The Concept of Secure Mobile Wallet

Hao Zhao, Sead Muftic
School of Information and Communication Technologies (ICT)
Royal Institute of Technology (KTH), Stockholm, Sweden
hzhao@fc.dsv.su.se, sead@dsv.su.se

Abstract

This paper describes our concept, design and current implementation of the Secure Mobile Wallet. Mobile Wallet is an application stored in mobile phones providing to subscribers the possibility to perform various mobile financial transactions. In our approach Secure Mobile Wallet is stored and running in the Javacard SIM chip, called UICC. It comprises several Javacard applets supporting several types of financial transactions – mobile banking, mobile payments, mobile commerce, mobile micro–loans, mobile ticketing, mobile promotions, and so on. Secure Mobile Wallet supports over–the-air (OTA) transactions based on SMS, GPRS, or mobile Internet protocols and also over–the–counter (OTC) transactions based on NFC or Bluetooth protocols. For users, messages and data stored in the Secure Mobile Wallet are managed and maintained using both, OTA and OTC, protocols. Security is guaranteed by a combination of symmetric and asymmetric cryptography. As a client's application, the Secure Mobile Wallet is integrated into our larger, secure mobile transactions system – SAFE™.

1. Introduction

Mobile phones are 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 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*. This can be illustrated by several examples: (a) SIM chips vendors – although new SIM chips are based on Java card technology, which may host multiple applications in a SIM chip, currently vendors of SIM chips do not allow dynamic download and updates of SIM chip applications; (b) Network operators – usage, management, billing and communication services available to mobile users are closely determined and controlled by network operators; (c) Mobile Services Providers – currently, mobile services are controlled by service providers and therefore subscribers are not in the situation to select or change those services. 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 [6].

Therefore, another important trend today is migration of mobile technologies, networks and applications towards an *open and service—oriented architecture*.

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. New financial, medical and other mobile applications, handling sensitive data and operations, also require extended security of users and applications. So, the third important requirement and trend in mobile technologies and applications is *the need for stronger security algorithms, protocols, applications and large—scale infrastructure*s that will provide protection of users, communication messages, applications, and their data [2].

2. Secure Mobile Wallet

Open service–oriented architecture for secure mobile transactions is the system that must be

978-0-9564263-7/6/$25.00©2011 IEEE

established as a large scale, secure and complete system comprising several components. It involves mobile network operators, banks, credit card processors, small merchants, Web merchants, and the most important, client users. This paper describes only subscribers' component of that large infrastructure, called Secure Mobile Wallet.

2.1. Significance for Markets

The primary market for the 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 the coverage of mobile networks is almost complete around the globe.

One of the very important initiatives for the described Wallet are so called "un-banked" users. Those are persons (mainly in developing countries) that do not have bank accounts. Telecom companies are especially targeting those customers for their financial transactions. Very important market for Secure Mobile Wallet are applications for un-banked users. Today, banks and telecom operators are very interested to expand their services to that population, but as we are all witnessing, that expansion goes very slowly mainly due to the lack of easy-to-use and readily available products to support such services.

One very important type of financial transactions is international transactions, called *remittance*. Today, especially transactions between developed and developing courtiers are very unstructured, unregulated and un-organized. Many Governments, international organizations, international and national law-enforcement agencies, and finally, end–users are all interested to use simple, secure, and readily available system for international financial transfers, with low fees and quick transfer times. The proposed Wallet could be one of the major incentives to establish such system in the future.

Finally, as suggested in [6], Secure Mobile Wallet can be extended with many new services – functions and internal data, to become truly multi–application UICC platform.

2.2. Possible Approaches to Design and Implementation

To implement Wallet for a mobile phone, there are several possible approaches. One approach is to use "no wallet", i.e. performing mobile transactions by using simple SMS messages. The same approach can also be used with the USSD protocol [3]. SMS messages and USSD are basic services in each mobile network. For mobile transactions users must memorize abbreviated SMS messages of target keywords. Background servers understand those commands and complete the operations according to the requests.

Since the previous two approaches are not so user-friendly, the other possibility is Mobile Wallet as software in mobile phones. This approach provides friendly GUI, so that users can perform transactions very easily and without mistakes. The most important advantage of this approach is application level end-to-end security. With this approach complete and integrated security system, including authentication, authorization, confidentiality and integrity, which is essential for every financial transaction system, can also be provided.

If Mobile Wallet is implemented in software stored in mobile phones, there are in principle two approaches: The first approach is to use Java technology, J2ME, which is today standard component in every mobile phone. Hundreds of thousands of applications for mobile phones, developed through J2ME, are available today on the market. These applications reside in the native memory of the handset or on an extra add–on memory card. The implementation can provide complete functions and very nice GUIs based on features available in Java. Security services, like strong authentication, confidentiality and integrity of messages, can also be provided. This approach is very convenient, but there are certain issues that have to be resolved: 1) Users must personally download and pre-install J2ME application; 2) If the application is stored in the native memory, it is not easy to change handset; 3) There are already some malware modules for mobile devices and they can cause various problems.

The second and much better approach is to use Javacard applet stored in the SIM chip of the mobile phone, called UICC. The code is stored in the chip by telecom vendor, during UICC personalization or over–the–air. Such Javacard application can construct nice GUIs supporting all application functions, and in addition provide also strong security, based on native crypto algorithms available in the chip. Such concept is called Multi–Application Platform [6]. Besides its main role, as Subscriber Identity Module (SIM), multiple other applications, like mobile transactions system, personal identity verification system, and heath care system, can be stored and run in the same UICC card at the same time.

