KTH Information and
Communication Technology

SECURE APPLICATIONS FOR FINANCIAL ENVIRONMENTS (*SAFE*) SYSTEM

A Dissertation submitted to
the Royal Institute of Technology (KTH)
in partial fulfillment of the requirements for
the degree of Licentiate of Philosophy

By

Feng Zhang
fengz@dsv.su.se

School of Information and Communication Technologies
Royal Institute of Technology
Forum 100, SE-16440 Kista, Sweden

March 2010

Summary

One of the main trends in the IT field today is to provide more mobility to existing IT based systems and users. With this trend, more and more people are using mobile financial transactions due to a widespread proliferation of mobile phones and wireless technologies. One of the most important concerns with such transactions is their security. The reasons are based on weaknesses of wireless protocols and additional requirements for handling of financial data. These aspects make mobile financial transactions and applications even more vulnerable to fraud and illegal use than similar transactions performed over fixed networks.

There are two important aspects related to security in mobile environments. First, security features provided by the communication protocols, such as GSM, SMS, Bluetooth, Mobile Internet, etc. are not adequate. Some security algorithms used by these protocols have even been broken, what requires upper layer applications to provide comprehensive protection in order to compensate the shortcomings of a transportation layer. Second, mobile devices have limited capabilities, limited processing speed, limited storage, etc, so that many security mechanisms are not suitable for mobile environments. Therefore, new, effective, lightweight and flexible security solutions are required.

In order to solve these two groups of security issues, in this research we created a service-oriented security infrastructure for mobile financial transactions and applications. Based on this infrastructure, we also designed and implemented a system, which is called *SAFE* (Secure Applications for Financial Environment), that represents a secure, convenient and reliable large–scale infrastructure for mobile financial transactions. The components of the system are Secure Mobile Wallet and three *SAFE* servers: Communications (Gateway) Server, IDMS (Identity Management System) Server, and Payment Server. Those core infrastructure components with secure messages exchanged between them provide a number of secure financial services. These services may be used for various types of mobile transactions: m–Banking, m–Commerce, m–Ticketing, m-Parking, m–Loans, etc. all supported by additional Application Services Provider servers, connected to the *SAFE* security system. This report gives the details of the concept design and current implementation of the *SAFE* system.

The structure of this report is the following:

In Chapter 1 we give the background and current situation with mobile financial transactions. Then, we overview the problems in existing mobile financial environments and list related literature. Motives and objectives of our research are given at the end of this chapter.

In Chapter 2 we give a brief illustration of the *SAFE* system and all the transactions supported by it. The transactions are categorized into four groups: mobile banking (m-Banking), mobile commerce (m-Commerce), mobile parking (m-Parking) and mobile ticketing (m-Ticketing).

In Chapter 3 we give the analysis of system requirements, which contain two parts: security requirements and deployment requirements.

In Chapter 4 the details of security infrastructure of the *SAFE* system are shown. We also describe security management operations supported by this infrastructure, such as registration of participants, certificates management, etc.

In Chapter 5 we give the details of secure applications mentioned in Chapter 2. This chapter describes all the functions, message formats for every transaction, and security features of the messages.

In Chapter 6 current implementations and functioning of the *SAFE* system are described.

Chapter 7 summarizes thesis contributions through publications and the solutions to the problems illustrated in Chapter 1.

Chapter 8 presents conclusions of this thesis and outlines our planned future work.

Keywords: Mobility, Mobile Phones, Financial Transactions, Security

Acknowledgement

I would like to take this opportunity to express my appreciation to my supervisor Prof. Sead Muftic for giving me the chance to do my Ph.D study under his supervision and for all his encouragement and patient guidance. Not only did I learn a lot from him, I also tremendously enjoyed my time as his student. Thank Prof. Louise Yngström for giving me study advices.

Also, many thanks to my colleagues: Dr. Matei Ciobanu Morogan, Abdul Ghafoor Abbasi, Muhammad Awais Shibli, Dr. Gernot Schmoelzer, Chenchen Yuan and many others for enormous help with various aspects of my research. It was my great honor to work with them, what also brings so much fun in my studies.

