Method and apparatus for ~~personalizing secure elements in~~settling payments using mobile devices

Abstract

Techniques for ~~personalizing secure elements in NFC devices to enable various secure transactions over a network (wired and/or wireless network) are disclosed. With a personalized secure element (hence secured element) in place, techniques for provisioning various applications or services are also provided. Interactions among different parties are managed to effectuate a personalization or provisioning process flawlessly to enable an NFC device for a user thereof to start enjoying the convenience of commerce over a data network with minimum effort~~mobile devices configured to support settlement of charges in electronic invoices or bills are described. A mobile device embedded with a secure element generates or is loaded with an electronic invoice. When the mobile device is brought to a consumer with an NFC mobile device, the data including the electronic invoice and other information regarding the mobile device or an owner thereof is read off wirelessly into the NFC mobile device. After the user verifies the amount being charged and authorizes the payment, the NFC mobile device communicates with a payment gateway or network for payment that is configured to proceed with the payment in accordance with a chosen payment methods.

Description

~~CROSS-REFERENCE TO RELATED APPLICATIONS~~

~~[0001]~~

~~This application is a continuation-in-part of co-pending U.S. patent application Ser. No.: 11/534,653 filed on Sep. 24, 2006, now US Pat. No. _______, and also a continuation-in-part of U.S. patent application Ser. No.: 11/739,044 filed on Apr. 23, 2007, which is a continuation-in-part of co-pending U.S. patent application Ser. No.: 11/534,653 filed on Sep. 24, 2006, now U.S. Pat. No. _______.~~

BACKGROUND OF THE INVENTION

~~[0002]~~

1. ~~Technical~~ Field of the Invention

~~[0003]~~

The present invention is generally related to the area of electronic commerce ~~over networks~~. Particularly, the present invention is related to ~~techniques for personalizing a secure element and provisioning an application such as an electronic purse that can be advantageously used in portable devices~~a mobile device configured ~~for both~~to settle payments using a mobile device reading electronic

~~commerce (a.k.a., e-commerce) and mobile commerce (a.k.a., m-commerce)~~bills or invoices off from another mobile device in a near field communication range.
~~[0004]~~

2. ~~Description~~The Background of~~ the~~ Related Art
~~[0005]~~

~~Single functional cards have been successfully used in enclosed environments such as transportation systems. One example of such single functional cards is MIFARE that has been selected as the most successful contactless smart card technology. MIFARE is the perfect solution for applications like loyalty and vending cards, road tolling, city cards, access control and gaming.~~
~~[0006]~~

~~However, single functional card applications are deployed in enclosed systems, which are difficult to be expanded into other areas such as e-commerce and m-commerce because stored values and transaction information are stored in data storage of each tag that is protected by a set of keys. The nature of the tag is that the keys need to be delivered to the card for authentication before any data can be accessed during a transaction. This constraint makes systems using such technology difficult to be expanded to an open environment such as the Internet for e-commerce and/or wireless networks for m-commerce as the delivery of keys over a public domain network causes security concerns.~~
~~[0007]~~

~~In general, a smart card, chip card, or integrated circuit card (ICC), is any pocket-sized card with embedded integrated circuits. A smart card or microprocessor cards contain volatile memory and microprocessor components. Smart cards may also provide strong security authentication for single sign-on (SSO) within large organizations. The benefits of smart cards are directly related to the volume of information and applications that are programmed for use on a card. A single contact/contactless smart card can be programmed with multiple banking credentials, medical entitlement, driver's license/public transport entitlement, loyalty programs and club memberships to name just a few. Multi-factor and proximity authentication can and has been embedded into smart cards to increase the security of all services on the card.~~
~~[0008]~~

~~Contactless smart cards that do not require physical contact between card and reader are becoming increasingly popular for payment and ticketing applications such as mass transit and highway tolls. Such Near Field Communication (NFC) between a contactless smart card and a reader presents significant business opportunities when used in NFC-enabled mobile phones for applications such as payment, transport ticketing, loyalty, physical access control, and other exciting new services.~~
~~[0009]~~

