SETECS
Secure Transactions and Electronic Commerce Systems

SETECS® Mobile Technologies

SETECS® SAFE™ System

Secure UICC Wallet for Financial Transactions

Trends in Mobile Technologies

Mobile phones are currently today used mainly for communication purposes: i.e. making phone calls or sending SMS messages. But, new, high—end phones are already introducing new mobile services where mobile phones are used not only as communication, but also as information distribution and sometimes even as local computing devices. For low–end phones current trends are to provide new mobile services, mostly based on background servers and simple communications using SMS or USSD messages. For smart phones and phones with memory cards additional functions are implemented and distributed as software applications stored in the memory cards of mobile phones. So, one important trend in mobile networks is to provide *new, additional mobile services* using *applications* stored in the memory of mobile phones.

Another characteristic of current mobile phone technologies and networks is that they are all functioning as a very *closed market*. Contrary to the current situation, ISO, ETSI, GSM and other standardization bodies for mobile technologies and networks suggest an open, secure and flexible architecture and protocols for mobile applications.

Finally, current mobile phones, SMS or USSD messages, applications and their data are usually without any privacy or security. With expanded reach of their connectivity and expanded scope of their applications, communication security becomes more and more important issue.

SETECS® UICC Wallet

SAFE™ system is our large–scale, service–oriented architecture for secure mobile transactions, comprising several components: communications server, payment server, security servers, and several mobile application servers. It can be used by mobile network operators, banks, credit card processors, small merchants, Web merchants, and the most important, the client users. This brochure describes only subscribers' component of that large infrastructure, called ***Secure Mobile Wallet***. Its core features are the following:

- It is based on the very capable and secure Java smart cards chip with large internal storage (256K EEPROM), contact (ISO 7816) and contactless (Near–Field–Communications – NFC) protocols, and extended security algorithms and capabilities, supporting multiple applications (Javacard applets);
- The next component is the set of Secure Mobile Wallet applications, designed in the form of several Javacard applets, supporting identity verification and authentication of subscribers (PIV applet), security features and protocols (Security applet), secure m-Banking and m-Commerce transactions (Mobile Wallet) and in the future other mobile application applets;
- The chip loaded with the collection of Javacard applets is used in mobile phones as the new, so called UICC chip, hosting multiple and dynamically managed applications;
- For communications with users Wallet supports Proactive Commands, specially designed APDUs, and NFC protocol;
- For communication with mobile network the Wallet supports GSM and CDMA messages for deployment and also for management of mobile applications; and
- Secure Mobile Wallet communicates in a secure way with mobile phone and through it with back—end components – network servers for mobile applications, management and security protocols.

Design of Secure Mobile Wallet

SAFE™ Secure Mobile Wallet is a set of Javacard applets loaded in the UICC chip of mobile phones. Following standard approach, each applet has its Application Identifier (AID). When designing applets several aspects must be specified:

- Applets functions, in the form of functional application–level functions;
- Internal data model needed to support those functions;
- Card Command Interface (CCI), i.e. ISO 7816 APDUs that the applet supports; and
- Eventually, applet middleware.

SAFE™ Secure Mobile Wallet supports four groups of functions: (1) user identification and authentication functions (using PIN and certificates), (2) various financial transactions (m–Banking, stored money payments, pre–paid accounts, etc.), (3) various m–Commerce transactions (mobile tickets, mobile parking, etc.), and (4) security functions (encryption, signatures). All its functions are specified in the form of high–level programming APIs and implemented in the form of SAFE Wallet Middleware. Examples are: SAFE_store_money(), SAFE_list_transactions(), etc.

Internal data model is the collection of data objects with attributes and structure optimized for support to all Secure Mobile Wallet application–level functions. All objects have their Object Identifiers (OIDs), Tag–Length–Value (TLV) encoding, and organization optimized for various transactions. At the moment OIDs are our own (proprietary) due to the lack of established international standards, but our intention is to submit our AID and OIDs for international standardization. Individual attributes are grouped in objects optimized for various transactions and two examples of such objects are shown in the Figure.

Card Command Interface (CCI) is the set of ISO 7816 compliant commands. Wallet middleware translates APIs into those commands and card responses to return codes and results. For verification of the PIN and digital signature, we used CCI commands from the FIPS 201 standard. However, since the Secure Mobile Wallet supports many m–banking and m–commerce functions, we designed our own CCI commands for those functions. They use data stored in the Secure Mobile Wallet, as appropriate.

Wallet middleware is a layer of software for "bridging" between application–level APIs and CCI commands. It is implemented in Java and therefore may be used in mobile phones, in PoS devices, and for applications in PCs.