Special thanks to my parents for your persistent support and encouragement. I owe you most of this work and my results achieved so far.

This research was funded by the Secure Applications for Financial Environment (*SAFE*) project from VINNOVA and SPIDER combined.

To my parents

Table of Contents

List of Figures

List of Tables

Chapter 1:

Introduction

At the very beginning of human society, people exchanged the goods with mostly equal values. Later, the concept of money was introduced, so people started to use money for almost all kinds of transactions. Because of industrial revolution and globalization, commercial transactions have rapidly increased. However, exchanging a large amount of money is a risky task. As a solution, people started using banking facilities for financial transactions. At present, banks provide attractive services for effective money transactions. However, many problems related to bank transactions are remaining. In developing countries, these problems have become even worse.

In many rural areas, there are no bank branches or bank facilities, such as ATMs. If people living there need to use bank facilities, they have to travel far away to the nearest town or city, what is inconvenient and influences the development of local economies. However, requirements for using bank facilities in rural areas are rapidly increasing. Every year migrants send billions of money back to their families, most of them living in rural areas. This is a large industry, but only some big companies, such as Western Union, are capable to deal with these transactions. The worse thing is that most of these companies do not have branches in rural areas. In addition, implementing and using IT-based solutions in developing countries is also a big challenge, due to poor communication and IT infrastructure, a bottleneck for expansion of bank facilities.

On the other hand, during past several years, wireless industry has been experiencing dramatic growth. Functional capabilities of mobile telephony have been rapidly expanding and have extended their usage well beyond the classical communication applications (telephone calls and short messaging). There is mounting evidence of positive financial, economic and social impacts of those technologies all over the world. Although the IT infrastructure is usually undeveloped in rural areas, remarkably in most of the developing countries, mobile telecommunication sector achieved a rapid expansion in recent years. [1] Therefore, mobile communication infrastructure could be used as a good deployment platform for electronic banking and financial systems. As the result, the concept of mobile commerce (m-Commerce) comes up. Mobile commerce is any transaction, involving the transfer of ownership or rights to use goods and services, initiated and/or completed by using mobile access to computer-mediated networks with the help of an electronic device [2]. In other words, all transactions in an m-Commerce system are conducted by using a mobile handset, e.g. a mobile phone (cell phone), a Personal Digital Assistant (PDA), a smart phone or some other mobile equipment. It is considered as an innovative way to improve existing paper-based financial system into cashless systems. Nowadays financial institutions put a lot of efforts to move payment transactions, such as transfers or bill payments, to electronic form instead of a paper form. In the meantime, thanks to the considerable decrease of the cost of mobile phones and mobile services, more and more people can afford at least one mobile phone, even in rural areas in the world. According to the GSMA, an industry group, the total number of subscribers in the world will reach 6 billion by 2013 [3].

Nowadays there are several systems in use offering mobile transactions, such as MTN in Uganda, M-PESA in Kenya, Smart Money in the Philippines, Wizzit in South Africa, etc. These systems achieved great successes in the field of mobile financial transactions and mobile banking. They introduced the concept of mobile-money or E-money linked to a mobile-money account, which is a virtual account registered under customer's mobile phone number. Some provide specific SIM chips, with preloaded applications in it. By using the applications preloaded in a SIM chip, customers could conduct transactions, such as transferring airtime or E-money between two mobile-money accounts or withdrawing/depositing money through authorized agents.

1.1 Problem Statements

There are several issues related to mobile financial transaction systems. One of the most important for mobile transactions is their security. The reasons are based on weaknesses of wireless protocols and their handling of financial data. These aspects make mobile financial applications even more vulnerable to fraud and illegal use than similar transactions performed over fixed networks.

Wireless technology has achieved great development during the last several years and it is extremely complex, compared with wired networks. Unfortunately, wireless engineers are usually not security experts and they all consider that security will be added later, if it is needed. This is not a good approach, since security must be integrated with wireless technologies. Under these circumstances, there are many security issues with wireless networks, which make hackers consider them as the weakest point in the communication chain of mobile financial transactions.

