Design and Implementation of a Mobile Transactions Client System: Secure UICC Mobile Wallet

Hao Zhao, Sead Muftic
School of Information and Communication Technologies (ICT)
Royal Institute of Technology (KTH)
Stockholm, Sweden

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 module. The Wallet comprises several Javacard applets supporting several types of financial transactions – mobile banking, mobile payments, mobile commerce, mobile micro–loans, mobile ticketing, and mobile promotions. 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. Users, messages and data stored in the Secure Mobile Wallet are managed and maintained using both, OTA and OTC, protocols. Security is supported by Integrated Security Platform, which is a separate application providing security services to other applications. Integrated Security Platform is the implementation of USSM concept, specified by ETSI. As a client's application, Secure Mobile Wallet is integrated into our larger, secure mobile transactions system.

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 [1].

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 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

Primary markets for Secure Mobile Wallet are telecom and banking markets. Secondary markets are Web services providers and alternative financial services providers. Telecom market is one of the largest and the fastest growing international market, 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 target audiences 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 is 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.

Another 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 [1], 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 as an application 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 usually basic services in each mobile network. For mobile transactions users must memorize abbreviated SMS messages or special 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 almost every smart 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 [1]. 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 described in this paper 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) [4];
- 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 [5]), 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 module, 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.

Distinctive features of our 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 [6].

3. Design of the Secure Mobile Wallet

Our Secure Mobile Wallet is a set of Javacard applets loaded in the UICC module of mobile phones. Following standardized methodology, each applet has its Application Identifier (AID). When designing Javacard applets several aspects must be specified [7]:

- Applet's 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's 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) [7]. Following the methodology in [5] all functions are specified in the form of high–level programming APIs and implemented in the form of Wallet Middleware. Some examples are: *Wallet_store_money(), Wallet_list_transactions(), etc.*

Internal data model is the collection of data objects with attributes and their structure optimized to support 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 (YYYYMMDD)	4

Table 2. Financial system data object

Financial 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 collection of applets) must be loaded into the UICC module 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) [8]. 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 module, 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 [9]. 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 [10]. 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 provides strong security for protection of data, stored in a phone and protection of messages transferred over-the-air. This is achieved using an application called Integrated Security Platform. It is the implementation of the USSM concept proposed by ETSI [11]. Integrated Security Platform is a separate application providing security functions to all other applications in UICC.

5.1. USSM

USSM, *UICC Security Services Module*, is the concept proposed by ETSI as a part of standards for UICC [11]. USSM is defined as a separate application in UICC modules providing general security functions to other UICC applications. For UICC module, as a multi-application platform, several applications may run simultaneously providing different functions to subscribers. The concept of USSM would bring huge benefits to the platform as:

- Decreasing the size of individual mobile applications in UICC;
- Providing standard security services for reliable protection to all UICC applications;
- Making applications developers focus more on application functions; and
- Simplifying the maintenance for mobile applications and security functions.

5.2. Integrated Security Platform

Our Integrated Security Platform is the implementation of the USSM concept in our project. At the same time, it also extends standard concept. Standard USSM is just another mobile application, but in our Integrated Security Platform, it is a complete infrastructure comprising: 1) native runtime environment storing and running mobile applications (UICC module); 2) collection of standard cryptographic components (symmetric and asymmetric cryptographic modules) used for protection of mobile applications and data; 3) additional applications (Javacard applets) providing security functions.

Secure Mobile Wallet uses security services provided by Integrated Security Platform to:

- protect its application and data;
- authenticate subscribers to other mobile transaction components; and
- protect communication contents.

Integrated Security Platform provides security protections to Secure Mobile Wallet with the following functions:

- application-level PINs;
- data encryption;
- FIPS 201 PIV authentications module; and
- Asymmetric and symmetric cryptography functions.

6. Security Functions of Our Integrated Security Platform

6.1. Application-Level PINs

Integrated Security Platform uses PINs for authentication of subscribers to Secure Mobile Wallet.

Integrated Security Platform compares customer's input with predefined values to verify if the customer is authentic. The predefined PIN is stored as Integrated Security Platform private application data. Secure Mobile Wallet invokes PIN functions and according to the returned result activates the application functions or rejects the requests.

Integrated Security Platform defines two PINs: User PIN and Master PIN. User PIN is a four digits number. It provides protection to other Secure Mobile Wallet application functions, data and other security objects stored in the Integrated Security Platform, i.e., certificates. In case that user PIN is verified correctly, the following operations follow:

- Secure Mobile Wallet displays the main menu and activates all functions;
- Integrated Security Platform generates key for decryption of Secure Mobile Wallet application data; and
- Integrated Security Platform activates all other security objects.

