emulator. As ~~sued~~ 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 a payment server. The card manager security (e.g., global platform security) is realized via a card manager to update security keys to establish appropriate channels for interactions between the server and the applets, wherein the e-purse applet(s) acts as a gatekeeper to regulate or control the data exchange.

3. Please amend paragraph [0034] as follows:

**[0034]** To personalize the cellphone **202**, 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 by an authorized person as shown in FIG. 2. 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 ~~an~~ a user of the e-purse as shown in FIG. 2.

4. Please amend paragraph [0037] as follows:

**[0037]** It is assumed that a user desires to personalize an e-purse embedded in a device (e.g., a cellphone). At **352** of FIG. 3C, a personalization process is initiated. Depending on implementation, the personalization process may be implemented in a module in the 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 for a user thereof via an ~~existing~~-new e-purse SA module **306** and an existing SA module **308** with the RFID 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 **304**, the e-purse applet **312** and the emulator **314** are personalized.

5. Please amend paragraph [0038] as follows:

**[0038]** Similarly, as shown in FIG. 3B, a user of an e-purse desires to initiate a personalization process to personalize the e-purse 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 cellphone 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** in a device acts as an agent to facilitate the communication between a payment server **324** and the e-purse **312** as well as the emulator **314**, wherein the payment server **324** has the access to the ~~existing~~-new e-purse SA module **306** and an existing SA module **308**. As a result of the personalization process, the e-purse applet **312** and the emulator **314** are personalized.

## AMENDMENTS TO THE CLAIMS

Please amend Claims 1, 3, 11, 14 and 15 as follows:

- (Currently amended)* A method for providing an e-purse, the method comprising:  
providing a portable device including or communicating with a smart card module pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate communication between an e-purse applet therein and a payment server over a wireless network, wherein the portable device further includes a contactless interface that facilitates communication between the e-purse applet therein and the payment server over a wired network;  
personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card or a payment server, wherein said personalizing the e-purse applet comprises:  
establishing an initial security channel between the smart card and the e-purse SAM module to install and personalize the e-purse applet in the smart card, and  
creating the security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet.
- (Original)* The method as recited in claim 1, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.
- (Currently amended)* The method as recited in claim 2, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel so that

various data is exchanged between the e-purse applet and ~~an existing~~ the e-purse SAM originally used to issue the e-purse as well as between the emulator and the existing SAM.

4. *(Original)* The method as recited in claim 2, wherein said personalizing the e-purse applet is done over a wireless network or a wired network.
5. *(Original)* The method as recited in claim 4, wherein, when said personalizing the e-purse applet is done over a wireless network, the midlet in the portable device is configured to facilitate communications between the e-purse and the payment server.
6. *(Original)* The method as recited in claim 5, wherein both of the e-purse applet and the emulator are personalized as a result of said personalizing the e-purse applet.
7. *(Original)* The method as recited in claim 1, further comprising:
  - initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;
  - sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;
  - transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and
  - sending a server response from the payment server to the midlet that is configured to process the server response before releasing the server response to the e-purse applet.
8. *(Original)* The method as recited in claim 7, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.

9. *(Original)* The method as recited in claim 8, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.
10. *(Original)* The method as recited in claim 1, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device, and the e-purse supports transactions in either e-commerce or m-commerce.
11. *(Currently amended)* A system for providing an e-purse, the system comprising:  
 a portable device including or communicating with a smart card ~~module~~ pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate wireless communication between an e-purse applet in the smart card therein and a payment server over a wireless network, the portable device further including a contactless interface that facilitates communication between the e-purse applet in the smart card therein and the payment server over a wired network, wherein said personalizing the e-purse applet comprises:  
establishing an initial security channel between the smart card and the e-purse SAM module to install and personalize the e-purse applet in the smart card, and  
creating the security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet;  
 the payment server associated with an issuer of authorizing the e-purse applet; and ~~an~~ the e-purse SAM configured to enable the e-purse applet, wherein ~~the~~ an SAM is behind the payment server and in communication with the e-purse applet when the e-purse applet is caused to communicate with the payment server via the midlet., ~~the SAM is communicated with the e-purse via the contactless interface when the e-purse is caused to communicate with the payment server over a wired network.~~

12. (*Original*) The system as recited in claim 11, wherein both of the e-purse applet and emulator are personalized by reading off data from the smart card, the data is then used to generate operation keys for the e-purse applet.
13. (*Original*) The system as recited in claim 12, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.
14. (*Currently amended*) The system as recited in claim 13, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and an existing security authentication module (SAM) originally used to issue the e-purse as well as between the emulator and the existing SAM.
15. (*Currently amended*) The system as recited in claim 11, wherein, when the portable device is used to have a transaction, there are operations of:
- initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;
  - sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;
  - transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and
  - sending a server response from the payment server to the midlet that is configured to process the server response before releasing the server response to the e-purse applet.

16. *(Original)* The system as recited in claim 15, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.

17. *(Original)* The system as recited in claim 16, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.

18. *(Original)* The system as recited in claim 11, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device.

## Remarks

Claims 1-18 were submitted for examination. In the Office Action dated 02/03/2010, Claims 1-18 are rejected under 35 USC 102(b) as being anticipated by Shmueli et al (US Publication No.: 20020145632, hereinafter "Shmueli").

The Applicants appreciate the Examiner for providing detailed comments in the Office Action. In the foregoing amendments, Claims 1, 3, 11, 14 and 15 have been amended. No new matters have been introduced. Reconsideration of pending claims is respectfully requested.

### Rejections of Claims 1-18 under 35 USC 102(e)

The Applicant respectfully traverses the rejections of Claims 1 - 18 under 35 USC 102. A cited prior art reference anticipates a claimed invention under 35 USC 102 only if every element of the claimed invention is identically shown in the single reference, arranged as they are in the claim. MPEP 2131; in re Bond, 910 F.2d 831, 832, 15 USPQ2d 1566, 1567 (Fed. Cir. 1990). Each and every limitation of the claimed invention is significant and must be found in the single cited prior reference. In re Donohue, 766 F.2d 531, 534, 266 USPQ 619, 621 (Feb. Cir. 1985). As set forth more fully below, Shmueli neither discloses nor suggests each and every element of the claimed invention.

In particular, the amended Claim 1 now recites:

...

personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card, wherein said personalizing the e-purse applet comprises:

establishing an initial security channel between the smart card and the e-purse SAM module to install and personalize the e-purse applet in the smart card, and  
creating the security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet.

*(emphasis added)*

As described in paragraphs [0024]-[0027], [0037] and shown in FIG. 1A and FIG. 3C, personalizing the e-purse applet requires a type of data communication with an e-



purse SAM that is not part of the smart card. The data communication includes install and personalize the e-purse applet in the smart card and create security means to protect subsequent operations of the smart cards with the e-purse SAM. To do so without a prior security channel, an initial security channel between the smart card and the e-purse SAM module shall be establish. For example, such an initial security channel is established by using a general security framework of a preload operating system in a smart card. Once an initial security channel is established, a (second) security channel on top of the initial security channel is established to protect subsequent operations of the smart card with the e-purse SAM. In addition, any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet. In other words, the emulator communicates externally either on top of the security channel or simply via e-purse applet (namely, the same security channel but through the e-purse applet).

In contrast, Shmueli is silent about such an external e-purse SAM that is needed to establish a security channel on top of an initial security channel (e.g., an industrially recognized framework) to facilitate subsequent operations of the smart cards with the external e-purse SAM. FIG.1 of Shmueli shows that there are three entities, a key 10, a host 12 and a server 14. Shmueli does not teach nor suggests that the key 10 needs to be personalized by an external e-purse SAM to create (two-level) security means to protect the subsequent operations of the smart cards with an external SAM. Further Shmueli is silent about having an emulator in the smart card conduct subsequent operations thereof over the security channel established by the e-purse applet or via the e-purse applet itself.

Accordingly, the Applicant respectfully submits Claim 1, as amended, shall be allowable over Shmueli. Reconsideration of Claims 1-10 is kindly requested.

Claim 10 has been amended to include similar limitations recited in Claim 1. The Applicant wishes to rely on the above arguments to support once-amended Claim 10, and respectfully submits Claim 10, as amended, is neither taught nor suggested by Shmueli and shall be allowable over Shmueli. Reconsideration of Claims 10 - 18 is kindly requested.

In view of the above amendments and remarks, the Applicant believes that Claims 1 - 18 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 " Box: Non-Fee Amendment Commissioner of Patents and Trademarks P. O. Box 1450, Alexandria, VA 22313-1450", on May 2, 2010.

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>	7541890
<b>Application Number:</b>	11534653
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	6327
<b>Title of Invention:</b>	Method and apparatus for providing electronic purse
<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-081
<b>Receipt Date:</b>	03-MAY-2010
<b>Filing Date:</b>	24-SEP-2006
<b>Time Stamp:</b>	19:51:20
<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	ResponseToFirstOfficeAction.pdf	90582 79ebc6b0641974383a415cf43ca9776dcdf1b5a0	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.

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>11/534,653</b>		Filing Date <b>09/24/2006</b>		<input type="checkbox"/> To be Mailed		
<b>APPLICATION AS FILED – PART I</b>					SMALL ENTITY <input checked="" type="checkbox"/>		OR		OTHER THAN SMALL ENTITY		
(Column 1)		(Column 2)									
FOR	NUMBER FILED	NUMBER EXTRA			RATE (\$)	FEE (\$)	OR		RATE (\$)	FEE (\$)	
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A			N/A				N/A		
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A			N/A				N/A		
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A			N/A				N/A		
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =		*		X \$ =				X \$ =		
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =		*		X \$ =				X \$ =		
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 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 <small>(37 CFR 1.16(j))</small>											
* If the difference in column 1 is less than zero, enter "0" in column 2.					TOTAL		OR		TOTAL		
<b>APPLICATION AS AMENDED – PART II</b>											
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR		OTHER THAN SMALL ENTITY	
AMENDMENT	<b>05/03/2010</b>	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR		RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 18	Minus	** 20	=	X \$ =				X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 2	Minus	***3	=	X \$ =				X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>										
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>										
						TOTAL ADD'L FEE		OR		TOTAL ADD'L FEE	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR		RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=	X \$ =				X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=	X \$ =				X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>										
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>										
						TOTAL ADD'L FEE		OR		TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.											
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".											
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".											
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.											
Legal Instrument Examiner: /ELMIRA HALL/											

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

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/534,653	09/24/2006	Liang Seng Koh	RFID-081	6327
26797                      7590                      07/14/2010 SILICON VALLEY PATENT AGENCY 7394 WILDFLOWER WAY CUPERTINO, CA 95014			EXAMINER STANFORD, CHRISTOPHER J	
			ART UNIT	PAPER NUMBER
			2887	
			NOTIFICATION DATE	DELIVERY MODE
			07/14/2010	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>Notice of Non-Compliant Amendment (37 CFR 1.121)</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	11/534,653	KOH ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	CHRISTOPHER STANFORD	2887	

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

The amendment document filed on 03 May 2010 is considered non-compliant because it has failed to meet the requirements of 37 CFR 1.121 or 1.4. In order for the amendment document to be compliant, correction of the following item(s) is required.

THE FOLLOWING MARKED (X) ITEM(S) CAUSE THE AMENDMENT DOCUMENT TO BE NON-COMPLIANT:

1. Amendments to the specification:

A. Amended paragraph(s) do not include markings.

B. New paragraph(s) should not be underlined.

C. Other \_\_\_\_\_.

2. Abstract:

A. Not presented on a separate sheet. 37 CFR 1.72.

B. Other \_\_\_\_\_.

3. Amendments to the drawings:

A. The drawings are not properly identified in the top margin as "Replacement Sheet," "New Sheet," or "Annotated Sheet" as required by 37 CFR 1.121(d).

B. The practice of submitting proposed drawing correction has been eliminated. Replacement drawings showing amended figures, without markings, in compliance with 37 CFR 1.84 are required.

C. Other \_\_\_\_\_.

4. Amendments to the claims:

A. A complete listing of all of the claims is not present.

B. The listing of claims does not include the text of all pending claims (including withdrawn claims)

C. Each claim has not been provided with the proper status identifier, and as such, the individual status of each claim cannot be identified. Note: the status of every claim must be indicated after its claim number by using one of the following status identifiers: (Original), (Currently amended), (Canceled), (Previously presented), (New), (Not entered), (Withdrawn) and (Withdrawn-currently amended).

D. The claims of this amendment paper have not been presented in ascending numerical order.

E. Other: Claim 7 has an incorrect status identifier. Claim 7 should be identified as Currently Amended.

5. Other (e.g., the amendment is unsigned or not signed in accordance with 37 CFR 1.4):  
\_\_\_\_\_

For further explanation of the amendment format required by 37 CFR 1.121, see MPEP § 714.

TIME PERIODS FOR FILING A REPLY TO THIS NOTICE:

1. Applicant is given **no new time period** if the non-compliant amendment is an after-final amendment or an amendment filed after allowance. If applicant wishes to resubmit the non-compliant after-final amendment with corrections, the **entire corrected amendment** must be resubmitted.

2. Applicant is given **one month**, or thirty (30) days, whichever is longer, from the mail date of this notice to supply the correction, if the non-compliant amendment is one of the following: a preliminary amendment, a non-final amendment (including a submission for a request for continued examination (RCE) under 37 CFR 1.114), a supplemental amendment filed within a suspension period under 37 CFR 1.103(a) or (c), and an amendment filed in response to a *Quayle* action. If any of above boxes 1. to 4. are checked, the correction required is only the **corrected section** of the non-compliant amendment in compliance with 37 CFR 1.121.

**Extensions of time** are available under 37 CFR 1.136(a) only if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action.

**Failure to timely respond** to this notice will result in:

**Abandonment** of the application if the non-compliant amendment is a non-final amendment or an amendment filed in response to a *Quayle* action; or

**Non-entry** of the amendment if the non-compliant amendment is a preliminary amendment or supplemental amendment.

/Seung H Lee/ Primary Examiner, Art Unit 2887	/CHRISTOPHER STANFORD/ Examiner, Art Unit 2887
--	---

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

**Applicant(s):** Liang Seng Koh et al  
**Title:** Method and apparatus for providing electronic purse  
**Serial No.:** 11/534,653  
**Confirmation No.:** 6327  
**Filing Date:** 09/24/2006  
**Examiner:** Chris Stanford  
**Group Art Unit:** 2887  
**Docket No:** RFID-081

---

July 29, 2010

Mail Stop: Non-fee amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**Response to 1<sup>st</sup> OA**

**(Replacement of corresponding Response filed May 3, 2010)**

Dear Sir:

In response to Office Action dated 02/03/2010, 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 [0027] as follows:

**[0027]** Card Manager Security **106**, referring to a general security framework of a preload operating system in a smart card, provides a platform for PIN management and security channels (security domains) for card personalization. This platform via a card manager can be used to personalize a purse in one embodiment. One example of the card manager security **106** is what is referred to as a Global Platform (GP) that is created by a cross-industry membership organization ~~created~~ to advance standards for smart card growth. A GP combines the interests of smart card issuers, vendors, industry groups, public entities and technology companies to define requirements and technology standards for multiple application smart cards. In one embodiment, a global platform security is used to personalize a smart card. As a result, both e-purse keys and card access keys are personalized into the target tag.

2. Please amend paragraph [0029] as follows:

**[0029]** In reference to FIG. 1A, the physical security is realized in an emulator. As ~~sued~~ 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 a payment server. The card manager security (e.g., global platform security) is realized via a card manager to update security keys to establish appropriate channels for interactions between the server and the applets, wherein the e-purse applet(s) acts as a gatekeeper to regulate or control the data exchange.

3. Please amend paragraph [0034] as follows:

**[0034]** To personalize the cellphone **202**, 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 by an authorized person as shown in FIG. 2. 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 ~~an~~ a user of the e-purse as shown in FIG. 2.

4. Please amend paragraph [0037] as follows:

**[0037]** It is assumed that a user desires to personalize an e-purse embedded in a device (e.g., a cellphone). At **352** of FIG. 3C, a personalization process is initiated. Depending on implementation, the personalization process may be implemented in a module in the 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 for a user thereof via an ~~existing~~ new e-purse SA module **306** and an existing SA module **308** with the RFID 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 **304**, the e-purse applet **312** and the emulator **314** are personalized.

5. Please amend paragraph [0038] as follows:

**[0038]** Similarly, as shown in FIG. 3B, a user of an e-purse desires to initiate a personalization process to personalize the e-purse 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 cellphone 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** in a device acts as an agent to facilitate the communication between a payment server **324** and the e-purse **312** as well as the emulator **314**, wherein the payment server **324** has the access to the ~~existing~~ new e-purse SA module **306** and an existing SA module **308**. As a result of the personalization process, the e-purse applet **312** and the emulator **314** are personalized.

## AMENDMENTS TO THE CLAIMS

Please amend Claims 1, 3, 11, 14 and 15 as follows:

- (Currently amended)* A method for providing an e-purse, the method comprising:  
providing a portable device including or communicating with a smart card module pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate communication between an e-purse applet therein and a payment server over a wireless network, wherein the portable device further includes a contactless interface that facilitates communication between the e-purse applet therein and the payment server over a wired network;  
personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card ~~or a payment server~~, wherein said personalizing the e-purse applet comprises:  
establishing an initial security channel between the smart card and the e-purse SAM module to install and personalize the e-purse applet in the smart card, and  
creating the security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet.
- (Original)* The method as recited in claim 1, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.
- (Currently amended)* The method as recited in claim 2, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel so that

various data is exchanged between the e-purse applet and ~~an existing~~ the e-purse SAM originally used to issue the e-purse as well as between the emulator and the existing SAM.

4. (*Original*) The method as recited in claim 2, wherein said personalizing the e-purse applet is done over a wireless network or a wired network.
5. (*Original*) The method as recited in claim 4, wherein, when said personalizing the e-purse applet is done over a wireless network, the midlet in the portable device is configured to facilitate communications between the e-purse and the payment server.
6. (*Original*) The method as recited in claim 5, wherein both of the e-purse applet and the emulator are personalized as a result of said personalizing the e-purse applet.
7. (*Currently amended*) The method as recited in claim 1, further comprising:
  - initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;
  - sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;
  - transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and
  - sending a server response from the payment server to the midlet that is configured to process the server response before releasing the server response to the e-purse applet.
8. (*Original*) The method as recited in claim 7, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.

9. *(Original)* The method as recited in claim 8, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.
10. *(Original)* The method as recited in claim 1, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device, and the e-purse supports transactions in either e-commerce or m-commerce.
11. *(Currently amended)* A system for providing an e-purse, the system comprising:  
a portable device including or communicating with a smart card ~~module~~ pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate wireless communication between an e-purse applet in the smart card therein and a payment server over a wireless network, the portable device further including a contactless interface that facilitates communication between the e-purse applet in the smart card therein and the payment server over a wired network, wherein said personalizing the e-purse applet comprises:  
establishing an initial security channel between the smart card and the e-purse SAM module to install and personalize the e-purse applet in the smart card, and  
creating the security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet;  
the payment server associated with an issuer of authorizing the e-purse applet; and ~~an~~ the e-purse SAM configured to enable the e-purse applet, wherein ~~the~~ an SAM is behind the payment server and in communication with the e-purse applet when the e-purse applet is caused to communicate with the payment server via the midlet., ~~the SAM is communicated with the e-purse via the contactless interface when the e-purse is caused to communicate with the payment server over a wired network.~~

12. (*Original*) The system as recited in claim 11, wherein both of the e-purse applet and emulator are personalized by reading off data from the smart card, the data is then used to generate operation keys for the e-purse applet.
13. (*Original*) The system as recited in claim 12, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.
14. (*Currently amended*) The system as recited in claim 13, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and an existing security authentication module (SAM) originally used to issue the e-purse as well as between the emulator and the existing SAM.
15. (*Currently amended*) The system as recited in claim 11, wherein, when the portable device is used to have a transaction, there are operations of:
- initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;
  - sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;
  - transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and
  - sending a server response from the payment server to the midlet that is configured to process the server response before releasing the server response to the e-purse applet.

16. *(Original)* The system as recited in claim 15, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.

17. *(Original)* The system as recited in claim 16, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.

18. *(Original)* The system as recited in claim 11, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device.

## Remarks

Claims 1-18 were submitted for examination. In the Office Action dated 02/03/2010, Claims 1-18 are rejected under 35 USC 102(b) as being anticipated by Shmueli et al (US Publication No.: 20020145632, hereinafter "Shmueli").

The Applicants appreciate the Examiner for providing detailed comments in the Office Action. In the foregoing amendments, Claims 1, 3, 11, 14 and 15 have been amended. No new matters have been introduced. Reconsideration of pending claims is respectfully requested.

### Rejections of Claims 1-18 under 35 USC 102(e)

The Applicant respectfully traverses the rejections of Claims 1 - 18 under 35 USC 102. A cited prior art reference anticipates a claimed invention under 35 USC 102 only if every element of the claimed invention is identically shown in the single reference, arranged as they are in the claim. MPEP 2131; in re Bond, 910 F.2d 831, 832, 15 USPQ2d 1566, 1567 (Fed. Cir. 1990). Each and every limitation of the claimed invention is significant and must be found in the single cited prior reference. In re Donohue, 766 F.2d 531, 534, 266 USPQ 619, 621 (Feb. Cir. 1985). As set forth more fully below, Shmueli neither discloses nor suggests each and every element of the claimed invention.

In particular, the amended Claim 1 now recites:

...

personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card, wherein said personalizing the e-purse applet comprises:

establishing an initial security channel between the smart card and the e-purse SAM module to install and personalize the e-purse applet in the smart card, and  
creating the security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet.

*(emphasis added)*

As described in paragraphs [0024]-[0027], [0037] and shown in FIG. 1A and FIG. 3C, personalizing the e-purse applet requires a type of data communication with an e-



purse SAM that is not part of the smart card. The data communication includes install and personalize the e-purse applet in the smart card and create security means to protect subsequent operations of the smart cards with the e-purse SAM. To do so without a prior security channel, an initial security channel between the smart card and the e-purse SAM module shall be establish. For example, such an initial security channel is established by using a general security framework of a preload operating system in a smart card. Once an initial security channel is established, a (second) security channel on top of the initial security channel is established to protect subsequent operations of the smart card with the e-purse SAM. In addition, any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet. In other words, the emulator communicates externally either on top of the security channel or simply via e-purse applet (namely, the same security channel but through the e-purse applet).

In contrast, Shmueli is silent about such an external e-purse SAM that is needed to establish a security channel on top of an initial security channel (e.g., an industrially recognized framework) to facilitate subsequent operations of the smart cards with the external e-purse SAM. FIG.1 of Shmueli shows that there are three entities, a key 10, a host 12 and a server 14. Shmueli does not teach nor suggests that the key 10 needs to be personalized by an external e-purse SAM to create (two-level) security means to protect the subsequent operations of the smart cards with an external SAM. Further Shmueli is silent about having an emulator in the smart card conduct subsequent operations thereof over the security channel established by the e-purse applet or via the e-purse applet itself.

Accordingly, the Applicant respectfully submits Claim 1, as amended, shall be allowable over Shmueli. Reconsideration of Claims 1-10 is kindly requested.

Claim 10 has been amended to include similar limitations recited in Claim 1. The Applicant wishes to rely on the above arguments to support once-amended Claim 10, and respectfully submits Claim 10, as amended, is neither taught nor suggested by Shmueli and shall be allowable over Shmueli. Reconsideration of Claims 10 - 18 is kindly requested.

In view of the above amendments and remarks, the Applicant believes that Claims 1 - 18 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 " Box: Non-Fee Amendment Commissioner of Patents and Trademarks P. O. Box 1450, Alexandria, VA 22313-1450", on July 29, 2010.

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>	8112618
<b>Application Number:</b>	11534653
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	6327
<b>Title of Invention:</b>	Method and apparatus for providing electronic purse
<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-081
<b>Receipt Date:</b>	29-JUL-2010
<b>Filing Date:</b>	24-SEP-2006
<b>Time Stamp:</b>	08:19:22
<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	ReplacedResponseTo1stOA.pdf	99916 fb493854f5c18d88415951fcc1537bd42ba93cc	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.

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>11/534,653</b>		Filing Date <b>09/24/2006</b>		<input type="checkbox"/> To be Mailed			
<b>APPLICATION AS FILED – PART I</b>					(Column 1)		(Column 2)		SMALL ENTITY <input checked="" type="checkbox"/> OR OTHER THAN SMALL ENTITY			
FOR		NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR		RATE (\$)	FEE (\$)			
<input type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A	N/A		OR		N/A				
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A	N/A	N/A		OR		N/A				
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A	N/A		OR		N/A				
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =	*	X \$ =		OR		X \$ =				
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =	*	X \$ =		OR		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 \$250 (\$125 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))												
					TOTAL		TOTAL					
					TOTAL		TOTAL					
					TOTAL		TOTAL					
<b>APPLICATION AS AMENDED – PART II</b>					(Column 1)		(Column 2)		(Column 3)			
AMENDMENT	<b>07/29/2010</b>		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))		* 18	Minus	** 20	= 0	X \$26 =	0	OR	X \$ =		
	Independent (37 CFR 1.16(h))		* 2	Minus	***3	= 0	X \$110 =	0	OR	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		0		OR		TOTAL ADD'L FEE	
AMENDMENT			CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))		*	Minus	**	=	X \$ =		OR	X \$ =		
	Independent (37 CFR 1.16(h))		*	Minus	***	=	X \$ =		OR	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				OR		TOTAL ADD'L FEE	

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

Legal Instrument Examiner:  
 /STELLA LITTLE/

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

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/534,653	09/24/2006	Liang Seng Koh	RFID-081	6327
26797                      7590                      10/01/2010 SILICON VALLEY PATENT AGENCY 7394 WILDFLOWER WAY CUPERTINO, CA 95014			EXAMINER STANFORD, CHRISTOPHER J	
			ART UNIT	PAPER NUMBER
			2887	
			NOTIFICATION DATE	DELIVERY MODE
			10/01/2010	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> 11/534,653	<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 29 July 2010.
- 2a)  This action is **FINAL**.                      2b)  This action is non-final.
- 3)  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**

- 4)  Claim(s) 1-18 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5)  Claim(s) \_\_\_\_\_ is/are allowed.
- 6)  Claim(s) 1-18 is/are rejected.
- 7)  Claim(s) \_\_\_\_\_ is/are objected to.
- 8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9)  The specification is objected to by the Examiner.
- 10)  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).
- 11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**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)  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_.
- 4)  Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_\_.

**DETAILED ACTION**

***Response to Amendment***

1. Receipt is acknowledged of the amendment filed 7/29/2010. Claims 1, 3, 7, 11, and 14-15 are amended and claims 1-18 are currently pending.