Our research and its main results are focused on solutions directed towards open, dynamic, standardized and secure mobile network environments and applications. One component of that environment is Secure Mobile Wallet, which is described in this paper. The characteristics of this Secure Mobile Wallet 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) [8];
- 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 [7]), 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;
- Secure Mobile Wallet supports standard APDUs and GSM messages for deployment and management of mobile applications; and
- Secure Mobile Wallet communicates with mobile phone and through it with back—end components of service—oriented architecture – network servers for mobile applications, management and security protocols.

The concept of the Secure Mobile Wallet is that it is based on all relevant emerging standards, it provides functionalities of existing mobile phones, but it also extends those functionalities with additional functions and applications, it provides secure environment for users and applications, and it is applicable in open, standard, mobile environments [1].

3. Design of the Secure Mobile Wallet

Our 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 [7]:

- 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.

Our 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) [10]. Following the methodology in [7] all functions are specified in the form of high–level programming APIs and implemented in the form of SAFE Wallet Middleware. Some 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:

Table 1. Bank Account Object

Bank Account Data (Container ID=03, 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(YYYY MMDD)	4

Table 2. SAFE System Data Object

SAFE System Data (Container ID=04, 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(YYYY MMDD)	4
SAFE Server Mobile Number	06	Variable	15
SAFE Server IP Number	07	Fixed	4
SAFE Server Port	08	Fixed	2

Card Command Interface (CCI) is the set of ISO 7816 compliant commands. Wallet middleware translates APIs into those commands and card responses with 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.

4. 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 the FIPS 201 and ETSI standards, these operations may be performed “over–the–counter” (OTC) and also “over–the–air” (OTA) [5]. 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 [8]. 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.

At the moment we did not design and implement OTA Wallet management.

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

4.1. Combination with J2ME Application

In this case, besides Secure Mobile Wallet applets in the UICC chip, we also load into a phone Wallet Application and Wallet middleware implemented as J2ME applications. 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 for all types of mobile phones.

4.2. SIM Chip Application

In this case, Secure Mobile Wallet is the only software loaded in a SIM chip of a mobile phone. Loading is performed as described earlier. In this case, Secure Mobile Wallet uses proactive commands to communicate with the terminal device [4]. Using proactive commands Secure Mobile Wallet can implement all functions using APIs provided only 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 a SIM chip and since users insert SIM chip into the handset, Secure Mobile Wallet is ready. No any pre-installations are needed.

The other technology we used for alternative implementation is WIB [9]. In this case Wallet does not use proactive commands but special interface between itself and mobile phone.

4.3. Near–Field Communications (NFC) Application

Our Secure Mobile Wallet works with both, contact and contactless, protocols. When used in combination with 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.

5. Security

Secure Mobile Wallet has strong security protecting for data, whenever they are stored in a phone or transferred over-the-air. This is achieved using security features of a SIM card so it is impossible to access data stored in the card illegally. Besides that, in our approach PKI infrastructure is chosen to protect data when they are transferred through GSM and Internet.

Another important security issue is the integrity of data. Roll-back and backup mechanisms will be designed and implemented in Secure Mobile Wallet. They can prevent the data losing correctness when accidents happen, i.e. the mobile phone crashes and communication through networks fails.

6. Conclusion

Our Secure Mobile Wallet is the product belonging to the latest technology trends in mobile communications and IT security. As the client application of the larger system, SAFE^{TM}, Secure Mobile Wallet will introduce convenience, functionality and security in financial mobile transaction. The aim of the design is to provide people a more flexible way to use cash and credit cards securely. To implement it, OTA and OTC protocols are used as communication channels and the SIM/UICC SIM card which is actually a smart card in the mobile phone is selected as the container to hold and run the application. The Secure Mobile Wallet may be either a Javacard applet or a SMARTTRUST wiblet but both can exploit the security advantages of the smart card to guarantee the safe of the data during storage and communication.

7. Future Work

Our research and development in the near future will include:

- Developing WIB version Secure Mobile Wallet
- Extending Secure Mobile Wallet functions to support additional financial transactions and applications;
- Design and implementation of a large–scale m–PKI that will support certificate functions for mobile devices and applications;
- Design and implementation of a m-PKI client in the UICC, so that all certificate functions can originate in the UICC;
- Security for communication messages bases on a combined use of secret key and public key cryptography, with all security functions performed inside the UICC; and
- Secure OTA management of applets and data in the UICC.

8. References

[1] Article, "*SETECS eyes market with security software*", East and Central African Business Mirror, May – June 2009

[2] Baribea, S., "*Your Bank in Your Pocket*", Washington Post, January 2010

[3] ETSI, "*Digital cellular telecommunications system(Phase 2+); Unstructured Supplementary Service Data (USSD) - Stage 1",* ETSI TS 100.625

[4] ETSI, "*Smart Cards, Card Application Toolkit (CAT)(Release 8)",* ETSI TS 102.223 V 8.2.0

[5] ETSI, "*Smart Cards, Remote APDU structure for UICC based Applications*", ETSI TS 102.226

[6] Lenhart. G., "*The Smart Card Platform*", ETSI Technical Committee Smart Card Platform, http://portal.etsi.org/scp/summary.asp (Access date: 23 September 2009)

[7] NIST, "*Federal Information Processing Standard (FIPS 201): Personal Identity Verification (PIV) System*", www.nist.gov (Access date: 17 November 2009)

[8] SETECS Inc., "*OneCARD System*", Internal documentation, www.setecs.com (Access date: 16 June 2010)

[9] Smart Trust WIB^{TM}, www.smarttrust.com (Access date: 27 September 2010)

[10] Zhang, F., "*Secure Applications for Financial Environments (SAFE) System*", Licentiate thesis, Royal Institute of Technology, Stockholm, Sweden, June 2010