User PIN can only be tried three times. If that limitation is exceeded, Secure Mobile Wallet is blocked. User PIN can be changed by customers. To do that, the old PIN must be verified before setting the new PIN.

Master PIN is a six digits number. It is used to reset User PIN. If Secure Mobile Wallet is blocked for wrong User PIN input, with Master PIN customer can reset User PIN. Customers cannot change Master PIN. Once Master PIN is lost, subscribers must contact the application issuer to reset the Master PIN.

Both the User PIN and Master PIN are application level PINs. They are defined and stored in the Integrated Security Platform and used by other applications. All functions including setting, verifying, changing PIN and blocking application are implemented and supported by our Integrated Security Platform. There is nothing with the PINs used in file access control mechanism applied by UICC on-card operating system [12].

6.2. Data Encryption

Data of Secure Mobile Wallet are structured in several independent groups and represented as appropriate data modules. Each data object is implemented as internal buffer of the application. The contents of buffers are not data values in clear, but encrypted data values. This is complementary security measure to prevent bypassing internal access control.

As specified by ETSI, all applications and data are stored in files on the UICC module. Even data defined in other applications is actually represented in those files. ISO7816-4 [13] standard commands for operating files, READ BINARY, UPDATE BINARY and ERASE BINARY, etc., are supported by the UICC module.

For example, some curious person wants to know the subscribers' first name. He/she can send using OTA protocol READ BINARY command to application files containing first name. Then the contents of the file is sent back. From analyzing the contents, the first name and other interesting information can be discovered. Another example is that an application in the UICC module wants to know the account information from another application in the same UICC module. From the 'bad' application point of view, another application is just a collection of files stored on the chip. The hacker reads another application files by sending file operating commands. In that way all data values from another applications can be retrieved.

To prevent such problems very strict access control rules are applied to files in the UICC module, compliant to the ETSI 102.221 standard. Without the correct PIN accessing internal files is prevented. Access control mechanism makes UICC module logically structured into several separate and mutually isolated areas for different applications. But if the PINs are lost, caused by lapse from application issuers, for example, the access controls mechanisms are bypassed. Another case is that if an application is activated by subscribers with correct PINs, all security conditions for operating files of this application are satisfied. At this time if some other applications running simultaneously intend to look inside the files for bad purposes, they will succeed. For Secure Mobile Wallet, data stored inside applications are very sensitive and related to subscribers' interests quite closely, i.e., credit card number and CVV. Loss of such data would cause serious damage to subscribers. To prevent that, another layer of security protection is added to the Secure Mobile Wallet. That is encryption of data. Therefore even if access control mechanism is bypassed confidentiality o data is guaranteed.

Each time Secure Mobile Wallet is initiated, a temporary buffer is created in the application. When some Wallet data object is used, decryption of data is performed first and the result is stored in the temporary buffer for further use. This temporary buffer is cleaned when Secure Mobile Wallet is closed. All cryptographic functions are performed inside the UICC module and because of those security features, it is impossible for other applications to access and read the plaintext of data object in UICC RAM without appropriate interfaces.

Integrated Security Platform uses symmetric algorithms for encryption and decryption of data for other applications, including Secure Mobile Wallet. The algorithms used to encrypt data are listed according to their priority:

1) AES-CBC: encrypt 16-byte data block with 16-byte key using AES algorithm in CBC mode. 16-byte Initial Vector is used;
2) 3-key triple DES-CBC mode: encrypt 8-byte data block with three 8-byte keys. 8-byte Initial Vector is used;
3) AES-ECB: encrypt 16-byte data block with 16-byte key using AES algorithm in ECB mode;
4) 3-key triple DES-ECB mode: encrypt 8-byte data block with three 8-byte keys.

For AES algorithms data block must be 16 bytes. Therefore padding method is required, that works as follows:

- if the size of the data block is a multiple of 16 bytes, no padding is needed;
- if the size of the data block is not a multiple of 16 bytes, the difference is padded by a byte array started with hex value 80. After the first byte all others are hex value 0.

DES algorithm for both CBC or ECB mode uses ISO9797 method 2 [14] to pad the data block. That is:

- if the size of the data block is a multiple of 8 bytes, a byte array started with hex value 80 and followed with seven zeros is added to the end of the data block;
- if the size of the data block is not a multiple of 8 bytes, the difference is padded by a byte array started with hex value 80. After the first byte all other bytes are hex value 0. Finally, another 8-byte zeros are added.