***Claim Objections***

2. Claim 11 is objected to because of the following informalities: the phrase “the security channel” (lines 13 and 15-16) lacks antecedent basis. Appropriate correction is required. For the purpose of examination, the phrase will be interpreted to mean “a security channel”.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation “a secured channel between the e-purse applet and an e-purse [SAM]”, “an initial security channel”, “the security channel on top of the initial security channel”, “the security channel” in lines 10-11, line 14, line 17, and lines 19-20 respectively. There is insufficient antecedent basis for this limitation in the claim. It is unclear whether “the security channel” of lines 17 and 19-20 is intended to reference “a



secured channel” or “an initial security channel” or a third and distinct security channel that is “on top of the initial security channel”.

For the purposes of examination “the security channel” of line 17 and 19-20 will be interpreted as “a security channel”.

5. Claims 11-18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 11 sequentially recites: “an e-purse applet in the smart card ... wherein said personalizing the e-purse applet comprises: establishing an initial security channel between the smart card and the e-purse SAM module to install and personalize the e-purse applet in the smart card”. The claim discloses that the applet is ***in the smart card***, as opposed to configured to be in the smart card, and further limits (via the term “wherein”) the applet (already in the smart card) by reciting that a security channel is established “to install ... the e-purse applet in the smart card”. The conventional definition of installation is to set-up, establish, or place something that does not already exist in the ultimate location. It is unclear whether the installation is for setting up an applet that already exists in the smart card or setting up an applet for the first time in the smart card.

***Claim Rejections - 35 USC § 103***

6. **Claims 1-18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Shmueli et al. (US 2002/0145632 A1; hereinafter Shmueli; previously cited) in view of Atsmon et al. (US 6,607,136 B1; hereinafter Atsmon).

**Regarding claim 1**, Shmueli teaches providing an e-purse (e-wallet 82, Fig. 6; para [0053]), the method comprising: providing a portable device (host system 12 embodied as a cell phone, Fig. 1; para [0029]) including or communicating with a smart card module (key 10 embodied as smart card 10B, Figs. 1 & 2B; para [0033]) pre-loaded with an emulator (para [0027-0028]), the portable device including a memory space (memory 28, Fig. 1; para [0029]) loaded with a midlet (keylets such as web keylet 56, Fig. 4) that is configured to facilitate communication between an e-purse applet (key manager application 58, Fig. 4; para [0041-0044]) therein and a payment server (server 14 running web servlet 66, Figs. 1 & 4) over a wireless network (mobile phone network is partially wireless), wherein the portable device further includes a contactless interface (mobile phone network interface 38, Fig. 1) that facilitates communication between the e-purse applet therein and the payment server over a wired network (host 12 embodied as a mobile phone accessing network 16 via the internet would include a partially wired network, i.e. the internet); personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys (Figs. 3A-3B) that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card (para [0037-0042]), wherein the personalizing the e-purse applet comprises: establishing an initial security

channel between the smart card and the e-purse SAM module to update and personalize the e-purse applet in the smart card, and creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet.

Shmueli discloses the claimed invention as cited above though does not explicitly disclose establishing a security channel to install the e-purse applet in the smart card.

Atsmon discloses: establishing a security channel to install the e-purse applet in the smart card (col. 66, ln. 29-col. 68, ln. 51 & col. 70, ln. 50-col. 74, ln. 31).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to install the e-purse applet in the card as taught by Atsmon with the device as disclosed by Shmueli. The motivation would have been to make on-line shopping faster and more convenient (col. 66, ln. 29-40).

**Regarding claims 2 and 13**, Shmueli teaches the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords (Figs. 3A-3B; para [0037-0042]).

**Regarding claims 3 and 14**, Shmueli teaches at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server (Figs. 3A-3B; para [0037-0042]), and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and an existing

SAM (e.g. VISA) originally used to issue the e-purse as well as between the emulator and the existing SAM (para [0044-0047, 0063-0064]).

**Regarding claim 4**, Shmueli teaches the personalizing the e-purse applet is done over a wireless network or a wired network (via network 16 which is embodied as a mobile phone network and the internet, Figs. 3A-3B; para [0037-0042]).

**Regarding claim 5**, Shmueli teaches when the personalizing the e-purse applet is done over a wireless network, the midlet in the portable device is configured to facilitate communications between the e-purse and the payment server (keylets such as web keylet 56, Fig. 4; para [0037-0042]).

**Regarding claim 6**, Shmueli teaches both of the e-purse applet and the emulator are personalized as a result of said personalizing the e-purse applet (key 10 and host 12 contain applet and emulator and all are personalized via authentication, Figs. 3A, 3B, & 4; para [0037-0042]).

**Regarding claims 7 and 15**, Shmueli teaches initiating a request (para [0042-0045]) from the e-purse after valid personal identification numbers are entered and accepted on the portable device (steps 114-120, Fig. 3A); sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet (data from files 60, 62, 64 sent from key manager application to web keylets in the interaction with web servlets 66, Fig. 4; para [0042-0045,0057,0064]); transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse (authenticated prior to running keylet, Fig. 3A-B), wherein the payment server further communicates with a financial institution (business partners of

third party services 70, para [0044,0063-0064]) to authorize a transaction therewith; and sending a response (update key automatically, step 124 of Fig. 3B) from the payment server to the midlet that is configured to process the response before releasing the response to the e-purse applet (para [0039]).

**Regarding claims 8 and 16**, Shmueli teaches messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages (files sent via network; para [0027-0028,0041-0042]).

**Regarding claims 9 and 17**, Shmueli teaches the commands are applicable for Application Protocol Data Unit (APDU) (data files system; para [0027-0028,0041-0042,0096-0098]). Shmueli teaches commands for authentication, access, and data transfer just as is evident in APDU and therefore the commands ***are applicable*** for APDU. The prior art need not teach the specific format of APDU commands in order to teach the applicability of the commands.

**Regarding claims 10 and 18**, Shmueli teaches the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device (para [0063-0064]), and the e-purse supports transactions in either e-commerce or m-commerce (para [0063-0064]).

**Regarding claim 11**, Shmueli teaches a system for providing an e-purse (e-wallet 82, Fig. 6; para [0053]), the system comprising: a portable device (host system 12 embodied as a cell phone, Fig. 1; para [0029]) including or communicating with a smart card module (key 10 embodied as smart card 10B, Figs. 1 & 2B; para [0033]) pre-loaded with an emulator (para [0027-0028]), the portable device including a memory

space (memory 28, Fig. 1; para [0029]) loaded with a midlet (keylets such as web keylet 56, Fig. 4) that is configured to facilitate wireless communication between an e-purse applet (key manager application 58, Fig. 4; para [0041-0044]) in a smart card and a payment server (server 14 running web servlet 66, Figs. 1 & 4) over a wireless network (mobile phone network is partially wireless), the portable device further including a contactless interface (mobile phone network interface 38, Fig. 1) that facilitates communication between the e-purse applet in the smart card and the payment server over a wired network (host 12 embodied as a mobile phone accessing network 16 via the internet would include a partially wired network, i.e. the internet); wherein the personalizing the e-purse applet comprises: establishing an initial security channel between the smart card and the e-purse SAM module to update and personalize the e-purse applet in the smart card, and creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel or via the e-purse applet; the payment server associated with an issuer authorizing the e-purse applet (para [0044-0047, 0063-0064]); and the e-purse SAM (third party services behind extended application program interface 74 of server 14, Figs. 1 and 3-4) configured to enable the e-purse applet, wherein the SAM is behind the payment server and in communication with the e-purse applet when the e-purse is caused to communicate with the payment server via the midlet over a wireless network (Figs. 3A-3B; para [0037-0047,0063-0064]).

Shmueli discloses the claimed invention as cited above though does not explicitly disclose establishing a security channel to install the e-purse applet in the smart card.

Atsmon discloses: establishing a security channel to install the e-purse applet in the smart card (col. 66, ln. 29-col. 68, ln. 52).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to install the e-purse applet in the card as taught by Atsmon with the device as disclosed by Shmueli. The motivation would have been to make on-line shopping faster and more convenient (col. 66, ln. 29-40).

**Regarding claim 12**, Shmueli teaches both of the e-purse applet and emulator are personalized (Figs. 3A-3B) by reading off data from the smart card (para [0037-0042]), the data is then used to generate operation keys for the e-purse applet (para [0037-0042]).

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

1. Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new ground(s) of rejection.

### ***Conclusion***

2. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

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

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 , 7:30am-4:30pm.

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

/Seung H Lee/  
Primary Examiner, Art Unit 2887

<b>Notice of References Cited</b>	Application/Control No. 11/534,653	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-6,607,136 B1	08-2003	Atsmon et al.	235/492
	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	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>Search Notes</b>  	<b>Application/Control No.</b>  11534653	<b>Applicant(s)/Patent Under Reexamination</b>  KOH ET AL.
	<b>Examiner</b>  CHRISTOPHER STANFORD	<b>Art Unit</b>  2887

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
235	379,380,492	1/22-25/10	CS

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>
Inventor, Assignee Search	1/22-25/10	CS
NPL Search	1/22-25/10	CS
Text Search (see search history report print out)	1/22-25/10	CS
Text Search (see search history report print out)	7/07/10-9/24/10	CS

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

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

<b>Index of Claims</b> 	<b>Application/Control No.</b> 11534653	<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>

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

CLAIM		DATE							
Final	Original	01/25/2010	09/27/2010						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						
	15	✓	✓						
	16	✓	✓						
	17	✓	✓						
	18	✓	✓						

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: 11/534,653**

Attorney Docket No: RFID-081

Customer Number: 26797

Date of Electronic Notification: 10/01/2010

This is a courtesy reminder that new correspondence is available for this application. 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

Please verify that these email addresses are correct.

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.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.

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.

# REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL

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>11/534,653</b>
Filing Date	<b>09/24/2006</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-081</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(l) 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>12/31/2010</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>12/31/2010</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.

<b>Electronic Patent Application Fee Transmittal</b>				
<b>Application Number:</b>	11534653			
<b>Filing Date:</b>	24-Sep-2006			
<b>Title of Invention:</b>	Method and apparatus for providing electronic purse			
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh			
<b>Filer:</b>	Joe Zheng			
<b>Attorney Docket Number:</b>	RFID-081			
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	405	405
<b>Total in USD (\$)</b>				<b>405</b>



<b>Electronic Acknowledgement Receipt</b>	
<b>EFS ID:</b>	9147177
<b>Application Number:</b>	11534653
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	6327
<b>Title of Invention:</b>	Method and apparatus for providing electronic purse
<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-081
<b>Receipt Date:</b>	31-DEC-2010
<b>Filing Date:</b>	24-SEP-2006
<b>Time Stamp:</b>	20:23:01
<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	\$405
RAM confirmation Number	7197
Deposit Account	
Authorized User	

**File Listing:**

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

1	Amendment Submitted/Entered with Filing of CPA/RCE	ResponseToFinal.pdf	108184 4c3ac025104d7c7084c73d5c60b134225c217868	no	10
<b>Warnings:</b>					
<b>Information:</b>					
2	Request for Continued Examination (RCE)	RCETransmittal.pdf	39221 f56a5d4e922ee98368d16c23c7f3c3ce87f6e07	no	1
<b>Warnings:</b>					
This is not a USPTO supplied RCE SB30 form.					
<b>Information:</b>					
3	Fee Worksheet (PTO-875)	fee-info.pdf	29718 f577d5c883a285496e6290227de3407989618366	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>				177123	
<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>					

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

**Applicant(s):** Liang Seng Koh et al  
**Title:** Method and apparatus for providing electronic purse  
**Serial No.:** 11/534,653  
**Confirmation No.:** 6327  
**Filing Date:** 09/24/2006  
**Examiner:** Chris Stanford  
**Group Art Unit:** 2887  
**Docket No:** RFID-081

---

December 31, 2010

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

**Response to Final OA**

**Preliminary amendments in RCE filed concurrently**

Dear Sir:

In response to Office Action dated 10/01/2010, the Applicant respectfully requests the Examiner to enter the following minor 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 11 as follows:

- (Currently amended)* A method for providing an e-purse, the method comprising:  
providing a portable device including or communicating with a smart card module pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate communication between an e-purse applet therein and a payment server over a wireless network, wherein the portable device further includes a contactless interface that facilitates communication between the e-purse applet therein and the payment server over a wired network;  
personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card, wherein said personalizing the e-purse applet comprises:  
establishing an initial security channel between the smart card and the e-purse SAM module to install and personalize the e-purse applet in the smart card, and  
creating ~~the a~~ security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel ~~or~~ via the e-purse applet.
- (Original)* The method as recited in claim 1, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.
- (Previously amended)* The method as recited in claim 2, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel

so that various data is exchanged between the e-purse applet and the e-purse SAM originally used to issue the e-purse as well as between the emulator and the existing SAM.

4. *(Original)* The method as recited in claim 2, wherein said personalizing the e-purse applet is done over a wireless network or a wired network.
5. *(Original)* The method as recited in claim 4, wherein, when said personalizing the e-purse applet is done over a wireless network, the midlet in the portable device is configured to facilitate communications between the e-purse and the payment server.
6. *(Original)* The method as recited in claim 5, wherein both of the e-purse applet and the emulator are personalized as a result of said personalizing the e-purse applet.
7. *(Previously amended)* The method as recited in claim 1, further comprising:
  - initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;
  - sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;
  - transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and
  - sending a server response from the payment server to the midlet that is configured to process the server response before releasing the server response to the e-purse applet.
8. *(Original)* The method as recited in claim 7, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.

9. (*Original*) The method as recited in claim 8, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.
10. (*Original*) The method as recited in claim 1, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device, and the e-purse supports transactions in either e-commerce or m-commerce.
11. (*Currently amended*) A system for providing an e-purse, the system comprising:  
a portable device including or communicating with a smart card pre-loaded with an emulator, the portable device including a memory space loaded with a midlet that is configured to facilitate wireless communication between an e-purse applet in the smart card and a payment server over a wireless network, the portable device further including a contactless interface that facilitates communication between the e-purse applet in the smart card and the payment server over a wired network, wherein said personalizing the e-purse applet comprises:  
    establishing an initial security channel between the smart card and the e-purse security authentication module (SAM) module to install and personalize the e-purse applet in the smart card, and  
    creating ~~the~~ a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel ~~or~~ via the e-purse applet;  
the payment server associated with an issuer authorizing the e-purse applet; and  
the e-purse SAM configured to enable the e-purse applet, wherein an SAM is behind the payment server and in communication with the e-purse applet when the e-purse applet is caused to communicate with the payment server via the midlet.
12. (*Original*) The system as recited in claim 11, wherein both of the e-purse applet and emulator are personalized by reading off data from the smart card, the data is then used to generate operation keys for the e-purse applet.

13. (*Original*) The system as recited in claim 12, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.
14. (*Previously amended*) The system as recited in claim 13, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and an existing security authentication module (SAM) originally used to issue the e-purse as well as between the emulator and the existing SAM.
15. (*Previously amended*) The system as recited in claim 11, wherein, when the portable device is used to have a transaction, there are operations of:
- initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;
  - sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;
  - transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and
  - sending a server response from the payment server to the midlet that is configured to process the server response before releasing the server response to the e-purse applet.
16. (*Original*) The system as recited in claim 15, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.
17. (*Original*) The system as recited in claim 16, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.

18. (*Original*) The system as recited in claim 11, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device.



## Remarks

Claims 1-18 were submitted for examination. In the Office Action dated 10/01/2010, Claims 1-18 are rejected under 35 USC 103(a) as being unpatentable over Shmueli et al (US Publication No.: 20020145632, hereinafter "Shmueli") in view of Atsmon et al (US Pat. No.: 6,607,136, hereinafter "Atsmon").

The Applicants appreciate the Examiner for providing detailed comments in the Office Action. In the foregoing amendments, Claims 1, and 11 have been amended to correct some informalities. These amendments will not require the Examiner to perform another search. Reconsideration of pending claims is respectfully requested.

### Rejections of Claims 1-18 under 35 USC 103(a)

On page 2, the Examiner rejects Claim 1 under 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards the invention.

The Applicant respectfully disagrees with the Examiner as it is believed that the Examiner seemed to have been confused with the security mechanisms recited in Claim 1. The Response dated 07/29/2010 explicitly states that "there are two security channels". As demonstrated on pages 2 and 3 of the Office Action, the Examiner assumed that the security channel between the e-purse applet and an e-purse SAM is the same as the initial security channel, such misunderstanding may have led the Examiner a misleading search result, and thus the erroneous rejections.

As amended, Claim 1 explicitly recites:

...

personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card, wherein said personalizing the e-purse applet comprises:

establishing an initial security channel between the smart card and the e-purse SAM module to install and personalize the e-purse applet in the smart card, and

creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet.

(emphasis added)

As described in paragraphs [0024]-[0027], [0037] and shown in FIG. 1A and FIG. 3C, personalizing the e-purse applet requires a type of data communication with an e-purse SAM that is not part of the smart card. The data communication includes installing and personalizing the e-purse applet in the smart card and creating security means to protect subsequent operations of the smart cards with the e-purse SAM. To do so without a *prior* security channel, an initial security channel between the smart card and the e-purse SAM module shall be established. For example, such an initial security channel is established by using a general security framework of a preload operating system in a smart card. Once an initial security channel is established, a (second) security channel on top of the initial security channel is established to protect subsequent operations of the smart card with the e-purse SAM. In addition, any subsequent operation of the emulator is conducted over the security channel via the e-purse applet. In other words, as explicitly shown in FIG. 2, the emulator 208 communicates externally on top of the security channel via e-purse applet 206 to conduct either e-commerce or m-commerce.

In contrast, Shmueli is silent about such an external e-purse SAM that is needed to establish a security channel on top of an initial security channel (e.g., an industrially recognized framework) to facilitate subsequent operations of the smart cards with the external e-purse SAM. FIG. 1 of Shmueli shows that there are three entities, a key 10, a host 12 and a server 14. Shmueli does not teach nor suggests that the key 10 needs to be personalized by an external e-purse SAM to create (two-level) security means to protect the subsequent operations of the smart cards with an external SAM. Further Shmueli is silent about having an emulator in the smart card conduct subsequent operations thereof over the security channel established by the e-purse applet to conduct either e-commerce or m-commerce.

On page 5 of the Office Action, the Examiner also admits that Shmueli does not explicitly disclose establishing a security channel to install the e-purse applet in the smart card, and thus cites Atsmon to show the teaching.

The Applicant respectfully contests the combination of Shmueli and Atsmon as it is believed that there is no motivation to combine these two references in the manner proposed by the Examiner. In order to establish a *prima facie* case of obviousness

under 35 USC 103, *Graham v. John Deer Co. of Kansas City*, 383 US 1 (1966) requires determining, respectively, the scope and content of the prior art, the difference between the prior art and the claims at issue, and the level of ordinary skilled in the art. Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning, to support the legal conclusion of obviousness. *KSR v. Teleflex*, No. 04-1350 (US Apr. 30, 2007) (citing *In re Kahn*, 441 F. 3d 977, 988 (Canada Fed. 2006)). The suggestion to make the claim combination must be found in the prior art, not in the Applicant's disclosure. *In re Vaek*, 20 USPQ2d 1438 (Fed. Cir. 1991). Moreover, in accordance with MPEP 2142.02, each prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L. Gore & Associates Inc. v. Garlock, Inc.* 220 USPQ 303 (Fed. Cir. 1993). A third essential requirement for establishing a *prima facie* case, set forth in MPEP 2143.01, is that the proposed modification cannot render the prior art unsatisfactory for its intended purpose.

Atsmon teaches an interactive authentication system to allow a consumer to interact with a base station to receive coupons, special sales and other information with an electronic card. After a careful review, the Applicant concludes that Atsmon does not teach how to use a security channel to install and personalize an e-purse applet in a smart card. Atsmon only says that special client remote access software is downloaded, see Col. 32, lines-56-63, where that special client remote access software is for access to the website (e.g., a base station), no encryption, or any mechanism for a security channel are mentioned or described.

Accordingly, the Applicant submits Shmueli could not be modified with Atsmon or such modification would render Shmueli inoperable. The Applicant wishes to further point out that Atsmon describes entirely about e-wallet. It is commonly known in the art that e-wallet is not the same as e-purse. An e-wallet system has a user credit-card and personal info at the backend, an e-card in the e-wallet system is used as an identity card for logging in into the system. When shopping, the e-card can be used to identify the user to retrieve the info and submit the info to the merchant site. Evidently, an e-purse in the instant application describes about electronic money in a local portable device. Accordingly, the combination of Shmueli and Atsmon neither teaches nor

suggests Claim 1, and Claim shall be allowable over Shmueli and Atsmon.  
Reconsideration of Claims 1-10 is kindly requested.

Claim 11 has been amended to include similar limitations recited in Claim 1. The Applicant wishes to rely on the above arguments to support once-amended Claim 11, and respectfully submits Claim 11, as amended, is neither taught nor suggested by Shmueli and Atsmon, viewed alone or in combination, and shall be allowable over Shmueli and Atsmon. Reconsideration of Claims 11 - 18 is kindly requested.

In view of the above amendments and remarks, the Applicant believes that Claims 1 - 18 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 " Box: Non-Fee Amendment Commissioner of Patents and Trademarks P. O. Box 1450, Alexandria, VA 22313-1450", on Dec. 31, 2010.

Name: Joe Zheng

Signature: / Joe Zheng /

Respectfully submitted,

/ joe zheng /

Joe Zheng  
Reg. No.: 39,450

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>11/534,653</b>	Filing Date <b>09/24/2006</b>	<input type="checkbox"/> To be Mailed			
<b>APPLICATION AS FILED – PART I</b>					SMALL ENTITY <input checked="" type="checkbox"/> OR OTHER THAN SMALL ENTITY					
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)			
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		OR	N/A				
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A		OR	N/A				
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		OR	N/A				
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =	*	X \$ =		OR	X \$ =				
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		OR	X \$ =				
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 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).				OR					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>					OR					
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL		OR	TOTAL				
<b>APPLICATION AS AMENDED – PART II</b>					SMALL ENTITY OR OTHER THAN SMALL ENTITY					
AMENDMENT	12/31/2010	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 18	Minus	** 20	= 0	X \$26 =	0	OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 2	Minus	***3	= 0	X \$110 =	0	OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>							OR		
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>							OR		
			TOTAL ADD'L FEE		0	OR	TOTAL ADD'L FEE			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=	X \$ =		OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=	X \$ =		OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>							OR		
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>							OR		
			TOTAL ADD'L FEE		TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
 \*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
 \*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

Legal Instrument Examiner:  
/AMANDA FORD/

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

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/534,653	09/24/2006	Liang Seng Koh	RFID-081	6327
26797                      7590                      05/25/2011 SILICON VALLEY PATENT AGENCY 7394 WILDFLOWER WAY CUPERTINO, CA 95014			EXAMINER STANFORD, CHRISTOPHER J	
			ART UNIT	PAPER NUMBER
			2887	
			NOTIFICATION DATE	DELIVERY MODE
			05/25/2011	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>	<b>Applicant(s)</b>	
	11/534,653	KOH ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	CHRISTOPHER STANFORD	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 31 December 2010.
- 2a)  This action is **FINAL**.                      2b)  This action is non-final.
- 3)  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**

- 4)  Claim(s) 1-18 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5)  Claim(s) \_\_\_\_\_ is/are allowed.
- 6)  Claim(s) 1-18 is/are rejected.
- 7)  Claim(s) \_\_\_\_\_ is/are objected to.
- 8)  Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9)  The specification is objected to by the Examiner.
- 10)  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).
- 11)  The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**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)  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3)  Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_.
- 4)  Interview Summary (PTO-413)  
 Paper No(s)/Mail Date \_\_\_\_\_.
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_\_.

**DETAILED ACTION**

***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/31/2010 has been entered.

***Response to Amendment***

2. Receipt is acknowledged of the amendment filed 12/21/2010. Claims 1 and 11 are amended and claims 1-18 are currently pending.

***Claim Rejections - 35 USC § 103***

3. 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.

4. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shmueli et al. (US 2002/0145632 A1; hereinafter Shmueli; previously cited) in view of Nystrom (US 2009/0313689 A1; hereinafter Nystrom). Nystrom is a National Stage entry of PCT/IB05/03792.



**Regarding claim 1**, Shmueli teaches providing an e-purse (e-wallet 82, Fig. 6; para [0053]), the method comprising: providing a portable device (host system 12 embodied as a cell phone, Fig. 1; para [0029]) including or communicating with a smart card module (key 10 embodied as smart card 10B, Figs. 1 & 2B; para [0033]) pre-loaded with an emulator (“the memory 18 will emulate a file system on a memory device, such as a hard disk drive, accessible by the host 12 wherein at least certain aspects of the software 20 are capable of running or executing on the host 12”; para [0027-0028]), the portable device including a memory space (memory 28, Fig. 1; para [0029]) loaded with a midlet (keylets such as web keylet 56, Fig. 4) that is configured to facilitate communication between an e-purse applet (key manager application 58, Fig. 4; para [0041-0044]) therein and a payment server (server 14 running web servlet 66, Figs. 1 & 4) over a wireless network (mobile phone network is partially wireless), wherein the portable device further includes a contactless interface (mobile phone network interface 38, Fig. 1) that facilitates communication between the e-purse applet therein and the payment server over a wired network (host 12 embodied as a mobile phone accessing network 16 via the internet would include a partially wired network, i.e. the internet); personalizing the e-purse applet by reading off data from the smart card to generate one or more operation keys (Figs. 3A-3B) that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card (“the user will provide authentication indicia to the host 12. The authentication routine, which is running on the host 12, will receive the authentication indicia from the user (block 114), and determine

if the user is authenticated (block 116)”, note: the host 12 is “external” to the key 10; para [0037-0042]), wherein the personalizing the e-purse applet comprises: establishing an initial security channel (unauthenticated communication between key 10 and host 12) between the smart card and the e-purse SAM module to update and personalize the e-purse applet in the smart card (“If the user is authenticated (block 116), one or more additional keylets based on the user authentication are executed according to the interaction of the user (block 120)”; para [0037-0042]), and creating a security channel (authenticated communication between key 10 and host 12 and network 16) on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM (“During execution of any of the keylets, data may be accessed from the key 10 as necessary based on the keylet and the authentication or security level (block 122)”; para [0039]), wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet (para [0039]).

Note: the claim explicitly requires the SAM to be “external to the smart card” but does not require the SAM to be external to the portable device.

Shmueli discloses the claimed invention as cited above though does not explicitly disclose establishing a security channel on top of the initial security channel to install the e-purse applet in the smart card.

Further, Applicant’s disclosure states “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”. This is in-line with the memory disclosed in Shmueli (para [0027-0028]).