Bank Account Data (Container ID=01, MAX LENTH = 84 Bytes)

Attributes (TLV)	Tag	Type	Max.Bytes
Bank IBAN	01	Variable	34
Bank SWIFT Code	02	Variable	11
Bank Routing Number	03	Variable	9
Clearing Number	04	Fixed	4
Account Number	05	Variable	16
Account Type	06	Fixed	1
Balance	07	Fixed	5
Account Open Date	08	Date(YYYYMMDD)	4

SAFE System Data (Container ID=01, MAX LENGTH = 54 Bytes)

Attributes (TLV)	Tag	Type	Max.Bytes
SAFE System Short Code	01	Fixed	6
SAFE Account Number	02	Fixed	10
SAFE PIN/ Password	03	Fixed	8
Balance	04	Fixed	5
Account Open Date	05	Date(YYYYMMDD)	4
SAFE Server Mobile Number	06	Variable	15
SAFE Server IP Number	07	Fixed	4
SAFE Server Port	08	Fixed	2

Usage of Secure Mobile Wallet

Before being used, Secure Mobile Wallet (as applets) must be loaded into the UICC chip and also personalized. Based on FIPS 201 and ETSI standards, these operations may be performed "over–the–counter" (OTC) and also "over–the–air" (OTA). For OTC Wallet management we use two approaches: extended Eclipse environment to manage smart card applets (JCOP) and extended PIV Card Management System to load and personalize Secure Mobile Wallet applets. Of course, during OTC management the UICC is still in the smart card housing. After OTC loading and personalization, UICC can be separated from the smart card housing into SIM housing and inserted in the mobile phone.

Once inserted into a mobile phone, Secure Mobile Wallet can be used in several ways:

Combination with J2ME Application

In this case, besides Secure Mobile Wallet applets in the UICC chip, Wallet Application and Wallet middleware, implemented as J2ME applications, are also loaded. In this case, Wallet Application provides nice selection (drop–down) menus, data forms and display screens. The applets contain data and perform various functions with that data, initiated by the Wallet Application.

The advantage of this approach is that user interfaces are very nice and data are strongly protected in the applets. The disadvantage is that Wallet Application must be separately loaded into mobile phones. Thus, this approach may not be feasible in all types of mobile phones.

Usage without J2ME Application

In this case, Secure Mobile Wallet is the only software loaded in a SIM chip of a mobile phone. In this case, Secure Mobile Wallet uses proactive commands to communicate with the terminal device. Using proactive commands the Secure Mobile Wallet can implement all functions using APIs only provided by the libraries available in the card. All GUIs, financial functions, communication and security are achieved without any outside component. The complete Secure Mobile Wallet is encapsulated in the card and since users insert SIM card into the handset, the Secure Mobile Wallet is ready. No any pre-installations are needed.

Using Near-Field-Communications Protocol (NFC)

Our Secure Mobile Wallet works with both, contact and contactless, protocols. When used in combination with the J2ME application or with proactive commands, Secure Mobile Wallet communicates with the outside world through over–the–air protocol, GSM, and over-the-counter protocol, Bluetooth. But, if the UICC is also contactless (NFC), Secure Mobile Wallet can also be used for transactions through over–the–counter protocol, NFC. In that case, standard contactless readers for smart cards or special PoS devices with NFC protocol are used for interactions with the phone.

Primary Markets

The primary market for SAFE™ Secure Mobile Wallet is telecom market. Secondary markets are Web services providers and financial services providers. Telecom market is one of the largest and the fastest growing international markets, not only in developed, but also in developing countries. The number of mobile phones in use today is in the range of several billions and mobile network is one of the most global networks around the world.

One of the very important markets for the described product is "un-banked" users. Those are persons (mainly in developing countries) that do not have bank accounts. Telecom companies are targeting those customers for their financial transactions. Several World Bank and IFC documents contain interesting quote that "*there are 10% people in the World that have bank accounts and 90% do not, while there are 90% of people who have mobile phones and 10% do not*". Banks and telecom operators are very interested to expand their services to that population, but that expansion goes very slowly mainly due to the lack of easy-to-use and readily available approaches to support such services.

Finally, many governments, international organizations, international and national law-enforcement agencies, and end–users are all interested to use simple, secure, and readily available mobile system for commercial and financial transactions, with low fees and quick transfer times.

Secure Mobile Applications

Secure Mobile Banking

Wallet stores user's bank account number and also identification of the bank (its IBAN or Routing number). Therefore individuals and companies may access their bank accounts and perform transactions banked users, using mobile phones.

Secure Mobile Financial Transactions for Un-banked Users

Wallet stores user's pre–paid (mobile) account. Using their mobile phones and those pre–paid accounts, users may perform various financial transactions using their mobile phones.

Secure Mobile Payments

Users may perform various types of payments using mobile phones, including cash–in/cash–out over–the–counter, person–to–person transfers, Web payments, stored–money payments, micro–payments, etc., based on their bank accounts, credit or debit cards, or pre–paid accounts.

Mobile Micro–Loans

This application supports inquiring, applying, managing, and using micro–loans, accessing the system and performing all those operations by using mobile phones.

Mobile Remittance

Wallet also supports performing international financial transfers by senders as well as receivers, located in two different countries, both using mobile phones.

Mobile Payments (Over-The-Counter)

This feature uses money stored in the wallet to pay merchants, transportation and other proximity (over-the-counter) payments, using NFC protocol.

Mobile Ticketing

With this mobile application users may inquire, select and purchase various tickets, store them in the Wallet and later use them at the entrance of show facilities using NFC protocol.

Mobile Parking

Wallet stores registration number of the owner's car so it may be used to pay parking fees using mobile phones.

Mobile Promotions

Wallet may store various coupons, gift cards, various bonus tickets and other benefits and thus supports mobile marketing and promotions.

Mobile Government Services

This application enables Governments to distribute and enables population to receive and use various Government subsidies and payments.

Additional Information

SETECS Mobile Technologies, Inc.

Sead Muftic
President/CEO
Tel: +1–240–535–2095
E-mail: sead.muftic@setecs.com
mobile.setecs.com

Local Partner