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

~~[0010]~~

~~One of the concerns in the NFC mobile ecosystem is its security in an open network. Thus there is a need to provide techniques to personalize a secure element in a contactless smart card or an NFC-enabled mobile device so that such a device is so secured and personalized when it comes to financial applications or secure transactions. With a personalized secure element in an NFC-enabled mobile device, various applications or services, such as electronic purse or payments, can be realized. Accordingly, there is another need for techniques to provision or manage an application or service in connection with a personalized secure element~~

For many credit or debit card transactions, the payment process is started by a customer asking for a bill when checking out a purchase. A cashier or service member brings a bill to the customer for verification. The customer then hands out a credit/debit card to the service staff member. The service member brings the card to a Point of Sales (POS) counter to initiate a transaction payment. The service member then brings back a receipt to the customer for signature to authorize the transaction. It is a lengthy process that typically takes a couple of minutes or much longer when the service member has to take care of multiple payment transactions at a time. In addition, in the case for the debit card transactions, the process may be even more troublesome when a PIN is needed to authorize the transaction at the POS.

There is a need to simplify the payment process. With the advancement in mobile devices, it is anticipated that many consumers will carry one with them. Thus there is an opportunity of using a mobile device to quickly settle the payment at a point of sale (POS).

SUMMARY OF THE INVENTION

~~[0011]~~

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.

~~[0012]~~

~~Broadly speaking, the invention is related to techniques for personalizing secure elements in NFC devices to enable various secure transactions over a network~~

~~(wired and/or wireless network). With a personalized secure element (hence secured element), techniques for provisioning various applications or services are also provided. Interactions among different parties are managed to effectuate a personalization or provisioning process flawlessly to enable an NFC device for a user thereof to start enjoying the convenience of commerce over a data network with minimum effort.~~

~~[0013]~~

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

~~[0014]~~

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

~~[0015]~~

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

~~[0016]~~

~~According to another embodiment, the present invention is a method for personalizing a secure element associated with a computing device. The method comprises receiving an inquiry to establish data communication between a server and the computing device, sending a request from the server to the computing device to request device information of the secure element after the server determines that the computing device is registered therewith, wherein the device information is a sequence of characters uniquely identifying the secure element, and the request is a command that subsequently causes the computing device to retrieve the device information from the secure element therein, generating at least a set of keys in accordance with the device information received, delivering the set of keys through a secured channel over a data network to the computing device, wherein the set of keys is caused to be stored in the secure element with the computing device, and notifying at least a related party that the secure element is now personalized for subsequent trusted transactions.~~
~~[0017]~~

The present invention is related to techniques for mobile devices configured to support settlement of charges in electronic invoices or bills. According to one aspect of the present invention, a mobile device embedded with a secure element generates or is loaded with an electronic invoice. When the mobile device is brought to a consumer with an NFC mobile device, the data including the electronic invoice and other information regarding the mobile device or an owner thereof is read off wirelessly into the NFC mobile device. After the user verifies the amount being charged and authorizes the payment, the NFC mobile device communicates with a payment gateway or network for payment that is configured to proceed with the payment in accordance with a chosen payment methods.

According to another aspect of the present invention, the mobile device is a contactless card or part of a point of sale (POS) machine used to generate the electronic invoice. One embodiment of the present invention provides unanticipated benefits and advantages in an application in which a payment process would otherwise have to be involved in more than one contacts between a merchant and the consumer. One of such applications is a payment process in a restaurant, where a consumer is given a check first for verification and a chance to add a gratitude before a final charge is determined and paid. Using the NFC mobile device, the consumer can finish the payment using a chosen payment method at the point of sale without further contacting the merchant.

According to still another aspect of the present invention, a consumer uses his/her mobile device, per the data received therein, to settle the payment process with a payment network, where the payment network may be an existing payment

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.