Nystrom discloses personalizing the e-purse applet (Reload & Update Procedures; para [0111-120]) by reading off data from the smart card to generate one or more operation keys (“a reloading of relevant application related code sections, i.e. program code and/or user interface definitions” in light of association procedures: “request for authentication is preferably preformed prior to any operation of the secure storage subsystem 190”; para [0112,0127-0130]) that are subsequently used to establish a secured channel between the e-purse applet (“application programs created on the basis of JAVA ME the terminal device 100 implements a JAVA MIDP (Mobile Information Device Profile), which defines an interface between a JAVA ME application program, also known as a JAVA MIDlet, and the terminal device 100” associated with “the data stored in the secure storage subsystem 190 such as entering additional credit into an account maintained by electronic prepaid payment application or electronic wallet application, loading electronic tickets into an electronic ticket application”; para [0071,0086]) and an e-purse security authentication module (SAM) (network operator control center 300, secure storage management center 320, application service provider center 310, Fig. 4a-4b) external to the smart card (SIM 185 in portable terminal device 100, Fig. 2), wherein said personalizing the e-purse applet comprises: establishing an initial security channel (“the terminal device 100 and its network connectivity subsystem 250 authenticates against the authentication entity of the network by the means of the network authentication module”; para [0124]) between the smart card and the e-purse SAM (authentication entities include: network operator control center 300, secure storage management center 320, application service provider center 310, Fig. 4a-4b) to

install and personalize (reload, update, exchange and/or associate) the e-purse applet in the smart card (para [0111-0137]), and creating a security channel on top of the initial security channel (“operability of the secure storage subsystem 190 may be linked to the network authentication module to prevent usage of the secure storage subsystem 190 with any other network authentication module and to provide additional control by the cellular network operator over the operability of the secure storage subsystem 190” and “request for authentication is preferably preformed prior to any operation of the secure storage subsystem 190”; para [0126,0130]) to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation is conducted over the security channel via the e-purse applet (para [0100-0103]).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to provide a security channel on top of an initial security channel for installation as taught by Nystrom with the device as disclosed by Shmueli. The motivation would have been to prevent usage of the secure storage subsystem with any other network authentication module and to provide additional control by the cellular network operator over the operability of the secure storage subsystem (para [0126]).

**Regarding claims 2 and 13**, Shmueli teaches the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords (Figs. 3A-3B; para [0037-0042]).

**Regarding claims 3 and 14**, Shmueli teaches at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server (Figs. 3A-3B; para [0037-0042]),

and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and an existing SAM (e.g. VISA) originally used to issue the e-purse as well as between the emulator and the existing SAM (para [0044-0047, 0063-0064]).

**Regarding claim 4**, Shmueli teaches the personalizing the e-purse applet is done over a wireless network or a wired network (via network 16 which is embodied as a mobile phone network and the internet, Figs. 3A-3B; para [0037-0042]).

**Regarding claim 5**, Shmueli teaches when the personalizing the e-purse applet is done over a wireless network, the midlet in the portable device is configured to facilitate communications between the e-purse and the payment server (keylets such as web keylet 56, Fig. 4; para [0037-0042]).

**Regarding claim 6**, Shmueli teaches both of the e-purse applet and the emulator are personalized as a result of said personalizing the e-purse applet (key 10 and host 12 contain applet and emulator and all are personalized via authentication, Figs. 3A, 3B, & 4; para [0037-0042]).

**Regarding claims 7 and 15**, Shmueli teaches initiating a request (para [0042-0045]) from the e-purse after valid personal identification numbers are entered and accepted on the portable device (steps 114-120, Fig. 3A); sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet (data from files 60, 62, 64 sent from key manager application to web keylets in the interaction with web servlets 66, Fig. 4; para [0042-0045,0057,0064]); transporting the response to the payment server that is configured to verify that the response is from

an authenticated e-purse (authenticated prior to running keylet, Fig. 3A-B), wherein the payment server further communicates with a financial institution (business partners of third party services 70, para [0044,0063-0064]) to authorize a transaction therewith; and sending a response (update key automatically, step 124 of Fig. 3B) from the payment server to the midlet that is configured to process the response before releasing the response to the e-purse applet (para [0039]).

**Regarding claims 8 and 16**, Shmueli teaches messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages (files sent via network; para [0027-0028,0041-0042]).

**Regarding claims 9 and 17**, Shmueli teaches the commands are applicable for Application Protocol Data Unit (APDU) (data files system; para [0027-0028,0041-0042,0096-0098]). Shmueli teaches commands for authentication, access, and data transfer just as is evident in APDU and therefore the commands are “applicable” for APDU. The prior art need not teach the specific format of APDU commands in order to teach the applicability of the commands.

**Regarding claims 10 and 18**, Shmueli teaches the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device (para [0063-0064]), and the e-purse supports transactions in either e-commerce or m-commerce (para [0063-0064]).

**Regarding claim 11**, Shmueli teaches a system for providing an e-purse (e-wallet 82, Fig. 6; para [0053]), the system comprising: a portable device (host system 12 embodied as a cell phone, Fig. 1; para [0029]) including or communicating with a smart

card module (key 10 embodied as smart card 10B, Figs. 1 & 2B; para [0033]) pre-loaded with an emulator (para [0027-0028]), the portable device including a memory space (memory 28, Fig. 1; para [0029]) loaded with a midlet (keylets such as web keylet 56, Fig. 4) that is configured to facilitate wireless communication between an e-purse applet (key manager application 58, Fig. 4; para [0041-0044]) in a smart card and a payment server (server 14 running web servlet 66, Figs. 1 & 4) over a wireless network (mobile phone network is partially wireless), the portable device further including a contactless interface (mobile phone network interface 38, Fig. 1) that facilitates communication between the e-purse applet in the smart card and the payment server over a wired network (host 12 embodied as a mobile phone accessing network 16 via the internet would include a partially wired network, i.e. the internet); wherein the personalizing the e-purse applet comprises: establishing an initial security channel (unauthenticated communication between key 10 and host 12) between the smart card and the e-purse security authentication module (SAM) module (“the user will provide authentication indicia to the host 12. The authentication routine, which is running on the host 12, will receive the authentication indicia from the user (block 114), and determine if the user is authenticated (block 116)”, note: the host 12 is “external” to the key 10; para [0037-0042]) to update and personalize the e-purse applet in the smart card (“If the user is authenticated (block 116), one or more additional keylets based on the user authentication are executed according to the interaction of the user (block 120)”; para [0037-0042]), and creating a security channel on top of the initial security channel (authenticated communication between key 10 and host 12 and network 16) to protect

subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet (“During execution of any of the keylets, data may be accessed from the key 10 as necessary based on the keylet and the authentication or security level (block 122)”; para [0039]); the payment server associated with an issuer authorizing the e-purse applet (para [0044-0047, 0063-0064]); and the e-purse SAM (third party services behind extended application program interface 74 of server 14, Figs. 1 and 3-4) configured to enable the e-purse applet, wherein the SAM is behind the payment server and in communication with the e-purse applet when the e-purse is caused to communicate with the payment server via the midlet over a wireless network (Figs. 3A-3B; para [0037-0047,0063-0064]).

Note: the claim explicitly requires the SAM to be “external to the smart card” but does not require the SAM to be external to the portable device.

Shmueli discloses the claimed invention as cited above though does not explicitly disclose establishing a security channel on top of the initial security channel to install the e-purse applet in the smart card.

Further, Applicant’s disclosure states “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”. This is in-line with the memory disclosed in Shmueli (para [0027-0028]).

Nystrom discloses personalizing the e-purse applet (Reload & Update Procedures; para [0111-120]) by reading off data from the smart card to generate one



or more operation keys (“a reloading of relevant application related code sections, i.e. program code and/or user interface definitions” in light of association procedures: “request for authentication is preferably preformed prior to any operation of the secure storage subsystem 190”; para [0112,0127-0130]) that are subsequently used to establish a secured channel between the e-purse applet (“application programs created on the basis of JAVA ME the terminal device 100 implements a JAVA MIDP (Mobile Information Device Profile), which defines an interface between a JAVA ME application program, also known as a JAVA MIDlet, and the terminal device 100” associated with “the data stored in the secure storage subsystem 190 such as entering additional credit into an account maintained by electronic prepaid payment application or electronic wallet application, loading electronic tickets into an electronic ticket application”; para [0071,0086]) and an e-purse security authentication module (SAM) (network operator control center 300, secure storage management center 320, application service provider center 310, Fig. 4a-4b) external to the smart card (SIM 185 in portable terminal device 100, Fig. 2), wherein said personalizing the e-purse applet comprises: establishing an initial security channel (“the terminal device 100 and its network connectivity subsystem 250 authenticates against the authentication entity of the network by the means of the network authentication module”; para [0124]) between the smart card and the e-purse SAM (authentication entities include: network operator control center 300, secure storage management center 320, application service provider center 310, Fig. 4a-4b) to install and personalize (reload, update, exchange and/or associate) the e-purse applet in the smart card (para [0111-0137]), and creating a security channel on top of the initial

security channel (“operability of the secure storage subsystem 190 may be linked to the network authentication module to prevent usage of the secure storage subsystem 190 with any other network authentication module and to provide additional control by the cellular network operator over the operability of the secure storage subsystem 190” and “request for authentication is preferably preformed prior to any operation of the secure storage subsystem 190”; para [0126,0130]) to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation is conducted over the security channel via the e-purse applet (para [0100-0103]).

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to provide a security channel on top of an initial security channel for installation as taught by Nystrom with the device as disclosed by Shmueli. The motivation would have been to prevent usage of the secure storage subsystem with any other network authentication module and to provide additional control by the cellular network operator over the operability of the secure storage subsystem (para [0126]).

**Regarding claim 12**, Shmueli teaches both of the e-purse applet and emulator are personalized (Figs. 3A-3B) by reading off data from the smart card (para [0037-0042]), the data is then used to generate operation keys for the e-purse applet (para [0037-0042]).

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

5. Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new ground(s) of rejection.

For the sake of compact prosecution, Examiner notes that portions of Applicant's arguments are not persuasive and Examiner respectfully disagrees.

Specifically on page 8 of the Response, Applicant argues:

In contrast, Shmueli is silent about such an external e-purse SAM that is needed to establish a security channel on top of an initial security channel (e.g., an industrially recognized framework) to facilitate subsequent operations of the smart cards with the external e-purse SAM. FIG. 1 of Shmueli shows that there are three entities, a key 10, a host 12 and a server 14. Shmueli does not teach nor suggests that the key 10 needs to be personalized by an external e-purse SAM to create (two-level) security means to protect the subsequent operations of the smart cards with an external SAM.

Examiner contends that there is a two-level security means of communication disclosed by Shmueli. Figure 3A of Shmueli shows that there is key recognition and configuration (steps 102-106), thus communication, prior to authentication (step 110-116). Para [0035] discloses several embodiments of personalization. Examiner interprets the language "external" in claims 1 and 11 broadly. Thus claims 1 and 11 do not require initial secure communications to be between a smart card and a module behind a payment server (as shown in Applicant's Figs. 2, 3B, and 4C). However, the Nystrom reference, used to teach other portions of claim 1 and 11, discusses an authentication routine with an external security entity occurring prior to opening a channel to secured memory.

Additionally on page 8 of the Response, Applicant argues:

Further  
Shmueli is silent about having an emulator in the smart card conduct subsequent operations thereof over the security channel established by the e-purse applet to conduct either e-commerce or m-commerce.

Shmueli discloses hardware or software program that pretends to be another particular device or program that other components expect to interact with (para [0027-0028]).

### ***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 , 7:30am-4:30pm.

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.

/THIEN M LE/

Application/Control Number: 11/534,653  
Art Unit: 2887

Page 15

Primary Examiner, Art Unit 2887

/CHRISTOPHER STANFORD/  
Examiner, Art Unit 2887

<b>Notice of References Cited</b>	Application/Control No. 11/534,653	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-2009/0313689 A1	12-2009	Nystrom et al.	726/9
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	Classification
N	WO 2007068991 A1	06-2007	World Intellect	NYSTROEM et al.	
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.

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
21 June 2007 (21.06.2007)

PCT

(10) International Publication Number  
WO 2007/068991 A1

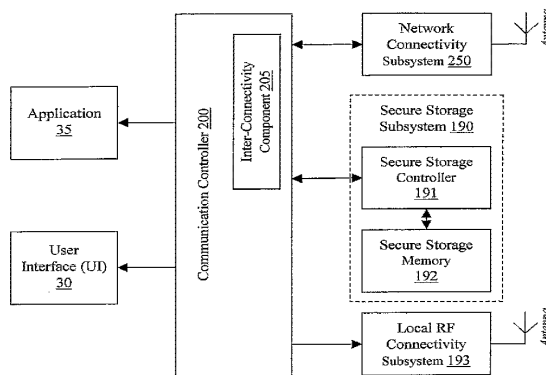
- (51) International Patent Classification:  
H04L 12/12 (2006.01) H04L 9/32 (2006.01)  
H04L 12/24 (2006.01)
- (21) International Application Number:  
PCT/IB2005/003792
- (22) International Filing Date:  
15 December 2005 (15.12.2005)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (for all designated States except US): **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **NYSTRÖM, Sebastian** [FI/FI]; Koivuhovintie 8 E 14, FIN-02750 Espoo (FI). **PESONEN, Lauri** [FI/FI]; Sinitiasentie 20, FIN-02660 Espoo (FI).
- (74) Agent: **KURIG, Thomas**; Becker, Kurig, Straus, Bavariastrasse 7, D-80336 München (DE).

- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:  
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD, DEVICE, AND SYSTEM FOR NETWORK-BASED REMOTE CONTROL OVER CONTACTLESS SECURE STORAGES



(57) Abstract: A typical system environment comprises a terminal device, a secure storage subsystem, and an interconnectivity component. The terminal device has a network connectivity subsystem enabled for data connectivity with a wireless communications network. The secure storage subsystem has a secure storage memory for securely storing contents and is enabled for local RF connectivity through a local RF communication subsystem. The secure storage subsystem is operable as a contactless smartcard in accordance with any contactless technology. The interconnectivity component is adapted to enable communication of the secure storage subsystem through the network connectivity subsystem with the network. The interconnectivity component is further configured to detect that messages received from the network are destined for the secure storage subsystem and is configured to supply that identified messages to the secure storage subsystem. The messages enable exercising control over the secure storage subsystem in that the messages comprise one or more instructions to be processed by a secure memory controller of the secure storage subsystem.

WO 2007/068991 A1

METHOD, DEVICE, AND SYSTEM FOR NETWORK-BASED REMOTE CONTROL  
OVER CONTACTLESS SECURE STORAGES

5 The present invention relates to the management of secure storages or smart storages. In particular, the present invention relates to remote management of secure storages such as smart cards applicable with contactless technology applications.

Contactless technology is a generic term for technologies using electromagnetic and/or  
10 electrostatic coupling technologies for low-power (LP), short-range (SR) radio frequency (RF) data communication services to offer security enhanced data communication features. Contactless technology is typically implemented on contactless smart chip technology, a specific form of smart card technology, which is used increasingly in applications handling with sensitive information. Contactless smart cards offer advantages to both the issuing organization as well as  
15 the cardholder. The issuing organization can support multiple applications on a single card and a variety of security policies for different situations. Typical applications are physical access control e.g. to a secured or monitored range, logical access control e.g. to networks, object and/or person identification, electronic payment, electronic ticketing, and logistic. In general, contactless smart chips have the ability to store, protect, manage, and provide access to sensitive  
20 information and to support security protocols and algorithms required by such application. The cardholder can take advantages of convenience, durability, and reliability provided by the contactless smart chip technology.

A contactless smart chip-based device includes an embedded secure microcontroller or  
25 equivalent intelligence, internal memory, and a small antenna, and communicates with a reader through a contactless radio frequency (RF) interface. The contactless interface provides users with the convenience of allowing the contactless device to be read at short distances with fast transfer of data. Contactless smart chip technology is available in a variety of forms – plastic cards, watches, key fobs, documents, and other handheld devices such as mobile phones.

30 The wide spread of mobile computing devices, in particular cellular terminal devices (cellular phones, smart phones, communicators), Personal Digital Assistants (PDAs) and related or similar consumer electronics, promotes the integration of contactless technology and in particular contactless smart chip technology into those mobile computing devices and in particular personal  
35 mobile computing devices which are conventionally carried along by consumers.

CONFIRMATION COPY



5 The mobile computing devices with integrated contactless technology offer input and output means, i.e. keys and keypad as well as display with user interface, which enable user exercised control over one or more individual application services operable with the contactless technology. However, it should be noted that the primary motive for integration is driven by the facts of usability, consumer convenience, handling expediency, and acceptance as well as single-homed multi-functionality promoting an aspired economic success of such mobile computing devices as well as contactless technology services.

10 Contactless technology as well as contactless smart chip technology has been developed as stand-alone technology. The contactless radio frequency (RF) interface enables for read and/or write access communication with the corresponding reader. Whereas the contactless technology implementation asserts of security, integrity, and authenticity aspects in access to a contactless smart chip and communication with a reader, the validity of the information obtained from a  
15 contactless smart chip has to be verified on reader side. The validity verification is conventionally performed by an on-line check against a data base of a service provider delivering validity confirmation. For instance in case of micro-payment applications (low price) or ticketing application (having a small value) on-line validity verification would cause costs which are incommensurate with such applications. Lacking validity verification represents a latent risk for  
20 all parties participating in the application service.

Moreover, inherent risks can also be identified in the field of identification and access control applications. In case of a loss of a contactless smart chip utilized for such applications, the cardholder is unable to prevent unauthorized use and a counter party may trust obtained card  
25 information by mistake.

An object of the present invention is to overcome the aforementioned implementation deficiencies, to which state of the art contactless technology implementations are subjected.

30 In particular, an object of the present invention is to enable a cardholder as well as a service provider to remotely exercise active and/or passive control.

The object of the present invention is solved by the features defined in the accompanying claims.

35 According to an aspect of the present invention, a terminal device is provided. The terminal device comprises a network connectivity subsystem enabled for data connectivity with a wireless communications network, a secure storage subsystem having a secure storage memory for

securely storing contents and enabled for local RF connectivity through a local RF communication subsystem, and an interconnectivity component which is adapted to enable communication of the secure storage subsystem through the network connectivity subsystem with the network. The secure storage subsystem is operable with any contactless technology, i.e. the secure storage subsystem interoperates with any external counterpart device as a contactless transponder. In particular, the external counterpart device may be capable for contactless connectivity, e.g. the external counterpart device may comprise a contactless reader, which communicates with the secure storage subsystem operable as a contactless smartcard. The interconnectivity component is configured to detect that messages received from the network are destined for the secure storage subsystem. Further, the interconnectivity component is configured to supply the messages to the secure storage subsystem. The messages enable exercising control over the secure storage subsystem in that the messages comprise one or more instructions to be processed by a secure memory controller of the secure storage subsystem.

According to another aspect of the present invention, a secure storage subsystem is provided. The secure storage subsystem comprises a secure storage controller adapted to operate the secure storage subsystem, a secure storage memory provided for secure storing of contents, and a local radio frequency connectivity subsystem arranged for local RF connectivity. The secure storage subsystem is operable as contactless smartcard. The secure storage controller is enabled for data communication with a wireless communications network through an interconnectivity component coupling the secure storage subsystem to a network connectivity subsystem enabled for data connectivity with the network. The secure storage subsystem receives messages from the network destined for the secure storage subsystem through the interconnectivity component. The messages enable exercising control over the secure storage subsystem in that the messages comprise one or more instructions to be processed by a secure memory controller of the secure storage subsystem.

According to another aspect of the present invention, a system is provided. The system comprises a terminal device, a secure storage subsystem, and an interconnectivity component. The terminal device has a network connectivity subsystem enabled for data connectivity with a wireless communications network. The secure storage subsystem has a secure storage memory for securely storing contents and enabled for local RF connectivity through a local RF communication subsystem. The secure storage subsystem is operable as a contactless smartcard. The interconnectivity component is adapted to enable communication of the secure storage subsystem through the network connectivity subsystem with the network. The interconnectivity component is further configured to detect that messages received from the network are destined for the secure storage subsystem and is configured to supply those messages, which are identified

to be destined to the secure storage subsystem, to the secure storage subsystem. The messages enable exercising control over the secure storage subsystem in that the messages comprise one or more instructions to be processed by a secure memory controller of the secure storage subsystem.

5 According to another aspect of the present invention, a method of network-based remote control over a secure storage subsystem is provided, which secure storage subsystem comprises a secure storage memory for securely storing contents and is enabled for local RF connectivity through a local RF communication subsystem. The secure storage subsystem is operable as a contactless smartcard. Messages are received at a network connectivity subsystem from a wireless  
10 communications network. The network connectivity subsystem is enabled for data connectivity with the network. The network messages are received at an interconnectivity component and those messages are identified which are destined for the secure storage subsystem. The identified messages are supplied to the secure storage subsystem. The messages are processed at a secure memory controller of the secure storage subsystem. The messages comprise one or more  
15 instructions enabling exercising control over the secure storage subsystem.

According to another aspect of the present invention, a computer program product is provided, which enables network-based remote control over a secure storage subsystem. The computer program product comprises program code sections for carrying out the steps of the method  
20 according to an aforementioned embodiment of the invention, when the program is run on a computer, a terminal, a network device, a mobile terminal, a mobile communication enabled terminal or an application specific integrated circuit. Alternatively, an application specific integrated circuit (ASIC) may implement one or more instructions that are adapted to realize the aforementioned steps of the method of an aforementioned embodiment of the invention, i.e.  
25 equivalent with the aforementioned computer program product.

For a better understanding of the present invention and to understand how the same may be brought into effect reference will now be made, by way of illustration only, to the accompanying drawings, in which:

30

Fig. 1 illustrates schematically principle block diagrams depicting typical components of a contactless smartcard and a contactless reader subsystem;

35

Fig. 2 illustrates schematically a principle block diagram of a terminal device enabled for network data connectivity and contactless local radio frequency (RF) communication according to an embodiment of the present invention;

Figs. 3a and 3b illustrate schematically further principle block diagrams of the terminal device of Fig. 2 enabled for networks data connectivity and contactless local radio frequency (RF) communication according to embodiments of the present invention;

5

Figs. 4a and 4b illustrate schematically principle block diagrams of system arrangements according to embodiments of the present invention; and

10

Figs. 5a to 5b illustrate schematically time flow message charts depicting message exchange between entities of the system of Figs. 4a or 4b according to embodiments of the present invention.

Throughout the description below, same and/or equal components will be referred by the same reference numerals.

15

Throughout the following detailed description of embodiments of the present invention, the concept of the present invention will be described with reference to a cellular communication subsystem, which in particular supports GSM, GSM/GPRS, and/or GSM/EDGE, UMTS, and/or cdma2000, cellular communication. Moreover, the local radio frequency (RF) connectivity communication will be described with reference to specific implementation standards including in particular ISO/IEC 10536 (close coupling cards), ISO/IEC 14443 type A and type B (proximity cards), ISO/IEC 15693 (vicinity cards), ISO/IEC 18092 (Near Field Communication, NFC) standard, and EPCglobal standard. It should be noted that the aforementioned specifications of the cellular communication subsystem as well as the local radio frequency (RF) connectivity communication are embodied for the sake of illustration. The invention should be understood as not being limited thereto.

20

Originally, radio frequency identification (RFID) technology has been developed and introduced to identify objects and people. These applications range from tracking animals and tagging goods for inventory control and logistics to enabling fast payment and securely identifying people. While these applications all use radio waves to communicate information, the RF chip technology used for each is quite different, addressing the storage, range, and security requirements of a specific application. As a general definition, radio frequency identification (RFID) tag technology is used in applications that identify or track objects and contactless smart card technology is used in applications that identify people or store financial or personal information. A generic term of the overall technical field may be defined as contactless technology. Applications most often have differing requirements in their use of RF technology,

30

35

with RFID transponders and contactless smart card technologies providing very different capabilities. However, the basic data communication is based on the same physical data communication concept.

5 A typical implementation of a state of the art radio frequency contactless smartcard is shown with respect to Fig. 1, which depicts a smart card module 10 for the sake of illustration. The typical smart card module 10 includes conventionally an electronic circuit, depicted exemplarily as smart card logic 12, with data storage capacity, depicted herein as smart card memory 13, and a radio frequency (RF) interface 11, which couples an antenna 14 to the logic 12. Such RF-based  
10 contactless smartcards may be accommodated in small containers such as ISO standard cards (known from the form factor of credit cards), key fobs, modules, self-adhesive labels, paper tickets, and the like. Depending on the requirements made on envisaged applications of the contactless smartcards (i.e. data transmission rate, kind of energizing, transmission range etc.) different types are provided for data/information transmission at different radio frequencies  
15 within a range from several 10 - 100 kHz to some GHz.

Two main classes of contactless smartcard modules can be distinguished. Passive contactless smartcard modules are activated and energized by contactless reader modules, which generate an excitation radio frequency signal or interrogation radio frequency signal (continuous wave), for  
20 example a radio frequency (RF) signal at a predefined frequency. Active contactless smartcard modules comprise their own power supplies (not shown) such as batteries or accumulators for energizing. Moreover, it should be noted that hybrid implementations exist. One type of hybrid contactless smartcard module may comprise its own power source, which energizes the transponder logic 12 and/or memory 13, whereas the RF interface 11 is energized by an  
25 interrogation RF signal received from a contactless reader module. However, other types of hybrid contactless smartcard modules may be realizable.

Upon activation of a contactless smartcard by the means of a contactless reader module 20, the informational contents stored in the transponder memory 13 are modulated onto a radio  
30 frequency (RF) signal (i.e. the interrogation RF signal), which is emitted by the antenna 14 of the contactless smartcard module 10 to be detected and received by the contactless reader module 20. More particularly, in the case of a passive contactless smartcard module (i.e., without any local power source), the contactless smartcard module 10 is conventionally energized by a time-varying electromagnetic radio frequency (RF) signal (continuous RF wave) generated by the  
35 interrogating contactless reader module 20. When the radio frequency (RF) field passes through the antenna coil associated with the contactless smartcard module 10, a voltage is generated across the coil. This voltage is used to energize the contactless smartcard module 10, and enables

back-transmission of information from the contactless smartcard module 10 to the contactless reader module 20, which is conventionally referred to as back-scattering.

5 In accordance with the application purpose of a contactless smartcard module 10, information or data stored in the transponder memory 13 may be either hard-coded or soft-coded. Hard-coded means that information or data stored in the transponder memory 13 is predetermined and unmodifiable. Soft-coded means that information or data stored in the transponder memory 13 is configurable by an external entity. The configuration of the transponder memory 13 may be performed by a radio frequency (RF) signal received via the antenna 14 or may be performed via  
10 a configuration interface (not shown), which allows access to the transponder memory 13.