6.3. Key Generation

The keys used to encrypt/decrypt data are generated from user's PIN in the UICC module. Each time the correct user PIN is given, a temporary buffer is created. A key generated from user's PIN is stored in the buffer for decryption of application data. When Secure Mobile Wallet is terminated, temporary buffer is cleared. All operations are performed by modules in the Integrated Security Platform. The process of generating a key is the following:

1) pad four digits PIN represented by 4 bytes with padding approach used in ISO9797 method 2 [14] and shift one digit. A 16-byte data block is output;
2) pad the new four digits array with padding approach used in ISO 9797 method 2 [14] and shift one digit. Repeat the process three times until a 48-byte data blocks is created;
3) combine the data blocks generated in steps 1 and 2 as a 64-byte data block;
4) hash the data block. A 20-byte hash code 1 is created;
5) reverse the data block and hash it. A 20- byte hash code 2 is created;
6) combine hash code 1 and hash code 2 as a 40-byte data block.
7) use the 40-byte data block as key to encrypt the 64-byte data block generated in step 3. A 64-byte cipher result is created;
8) hash the cipher result. A 20-byte hash code 1 is created;
9) reverse the cipher result and hash it. A 20 -byte hash code 2 is created;
10) combine hash code 1 and hash code 2 as a 40-byte encrypting key.

Selection of encryption and hash algorithms used in step 7 is up to the chip capability. The options are listed below according to their priority:

1) AES-CBC mode. The first 16 bytes of the 40-byte data block are used as key and the second 16 bytes are used as Initial Vector;
2) 3-key triple DES-CBC mode. The first 24 bytes of the 40-byte data block are used as the keys and the following 8 bytes are used as Initial Vector;
3) AES-ECB mode. The first 16 bytes of the 40-byte data block are used as the key;
4) 3-key triple DES-ECB mode. The first 24 bytes of the 40-byte data block are used as the keys.

Hash Algorithms for step 4 and 8 are:

1) SHA-1: input 64 bytes data block and output 20-byte hash code;
2) SHA-0: input 64 bytes data block and output 20-byte hash code.

The final result is a 40-byte data block. Use of the data block as key is same as in step 7.

6.4. Authentication Module

FIPS 201 (PIV) standard is used in our Integrated Security Platform as authentication module for subscribers to off-card components. FIPS 201 has been established by the National Institute of Standards and Technology (NIST). PIV applet and smart card represent reliable identity verification token with demographic data, four certificates, two fingerprints, and facial image [5].

In our Integrated Security Platform, PIV is implemented as a separate application (Javacard applet). All authentication objects of subscribers are stored in the PIV applet. Other applications, including Secure Mobile Wallet, use that applet for authentication functions.

6.5. Other Security Functions

Secure Mobile Wallet works together with other components in a larger mobile financial transaction environment. Security and reliability of the communication is guaranteed by application level communication protocol. Since Secure Mobile Wallet is the client side of our larger mobile transaction system, the protocol should be predefined to work in combination with other components. In order to support the protocol, several cryptographic functions are provided in the Integrated Security Platform. They include:

1) RSA algorithm. Used for asymmetric encryption and decryption and signing of messages;
2) symmetric cipher algorithms which have been introduced in section 6.2;
3) signature with symmetric cipher algorithms, i.e. AES, DES, etc.; and
4) hash algorithms: SHA-0 and SHA-1.

7. Conclusions

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, Secure Mobile Wallet introduces convenience, functionality and security for 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 card which is actually a smart card in the mobile phone is selected as the container to store and run the application. The Integrated Security Platform, as a separate application, exploits the secure advantages of the smart card providing security functions to other applications in the multi-application platform through interfaces guaranteeing security of data during storage and communication.

8. Future Work

Our research and development in the near future will include:

- Developing WIB version of the Secure Mobile Wallet
- Extending Secure Mobile Wallet functions to support additional financial transactions and applications;
- Design and implementation of PKI based application-level communication protocol using Integrated Security Platform cryptographic interfaces protecting transmitting data; and
- Secure OTA management of applets and data in the UICC module.
-

9. References

[1] Lenhart. G., "*The Smart Card Platform*", ETSI Technical Committee Smart Card Platform, http://portal.etsi.org/scp/summary.asp (Access date: 23 September 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] SETECS Inc., "*OneCARD System*", Internal documentation, www.setecs.com (Access date: 16 June 2010).

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

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

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

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

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

[10] Smart Trust WIB™, www.smarttrust.com (Access date: 27 September 2010).

[11] ETSI, "*Smart Cards, USSM, UICC Security Service Module; Stage 1"*, ETSI TS 102.266 V 7.1.0.

[12] ETSI, "*Smart Cards; UICC-Terminal Interface; Physical and logical characteristics (Release 9)*", ETSI TS 102.221 V 9.0.0.

[13] ISO, "*Identification cards-Integrated circuit cards-Part 4: Organization, security and command for interchange*", ISO7816-4, second edition.

[14] ISO, "*Message Authentication Codes (MACs)-Part 2: Mechanisms using a dedicated hash-function*", ISO9797-2, edition 1.