A contactless reader module 20 typically comprises a RF interface 21, a reader logic 22, and a data interface 23. The data interface 23 is conventionally connected with a host system such as a portable terminal, which, inter alia, on the one hand exercises control over the operation of the  
15 contactless reader 20 by the means of instructions transmitted from the host to the reader logic 22 via the data interface 23 and on the other hand receives data provided by the reader logic 22 via the data interface 23. Upon instruction to operate, the reader logic 22 initiates the RF interface 21 to generate the excitation / interrogation signal to be emitted via the antenna 24 coupled to the RF interface 21 of the contactless reader module 20. In case that a contactless smartcard such as  
20 the contactless smartcard module 10 is within the coverage area of the excitation / interrogation signal, the contactless smartcard module 10 is energized and a modulated RF signal (back-scatter RF signal) is received therefrom. Particularly, the modulated RF signal carries the data stored in the transponder memory 13 modulated onto the excitation / interrogation RF signal. The modulated RF signal is coupled into the antenna 24, demodulated by the RF interface 21, and  
25 supplied to the reader logic 22, which is then responsible to obtain the data from the demodulated signal. Finally the data obtained from the received modulated RF signal is provided via the data interface of the contactless reader module 20 to the host system connected thereto.

The communication between contactless reader module and contactless smartcard module may  
30 comprise a simple response generated by the contactless smartcard module upon interrogation by the contactless reader module. In a more sophisticated manner, the communication between contactless reader module and contactless smartcard module may occur in a packetized manner, where one or more packets, each of which contains a complete command from the contactless reader module and a complete response from the contactless smartcard module. Typically, the  
35 command and response permit half-duplex communication between the contactless reader module and contactless smartcard module.

Depending on the requirements and/or complexity of the contactless application, the contactless technology is distinguished into radio frequency identification (RFID) technology and contactless smart card technology. For this reason, the term contactless smartcard should be understood as generic term including at least radio frequency identification (RFID) transponder, contactless smart cards and similar or like modules capable for contactless connectivity as defined in this application. The same definition will be used in relationship with counterpart devices capable for communication with the contactless smartcard, especially capable for reading access thereto. The term contactless reader should be understood as generic term including at least radio frequency identification (RFID) readers, contactless smart card readers and similar or like reader modules capable for contactless connectivity as defined in this application.

The term radio frequency identification (RFID) transponder is typically used to designate contactless smartcards, which are simple, low-cost, and disposable, and which are used for simple identification purposes (such as identifying animals), tracking goods logistically and replacing printed bar codes at retailers. Radio frequency identification (RFID) transponder modules include conventionally a chip that typically stores a static number, typically denoted as an identifier (ID), and an antenna that enables the chip to transmit the stored static number to reader modules. When the transponder module comes within range of an appropriate reader module, the transponder module is energized by the reader module's radio frequency field and transmits its identifier (ID) to the reader module. There is conventionally only little to no security provision on the radio frequency transponder module or during radio frequency (RF) communication with the reader module. Any reader module using the appropriate radio frequency (RF) signal, typically a RF signal having a predefined frequency, can initiate the radio frequency identification transponder to communicate its contents stored therein. Typical radio frequency identification (RFID) transponder module may be easily read from distances of several centimeters or inches to several meters or yards to allow easy tracking of goods and/or objects. RFID tags have common characteristics, including:

- Low cost, high volume manufacturing to minimize investment required in implementation.
- Minimal or limited security technology with radio frequency identification (RFID) transponder modules able to be read by any compatible radio frequency identification (RFID) reader module.
- Disposable or one-time use.

- Minimal or limited data storage capacity (comparable to bar code) usually a fixed format written once when the radio frequency identification (RFID) transponder is manufactured.
- Read range optimized to increase speed and utility.

5

Contactless smart card technology is conventionally used in applications that need to protect personal information or deliver secure transactions. Contact smart card technology provides similar capabilities but does not have any radio frequency (RF) interface that allows contactless smart card modules to be conveniently read at a short distance from the smart card reader modules. Current and emerging applications using contactless smart card technology include transit fare payment cards, government, and corporate identification cards, documents such as electronic passports and visas, and contactless financial payment cards. The contactless device typically includes a smart card secure component, or equivalent logics, and internal memory component and has the unique ability to securely manage, store, and provide access to data stored in the memory component, perform complex functions (for example, encryption or other security functions) and interact intelligently via radio frequency (RF) communication with a appropriate contactless reader module. Applications that require higher or highest degree of information and communications security (for example, payment applications, government identifications, electronic passports) use preferably contactless smart card technology based on international standards that limit the ability to read the contactless card module to approximately 10 centimeters (4 inches). Applications that need longer reading distances may use other forms of contactless technologies that can be read at longer distances.

Applications using contactless smart cards support many security features that ensure the integrity, confidentiality, and privacy of information stored or transmitted, including the following:

- Mutual authentication: For applications requiring secure data access, a contactless smart card-based device may verify that the smart card reader module is authentic and may prove its own authenticity to the smart card reader before starting a secure transaction.
- Strong information security: For applications requiring complete data protection, information stored in such smart card modules or documents using contactless smart card technology can be encrypted and RF communication between a contactless smart card-based device and a smart card reader module may be encrypted to prevent eavesdropping. Additional security technologies may also be used to ensure information integrity.



- 5 - Strong contactless device security: Like contact smart cards, contactless smart card technology is extremely difficult to duplicate or forge and has built-in tamper-resistance. Smart card chips include a variety of hardware and software capabilities that detect and react to tampering attempts and help counter possible attacks.
- 10 - Authenticated and authorized information access: The ability of contactless smart card module to process information and react to its environment allows the contactless smart card module to uniquely provide authenticated information access and protect the privacy of personal information. The contactless smart card can verify the authority of the information requestor and then allow access only to the information required. Access to stored information can also be further protected by a personal identification number (PIN) or biometric to protect privacy and counter unauthorized access.
- 15 - Strong support for information privacy: The use of smart card technology strengthens the ability of a system to protect individual privacy. Unlike other technologies, smart card-based devices may implement firewall technology for an individual, releasing only the information required and only when it is required.

20 It is important to note, however, that information privacy and security must be designed into an application at the system level by the organization issuing the contactless smart card-based device, smart card module, or document. It is critical that issuing organizations have the appropriate policies in place to support the security and privacy requirements of the application being deployed and then implement the appropriate technology that delivers those features.

25 Those skilled in the art will understand on the basis of the aforementioned description that the fields of technology referred to above are not well separated. In view of future developments especially in the field of integrated circuit (IC) technology, radio frequency identification (RFID) technology and contactless smart card technology may converge; i.e. one or more specific features of today's contactless smart card technology such as production costs and storage capacity will be available at reasonable costs.

30

Currently, following typical frequencies are used in the field of contactless technology:

- 35 Low frequency range at less than 135 kHz, typically around 125 kHz;
- High frequency range at around 13.56 MHz;
- Ultra-High Frequency range (UHF) in the range from 860 MHz to 960 MHz; and
- Microwave frequency range at around 2.54 GHz ISM frequency band.

The 125 kHz contactless technology is used by the majority of today's radio frequency identification (RFID) transponder based access control system also called proximity access control systems). The 125 kHz contactless technology is based on de facto industry standards. One major de facto industry standard for 125 kHz technology access control systems Typically, 5 the 125 kHz contactless technology is a passive radio frequency communication technology because the radio frequency field emitted by a corresponding reader energized the logic of such a card.

10 The 13.56 MHz contactless technology is standardized on the basis of several standards including especially ISO/IEC 14443, ISO/IEC 15693, and ISO/IEC 18092. These technologies are considered to satisfy application requirements for higher security, to accommodate multiple applications on a single smart card module implementation and to protect privacy aspects of cardholder information.

15 The 13.56 MHz technology conform to ISO/IEC 14443 standard is a contactless technology with a read range of up to approx. 10 centimeters (4 inches). This technology is originally designed for electronic ticketing and electronic cash. For these applications, short read ranges and fast transaction speeds are critical. The ISO/IEC 14443 standard includes two versions, type A and type B, with different modulation approaches. The key features of ISO/IEC 14443 standard 20 include the operating frequency at around 13.56 MHz with a read/write range up to 10 centimeters and an ISO/IEC standard data rate of 106 Kbps (kilobit per second; kbits/s). In the meantime, ISO/IEC 14443 technology (A or B) is capable of 212 Kbps, 424 Kbps, and 848 Kbps; higher data rates are under discussion. The typical storage capacity is in a range from 64 bytes to 64 Kbytes. Security aspects are taken into consideration with implementations 25 comprising wired logics enabling authentication mechanisms, microcontroller based logics enabling security mechanisms, and/or crypto coprocessor based logics enabling cryptographic mechanisms such as 3DES, AES, ECC, and RSA. The close proximity requirement to enable communication supports to prevent or at least limit unintended communication.

30 The 13.56 MHz technology conform to ISO/IEC 15693 standard is designed to operate at ranges of up to approx. 1 meter (3.3 feet). The specification is well suited for facility access control in buildings, where read ranges are set to for instance 10 to 15 centimeters (4 to 6 inches) for building doors, and for parking lot access systems, where read ranges can be set to higher ranges, making it unnecessary for drivers to extend an arm out of the car window. The key features of 35 ISO/IEC 15693 standard include operating frequency at around 13.56 MHz, a read range up to approx. 1 meter (3.3 feet), a data rate of 26 Kbps and storage capacity including typically 1 Kbit (128 bytes), 2 Kbit (256 bytes), and 16 Kbit (2 Kbytes). Security aspects are considered on the

basis of wired logic/memory-based only credentials enabling authentication and/or encryption mechanisms, mutual authentication between card and reader, and/or DES and 3DES data encryption implementation.

5 The ISO/IEC 18092 standard designed Near Field Communication (NFC) defines a protocol based on a wireless interface for enabling peer-to-peer communication. The interface operates at the 13.56 MHz radio frequency band and operating distances of approx 0 to 20 cm are realizable. Generally the Near Field Communication defines a reader-to-reader communication, which includes transponder-to-reader communication. The NFC protocol distinguishes between a  
10 communication Initiator, which initiates and controls the exchange of data, and a communication Target, which answers the request from the Initiator. NFC protocol also distinguishes between two modes of operation: active mode and passive mode. In Active mode both devices (Initiator and Target) generate their own RF field to carry the data. In Passive mode only one device (Initiator) generates the RF field while the other device (Target) uses load modulation to transfer  
15 the data. The application sets the initial communication speed at 106 Kbps, 212 Kbps, or 424 Kbps. Subsequently the application and/or the communication environment may require speed adaptation.

In the field of UHF, contactless technology is standardized on the basis of EPCglobal  
20 specification. The EPCglobal specification relates to Electronic Product Codes (EPC), which will replace the conventional bar codes for product labeling in the field of enable product chain management and logistics of goods. The UHF contactless technology enables reader distances up to several meters.

25 All these standards are distinguished by well-defined communication protocols, which typically comprise half-duplex communication. As aforementioned, the communication is typically based on one or more command and response exchanges through the RF interfaces.

It should be noted that the aforementioned enumeration of standards is given for the sake of  
30 illustration to enlighten the field of contactless technology and a selection of the multiple, various standards available in this field. Those skilled in the art will appreciate that the inventive concept is applicable with any available and/or future standard.

Fig. 2 shows a schematic block illustration of components of a user terminal device in an  
35 exemplary form of a portable cellular communication enabled terminal 100. The terminal device 100 exemplarily represents any kind of processing terminal or device employable with the

present invention. It should be understood that the present invention is neither limited to the illustrated terminal device 100 nor to any other specific kind of processing terminal or device.

5 As aforementioned, the illustrated terminal device 100 is exemplarily embodied as a cellular communication enabled portable user terminal with contactless secure storage capability. In particular, the terminal device 100 is embodied as a processor-based or micro-controller based system comprising a central processing unit (CPU) and a mobile processing unit (MPU) 110, respectively, a data and application storage 120, cellular communication means including cellular radio frequency interface (I/F) 180 with correspondingly adapted RF antenna (outlined) and  
10 subscriber identification module (SIM) 185, user interface input/output means including typically audio input/output (I/O) means 140 (conventionally a microphone and a loudspeaker), keys, keypad and/or keyboard with key input controller (Ctrl) 130 and a display with display controller (Ctrl) 150, and a (local) wireless and/or wired data interface (I/F) 160.

15 The operation of the terminal device 100 is controlled by the central processing unit (CPU) / mobile processing unit (MPU) 110 typically on the basis of an operating system or basic controlling application, which controls the functions, features and functionality of the terminal device 100 by offering their usage to the user thereof. The display and display controller (Ctrl) 150 are typically controlled by the processing unit (CPU/MPU) 110 and provide information for  
20 the user including especially a (graphical) user interface (UI) allowing the user to make use of the functions, features and functionality of the terminal device 100. The keypad and keypad controller (Ctrl) 130 are provided to enable the user inputting information. The information input via the keypad is conventionally supplied by the keypad controller (Ctrl) to the processing unit (CPU/MPU) 110, which may be instructed and/or controlled in accordance with the input  
25 information. The audio input/output (I/O) means 140 includes at least a speaker for reproducing an audio signal and a microphone for recording an audio signal. The processing unit (CPU/MPU) 110 can control conversion of audio data to audio output signals and the conversion of audio input signals into audio data, where for instance the audio data have a suitable format for transmission and storing. The audio signal conversion of digital audio to audio signals and vice  
30 versa is conventionally supported by digital-to-analog and analog-to-digital circuitry e.g. implemented on the basis of a digital signal processor (DSP, not shown).

The keypad operable by the user for input comprises for instance alphanumeric keys and telephony specific keys such as known from ITU-T keypads, one or more soft keys having  
35 context specific input functionalities, a scroll-key (up/down and/or right/left and/or any combination thereof for moving a cursor in the display or browsing through the user interface (UI), a four-way button, an eight-way button, a joystick or/and a like controller.

The terminal device 100 according to a specific embodiment illustrated in Fig. 4 includes the cellular communication subsystem 180 coupled to the radio frequency antenna (outlined) and operable with the subscriber identification module (SIM) 185. The cellular communication subsystem 180 may be also designed as cellular (communication) interface (I/F). The cellular communication subsystem 180 is arranged as a cellular transceiver to receive signals from the cellular antenna, decodes the signals, demodulates them, and also reduces them to the base band frequency. The cellular communication subsystem 180 provides for an over-the-air interface, which serves in conjunction with the subscriber identification module (SIM) 185 for cellular communications with a corresponding base station (BTS) of a radio access network (RAN) of a public land mobile network (PLMN). The output of the cellular communication subsystem 180 thus consists of a stream of data that may require further processing by the processing unit (CPU/MPU) 110. The cellular communication subsystem 180 arranged as a cellular transceiver is also adapted to receive data from the processing unit (CPU/MPU) 110, which is to be transmitted via the over-the-air interface to the base station (BTS) of the radio access network (RAN) (not shown). Therefore, the cellular communication subsystem 180 encodes, modulates and up-converts the data embodying signals to the radio frequency, which is to be used for over-the-air transmissions. The antenna (outlined) of the terminal device 100 then transmits the resulting radio frequency signals to the corresponding base station (BTS) of the radio access network (RAN) of the public land mobile network (PLMN). The cellular communication subsystem 180 preferably supports a 2<sup>nd</sup> Generation digital cellular network such as GSM (Global System for Mobile Communications) which may be enabled for GPRS (General Packet Radio Service) and/or EDGE (Enhanced Data for GSM Evolution; 2.5 Generation), a 3<sup>rd</sup> generation digital cellular network such as any CDMA (Code Division Multiple Access) System including especially UMTS (Universal Mobile Telecommunications System) also designated as WCDMA (Wide-Band Code Division Multiple Access) System and cdma2000 System, and/or any similar, related, or future (3.9 Generation, 4<sup>th</sup> Generation) standards for cellular telephony.

It should be understood that the cellular communication subsystem 180 may support cellular communication at multiple different frequency bands. For instance, the cellular communication subsystem 180 supports cellular communication at the frequency bands GSM 850, GSM 900, GSM 1800, and/or GSM 1900. Moreover, the cellular communication subsystem 180 may support cellular communication at multiple different protocols. For instance, the cellular communication subsystem 180 supports cellular communication according to the GSM standard and the UMTS standard or the GSM standard and the cdma2000 standard or any other combination thereof. The cellular communication subsystem 180 supporting cellular communication at multiple different frequency bands should be also designated as multi-band

cellular communication subsystem 180, whereas the cellular communication subsystem 180 supporting cellular communication at multiple different protocols should be also designated as multi-mode cellular communication subsystem 180. Note that the cellular communication subsystem 180 may be a multi-band and multi-mode cellular communication subsystem 180.

5

The wireless and/or wired data interface (I/F) 160 is depicted exemplarily and should be understood as representing one or more data interfaces, which may be provided in addition to the above described cellular communication subsystem 180 implemented in the exemplary terminal device 100. A large number of wireless communication standards are available today. For instance, the terminal device 100 may include one or more wireless interfaces operating in accordance with any IEEE 802.xx standard, Wi-Fi standard, WiMAX standard, any Bluetooth standard (1.0, 1.1, 1.2, 2.0 + EDR, LE), ZigBee (for wireless personal area networks (WPANs)), Infra-Red Data Access (IRDA), Wireless USB (Universal Serial Bus), and/or any other currently available standards and/or any future wireless data communication standards such as UWB (Ultra-Wideband).

10  
15

The terminal device 100 comprising several communication interfaces including for instance a cellular communication interface 180, and one or more wireless communication interfaces 160 may be designed as multi-radio terminal device 100.

20

Moreover, the data interface (I/F) 160 should also be understood as representing one or more data interfaces including in particular wired data interfaces implemented in the exemplary terminal device 100. Such a wired interface may support wire-based networks such as Ethernet LAN (Local Area Network), PSTN (Public Switched Telephone Network), DSL (Digital Subscriber Line), and/or other available as well as future standards. The data interface (I/F) 160 may also represent any data interface including any proprietary serial/parallel interface, a universal serial bus (USB) interface, a Firewire interface (according to any IEEE 1394/1394a/1394b etc. standard), a memory bus interface including ATAPI (Advanced Technology Attachment Packet Interface) conform bus, a MMC (MultiMediaCard) interface, a SD (SecureData) card interface, Flash card interface and the like.

25

30

The terminal device 100 according to an embodiment of the present invention comprises secure storage subsystem 190 capable for contactless communication through a RF front-end interface coupled to a RF antenna (outlines). Reference should be given to Fig. 1 and the aforementioned description thereof, which illustrates the basic implementation and operation of contactless smartcard module 10. The secure storage subsystem 190 may be included in the terminal 100, fixely connected to the terminal 100, or detachably coupled to the terminal 100. In particular, the

35

secure storage subsystem 190 may be arranged on or in a cover of the terminal device 100, where the cover is preferably a detachable functional cover of the terminal device 100. In accordance with the inventive concept of the present invention, an interconnectivity component 205 is comprised by the terminal device 100. The interconnectivity component 205 is provided to  
5 enable connectivity between a network connectivity subsystem, herein the cellular communication subsystem 180, and the secure storage subsystem 190. Details about the specific implementation of the secure storage subsystem 190 and the interconnectivity component 205 will be presented below in detail.

10 The components and modules illustrated in Fig. 2 may be integrated in the terminal device 100 as separate, individual modules, or in any combination thereof. Preferably, one or more components and modules of the terminal device 100 may be integrated with the processing unit (CPU/MPU) forming a system on a chip (SoC). Such system on a chip (SoC) integrates preferably all components of a computer system into a single chip. A SoC may contain digital, analog, mixed-  
15 signal, and also often radio-frequency functions. A typical application is in the area of embedded systems and portable systems, which are constricted especially to size and power consumption constraints. Such a typical SoC consists of a number of integrated circuits that perform different tasks. These may include one or more components comprising microprocessor (CPU/MPU), memory (RAM: random access memory, ROM: read-only memory), one or more UARTs  
20 (universal asynchronous receiver-transmitter), one or more serial/parallel/network ports, DMA (direct memory access) controller chips, GPU (graphic processing unit), DSP (digital signal processor) etc. The recent improvements in semiconductor technology have allowed VLSI (Very-Large-Scale Integration) integrated circuits to grow in complexity, making it possible to integrate all components of a system in a single chip.

25 Typical applications operable with the terminal device 100 comprise beneath the basic applications enabling the data and/or voice communication functionality a contact managing application, a calendar application, a multimedia player application, a WEB/WAP browsing application, and/or a messaging application supporting for instance Short Message Services  
30 (SMS), Multimedia Message Services (MMS), and/or email services. Modern portable electronic terminals are programmable; i.e. such terminals implement programming interfaces and execution layers, which enable any user or programmer to create and install applications operable with the terminal device 100. A today's well established device-independent programming language is JAVA, which is available in a specific version adapted to the functionalities and  
35 requirements of mobile device designate as JAVA Micro Edition (ME). For enabling execution of application programs created on the basis of JAVA ME the terminal device 100 implements a JAVA MIDP (Mobile Information Device Profile), which defines an interface between a JAVA

ME application program, also known as a JAVA MIDlet, and the terminal device 100. The JAVA MIDP (Mobile Information Device Profile) provides an execution environment with a virtual JAVA engine arranged to execute the JAVA MIDlets. However, it should be understood that the present invention is not limited to JAVA ME programming language and JAVA MIDlets; other programming languages especially proprietary programming languages are applicable with the present invention.

With reference to Figs. 3a and 3b, schematic block diagrams or illustrated, which comprises principle structural components according to embodiments of the present invention.

The network connectivity subsystem 250 represents any data communication subsystem, in particular any of the aforementioned communication subsystems, wireless and/or wired data interfaces. The network connectivity subsystem 250 may be a cellular communication subsystem such as the cellular communication subsystem 180 described detailed with reference to Fig. 2. Moreover, the network connectivity subsystem 250 may be a wireless communication subsystem such as the wireless data interface 160 or wired communication subsystem such as the wired data interface 160 both described detailed with reference to Fig. 2.

The secure storage subsystem 190 may be realized according to an embodiment of the invention on the basis of a secure storage memory 192 and a secure storage controller 191. The secure storage memory 192 is coupled through the secure storage controller 191 and a communication controller 200 to a separate local radio frequency (RF) connectivity subsystem 193, which enables for radio frequency communication with an appropriate contactless reader subsystem such as contactless reader module 20. Schematically, the secure storage subsystem 190 may be understood as comprising the local radio frequency (RF) connectivity subsystem 193. However, it should be noted that the local radio frequency (RF) connectivity subsystem 193 may or may not be included within the secure storage subsystem 190 including at least the secure storage memory 192 and the secure storage controller 191. In a general case, the local radio frequency (RF) connectivity subsystem 193 may be provided by the terminal device 100 and an interface (hardware and/or software interface, application program interface, and the like) is provided to interface communication between the secure storage subsystem 190 and the local radio frequency (RF) connectivity subsystem 193.

The secure storage subsystem 190 according to an embodiment of Fig. 3a should illustratively represent an integrated implementation on the basis of a secure storage memory 192. The secure memory 192 may be a specific storage memory component or may be a portion of a general storage memory. The secure storage memory 192 is preferably enabled for functionality known



in the field of (contactless) smart card technology. The secure storage controller 191, which is preferably based on a software implementation eventually supported by mechanisms operable with hardware components (e.g. cryptographic engines), is adapted to provide an interface (preferably an application program interface, API) for controlling access to the secure storage memory as aforementioned with reference to the smart contactless technology. The access control includes in particular read access control, write access control, security mechanisms, authentication check mechanisms, integrity check mechanisms, and the like. The access control should meet the requirement issues of the application, for which the secure storage subsystem 190 is intended to be used.

10

Likewise, the secure storage subsystem 190 according to another embodiment of Fig. 3a should illustratively represent an implementation being based on a (contact) smart card. This means, the secure storage memory 192 as well as the secure storage controller 191 may be implemented on the basis of a smart card, which forms the secure storage subsystem 190. The smart card implements the aforementioned functionality, especially access control to the secure storage memory 192. The access control includes in particular read access control, write access control, security mechanisms, authentication check mechanisms, integrity check mechanisms, and the like. The access control should meet the requirement issues of the application, for which the secure storage subsystem 190 is intended to be used. The smart card, i.e. herein the secure storage subsystem 190 according to this embodiment, may be fixely attached and connected to the terminal device 100 or may be detachably connected to the terminal device 100 providing a receptacle (not shown), such as a card slot, which is provided with a (physical) interface to enable connectivity between the terminal device 100 and an inserted smart card, which forms the secure storage subsystem 190. In general, the smart card (either fixely or detachable connected) and the terminal device 100 are interconnected through a (physical) interface.

25

The capability of contactless communication as illustrated above with reference to the contactless technology is enabled through the local RF connectivity subsystem 193.

Alternatively, the secure storage subsystem 190 may be realized according to an embodiment of the invention of Fig. 3b on the basis of a contactless smart card which is conform to any contactless technology and/or standard thereof. The secure storage subsystem 190 includes a secure storage memory 192, a secure storage controller 191, and a local radio frequency (RF) connectivity subsystem 193, wherein the secure storage memory 192 is coupled through the secure storage controller 191 to an implemented local radio frequency (RF) connectivity subsystem 193, which enables for radio frequency communication with an appropriate contactless reader subsystem such as contactless reader module 20. The contactless smart card,

30  
35

i.e. herein the secure storage subsystem 190 according to this embodiment, may be fixely attached and connected to the terminal device 100 or may be detachably connected to the terminal device 100, which provides a receptacle such as a card slot, which is provided with a (physical) interface to enable connectivity between terminal device 100 and contactless smart card forming the secure storage subsystem 190. Alternatively, the contactless smart card may be attached to or included in a detachable cover of the terminal device 100. In general, the contactless smart card and the terminal device 100 are interconnected through a (physical) interface.

10 It should be further noted that the secure storage controller 191 may be hardware and/or software implemented and is adapted to provide a hardware and/or software (application program) interface for controlling the access to the secured storage memory including in particular read access, write access, security mechanisms, authentication check mechanisms, integrity check mechanisms, and the like. In general, the secure storage controller 191 is primarily configured to enable the security functionality of the secure storage subsystem 190.

In principle, it should be understood that independent of the detailed implementation according to any of the aforementioned embodiments according to the present invention the secure storage subsystem 190 with the local radio frequency (RF) connectivity subsystem 193 is capable of representing and acting as a contactless smartcard module 10 in view of any external contactless reader such as contactless reader module 20. The secure storage controller 191 operates the secure storage specific functionality, in particular the secure storage controller 191 may be a management application performing the secure storage specific functionality, which is preferably implemented on the basis of hardware and/or stored in the secure storage memory (representing secure memory). The secure storage controller 191 may comprise a secure storage operating system, in particular a card operating system (OS). In general secure storage or secure memory should be understood to designate a memory being based on any storage technology which is capable to store data contents, which access (read and/or write access including modifying and deleting) is subjected to access policies defined by the application, with which the data contents is applicable.

The communication controller 200 is adapted to control operations of the data communication subsystems of the terminal device 100, in particular to exercise control of the network connectivity subsystem 250 and the local radio frequency (RF) connectivity subsystem 193. Depending on implementation details of the secure storage subsystem 190, the control over the local radio frequency (RF) connectivity subsystem 193 may be directly exercised or may be exercised through the secure storage controller 191.

The local radio frequency (RF) connectivity subsystem 193 is adapted to operate radio frequency (RF) communication on the basis of contactless technology. In particular, the local radio frequency (RF) connectivity subsystem 193 is adapted to operate radio frequency (RF) communication in accordance with any current available or future contactless technology standard including especially ISO/IEC 14443A (Mifare), ISO/IEC 14443B, ISO/IEC 15693, and/or ISO/IEC 18092 (NFC, FeliCa).

More particularly, the communication controller 200 is adapted to interoperate with the secure storage controller 191 of the secure storage subsystem 190. The communication controller 200 and in particular a interconnectivity component 205, which may be part of the communication controller 200 or which may be provided as a separate component in association with the communication controller 200 enables data exchange between the network connectivity subsystem 250 and the secure storage subsystem 190 operated by the means of the secure storage controller 191.

In view of typical use cases including electronic ticket applications such as electronic commuter ticket applications, identification application, electronic access control applications, electronic payment applications such as electronic prepaid payment applications, electronic credit card applications, electronic membership identification applications, point card application, check-in and/or mileage services applications various security requirements have to be met including especially integrity and authenticity of contents relating to one or more of the aforementioned applications, (read and/or write) access control to contents, tamper-proof of contents, secured communication of contents with reader-based counterpart devices such as ticket gates or points of sales. These issues relating to security requirements are realized on the basis of the secure storage controller 191 and pre-defined security policies. The application related contents and security policies are stored in the secure storage memory 192 of the secure storage subsystem 190. It should be noted that in general contents and security policies relating to several applications may be stored in the secure storage memory 192.

Conventionally, secure storage subsystem 190 is provided by card issuers or application service providers with predefined application related contents and predefined security policies. Moreover, the secure storage subsystem 190 may store application related code sections including program code for being executed e.g. by the secure storage controller 191 and/or the terminal device 100. The application related code sections enable, when executed by the secure storage controller 191 and/or the processor 110 of the terminal device 100, the data communication of the secure storage subsystem 190 with reader-based counterpart devices in

accordance with the application for which the secure storage subsystem 190 is destined. Further, the secure storage subsystem 190 may store application related code sections including user interface definitions enabling displaying of one or more user interface elements to a user by the display 150 of the portable terminal 100. The user interface elements are provided to the user to control the operation of the secure storage subsystem 190 and especially the secure storage controller 191 thereof including especially initiating of an application related data communication of the secure storage subsystem 190 with reader-based counterpart devices. In view of the aforementioned capabilities of the terminal device 100, the application related code sections, i.e. program code and/or user interface definitions, may be provided on the basis of JAVA MIDlets executable with a virtual JAVA engine.

Conventionally, modifications on the data stored in the secure storage subsystem 190 such as entering additional credit into an account maintained by electronic prepaid payment application or electronic wallet application, loading electronic tickets into an electronic ticket application, loading access control information into electronic access control application, identification information into an electronic identification application is, if at all, performed via the radio frequency interface established by the local radio frequency (RF) connectivity subsystem 193 and in accordance with the access policies defined.

The integration of a secure storage technology with a portable terminal 100 having network connectivity enables advantageously provision of additional data connectivity through the network connectivity subsystem 250 of the portable terminal 100. This additional data connectivity enables access to the secure storage subsystem 190. It should be noted that in view of the concept of the secure storage subsystem 190 provisions have to be taken which meet the security requirements thereof. The following description illustrates the concept of the present invention.

In general, the basic concept of the present invention enables application service providers and/or network operators to exercise control over the secure storage subsystem 190 and in particular over the secure storage controller 191, the contents stored in the secure storage memory 192, the application related security policies, and/or the application related code sections including program code and/or user interface definitions.

With reference to Fig. 4a, a block diagram is predicted, which schematically illustrates network entities which may be included in a system environment according to an embodiment of the present invention. In general, the control is exercised through the network 260 to which the terminal device 100 is connectable via the network connectivity subsystem 180. The network 260

5 may be a public land mobile network (PLMN), a cellular network including in particular any type of GSM network, any type of CDMA (Code Division Multiple Access) network such as a UMTS (Universal Mobile Telecommunications System) network or cdma2000 network, a wireless data network including in particular a WLAN (wireless local area network), a Wi-Fi network, a WiMAX network, a WPAN (Wireless Personal Area Network), a Bluetooth network or a UWB (Ultrawide Band) network, a wire-based network including in particular a LAN (Local Area Network), a PSTN (Public Switched Telephone Network), DSL (Digital Subscriber Line), the Internet and/or any combination thereof.

10 The exercise of control over the secure storage subsystem 190 as described above is naturally strictly limited due to security requirement issues. Consequently, only distinct trusted network entities which are in knowledge of highly sensitive information required for the exercise of control should be applicable in accordance with the concept of the present invention. Especially, the application service provider (ASP) may operate its own ASP center 310 connected to the  
15 network 260 to exercise control, the network operator may be capable by the means of a network operator control center 300 for exercising control and/or a designated secure storage management (SSM) center 320 operated by the application service provider (ASP) and/or the network operator may be provided to allow exercising control.

20 With reference to Fig. 4b, a block diagram is depicted, which schematically illustrates a system environment on the basis of a GSM Public Land Mobile Network (PLMN) environment according to a specific embodiment of the present invention. It should be noted that the present invention is not limit to any specific system implementation; in particular the present invention is not limited to that specific system environment illustrated in Fig. 4b. The system environment  
25 embodied in Fig. 4b is illustrated and described for the sake of completeness and illustration.

The GSM PLMN comprises typically a Radio Access Network (RAN) 470 comprising one or more Base Station Controller (BC) 410 each being connected to one or more Base Stations (BTS) 400, each in turn spanning a coverage area within which one or more terminal devices 100  
30 communicate with the respective Base Station (BTS) 400 through an air (radio frequency) interface. The Radio Access Network (RAN) is connected to the Core Network (CN) 460 comprising inter alia a Mobile Switching Center (MSC) 420 connected to the Mobile Switching Center (MSC) 420, a Gateway Mobile Switching Center (GMSC) 430 providing connectivity to further networks including especially PSTNs (Public Switched Telephone Networks), external  
35 PLMNs (Public Land Mobile Networks) and the Internet, as well as a Operation and Maintenance Center (OMC) 440 operable with Operation and Maintenance Subsystem (OMSS) functions. The Operation and Maintenance Center (OMC) 440 is conventionally connected to an

Equipment Identity Register (EIR) (not shown) and an Authentication Center (AUC) 450 supporting the Operation and Maintenance Subsystem (OMSS) operation.

5 According to the specific embodiment of Fig. 4b, the Secure Storage Maintenance (SSM) Center 320 arranged as a part of the Core Network (CN) 460 and connected to the Operation and Maintenance Center (OMC) 440. The Application Service Provider (ASP) Center 310 as well as the Network Operator Control Center 300 is connected via any network(s) to the Gateway MSC 430 of the Core Network 460. In a GPRS-enabled and/or EDGE-enabled GSM PLMN the Application Service Provider (ASP) Center 310 as well as the Network Operator Control Center 10 300 may be connected through a Gateway GPRS Support Node (GGSN) (not shown) and a Serving GPRS Support Node (SGSN) (not shown) to the Core Network (CN) 460. The Gateway GPRS Support Node (GGSN) (not shown) and the Serving GPRS Support Node (SGSN) enable for packetized data communication. It should be noted that arrangement of the Application Service Provider (ASP) Center 310, the Network Operator Control Center 300, and/or the Secure 15 Storage Maintenance (SSM) Center 320 is illustratively and the present invention is not limited thereto.

#### Verification Procedure

20 Reference should be given to Fig. 5a. Typically, the subscription of a terminal device 100 capable for network connectivity to any public and/or private network infrastructure requires registration and authentication of the terminal device 100 thereon such that the network operator is capable to control the access to its network, to charge for its network service, to allow network operation, network configuration, network performance management and security management. 25 The registration and authentication is typically operable with registration and authentication centers; e.g. in view of a GSM network the registration is operable with location registers (Home Location Register and/or Visitor Location Register), whereas the authentication is operable with the Authentication Center (AUC) 450 being part of the Operation and Maintenance Subsystem controlled through the Operation and Maintenance Center (OMC) 440.

30 The terminal device 100 authenticates towards the network at least each time the terminal device is subscribed thereto; i.e. each time the network connectivity subsystem 180 of the terminal device 100 is registered to the network such that data communication with the network is operable. The subscription is at least performed each time the network connectivity subsystem 35 180 and the terminal device 100 is put into operation, respectively.

Upon registration, an authentication entity such as the Authentication Center (AUC) 450 is accessed, which stores information about the subscriber identification and subscriber authentication as well as device registrations, sensible/personal data and (cipher) keys. The (cipher) keys enable performing subscriber authentication and authorization of services provided by the network. The authentication may be performed in at start-up of the network connectivity subsystem 250, at predefined points in time, and/or at any predefined (regular or irregular) intervals during (normal) operation of the network connectivity subsystem 250. The network connectivity subsystem 180 of the terminal device comprises a network authentication module, which interoperates with the authentication entity for authentication. For example, cellular terminal device comprise a SIM (Subscriber Identification Module) such as the SIM 185 of terminal device 100, which enables the authentication against authentication information stored at the Authentication Center (AUC) 450. The authentication may be based on a request-response challenge communication, which is performed to ensure that even in case an unauthorized party eavesdrop the communication exchanged secrets are not extractable from the eavesdropped communication.

Upon authentication, such as operation S200, which is illustratively shown in Fig. 5a, a check for one or more exceptions is operable, where the exceptions are provided by the application service provider (ASP), preferably through the Application Service Provider (ASP) Center 310. The Secure Storage Maintenance (SSM) Center 320 is informed by the Application Service Provider (ASP) Center 310 about the one or more exceptions. During authentication the authentication entity, e.g. the Authentication Center (AUC) 450, informs the Secure Storage Maintenance (SSM) Center 320, which may comprise a fraud management function, about the authentication operation including especially an indication about a successful authentication. Upon indication of the authentication entity the Secure Storage Maintenance (SSM) Center 320 checks whether one or more exceptions concerning the secure storage subsystem 190 of the terminal device 100 are present. In case such an exception is identified by the Secure Storage Maintenance (SSM) Center 320 to be processed, the Secure Storage Maintenance (SSM) Center 320 is operable to initiate communication with the secure storage subsystem 190 of the terminal device 100. The communication between the Secure Storage Maintenance (SSM) Center 320 and the secure storage subsystem 190 is operable through the network connectivity subsystem 250 and the interconnectivity component 205. Such communication may comprise a request-response communication including one or several requests directed to the secure storage subsystem 190 and the secure storage controller 191 thereof as well as one or several responses from the secure storage subsystem 190 and the secure storage controller 191 thereof back to the Secure Storage Maintenance (SSM) Center 320.

For instance, an exception may be defined in consequence of a call by the user to the application service provider (ASP) requiring the close of the application (cancelling of the application service provided by the ASP, e.g. in case of loss of the terminal device 100 or in response to expiration), an initialization of the application and/or upload/modification of data stored by the secure storage subsystem 190. Moreover an exception may be defined on initiative of the application service provider (ASP), e.g. to enable automatic notification of recharging, (temporarily) blocking of the use of an application service due to user account balance, and the like.

10 With reference to operation S210, one or more messages are transmitted by the network to the network connectivity subsystem 250 of the terminal device 100; the messages preferably originate from the Secure Storage Maintenance (SSM) Center 320. The messages are supplied to the interconnectivity component 205, which detects that the messages are intended to terminate at the secure storage subsystem 190 and the secure storage controller 191 thereof. Upon  
15 detection, the messages are supplied by the interconnectivity component 205 to the secure storage controller 191, which is instructed by one or more commands included in the messages to perform commanded operations; e.g. disabling/blocking an application service enabled by the secure storage subsystem 190, initializing an application service enabled by the secure storage subsystem 190, removing/deleting/modifying data stored in the secure storage memory 192 and  
20 the like. The secure storage controller 191 may transmit back one or more responses which may include reception acknowledgement and/or command result information. In particular, the information about command result may comprise information about the success of commands performed and/or data obtained in reaction to performing commands.

25 Preferably, the messages transmitted through the network and terminating at the secure storage subsystem 190 are cryptographically secured to ensure inter alia privacy, integrity, and/or authenticity. Correspondingly, the messages may be ciphered and are provided with a digital signature and/or a certificate. The ciphering ensures privacy, whereas the digital signature enables for integrity, and/or authenticity verification. The cryptographic protection of the  
30 messages is preferably based on a public key ciphering infrastructure as known in the art.

The deciphering mechanisms implementing deciphering of the ciphered messages and/or verification of digital signatures and/or certificates may be implemented in the interconnectivity component 205 or the secure storage controller 191. Cryptographic keys, signatures, and/or  
35 certificates may be provided by the secure storage controller 191 and may be stored in the secure storage memory 192.



The check whether one or more exceptions are present on network side may be set in accordance with the requirements of the application service provider and/or the network operator. The exception check may be performed inter alia at least at the point of time of initial authentication of the network connectivity subsystem 250 (at start-up), at any predefined points in time, and/or  
5 at any (regular or irregular) intervals during operation.

Furthermore, the application service provider (ASP) may require that one or more regular acknowledgements are sent to the secure storage subsystem 190 in order to assure that the secure storage subsystem 190 can not be used in local communication too long in the power off-mode.  
10 Such an acknowledgement check could be based on a request-response communication initiated by the Secure Storage Maintenance (SSM) Center 320 such as operation S220 of Fig. 5a and/or the acknowledgement check could be based on a request-response communication initiated by the secure storage subsystem 190 such as operation S240 of Fig. 5a.

15 The acknowledgement check may be operated inter alia at any predefined points in time, and/or at any (regular or irregular) intervals during operation. Moreover, the acknowledgement check may be operated inter alia in response to a predefined number of operations of the secure storage subsystem 190 through the local RF connectivity subsystem 193, a predefined number of transactions performed by the secure storage subsystem 190, transaction limits defined for  
20 transactions performed by the secure storage subsystem 190, and the like.

In case such an acknowledgement check fails, which may include that the acknowledgement is not available at one of the aforementioned check requirements or the acknowledgement itself indicates failure, the secure storage subsystem 190 or an application service operable with the  
25 secure storage subsystem 190 may be (temporarily and/or permanently) blocked or disabled. A blocked or disabled secure storage subsystem 190 or an application service operable with the secure storage subsystem 190 may be re-enabled in reaction to a successful acknowledgement check or the re-enablement may require a specific message to be received through the network  
30 260.

#### Disabling Procedure

In general, the basic concept of the present invention allows application service provider and/or network operator to exercise control over the secure storage subsystem 190. In particular, the  
35 control over the secure storage subsystem 190 includes disabling of the secure storage subsystem 190. For instance in view of a transaction service issuer (such as a credit card issuer, a payment card issuer, etc.) the possibility of disabling (payment) transaction services operable with the

secure storage subsystem 190 is a critical issue. A disabling may be required in case a (contactless) smart card (forming the secure storage subsystem 190) or the terminal device 100 comprising the secure storage subsystem 190 reported lost or stolen. Further, a disabling may be required in case of some kind of indication relating to possible misuse of the secure storage subsystem 190. Typically, such disabling of the secure storage subsystem 190 may require re-configuration of the secure storage subsystem 190 that may require inputting rebooting type of information to the secure storage subsystem 190 that cannot be done without having access to highly sensitive information that is typically accessible only to application service providers.

5

10 As aforementioned, an application service provider (ASP) can define exception events at the Secure Storage Maintenance (SSM) Center 320. The Secure Storage Maintenance (SSM) Center 320 is a trustworthy network entity at which such highly sensitive information can be provided by the application service provider (ASP). In addition to the aforementioned check for exceptions at the Secure Storage Maintenance (SSM) Center 320, preferably at predefined points in time and/or intervals in time, the Secure Storage Maintenance (SSM) Center 320 may be configured to react promptly on important exception events such as requirements for disabling. Consequently, such an exception is to be processed promptly.

15

With reference to operation S100, the Secure Storage Maintenance (SSM) Center 320 generates a message in accordance with the exception event, herein for instance a message containing instructions to disable the secure storage subsystem 190 and an application service operable with the secure storage subsystem 190, respectively, and transmits the message to the secure storage subsystem 190 and the secure storage controller 191 thereof, respectively.

20

The disabling message may also instruct the terminal device 100, the communication controller 200 thereof, the secure storage subsystem 190, or the secure storage controller 191 thereof to reply to the message when the message is received. The response to the message may be transmitted back to the Secure Storage Maintenance (SSM) Center 320, which then may inform application service provider (ASP) by an acknowledgment message to the Application Service Provider (ASP) Center 310 or the network operator by an acknowledgment message to the Network Provider Control (ASP) Center 300. Alternatively, the response may be transmitted directly to the application service provider (ASP) or the network operator.

25

30

The messages transmitted from the Secure Storage Maintenance (SSM) Center 320 to the secure storage subsystem 190 through the network 260, the network connectivity subsystem 180 and the interconnectivity component 205 may be some sort of dedicated "smart" Short Messages or Multimedia Messages in accordance with the corresponding Short Message Service and

35

Multimedia Message Service supported by today's cellular network. Such "smart" messages should be understood to include an indication the message is directed to the secure storage subsystem 190 and the terminal device 100 and the interconnectivity component 205, upon receiving such a message, processes the message without displaying it to the user. In particular, "smart" messages may employ the SMS message Toolkit functionality provided by SIMs (Subscriber Identification Modules) operated in cellular terminal devices. In general, the SMS message Toolkit functionality enables a SIM such as the SIM 185 of the terminal device 100 to drive the terminal device 100, build up an interactive exchange between a network application and the terminal device 100 and access or control access to the network 260. The SIM has a proactive role in the terminal device 100 and is configured to initiate commands independently of the terminal device 100 and the network 260.

#### Reload & Update Procedures

It should be assumed that a user may, from time to time, switch the secure storage subsystem 190 between different terminal devices. The concept of the present invention enables a reloading of relevant application related code sections, i.e. program code and/or user interface definitions, which may be required in reaction to the exchange between different terminal devices having different processing capabilities and functionalities and underlying different constraints.

For instance, the network operator identifies a changed user identifier and terminal device identifier combination in consequence of the device exchange. Upon detection of the change of the identifier combination, a status message is generated by the Application Service Provider (ASP) Center 310 and the Secure Storage Maintenance (SSM) Center 320, respectively, which comprises inter alia desired configuration status information of the secure storage subsystem 190 and/or one or more application services operable with the secure storage subsystem 190. The status message is transmitted through the network 260 to the secure storage controller 191, which compares the desired configuration status information with current configuration status information obtained by the secure storage controller 191. The configuration status information comprises in particular status information about program code and/or user interface definitions required for operating application services by the means of the secure storage subsystem 190.

In case the secure storage controller 191 identifies differences between the current configuration status and the desired configuration status, a request message is generated by the secure storage controller 191 and transmitted via the network 260 to the originator of the status message. The request message should be responded by a reload message, which may comprise data required to achieve the desired configuration status. In particular, the reload message may comprise

information enabling the secure storage controller 191 to download required data through the network 260. The download information may comprise a network address such as a URL (Uniform Resource Locator) or URI (Uniform Resource Indicator) and/or access information such as account identifier and/or account password.

5

It should be noted that the aforementioned process may be also initiated by the secure storage controller 191. Independently of the detection, the secure storage controller 191 may generate a message, which comprises a request for the desired configuration status information. The message is supplied to the interconnectivity component 205 for transmission over the network 10 260 to be sent to the Application Service Provider (ASP) Center 310 or to the Secure Storage Maintenance (SSM) Center 320. In reaction to this message, the addressee generates the requested desired configuration status information, which is transmitted back to the secure storage controller 191. Alternatively, the secure storage controller 191 may generate a network message, which comprises current configuration status information obtained by the secure 15 storage controller 191. The addressee, i.e. the Application Service Provider (ASP) Center 310 or to the Secure Storage Maintenance (SSM) Center 320, compares the received current configuration status information with desired configuration status information. On the basis of differences between the current configuration status and the desired configuration status, a reload message is generated by the addressee any transmitted to the secure storage controller 191.

20

The user of the terminal device 100 may have to confirm the initiation of a network data download.

In analogy to the aforementioned exchange procedure, a comparable procedure is operable when 25 new application related code sections have to be updated for instance due to new versions, new application services, and the like.

Upon initiation of the secure storage controller 191, the secure storage controller 191 may generate a message, which comprises a request for the desired configuration status information. 30 The message is supplied to the interconnectivity component 205 for transmission over the network 260 to be sent to the Application Service Provider (ASP) Center 310 or to the Secure Storage Maintenance (SSM) Center 320. In reaction to this message, the addressee generates the requested desired configuration status information, which is transmitted back to the secure storage controller 191. Alternatively, the secure storage controller 191 may generate a network 35 message, which comprises current configuration status information obtained by the secure storage controller 191. The addressee, i.e. the Application Service Provider (ASP) Center 310 or to the Secure Storage Maintenance (SSM) Center 320, compares the received current

configuration status information with desired configuration status information. On the basis of differences between the current configuration status and the desired configuration status, a reload message is generated by the addressee any transmitted to the secure storage controller 191.

5 Moreover, the Application Service Provider (ASP) Center 310 or to the Secure Storage Maintenance (SSM) Center 320 may generate a message comprising desired configuration status information at any one or more points in time or in regular or irregular intervals. On the basis of the received configuration status information the secure storage controller 191 checks the configuration status of the secure storage subsystem 190.

10

Similarly the reload message from the network 260 could indicate a desired configuration state in consequence to which a component comprising code sections is downloaded, which enable to remove application related code sections, i.e. program code and/or user interface definitions. The removal may be for instance instructed when the corresponding application has expired.

15 Likewise, application related code sections may be removed without requiring a component downloaded over the network.

Those skilled in the art will appreciate on the description above that the aforementioned procedures relating to updating and/or downloading are also applicable to update and/or  
20 download application related contents.

#### Removal Procedure

25 With reference to the verification and/or disabling procedures described above, the Application Service Provider (ASP) Center 310 or to the Secure Storage Maintenance (SSM) Center 320 may generate a request message directed to the secure storage controller 191, which instructs the secure storage controller 191 to remove application related contents from the secure storage memory 192 and imitate removing of application related code sections, i.e. program code and/or user interface definitions, which are associated with the application related contents to be  
30 removed.

Those skilled in the art will appreciate that the complete removal of data relating to an application service (where the data comprise application related contents and/or application related code sections) is especially applicable in conjunction with a disabling or blocking of the  
35 respective application service. In particular, the removal procedure will ensure that the application service cannot be re-activated against without approval of the application service

provider (ASP). In order to re-activate the application service, an update procedure may be operable, which requires the interaction of the application service provider (ASP).

#### Exchange Procedure

5

It should be assumed that a user may change the network authentication module and the secure storage subsystem 190 is fixedly associated with the network authentication module. For example, the user may change the SIM 185 of the terminal device 100 and the secure storage subsystem 190 is fixedly associated to a specific SIM 185 e.g. the former SIM. A methodology to associate the secure storage subsystem 190 to a specific SIM will be described below in detail. The fixed association guarantees that the secure storage subsystem 190 is only operable in case the respective SIM (to which the secure storage subsystem is associated) is present in the terminal device 100. In all other cases the secure storage subsystem 190 is not operable.

15

As aforementioned, the terminal device 100 and its network connectivity subsystem 250 authenticates against the authentication entity of the network by the means of the network authentication module. Upon authentication, the Secure Storage Maintenance (SSM) Center 320 may be informed about the authentication. The user can be identified by a subscriber identifier (ID) which is the same for the former and the new network authentication module.

20

The aforementioned reload procedure is applicable to reload the application related contents and application related code sections to a new secure storage subsystem which is associated to the new network authentication module. However, the application service provider (ASP) may be required to make provisions on the network side to enable the reload procedure upon detection of an exchange of the network authentication module. Moreover, the reload procedure may be alternatively initiated by the application service provider (ASP), e.g. through the Secure Storage Maintenance (SSM) Center 320 or the Application Service Provider (ASP) Center 310. The reload procedure may be enabled on information by the user or proactively by the application service provider (ASP).

25

#### Association Procedure

The operability of the secure storage subsystem 190 may be linked to the network authentication module to prevent usage of the secure storage subsystem 190 with any other network authentication module and to provide additional control by the cellular network operator over the operability of the secure storage subsystem 190.

30

The first case relates to a situation where an unauthorized (hostile) party might try to operate the terminal device 100 with the secure storage subsystem 190 by including a new network authentication module into the terminal device 100. For example, an unauthorized (hostile) party (such as a thief) might try to operate the terminal device 100 with the secure storage subsystem 190 by including a new SIM into the terminal device 100. Due to the fact that during authentication of the terminal device against the authentication entity of the network 260 the addressability of the terminal device 100 through the network 260 is defined, the terminal device 100 having a new network address can not receive messages from the Secure Storage Maintenance (SSM) Center 320 as well as the Application Service Provider (ASP) Center 310 because these messages are still addressed in accordance with the former network authentication module. Typically, the network authentication module comprises a subscriber identifier on the basis of which the network address information such as a telephone number, an IP address and the like, is obtained. With reference to cellular networks, the telephone numbers are retrieved from the Home Location Register, which stores telephone numbers in association with subscriber identifiers. The misuse of the secure storage subsystem 190 with a replacement network authentication module is not possible due to the association of the secure storage subsystem 190 and the network authentication module

The latter case relates to the desire of a network operator to control their customers, because the network operator may bind the usage of the secure storage subsystem 190 to the network authentication module so that if a user wants to change the network operator or give the secure storage subsystem 190 (in case the subsystem is detachable) to a friend or like, the operation of the is secure storage subsystem 190 prevented due to the association of the secure storage subsystem 190 and the network authentication module.

However, in cases where the user wants to place the detachable secure storage subsystem 190 to another terminal device that is owned by the same user (same or different network authentication module, but links to same user account), the authentication may be performed successfully as there is no contradictions between the user account and the secure storage subsystem 190.

In general, the secure storage controller 191 of the secure storage subsystem 190 can request an authentication of the network authentication module (e.g. the SIM 185) of the network connectivity subsystem 180 of the terminal device 100. The request for authentication is preferably preformed prior to any operation of the secure storage subsystem 190. In that way, the network identification module (e.g. SIM 185) and the secure storage subsystem 190 cannot be separated.

With reference to Fig. 5c, the secure storage controller 191 operating a management application may have two operational states:

5 The first operational state (State 1) is active when the secure storage subsystem 190 is not (yet) mutually authenticated with the network authentication module. The operation of the secure storage subsystem 190 is disabled; in particular any operation of the secure storage subsystem 190 through the local RF connectivity subsystem 193 is disabled. In this operational state the secure storage subsystem 190 may perform in accordance with a defined algorithm, e.g., with fixed intervals, on power-on, and/or any other triggers, requesting authentication from the  
10 network authentication module (SIM 185). This mutual authentication may be based on a public key infrastructure or a challenge-response algorithm. Once the mutual authentication (operation S300) has been confirmed the secure storage subsystem 190 and the secure storage controller 191 switches to the second operation state (State 2), respectively.

15 During second operation state (State 2), the secure storage subsystem 190 as well as the secure storage controller 191 is mutually authenticated with the network authentication module and local RF connectivity is operable with the secure storage subsystem 190 through the local RF connectivity subsystem 193. This second operational state (State 2) may require repetitive mutual authentication procedures (operations S310 and 320), i.e. in any (regular or irregular) intervals of  
20 time. This means that after passing of predefined time-out periods the secure storage subsystem 190 and the secure storage controller 191 switches automatically to the first operation state (State 1), respectively. Moreover, the repetitive mutual authentication procedures may be required after each local RF communication of the secure storage subsystem 190 through the local RF connectivity subsystem 193. This means, the secure storage subsystem 190 and the secure storage  
25 controller 191 switches automatically (operation S430) to the first operation state (State 1), respectively, after a local RF communication of the secure storage subsystem 190.

The authentication keys and/or authentication algorithms are preferably loaded into the secure storage controller 191 and the network authentication module (SIM 185) at the time of set-up.

30

The information exchange required during a mutual authentication procedure can be performed through a direct connection of the secure storage controller 191 and the network authentication module (SIM 185) or through the baseband of the network connectivity subsystem 180 via the communication controller 200.

35



In case of direct connection the secure storage controller 191 may exchange information directly with the network authentication module (SIM 185). An authentication software and/or hardware protocol implemented enables the mutual authentication procedure.

5 In the latter case, the secure storage subsystem 190 should be able to initiate an interrupt to the communication controller 200 or the communication controller 200 may poll the secure storage subsystem 190 on regular intervals. Once the communication controller 200 has the information that a network identification module (SIM 185) is to be authenticated a specific application on the network identification module (SIM 185) may be requested to respond to this authentication  
10 request. The communication controller 200 supplies the response to the authentication request to the secure storage controller 191 as a response to its query. If the response is satisfactory the secure storage controller switches to the second operational state where local RF communication is enabled.

15 Those skilled in the art will appreciate from the description above being based on different embodiments that operational state of the secure storage subsystem 190 can be controlled through the network by authorized network entities without any need for the user to take action. The concept of the present invention also enables the authorized network entities to define a solution, which allows controlling distribution of messages to the terminal devices. In this way  
20 the authorized network entities can ensure complete control of the application operable with the secure storage subsystem 190. This means in particular that the network operator enabling secure storage maintenance by the means of a Secure Storage Maintenance (SSM) Center can define the messages, e.g., SIM toolkit messages, as well as the frequency of exception control, in order to optimize network usage and load.

25

It will be obvious for those skilled in the art that as the technology advances, the inventive concept can be implemented in a broad number of ways. The invention and its embodiments are thus not limited to the examples described above but may vary within the scope of the claims.

## Claims

1. Terminal device, comprising  
5 a network connectivity subsystem (250) enabled for data connectivity with a wireless communications network (260);  
a secure storage subsystem (190) having a secure storage memory (192) for securely storing contents and enabled for local RF connectivity through a local RF communication subsystem (193), wherein said secure storage subsystem (190) operates as a contactless smartcard;  
10 an interconnectivity component (205) which is adapted to enable communication of said secure storage subsystem (190) through said network connectivity subsystem (250) with said network (260);  
wherein said interconnectivity component (205) is configured to detect that messages received from said network (260) are destined for said secure storage subsystem (190) and  
15 said interconnectivity component (205) is configured to supply said messages to said secure storage subsystem (190), wherein said messages enable exercising control over said secure storage subsystem (190) in that said messages comprise one or more instructions to be processed by a secure memory controller (191) of said secure storage subsystem (190).
- 20 2. Terminal device according to claim 1, wherein said interconnectivity component (205) is also configured to receive messages generated by said secure memory controller (191) and to supply said received messages to said network connectivity subsystem (250) for transmission to said network (260).
- 25 3. Terminal device according to claim 1 or claim 2, wherein said messages received from said network (260) originate from a secure storage maintenance center (320) arranged in said network (260) and/or said messages generated by said secure memory controller (191) are destined for said secure storage maintenance center (320).
- 30 4. Terminal device according to anyone of the preceding claims, wherein said messages received from said network (260) comprises commands relating to the operability of the secure storage subsystem (190) and/or commands relating to modifications on contents stored in a secure storage memory (192) of said secure storage subsystem (190).
- 35 5. Terminal device according to claim 4, wherein said commands relating to modifications on said stored contents comprises commands relating to modifications on application related

contents and/or commands relating to modifications on application related code sections including program code and/or user interface definitions.

- 5 6. Terminal device according to anyone of the preceding claims, wherein a disablement message from said network (260) is received in response to an exception event requiring disabling of as least one local application service operable with said secure storage subsystem (190), wherein upon reception of said disablement message, said secure memory controller (191) is configured to at least temporarily disable said local application service.
- 10 7. Terminal device according to anyone of the preceding claims, comprising:  
a network authentication module (185) operable to authenticate said network connectivity subsystem (250) at said network (260), wherein said network connectivity subsystem (250) is allowed for data connectivity with a network (260) after authentication at said network (260);  
15 wherein said secure storage subsystem (190) is configured to mutually authenticate with said network authentication module (185), wherein a local radio frequency communication operation of said secure storage subsystem (190) is disabled prior to mutual authentication and is enabled after mutual authentication.
- 20 8. Terminal device according to claim 7, wherein said mutual authentication is required at one or more predefined points in time and/or within predefined intervals to maintain an enabled local radio frequency communication operation, or wherein said mutual authentication is required after a local radio frequency communication operation to maintain said enabled local radio frequency communication operation.
- 25 9. Terminal device according to anyone of the preceding claims, wherein said network connectivity subsystem (250) is a wireless network connectivity subsystem (160) or a cellular network connectivity subsystem (180).
- 30 10. Terminal device according to anyone of the preceding claims, wherein said secure storage subsystem (190) is a contactless smartcard module or said secure storage subsystem (190) comprises a secure memory connected to a local radio frequency connectivity subsystem (193) adapted for radio frequency communication in accordance with any contactless technology.
- 35 11. Secure storage subsystem, comprising  
a secure storage controller (191) adapted to operate said secure storage subsystem (190);

- a secure storage memory (192) provided for secure storing of contents;  
a local radio frequency connectivity subsystem (193) arranged for local RF connectivity;  
wherein said secure storage subsystem (190) operates as a contactless smartcard;  
wherein said secure storage controller (191) is enabled for data communication with a  
5 wireless communications network (260) through an interconnectivity component (205)  
coupling said secure storage subsystem (190) to a network connectivity subsystem (250)  
enabled for data connectivity with said network (260);  
wherein said secure storage subsystem (190) receives messages from said network (260)  
10 destined for said secure storage subsystem (190) through said interconnectivity component  
(205), wherein said messages enable exercising control over said secure storage subsystem  
(190) in that said messages comprise one or more instructions to be processed by a secure  
memory controller (191) of said secure storage subsystem (190).
12. Secure storage subsystem according to claim 11, wherein said secure memory controller is  
15 configured to generate messages to be supplied to said interconnectivity component (205)  
to be supplied to said network connectivity subsystem (250) for transmission to said  
network.
13. Secure storage subsystem according to claim 11 or claim 12, wherein said messages  
20 received from said network (260) originate from a secure storage maintenance center (320)  
arranged in said network (260) and/or said messages generated by said secure memory  
controller (191) are destined for said secure storage maintenance center (320).
14. Secure storage subsystem according to of the claims 11 to 13, wherein said messages  
25 received from said network (260) comprises commands relating to the operability of the  
secure storage subsystem (190) and/or commands relating to modifications on contents  
stored in said secure storage memory (192) of said secure storage subsystem (190).
15. Secure storage subsystem according to claim 14, wherein said commands relating to  
30 modifications on said stored contents comprises commands relating to modifications on  
application related contents and/or commands relating to modifications on application  
related code sections including program code and/or user interface definitions.
16. Secure storage subsystem according to the claims 11 to 15, wherein a disablement message  
35 from said network (260) is received in response to an exception event requiring disabling  
of at least one local application service operable with said secure storage subsystem (190),

wherein upon reception of said disablement message, said secure memory controller (191) is configured to at least temporarily disable said local application service.

17. Secure storage subsystem according to the claims 11 to 16,  
5 wherein said secure memory subsystem (190) is configured to mutually authenticate with a network authentication module (185), wherein a local radio frequency communication operation of said secure storage subsystem (190) is disabled prior to mutual authentication and is enabled after mutual authentication;  
wherein said network authentication module (185) is arranged to authenticate said network  
10 connectivity subsystem (250) at said network (260), wherein said network connectivity subsystem (250) is allowed for data connectivity with a network (260) after authentication at said network (260).
18. Secure storage subsystem according to claim 17, wherein said mutual authentication is  
15 required at one or more predefined points in time and/or within predefined intervals to maintain an enabled local radio frequency communication operation, or wherein said mutual authentication is required after a local radio frequency communication operation to maintain said enabled local radio frequency communication operation.
- 20 19. Secure storage subsystem according to the claims 11 to 18, wherein said network connectivity subsystem (250) is a wireless network connectivity subsystem (160) or a cellular network connectivity subsystem (180).
- 25 20. Secure storage subsystem according to the claims 11 to 19, wherein said secure storage subsystem (190) is a contactless smartcard module or said secure storage subsystem (190) comprises a secure memory connected to a local radio frequency connectivity subsystem (193) adapted for radio frequency communication in accordance with any contactless technology.
- 30 21. System, comprising  
a terminal device (100) having a network connectivity subsystem (250) enabled for data  
connectivity with a wireless communications network (260);  
a secure storage subsystem (190) having a secure storage memory (192) for securely  
storing contents and enabled for local RF connectivity through a local RF communication  
35 subsystem (193), wherein said secure storage subsystem (190) operates as a contactless module;

an interconnectivity component (205) which is adapted to enable communication of said secure storage subsystem (190) through said network connectivity subsystem (250) with said network (260);

wherein said interconnectivity component (205) is configured to detect that messages received from said network (260) are destined for said secure storage subsystem (190) and said interconnectivity component (205) is configured to supply said messages to said secure storage subsystem (190), wherein said messages enable exercising control over said secure storage subsystem (190) in that said messages comprise one or more instructions to be processed by a secure memory controller (191) of said secure storage subsystem (190).

10

22. System according to claim 21, wherein said terminal device (100) is a terminal device according to anyone of the claims 1 to 10.

15

23. System according to claim 21 or 22, wherein said secure storage subsystem (190) is a secure storage subsystem according to anyone of the claims 11 to 20.

20

24. System according to anyone of the claims 21 to 23, wherein said interconnectivity component (205) is connected to network connectivity subsystem (250) of said terminal device (100) and provides an interface for coupling to said secure storage subsystem (190).

25

25. Method of network-based remote control over a secure storage subsystem (190) comprising a secure storage memory (192) for securely storing contents and enabled for local RF connectivity through a local RF communication subsystem (193), wherein said secure storage subsystem (190) operates as a contactless smartcard  
said method comprising:

at a network connectivity subsystem (250) receiving messages from a wireless communications network (260), wherein said network connectivity subsystem (250) is enabled for data connectivity with said network (260);

30

at an interconnectivity component (205), receiving messages from a network (260) from said network connectivity subsystem and identifying messages destined for said secure storage subsystem (190) and supplying said identified messages to said secure storage subsystem (190);

35

at a secure memory controller (191) of said secure storage subsystem (190), processing said messages comprising one or more instructions enabling exercising control over said secure storage subsystem (190).

26. Method according to claim 25, comprising:

- at said secure memory controller (191), generating messages destined for transmission to said network;
- at said interconnectivity component (205), receiving said generated messages and supplying said generated messages to said network connectivity subsystem (250); and
- 5 at said network connectivity subsystem (250), transmitting said generated messages.
27. Method according to claim 25 or claim 26, wherein said messages received from said network (260) originate from a secure storage maintenance center (320) arranged in said network (260) and/or said messages generated by said secure memory controller (191) are
- 10 destined for said secure storage maintenance center (320).
28. Method according to the claims 25 to 27, wherein said messages received from said network (260) comprises commands relating to the operability of the secure storage subsystem (190) and/or commands relating to modifications on contents stored in said
- 15 secure storage memory (192) of said secure storage subsystem (190).
29. Method according to claim 28, wherein said commands relating to modifications on said stored contents comprises commands relating to modifications on application related contents and/or commands relating to modifications on application related code sections
- 20 including program code and/or user interface definitions.
30. Method according to the claims 25 to 29, wherein a disablement message from said network (260) is received in response to an exception event requiring disabling of at least one local application service operable with said secure storage subsystem (190), wherein
- 25 upon reception of said disablement message, said secure memory controller (191) disables at least temporarily said local application service.
31. Method according to anyone of the claims 25 to 30, comprising:
- 30 mutually authenticating said secure memory subsystem (190) with a network authentication module (185), wherein a local radio frequency communication operation of said secure storage subsystem (190) is disabled prior to mutual authentication and is enabled after mutual authentication;
- 35 wherein said network authentication module (185) is provided to authenticate said network connectivity subsystem (250) at said network (260), wherein said network connectivity subsystem (250) is allowed for data connectivity with a network (260) after authentication at said network (260)

32. Method device according to claim 31, comprising:  
performing said mutual authentication at one or more predefined points in time and/or  
within predefined intervals to maintain an enabled local radio frequency communication  
operation; or  
5 performing said mutual authentication after a local radio frequency communication  
operation to maintain said enabled local radio frequency communication operation.
33. Method device according to the claims 25 to 32, wherein said network connectivity  
subsystem (250) is a wireless network connectivity subsystem (160) or a cellular network  
10 connectivity subsystem (180).
34. Method according to the claims 25 to 33, wherein said secure storage subsystem (190) is a  
contactless smartcard module or said secure storage subsystem (190) comprises a secure  
memory connected to a local radio frequency connectivity subsystem (193) adapted for  
15 radio frequency communication in accordance with any contactless technology.
35. Computer program product comprising program code sections stored on a machine-  
readable medium for carrying out the operations of anyone of the claims 25 to 34, when  
said program product is run on a processor-based device, a terminal device, a network  
20 device, a portable terminal, a consumer electronic device, or a wireless communication  
enabled terminal.



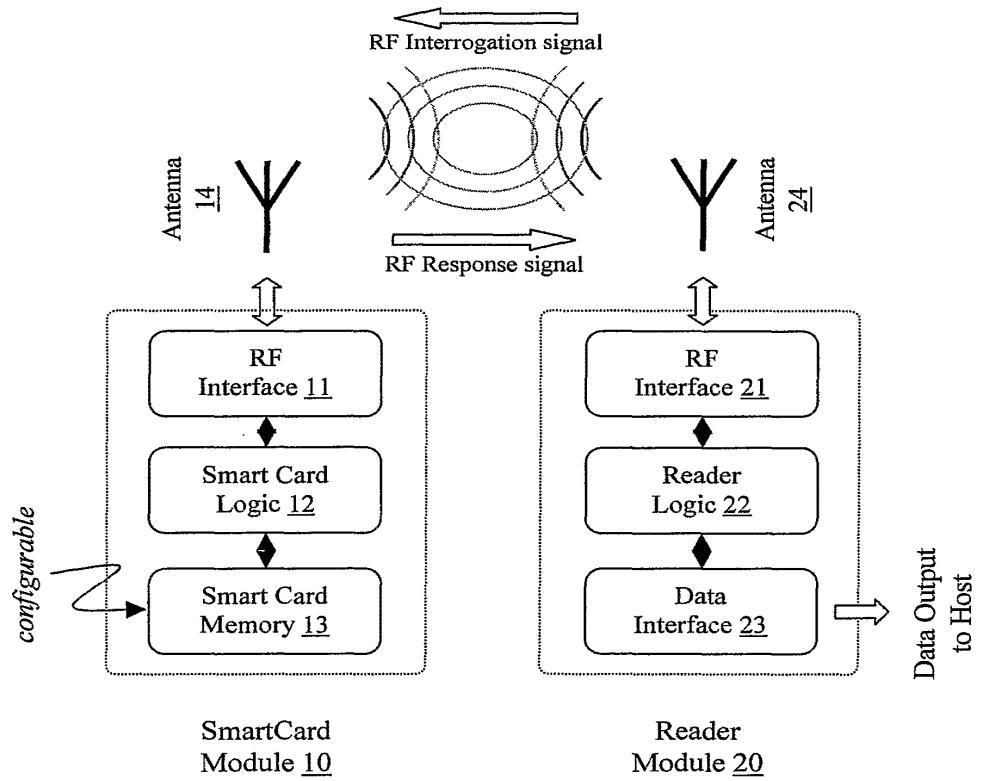
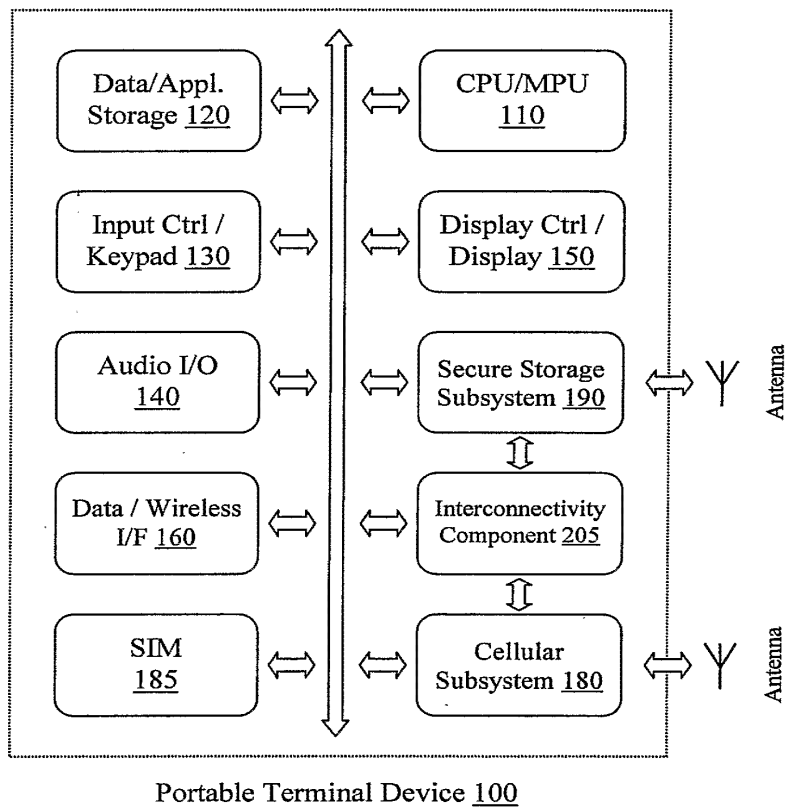


Fig. 1

Fig. 2



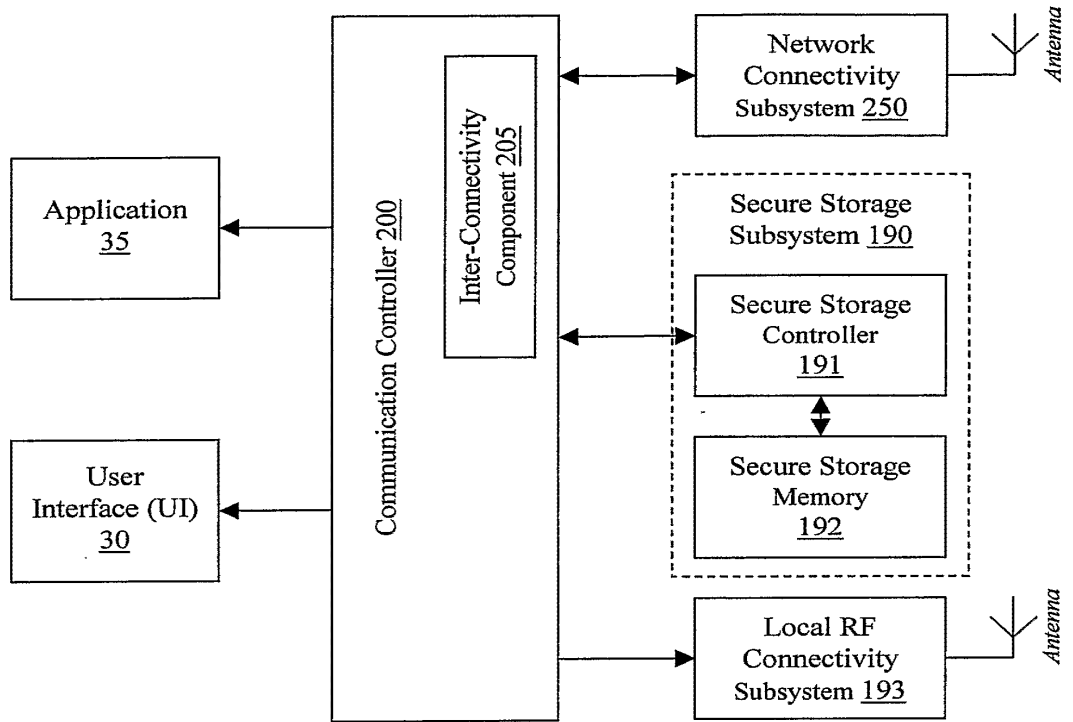


Fig. 3a

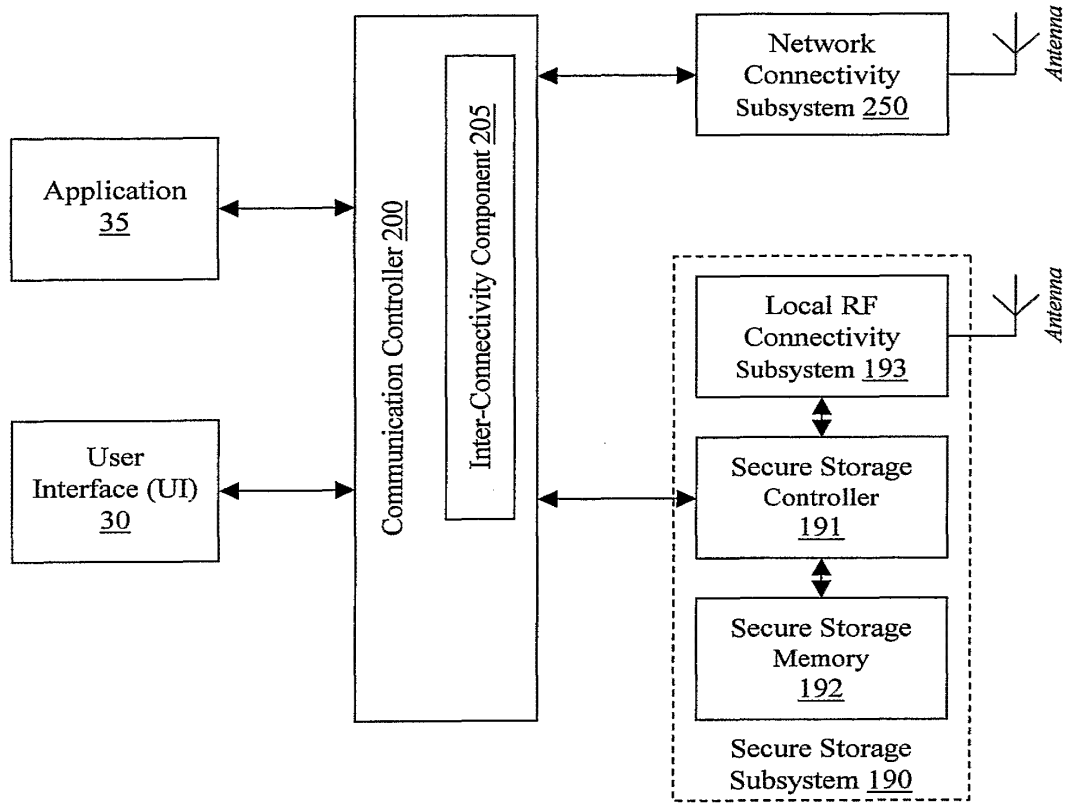


Fig. 3b

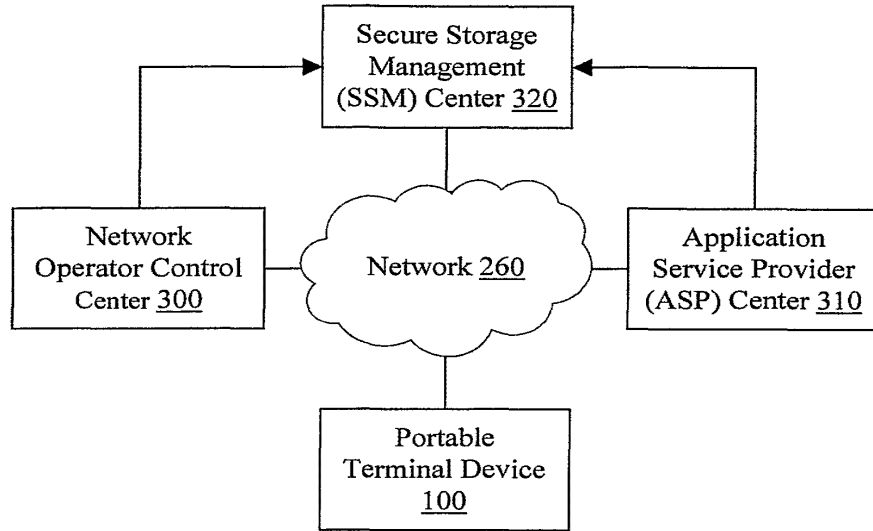


Fig. 4a

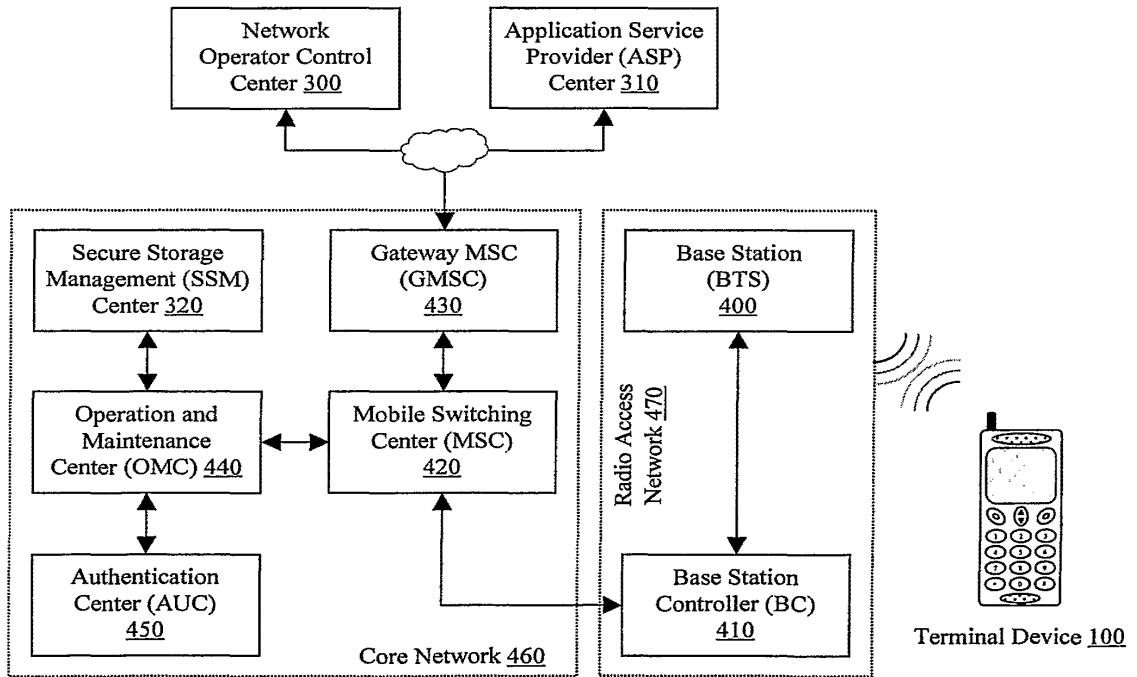


Fig. 4b

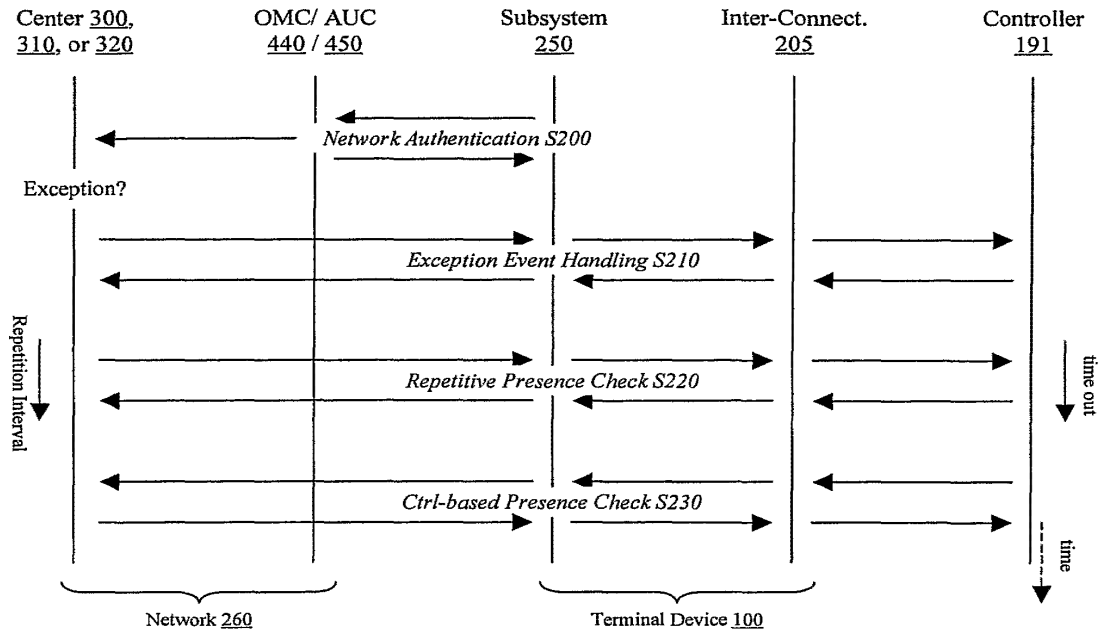


Fig. 5a

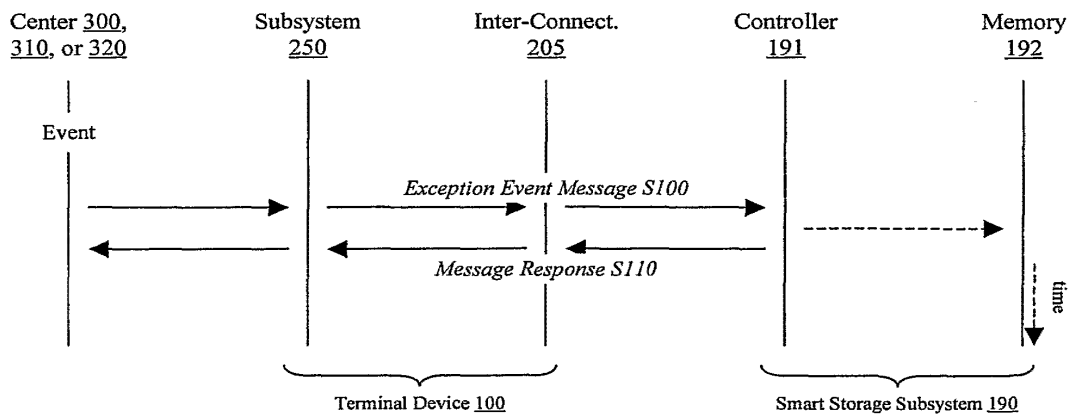


Fig. 5b

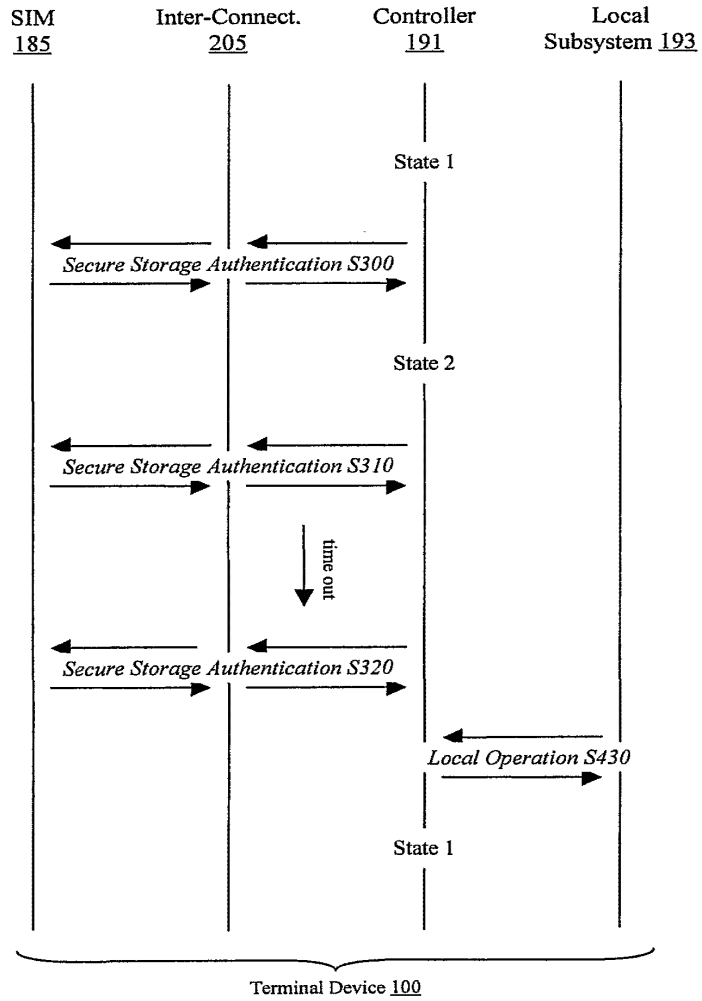


Fig. 5c

**INTERNATIONAL SEARCH REPORT**

International application No.  
**PCT/IB2005/003792**

<b>A. CLASSIFICATION OF SUBJECT MATTER</b>				
<p><b>IPC: see extra sheet</b> According to International Patent Classification (IPC) or to both national classification and IPC</p>				
<b>B. FIELDS SEARCHED</b>				
Minimum documentation searched (classification system followed by classification symbols)				
<b>IPC: H04L, G06F</b>				
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched				
<b>SE,DK,FI,NO classes as above</b>				
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)				
<b>EPO-INTERNAL, WPI DATA, PAJ</b>				
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>				
<b>Category*</b>	<b>Citation of document, with indication, where appropriate, of the relevant passages</b>	<b>Relevant to claim No.</b>		
<b>X</b>	<b>US 6934855 B1 (KIPNIS, S ET AL), 23 August 2005 (23.08.2005), column 8, line 22 - line 25; column 9, line 49 - line 66; column 10, line 1 - line 22, figure 1, abstract</b>	<b>1-35</b>		
--	--	--		
<b>X</b>	<b>ETSI TS 102 412 V7.1.0, (2005-11) Smart cards; Smart Card Platform Requirements Stage 1 (Release 7). See section 4.5.2.2 and figure 3</b>	<b>1-35</b>		
--	--	--		
<b>X</b>	<b>Open Mobile Alliance; DM Smart Card Requirements, Draft Version 1.0, 1 December 2005. See section 5.1</b>	<b>1-35</b>		
--	--	--		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.				
<p>* Special categories of cited documents:</p> <table style="width:100%; border:none;"> <tr> <td style="width:50%; border:none;"> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> </td> <td style="width:50%; border:none;"> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p> </td> </tr> </table>			<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>
<p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&amp;" document member of the same patent family</p>			
Date of the actual completion of the international search		Date of mailing of the international search report		
<b>28 Sept 2006</b>		<b>04 -10- 2006</b>		
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86		Authorized officer  <b>Stefan Dufva /LR</b> Telephone No. + 46 8 782 25 00		



INTERNATIONAL SEARCH REPORT

International application No.  
PCT/IB2005/003792

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>US 5774546 A (HANDELMAN, D ET AL), 30 June 1998 (30.06.1998), column 2, line 6 - line 20; column 3, line 40 - line 48, abstract</p> <p style="text-align: center;">-- -----</p>	1-35

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No.  
PCT/IB2005/003792

**International patent classification (IPC)**

**H04L 12/12** (2006.01)

**H04L 12/24** (2006.01)

**H04L 9/32** (2006.01)

**Download your patent documents at [www.prv.se](http://www.prv.se)**

The cited patent documents can be downloaded at [www.prv.se](http://www.prv.se) by following the links:

- In English/Searches and advisory services/Cited documents (service in English) or
- e-tjänster/anförda dokument (service in Swedish).

Use the application number as username.

The password is **XQRCVKWDKV**

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).


Cited literature, if any, will be enclosed in paper form.

INTERNATIONAL SEARCH REPORT  
Information on patent family members

International application No.  
PCT/IB2005/003792

US	6934855	B1	23/08/2005	GB	0325826	D	00/00/0000
				GB	2345232	A,B	28/06/2000
				GB	2392357	A,B	25/02/2004
				GB	9909359	D	00/00/0000
				IL	126552	D	00/00/0000
				US	20050216732	A	29/09/2005
				US	20060107038	A	18/05/2006
-----							
US	5774546	A	30/06/1998	AT	198523	T	15/01/2001
				AU	696725	B	17/09/1998
				AU	3303695	A	18/04/1996
				CA	2159779	A,C	04/04/1996
				DE	69519782	D,T	02/08/2001
				EP	0706291	A,B	10/04/1996
				ES	2153005	T	16/02/2001
				IL	111151	A	24/09/1998
				JP	3650448	B	18/05/2005
				JP	8214278	A	20/08/1996
				US	5666412	A	09/09/1997
				US	5878134	A	02/03/1999
				US	6298441	B	02/10/2001
				US	20010042049	A	15/11/2001
-----							

Form PCT/ISA/210 (patent family annex) (April 2005)

<b>Search Notes</b>  	<b>Application/Control No.</b>  11534653	<b>Applicant(s)/Patent Under Reexamination</b>  KOH ET AL.
	<b>Examiner</b>  CHRISTOPHER STANFORD	<b>Art Unit</b>  2887

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
235	379,380,492	1/22-25/10	CS

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>
Inventor, Assignee Search	1/22-25/10	CS
NPL Search	1/22-25/10	CS
Text Search (see search history report print out)	1/22-25/10	CS
Text Search (see search history report print out)	7/07/10-9/24/10	CS
Text Search (see search history report print out)	5/19/11	CS

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

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

## EAST Search History

## EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S19	3922	(electronic or e) (purse or wallet)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/07/07 09:47
S20	136146	(authentivat\$3 or certifiat\$3 or encrypt \$3 or cryptography or secur\$3) near2 (channel or connection)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/07/07 09:48
S21	666	S19 and S20	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/07/07 09:49
S22	36	S19 and (distinct or second or additional or separate or top) near2 S20	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/07/07 09:50
S23	50	(install\$3 or installation or load\$3) near3 S19 near3 (software or module or application or applet or midlet or program)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/07/07 10:55
S24	27	(install\$3 or installation or load\$3) near3 S19 near3 (software or module or application or applet or midlet or program) same (memory or card)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/07/07 10:55
S25	2	"6745944".pn.	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/07/07 10:57

S26	639	(phone or telephone or pda or personal digital assistant or blackberry or (portable or mobile) adj2 device) and (smart card or smartcard or rfid or (radio or rf or transponder or noncontact or non contact or contactless) adj2 (tag or card or transponder or id or identifier or identification) or felica) same emulat\$3	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:08
S27	116	"6442532" or "2009031689" or "20030163424"	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:10
S29	639	(phone or telephone or pda or personal digital assistant or blackberry or (portable or mobile) adj2 device) and (smart card or smartcard or rfid or (radio or rf or transponder or noncontact or non contact or contactless) adj2 (tag or card or transponder or id or identifier or identification) or felica) same emulat\$3	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:20
S30	150	S29 and (two or bi or dual or multi or multiple) near3 (secur \$3 or channel)	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:20
S31	24	S29 and (outside or external or internal) near3 (sam or secur\$3 near2 (application or module))	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:34

S32	3751	(phone or telephone or pda or personal digital assistant or blackberry or (portable or mobile) adj2 device) and (smart card or smartcard or rfid or (radio or rf or transponder or noncontact or non contact or contactless) adj2 (tag or card or transponder or id or identifier or identification) or felica) and emulat\$3	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:39
S33	616	(phone or telephone or pda or personal digital assistant or blackberry or (portable or mobile) adj2 device) and (smart card or smartcard or rfid or (radio or rf or transponder or noncontact or non contact or contactless) adj2 (tag or card or transponder or id or identifier or identification) or felica) and emulat\$3 with card	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:39
S34	24	S33 and (outside or external or internal) near3 (sam or secur\$3 adj2 (application or module))	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:39
S35	125	(phone or telephone or pda or personal digital assistant or blackberry or (portable or mobile) adj2 device) same (smart card or smartcard or rfid or (radio or rf or transponder or noncontact or non contact or contactless) adj2 (tag or card or transponder or id or identifier or identification) or felica) and (outside or	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:51

		external or internal or remote) near3 (sam or secur\$3 adj2 (application or module))				
S36	539	(phone or telephone or pda or personal digital assistant or blackberry or (portable or mobile) adj2 device) same (smart card or smartcard or rfid or (radio or rf or transponder or noncontact or non contact or contactless) adj2 (tag or card or transponder or id or identifier or identification) or felica) and (install\$3 or load \$3 or upload\$3 or download\$3 or transfer or transferr\$3 or transmit or transmitt \$3) near4 (epurse or e purse or wallet or ewallet or (payment or transaction or financial or banking) near2 (application or midlet or applet or weblet))	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:54
S37	5	S35 and S36	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:54
S38	319	(phone or telephone or pda or personal digital assistant or blackberry or (portable or mobile) adj2 device) same (smart card or smartcard or rfid or (radio or rf or transponder or noncontact or non contact or contactless) adj2 (tag or card or transponder or id or identifier or identification) or felica) and (install\$3 or load \$3 or upload\$3 or download\$3 or	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:56




		transfer or transferr\$3 or transmit or transmitt \$3) near4 (epurse or e purse or e wallet or ewallet or (payment or transaction or financial or banking) near2 (application or midlet or applet or weblet))				
S39	4	S35 and S38	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 11:56
S41	11	(epurse or e purse or e wallet or ewallet or vivowallet or vivo wallet) and (outside or external or internal or remote) near3 (sam or secur\$3 adj2 (application or module) or secur\$3 near3 (channel or connection))	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/24 12:04
S42	87	"6607136"	US-PGPUB; USPAT; USOCR; DERWENT	ADJ	ON	2010/09/27 12:18

**EAST Search History (Interference)**

< This search history is empty >

**9/ 27/ 2010 1:48:42 PM**

**C:\ Documents and Settings\ cstanford\ My Documents\ EAST\ Workspaces\ 11534653\_AOM2.  
wsp**

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 11534653	<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>

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

CLAIM		DATE							
Final	Original	01/25/2010	09/27/2010	05/19/2011					
	1	✓	✓	✓					
	2	✓	✓	✓					
	3	✓	✓	✓					
	4	✓	✓	✓					
	5	✓	✓	✓					
	6	✓	✓	✓					
	7	✓	✓	✓					
	8	✓	✓	✓					
	9	✓	✓	✓					
	10	✓	✓	✓					
	11	✓	✓	✓					
	12	✓	✓	✓					
	13	✓	✓	✓					
	14	✓	✓	✓					
	15	✓	✓	✓					
	16	✓	✓	✓					
	17	✓	✓	✓					
	18	✓	✓	✓					

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: 11/534,653**

Attorney Docket No: RFID-081

Customer Number: 26797

Date of Electronic Notification: 05/25/2011

This is a courtesy reminder that new correspondence is available for this application. 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

Please verify that these email addresses are correct.

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.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:** Method and apparatus for providing electronic purse  
**Serial No.:** 11/534,653  
**Confirmation No.:** 6327  
**Filing Date:** 09/24/2006  
**Examiner:** Chris Stanford  
**Group Art Unit:** 2887  
**Docket No:** RFID-081

---

September 7, 2011

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

**Response to 1st OA (RCE)**

In response to Office Action dated 05/25/2011, 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 11 as follows:

1. (*Currently amended*) A method for providing an e-purse, the method comprising:  
providing a portable device including or communicating with a smart card module pre-loaded with an emulator configured to execute a request from an e-purse applet and provide a response the e-purse applet is configured to expect, the portable device including a memory space loaded with a midlet that is configured to facilitate communication between ~~an~~ the e-purse applet and a payment server over a wireless network, wherein the e-purse applet is downloaded and installed in the smart card when the smart card is in communication with the payment server, the portable device further includes a contactless interface that facilitates communication between the e-purse applet ~~therein~~ in the smart card and the payment server over a wired network;  
personalizing the e-purse applet by reading off data from the smart card to generate in the smart card one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card, wherein said personalizing the e-purse applet comprises:
  - establishing an initial security channel between the smart card and the e-purse SAM to install and personalize the e-purse applet in the smart card,  
and
  - creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet.
2. (*Original*) The method as recited in claim 1, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.

3. *(Previously amended)* The method as recited in claim 2, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and the e-purse SAM originally used to issue the e-purse as well as between the emulator and the existing SAM.
4. *(Original)* The method as recited in claim 2, wherein said personalizing the e-purse applet is done over a wireless network or a wired network.
5. *(Original)* The method as recited in claim 4, wherein, when said personalizing the e-purse applet is done over a wireless network, the midlet in the portable device is configured to facilitate communications between the e-purse and the payment server.
6. *(Original)* The method as recited in claim 5, wherein both of the e-purse applet and the emulator are personalized as a result of said personalizing the e-purse applet.
7. *(Previously amended)* The method as recited in claim 1, further comprising:
  - initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;
  - sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;
  - transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and
  - sending a server response from the payment server to the midlet that is configured to process the server response before releasing the server response to the e-purse applet.

8. *(Original)* The method as recited in claim 7, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.
9. *(Original)* The method as recited in claim 8, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.
10. *(Original)* The method as recited in claim 1, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device, and the e-purse supports transactions in either e-commerce or m-commerce.
11. *(Currently amended)* A system for providing an e-purse, the system comprising:
  - a portable device including or communicating with a smart card pre-loaded with an emulator configured to execute a request from and provide a response an e-purse applet is configured to expect, the portable device including a memory space loaded with a midlet that is configured to facilitate wireless communication between ~~an~~ the e-purse applet in the smart card and a payment server over a wireless network, the portable device further including a contactless interface that facilitates communication between the e-purse applet in the smart card and the payment server over a wired network, wherein the e-purse applet is downloaded from the payment server when the smart card is in communication with the payment server, and said operations of personalizing the e-purse applet comprises:
    - establishing an initial security channel between the smart card and the e-purse security authentication module (SAM) to install and personalize the e-purse applet in the smart card, and
    - creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet;
  - the payment server associated with an issuer authorizing the e-purse applet; and

the e-purse SAM configured to enable the e-purse applet, wherein an SAM is behind the payment server and in communication with the e-purse applet when the e-purse applet is caused to communicate with the payment server via the midlet.

12. (*Original*) The system as recited in claim 11, wherein both of the e-purse applet and emulator are personalized by reading off data from the smart card, the data is then used to generate operation keys for the e-purse applet.

13. (*Original*) The system as recited in claim 12, wherein the operation keys include one or more of a load key and a purchase key, default personal identification numbers (PINs), administration keys, and passwords.

14. (*Previously amended*) The system as recited in claim 13, wherein at least some of the operation keys are used to establish a first secured channel so that various data is exchanged between the e-purse applet and the payment server, and at least another some of the operation keys are used to establish a second secured channel so that various data is exchanged between the e-purse applet and an existing security authentication module (SAM) originally used to issue the e-purse as well as between the emulator and the existing SAM.

15. (*Previously amended*) The system as recited in claim 11, wherein, when the portable device is used to have a transaction, there are operations of:

initiating a request from the e-purse after valid personal identification numbers are entered and accepted on the portable device;

sending a request by the midlet to the e-purse applet that is configured to compose a response to be sent to the midlet;

transporting the response to the payment server that is configured to verify that the response is from an authenticated e-purse, wherein the payment server further communicates with a financial institution to authorize a transaction therewith; and



sending a server response from the payment server to the midlet that is configured to process the server response before releasing the server response to the e-purse applet.

16. *(Original)* The system as recited in claim 15, wherein messages exchanged between the midlet and the payment server are in a type of commands encapsulated in network messages.

17. *(Original)* The system as recited in claim 16, wherein the commands are applicable for APDU which stands for Application Protocol Data Unit.

18. *(Original)* The system as recited in claim 11, wherein the e-purse is funded through a financial institution that maintains an account for a user being associated with the portable device.

## Remarks

Claims 1-18 were submitted for examination. In the Office Action dated 10/01/2010, Claims 1-18 are rejected under 35 USC 103(a) as being unpatentable over Shmueli et al (US Publication No.: 20020145632, hereinafter "Shmueli") in view of Nystrom (US 2009/0313689 A1; hereinafter Nystrom).

### Comments on Examiner's Response to Arguments

The Applicant respectfully disagrees with the comments made by the Examiner to the arguments presented in the previous Response dated 12/31/2010. On page 13, Examiner contends that there is a two-level security means of communication disclosed by Shmueli. The applicant wishes to point out that Shmueli teaches only the authentication of the key 10 to the host 12. As shown in FIG. 2A - FIG.2C of Shmueli, such a key is inserted to a host that runs a keylet to verify if the key is being used by an authorized user. As further described in paragraphs [0035]-[0039] of Shmueli, the authentication routine (using password) is the only step Shmueli needs before using the key. The Examiner evidently mistakes the steps 102-106 of FIG. 3 as a step before the authentication routine. The paragraph [0035] specifically states that "*the key 10 is identified (block 102) and the communication interface is configured to facilitate interaction (block 104)*". In contrast, Claim 1 of the instant application recites "establishing an initial security channel between the smart card and the e-purse SAM ..." and "creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM over the wired network". The applicant respectfully submits that it is a technical mistake to classify the identification of a key by a host as establishing an (initial) security channel. Further the communication between a key and a host is significantly and operationally different from operations of the smart card with the e-purse SAM over a wired network.

### Rejections of Claims 1-18 under 35 USC 103(a)

The Applicant respectfully disagrees with the Examiner as it is believed that the Examiner seemed to have been mistaken with the architecture aspects and security mechanism recited in Claim 1 and those of Shmueli.

As amended, Claim 1 explicitly recites:

providing a portable device including or communicating with a smart card pre-loaded with an emulator configured to execute a request from an e-purse applet and provide a response the e-purse applet is configured to expect, the portable device including a memory space loaded with a midlet that is configured to facilitate communication between the e-purse applet and a payment server over a wireless network, wherein the e-purse applet is downloaded and installed in the smart card when the smart card is in communication with the payment server, the portable device further includes a contactless interface that facilitates communication between the e-purse applet in the smart card and the payment server over a wired network;

personalizing the e-purse applet by reading off data from the smart card to generate in the smart card one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card, wherein said personalizing the e-purse applet comprises:

establishing an initial security channel between the smart card and the e-purse SAM to install and personalize the e-purse applet in the smart card,  
and  
creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet.

*(emphasis added)*

As described in paragraph [0029] and [0031], an emulator (e.g., Mifare emulator 208 in FIG. 2) is a hardware device or a program that pretends to be another particular device or program that other components expect to interact with. In the context of the instant invention, the emulator is able to execute a request from an e-purse applet and provide a response the e-purse applet is configured to expect. In other words, the smart card recited in Claim 1 that includes the emulator has the necessary computing power to execute commands with data. As further amended, the e-purse applet is personalized by reading off data from the smart card to generate in the smart card one or more operation keys for subsequent operations over a wired network, which again recites

clearly that the smart card is not just a memory card, the smart card is a computing device (i.e., an active device).

In contrast, Shmueli states explicitly in paragraph [0027] that the key 10 is a “passive” device, which means it has no computing power. As described in paragraph [0027], the key 10 is primarily includes memory 18 having software 20, where the software 20 is running on one of the hosts 12 with data 22. The memory 18 must be associated with a key interface 24 to facilitate communication with the hosts 12, where the memory 18 emulates a file system on a memory device accessible by the host 12. Evidently, anyone skilled in the art would understand the memory 18 is NOT an emulator *per se* in the industry. In fact, from a technical perspective, a file system in a storage device is merely to allow a host to locate a file stored in the storage device, it does not execute a request neither produce a response, despite the fact the key 10 can not computer by itself.

Accordingly, the Applicant respectfully submits that the Examiner interprets Shmueli beyond its original scope. Shmueli neither teaches nor suggests “*a smart card pre-loaded with an emulator execute a request from an e-purse applet and provide a response the e-purse applet is configured to expect*” and “*personalizing the e-purse applet by reading off data from the smart card to generate in the smart card one or more operation keys*” for the reasons stated above.

As supported in paragraph [0037], the e-purse applet is dynamically installed and personalized. In other words, the e-purse applet is NOT pre-installed. In contrast, the software 20 in the key 10 in Shmueli is pre-installed and must be uploaded to a host for execution, see paragraphs [0027] and [0028] of Shmueli. Thus, the Applicant submits Shmueli neither teaches nor suggests “*the e-purse applet is downloaded and installed in the smart card*” recited in Claim 1 as amended in the instant application.

Further as described in paragraphs [0007], [0024] – [0027], [0037] and shown in FIG. 1A and FIG. 3C, personalizing the e-purse applet requires a type of data communication with an e-purse SAM. The data communication includes installing and personalizing the e-purse applet in the smart card and creating security means to protect subsequent operations of the smart cards with the e-purse SAM over the wired network. To do so without a *prior* security channel, an initial security channel between

the smart card and the e-purse SAM module shall be established. For example, such an initial security channel is established by using a general security framework of a preloaded operating system in a smart card. Once an initial security channel is established, a (second) security channel on top of the initial security channel is established to protect subsequent operations of the smart card with the e-purse SAM. .

In contrast, Shmueli is silent about establishing a security channel on top of an initial security channel (e.g., an industrially recognized framework) to facilitate subsequent operations of the e-purse applet with the external e-purse SAM over a network. FIG. 1 of Shmueli shows that there are three entities, a key 10, a host 12 and a server 14. As pointed above, the key 10, which the Examiner has deemed as a “smart card”, is a passive device and has no computing power to establish a security channel with any other device. Accordingly, Shmueli does not teach nor suggests that the key 10 needs to be personalized using (two-level) security means. Further Shmueli is silent about having an emulator in the key 10 to conduct subsequent operations thereof over the security channel established by the e-purse applet to conduct either e-commerce or m-commerce.

On page 4 of the Office Action, the Examiner admits that Shmueli does not explicitly disclose establishing a security channel on top of an initial security channel to install the e-purse applet in the smart card, and then cites Nystrom to teach the same.

The Applicant respectfully contests the combination of Shmueli and Nystrom as it is believed that there is no motivation to combine these two references in the manner proposed by the Examiner. In order to establish a *prima facie* case of obviousness under 35 USC 103, *Graham v. John Deer Co. of Kansas City*, 383 US 1 (1966) requires determining, respectively, the scope and content of the prior art, the difference between the prior art and the claims at issue, and the level of ordinary skilled in the art. Rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning, to support the legal conclusion of obviousness. *KSR v. Teleflex*, No. 04-1350 (US Apr. 30, 2007) (citing *In re Kahn*, 441 F. 3d 977, 988 (Canada Fed. 2006)). The suggestion to make the claim combination must be found in the prior art, not in the Applicant’s disclosure. *In re Vaek*, 20 USPQ2d 1438 (Fed. Cir. 1991). Moreover, in

accordance with MPEP 2142.02, each prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention. *W.L. Gore & Associates Inc. v. Garlock, Inc.* 220 USPQ 303 (Fed. Cir. 1993). A third essential requirement for establishing a *prima facie* case, set forth in MPEP 2143.01, is that the proposed modification cannot render the prior art unsatisfactory for its intended purpose.

Nystrom teaches remote management of secure storages (e.g., smart cards) applicable with contactless technology applications. The Examiner states on page 5 of the Office Action that Nystrom discloses personalizing the e-purse applet (Reload & Update Procedures; para [0111-120]) by reading off data from the smart card to generate one or more operation keys ("a reloading of relevant application related code sections, i.e. program code and/or user interface definitions") in light of association procedures. However, a careful review of Nystrom, specifically these paragraphs para [0111-120]), indicates that Nystrom does not need to establish an initial security channel to install the e-purse applet or a software element in the smart card. In fact, Nystrom uses a SIM card 165 of FIG. 2 to authorize the smart card (including 190 of FIG. 3a) to communicate with a carrier's network. It is well known that SIM card, standing for subscriber identification module (SIM) card, is an authorized identifier to allow a device with a SIM to conduct permitted communication over a carrier's network (no need to establish a secure channel). What Nystrom teaches about reloading and update procedures is about reactions to the exchange between different terminal devices having different processing capabilities and functionalities and underlying different constraints. The Applicant respectfully submits the Examiner interprets Nystrom beyond its original intent. Nystrom neither teaches nor suggests about establishing a two-level security channel to protect subsequent operations over a wired network. In one perspective, Nystrom teaches away from Claim 1 by using a SIM card thus avoiding to personalize the e-purse applet in the smart card.

The Applicant further submits that the key 10 in Shmueli could not be modified by the SIM card or the smart card in Nystrom because Shmueli specifically states that an application must be uploaded to a host to be executed while a smart card is able to execute an application in the care itself. Accordingly, the combination of Shmueli and

Nystrom neither teaches nor suggests Claim 1, and Claim shall be allowable over Shmueli and Nystrom. Reconsideration of Claims 1-10 is kindly requested.

Claim 11 has been amended to include similar limitations recited in Claim 1. The Applicant wishes to rely on the above arguments to support once-amended Claim 11, and respectfully submits Claim 11, as amended, is neither taught nor suggested by Shmueli and Nystrom, viewed alone or in combination, and shall be allowable over Shmueli and Nystrom. Reconsideration of Claims 11 - 18 is kindly requested.

In view of the above amendments and remarks, the Applicant believes that Claims 1 - 18 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 " Box: Non-Fee Amendment Commissioner of Patents and Trademarks P. O. Box 1450, Alexandria, VA 22313-1450", on Sep. 7, 2010.

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>	11534653			
<b>Filing Date:</b>	24-Sep-2006			
<b>Title of Invention:</b>	Method and apparatus for providing electronic purse			
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh			
<b>Filer:</b>	Joe Zheng			
<b>Attorney Docket Number:</b>	RFID-081			
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>				
Extension - 1 month with \$0 paid	2251	1	65	65



Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>65</b>

<b>Electronic Acknowledgement Receipt</b>	
<b>EFS ID:</b>	10889228
<b>Application Number:</b>	11534653
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	6327
<b>Title of Invention:</b>	Method and apparatus for providing electronic purse
<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-081
<b>Receipt Date:</b>	07-SEP-2011
<b>Filing Date:</b>	24-SEP-2006
<b>Time Stamp:</b>	03:02:12
<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	\$65
RAM confirmation Number	7404
Deposit Account	502436
Authorized User	

**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	137398 d5a5a21ad5377042b1f62c3839a9b18d27 0f37f	no	12
<b>Warnings:</b>					
<b>Information:</b>					
2	Fee Worksheet (SB06)	fee-info.pdf	29814 5e6625b0c92999bcdcfb532cf99f49f3945c9 410	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			167212		
<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>					

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>11/534,653</b>		Filing Date <b>09/24/2006</b>		<input type="checkbox"/> To be Mailed									
<b>APPLICATION AS FILED – PART I</b>					(Column 1)		(Column 2)		SMALL ENTITY <input checked="" type="checkbox"/> OR OTHER THAN SMALL ENTITY									
FOR		NUMBER FILED		NUMBER EXTRA		RATE (\$)		FEE (\$)		RATE (\$)		FEE (\$)						
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>		N/A		N/A		N/A				N/A								
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>		N/A		N/A		N/A				N/A								
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>		N/A		N/A		N/A				N/A								
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>		minus 20 =		*		X \$ =		OR		X \$ =								
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>		minus 3 =		*		X \$ =		OR		X \$ =								
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 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 <small>(37 CFR 1.16(j))</small>																		
					TOTAL				TOTAL									
* If the difference in column 1 is less than zero, enter "0" in column 2.																		
<b>APPLICATION AS AMENDED – PART II</b>					(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY OR OTHER THAN SMALL ENTITY							
AMENDMENT	<b>09/07/2011</b>		CLAIMS REMAINING AFTER AMENDMENT				HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)		RATE (\$)		ADDITIONAL FEE (\$)	
	Total <small>(37 CFR 1.16(i))</small>		* 18		Minus		** 20		= 0		X \$26 =		0		OR		X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>		* 2		Minus		***3		= 0		X \$110 =		0		OR		X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>																	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>																	
					TOTAL ADD'L FEE		<b>0</b>		OR		TOTAL ADD'L FEE							
AMENDMENT			CLAIMS REMAINING AFTER AMENDMENT				HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		RATE (\$)		ADDITIONAL FEE (\$)		RATE (\$)		ADDITIONAL FEE (\$)	
	Total <small>(37 CFR 1.16(i))</small>		*		Minus		**		=		X \$ =		OR		X \$ =			
	Independent <small>(37 CFR 1.16(h))</small>		*		Minus		***		=		X \$ =		OR		X \$ =			
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>																	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>																	
					TOTAL ADD'L FEE				OR		TOTAL ADD'L FEE							
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.																		
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".																		
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".																		
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.																		
Legal Instrument Examiner: /SHARON HARRIS/																		

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

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

11/534,653	09/24/2006	Liang Seng Koh	RFID-081	6327
------------	------------	----------------	----------	------

26797 7590 09/09/2011  
 SILICON VALLEY PATENT AGENCY  
 7394 WILDFLOWER WAY  
 CUPERTINO, CA 95014

EXAMINER
----------

STANFORD, CHRISTOPHER J

ART UNIT	PAPER NUMBER
----------	--------------

2887

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

09/09/2011

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>Applicant-Initiated Interview Summary</b>	<b>Application No.</b> 11/534,653	<b>Applicant(s)</b> KOH ET AL.	
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887	

All participants (applicant, applicant's representative, PTO personnel):

(1) CHRISTOPHER STANFORD. (3) Joe Zheng.  
(2) Thien Le. (4) LiangSeng Koh & Sean Han.

Date of Interview: 31 August 2011.

Type:  Telephonic  Video Conference  
 Personal [copy given to:  applicant  applicant's representative]

Exhibit shown or demonstration conducted:  Yes  No.  
If Yes, brief description: \_\_\_\_\_.

Issues Discussed 101 112 102 103 Others  
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1.

Identification of prior art discussed: Shmueli and Nystrom.

Substance of Interview  
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicants provided proposed amendments highlighting differences between their invention and the applied prior art. Examiner recommended modifying the proposed amendments to clarify what was intended to be conveyed by the new claim language. A response will be filed and further search and/or consideration is required. Examiners will contact Applicants' representative if prosecution can be made more compact.

**Applicant recordation instructions:** The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

**Examiner recordation instructions:** Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Attachment

/THIEN M LE/ Primary Examiner, Art Unit 2887	/CHRISTOPHER STANFORD/ Examiner, Art Unit 2887
---	---

## Summary of Record of Interview Requirements

### Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

### Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,  
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

### Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.



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 11/29/2011
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014

EXAMINER

STANFORD, CHRISTOPHER J

ART UNIT PAPER NUMBER

2887

DATE MAILED: 11/29/2011

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

11/534,653 09/24/2006 Liang Seng Koh RFID-081 6327

TITLE OF INVENTION: METHOD AND APPARATUS FOR PROVIDING ELECTRONIC PURSE

Table with 7 columns: APPLN. TYPE, SMALL ENTITY, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

nonprovisional YES \$870 \$300 \$0 \$1170 02/29/2012

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 SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

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 11/29/2011  
**SILICON VALLEY PATENT AGENCY**  
 7394 WILDFLOWER WAY  
 CUPERTINO, CA 95014

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.
11/534,653	09/24/2006	Liang Seng Koh	RFID-081	6327

TITLE OF INVENTION: METHOD AND APPARATUS FOR PROVIDING ELECTRONIC PURSE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$870	\$300	\$0	\$1170	02/29/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
STANFORD, CHRISTOPHER J	2887	235-380000

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

- Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.  
 "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

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

1 \_\_\_\_\_  
 2 \_\_\_\_\_  
 3 \_\_\_\_\_

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document 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

4a. The following fee(s) are submitted:

- Issue Fee  
 Publication Fee (No small entity discount permitted)  
 Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- A check is enclosed.  
 Payment by credit card. Form PTO-2038 is attached.  
 The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number \_\_\_\_\_ (enclose an extra copy of this form).

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

- a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.  b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature \_\_\_\_\_

Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_

Registration No. \_\_\_\_\_

This collection of information 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.



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.
11/534,653 09/24/2006 Liang Seng Koh RFID-081 6327

26797 7590 11/29/2011
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014

EXAMINER

STANFORD, CHRISTOPHER J

ART UNIT PAPER NUMBER

2887

DATE MAILED: 11/29/2011

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

The Patent Term Adjustment to date is 727 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 727 day(s).

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 Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

## 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>	<b>Applicant(s)</b>	
	11/534,653	KOH ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	CHRISTOPHER STANFORD	2887	

**-- 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 9/07/2011.
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 1-18.
4.  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 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.  A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  6.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a)  including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1)  hereto or 2)  to Paper No./Mail Date \_\_\_\_.
    - (b)  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).**
7.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |  |  |
|--|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input type="checkbox"/> Notice of Informal Patent Application                      |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date ____ . |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date ____     | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment                    |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance   |
|  | 9. <input type="checkbox"/> Other ____.  |

/CHRISTOPHER STANFORD/  
Examiner, Art Unit 2887

**DETAILED ACTION**

***Response to Amendment***

1. Receipt is acknowledged of the amendment filed 9/07/2011. Claims 1 and 11 are amended and claims 1-18 are currently pending.

**EXAMINER'S AMENDMENT**

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The application has been amended in the claims as follows:

1. (Currently Amended) A method for providing an e-purse, the method comprising:  
providing a portable device including or communicating with a smart card pre-loaded with an emulator configured to execute a request from an e-purse applet and provide a response the e-purse applet is configured to expect, the portable device including a memory space loaded with a midlet that is configured to facilitate communication between the e-purse applet and a payment server over a wireless network, wherein the e-purse applet is downloaded and installed in the smart card when the smart ~~card~~ card is in communication with the payment server, the portable device further includes a contactless interface that facilitates

communication between the e-purse applet in the smart card and the payment server over a wired network;

personalizing the e-purse applet by reading off data from the smart card to generate in the smart card one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card, wherein said personalizing the e-purse applet comprises:

establishing an initial security channel between the smart card and the e-purse SAM to install and personalize the e-purse applet in the smart card, and

creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet.

11. (Currently amended) A system for providing an e-purse, the system comprising: a portable device including or communicating with a smart card pre-loaded with an emulator configured to execute a request from and provide a response an e-purse applet is configured to expect, the portable device including a memory space loaded with a midlet that is configured to facilitate wireless communication between the e-purse applet in the smart card and a payment server over a wireless network, the portable device further including a contactless interface that

facilitates communication between the e-purse applet in the smart card and the payment server over a wired network, wherein the e-purse applet is downloaded from the payment server when the smart ~~card~~ card is in communication with the payment server, and operations of personalizing the e-purse applet comprises:

establishing an initial security channel between the smart card and the e-purse security authentication module (SAM) to install and personalize the e-purse applet in the smart card, and

creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet;

the payment server associated with an issuer authorizing the e-purse applet; and the e-purse SAM configured to enable the e-purse applet, wherein an SAM is behind the payment server and in communication with the e-purse applet when the e-purse applet is caused to communicate with the payment server via the midlet.

***Allowable Subject Matter***

3. Claims 1-18 are allowed.
4. The following is an examiner's statement of reasons for allowance: neither the cited prior art of record taken alone or in combination with other references reasonably teach

a. a method for providing an e-purse, the method comprising: providing a portable device including or communicating with a smart card pre-loaded with an emulator configured to execute a request from an e-purse applet and provide a response the e-purse applet is configured to expect, the portable device including a memory space loaded with a midlet that is configured to facilitate communication between the e-purse applet and a payment server over a wireless network, wherein the e-purse applet is downloaded and installed in the smart card when the smart card is in communication with the payment server, the portable device further includes a contactless interface that facilitates communication between the e-purse applet in the smart card and the payment server over a wired network; personalizing the e-purse applet by reading off data from the smart card to generate in the smart card one or more operation keys that are subsequently used to establish a secured channel between the e-purse applet and an e-purse security authentication module (SAM) external to the smart card, wherein said personalizing the e-purse applet comprises: establishing an initial security channel between the smart card and the e- purse SAM to install and personalize the e-purse applet in the smart card, and creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet (claim 1)

b. a system for providing an e-purse, the system comprising: a portable device including or communicating with a smart card pre-loaded with an emulator configured to execute a request from and provide a response an e-purse applet is



configured to expect, the portable device including a memory space loaded with a midlet that is configured to facilitate wireless communication between the e-purse applet in the smart card and a payment server over a wireless network, the portable device further including a contactless interface that facilitates communication between the e-purse applet in the smart card and the payment server over a wired network, wherein the e-purse applet is downloaded from the payment server when the smart card is in communication with the payment server, and operations of personalizing the e-purse applet comprises: establishing an initial security channel between the smart card and the e-purse security authentication module (SAM) to install and personalize the e-purse applet in the smart card, and creating a security channel on top of the initial security channel to protect subsequent operations of the smart card with the e-purse SAM, wherein any subsequent operation of the emulator is conducted over the security channel via the e-purse applet; the payment server associated with an issuer authorizing the e-purse applet; and the e-purse SAM configured to enable the e-purse applet, wherein an SAM is behind the payment server and in communication with the e-purse applet when the e-purse applet is caused to communicate with the payment server via the midlet (claim 11).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

**Conclusion**


Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER STANFORD whose telephone number is (571)270-3337. The examiner can normally be reached on Monday through Fridays , 7:30am-4:30pm.

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

/THIEN M LE/  
Primary Examiner, Art Unit 2887

<b><i>Index of Claims</i></b>  	<b>Application/Control No.</b> 11534653	<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>

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

CLAIM		DATE							
Final	Original	01/25/2010	09/27/2010	05/19/2011	11/15/2011				
1	1	✓	✓	✓	✓				
2	2	✓	✓	✓	✓				
3	3	✓	✓	✓	✓				
4	4	✓	✓	✓	✓				
5	5	✓	✓	✓	✓				
6	6	✓	✓	✓	✓				
7	7	✓	✓	✓	✓				
8	8	✓	✓	✓	✓				
9	9	✓	✓	✓	✓				
10	10	✓	✓	✓	✓				
11	11	✓	✓	✓	✓				
12	12	✓	✓	✓	✓				
13	13	✓	✓	✓	✓				
14	14	✓	✓	✓	✓				
15	15	✓	✓	✓	✓				
16	16	✓	✓	✓	✓				
17	17	✓	✓	✓	✓				
18	18	✓	✓	✓	✓				




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. 6327

<b>SERIAL NUMBER</b> 11/534,653	<b>FILING or 371(c) DATE</b> 09/24/2006	<b>CLASS</b> 235	<b>GROUP ART UNIT</b> 2887	<b>ATTORNEY DOCKET NO.</b> RFID-081	
<b>APPLICANTS</b> Liang Seng Koh, Fremont, CA; Futong Cho, Milpitas, CA; Hsin Pan, Fremont, CA; Fuliang Cho, San Jose, CA;					
<b>** CONTINUING DATA *****</b> [CS/] <b>** FOREIGN APPLICATIONS *****</b> [CS/] <b>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED *** SMALL ENTITY **</b> [CS/] 10/17/2006					
Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No 35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No Verified and /CHRISTOPHER J STANFORD/ Acknowledged Examiner's Signature	<input type="checkbox"/> Met after Allowance Initials	<b>STATE OR COUNTRY</b> CA	<b>SHEETS DRAWINGS</b> 9	<b>TOTAL CLAIMS</b> 18	<b>INDEPENDENT CLAIMS</b> 2
<b>ADDRESS</b> SILICON VALLEY PATENT AGENCY 7394 WILDFLOWER WAY CUPERTINO, CA 95014 UNITED STATES					
<b>TITLE</b> Method and apparatus for providing electronic purse					
<b>FILING FEE RECEIVED</b> 490	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		

<b>Issue Classification</b> 	<b>Application/Control No.</b> 11534653	<b>Applicant(s)/Patent Under Reexamination</b> KOH ET AL.
	<b>Examiner</b> CHRISTOPHER STANFORD	<b>Art Unit</b> 2887

ORIGINAL						INTERNATIONAL CLASSIFICATION											
CLASS		SUBCLASS				CLAIMED				NON-CLAIMED							
235		380				G	0	6	K	5 / 00 (2006.01.01)							
<b>CROSS REFERENCE(S)</b>																	
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)																
235	451	492															
705	26	39	40	41	64												

<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	18	18																		
3	3																				
4	4																				
5	5																				
6	6																				
7	7																				
8	8																				
9	9																				
10	10																				
11	11																				
12	12																				
13	13																				
14	14																				
15	15																				
16	16																				

/CHRISTOPHER STANFORD/ Examiner.Art Unit 2887	11/15/2011 (Date)	<b>Total Claims Allowed:</b> 18	
(Assistant Examiner)	(Date)		
/Thien M. Le/ (Primary Examiner)	11/15/2011 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

**EAST Search History**

**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S53	4342	("235" or "705" or "713" or "340").clas. and "L3"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO	ADJ	ON	2011/11/15 09:24


**EAST Search History (Interference)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S65	8	S64 and ((e or electronic or digital) (purse or wallet) and (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification or tag))).clm. and (install\$3 or load\$3 or upload\$3 or download\$3) with (applet or java or midlet or keylet or (e or electronic or digital) (purse or wallet))	USPAT; UPAD	ADJ	ON	2011/11/15 09:32
S64	10968	235/380,451,492.ccls. or 705/26,39-41,64.ccls.	USPAT; UPAD	ADJ	ON	2011/11/15 09:32
S63	1	((e or electronic or digital) (purse or wallet) and (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification or tag))).clm. and (install\$3 or load\$3 or upload\$3 or download\$3) with (applet or java or midlet or keylet or (e or electronic or digital) (purse or wallet)).clm.	USPAT; UPAD	ADJ	ON	2011/11/15 09:29
S62	1	(emulat\$3 and (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification or tag))).clm. and (install\$3 or load\$3 or upload\$3 or download\$3) with (applet or java or midlet or keylet or (e or electronic or digital) (purse or wallet)).clm.	USPAT; UPAD	ADJ	ON	2011/11/15 09:29
S61	1	(emulat\$3 and (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification or tag))).clm. and channel with (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification or tag)).clm.	USPAT; UPAD	ADJ	ON	2011/11/15 09:25
S60	48	("235" or "705" or "713" or "340").clas. and S56	USPAT; UPAD	ADJ	ON	2011/11/15 09:24
S59	3	(emulat\$3 and (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification	USPAT; UPAD	ADJ	ON	2011/11/15 09:24

		(or tag))).clm. and (personaliz\$3 or personalization) with (applet or java or midlet or keylet or (e or electronic or digital) (purse or wallet) or (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification or tag)))				
S58	1	(emulat\$3 and (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification or tag))).clm. and (personaliz\$3 or personalization) with (applet or java or midlet or keylet or (e or electronic or digital) (purse or wallet))	USPAT; UPAD	ADJ	ON	2011/11/15 09:23
S57	4	(emulat\$3 and (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification or tag)) and security near3 module).clm.	USPAT; UPAD	ADJ	ON	2011/11/15 09:13
S56	62	(emulat\$3 and (smartcard or smart card or rfid or (rf or radio frequency of proximity or noncontact or non contact or contactless or contact less) adj2 (card or id or identification or tag))).clm.	USPAT; UPAD	ADJ	ON	2011/11/15 09:13

11/ 15/ 2011 11:12:01 AM

C:\Users\cstanford\Documents\EAST\Workspaces\11534653\_AOM4.wsp

<b>Search Notes</b>  	<b>Application/Control No.</b>  11534653	<b>Applicant(s)/Patent Under Reexamination</b>  KOH ET AL.
	<b>Examiner</b>  CHRISTOPHER STANFORD	<b>Art Unit</b>  2887

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
235	379,380,492	1/22-25/10	CS

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>
Inventor, Assignee Search	1/22-25/10	CS
NPL Search	1/22-25/10	CS
Text Search (see search history report print out)	1/22-25/10	CS
Text Search (see search history report print out)	7/07/10-9/24/10	CS
Text Search (see search history report print out)	5/19/11	CS
Text Search (see search history report print out)	11/15/11	CS

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>
235	380,451,492	11/15/11	CS
705	26,39-41,64	11/15/11	CS

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



**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 11/29/2011  
**SILICON VALLEY PATENT AGENCY**  
 7394 WILDFLOWER WAY  
 CUPERTINO, CA 95014

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)
01/16/2012	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/534,653	09/24/2006	Liang Seng Koh	RFID-081	6327

TITLE OF INVENTION: METHOD AND APPARATUS FOR PROVIDING ELECTRONIC PURSE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$870	\$300	\$0	\$1170	02/29/2012

EXAMINER	ART UNIT	CLASS-SUBCLASS
STANFORD, CHRISTOPHER J	2887	235-380000

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

- Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.  
 "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

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

1. Joe Zheng  
 2. \_\_\_\_\_  
 3. \_\_\_\_\_

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

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document 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 Rich House Global Technology Ltd., Shenzhen, China  
RF Cyber Corp., Fremont, CA  
 (B) RESIDENCE: (CITY and STATE OR COUNTRY)

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

4a. The following fee(s) are submitted:

- Issue Fee  
 Publication Fee (No small entity discount permitted)  
 Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- A check is enclosed.  
 Payment by credit card. Form PTO-2038 is attached. Paid via EFS  
 The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number \_\_\_\_\_ (enclose an extra copy of this form).

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

- a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.  b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature / joe zheng /  
 Typed or printed name Joe Zheng

Date 01/16/2012  
 Registration No. 39,450

This collection of information 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.

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	11534653			
<b>Filing Date:</b>	24-Sep-2006			
<b>Title of Invention:</b>	METHOD AND APPARATUS FOR PROVIDING ELECTRONIC PURSE			
<b>First Named Inventor/Applicant Name:</b>	Liang Seng Koh			
<b>Filer:</b>	Joe Zheng			
<b>Attorney Docket Number:</b>	RFID-081			
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>				
<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	870	870
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>1170</b>

<b>Electronic Acknowledgement Receipt</b>	
<b>EFS ID:</b>	11840128
<b>Application Number:</b>	11534653
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	6327
<b>Title of Invention:</b>	METHOD AND APPARATUS FOR PROVIDING ELECTRONIC PURSE
<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-081
<b>Receipt Date:</b>	16-JAN-2012
<b>Filing Date:</b>	24-SEP-2006
<b>Time Stamp:</b>	03:29:28
<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	\$1170
RAM confirmation Number	8353
Deposit Account	
Authorized User	

**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	91823 df3fe445b069a79d854836e3907d4a01fe5a0ccd	no	1
<b>Warnings:</b>					
<b>Information:</b>					
2	Fee Worksheet (SB06)	fee-info.pdf	31785 1f675027a648cc54e849233344550720fb9e5a2	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>				123608	
<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>					



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.
11/534,653	02/21/2012	8118218	RFID-081	6327

26797 7590 02/01/2012  
SILICON VALLEY PATENT AGENCY  
7394 WILDFLOWER WAY  
CUPERTINO, CA 95014

**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 1057 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;  
Futong Cho, Milpitas, CA;  
Hsin Pan, Fremont, CA;  
Fuliang Cho, San Jose, CA;