Since GSM network is the most popular environment for mobile transactions, we first analyze some threats and security issues in those networks. Five acknowledged attacker capabilities influence the security in GSM networks, shown in Table 1. The first capability is the easiest to conduct [4]. What is new, in December 2009, a German computer engineer announced that he had deciphered and published a secret code used to encrypt most of the world's digital mobile phone calls, saying it was his attempt to expose weaknesses in the security of global wireless systems [5]. Therefore, we may say that the security in existing GSM networks is not adequate.

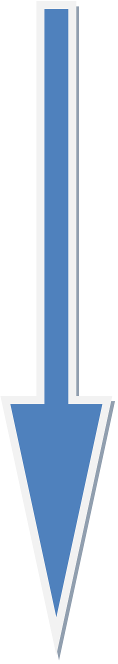
Difficulty to counter 	**Eavesdropping** The capability of an intruder to intercept traffic and signaling information transferred to other users. The required equipment is a modified mobile phone.
	Impersonation of a User This is the capability to send rogue data and/or signaling messages to the network with the intent of making them appear as originating from another user. This also requires only a modified mobile phone.
	Impersonation of the Network This is the capability to send rogue data and/or signaling messages to another user with the intent of making them appear as coming from a genuine network. This requires a modified BTS.
	MITM – Man-In-The-Middle Attack This is the capability of an attacker to insert itself between the network and the legitimate user in order to eavesdrop, modify, delete, re-order, re-play and spoof signaling data between the two parties. This requires a modified BTS in conjunction with a modified mobile phone.
	Network Authentication Compromise The intruder possesses a compromised authentication vector (challenge-response pairs, cipher keys, integrity keys, etc.)

Table 1. Attacker Capabilities

Second, mobile messaging market is rapidly growing and it is becoming a large profitable business for telecom operators, especially in developing countries. Most of these mobile transaction systems utilize SMS service as their communication system. However, there are several issues with SMS messages:

a. **SMS Spam**: Spamming is an action where the subscriber receives an unsolicited message, i.e. the one the subscriber did not want to receive. Spam SMS may take different forms including: commercial information, advertisement, bogus content and other messages generally intended to invite a response from the receiver.
b. **Flooding**: Flooding is the case when a large number of messages are sent to one or more destinations.

c. **SMS Fraud**: Nowadays there are many fraudsters trying to organize crime or terrorist cells – and they are using SMS fraud to fund their operations. For example, premium rate service (PRS) fraud is the case where the subscriber pays a higher than normal rate for a call in exchange for information (such as adult chat lines). Fraudsters send to subscribers an unsolicited SMS telling the subscribers that they have won a prize and need to call the specified number to collect their prize [6].

d. **Impersonation of a user**: There are some websites, such as https://www.hoaxmail.co.uk/ providing the service that a person, who has paid the fees for their service, can send SMS message from a specific originator to a specific destination. In other words, this person is able to impersonate other users as originators of short messages.

Third, Bluetooth, as a recently proposed standard for local wireless communications of devices such as mobile phones, wireless headsets, printers, cars, etc. is developing rapidly, so that more and more mobile users transfer or share data with each other. However, there are some security issues:

a. **Eavesdropping** – Bluetooth session starts with agreeing about a key by two communication entities and this key is vulnerable to attackers in some circumstances. Attackers can either get the key by exhaustively searching all possible PINs (without interacting with the victim devices) or by Man-in-the-Middle attack [7].

b. **Location Attack** – Attackers are able to determine geographic location of victims, what can be an advantage by some attackers for many illegal purposes.

c. **Vulnerable Cipher** – As Jakobsson and Wetzel mention [6], they conducted several attacks on the cipher, which indicate that the cipher of the Bluetooth is not strong enough.

Fourth, due to 3G and the newest 4G technology, mobile Internet became much more popular than ten years ago. Nowadays, more and more mobile users are surfing Internet by using mobile phones any time, any place. Security issues still exist in mobile Internet even though some users do not care about that. However, for customers who use mobile Internet for financial transactions, security is one of the most important concerns.

The most common security solution used for Internet security today is SSL, which relies on complex combination of public key cryptography, symmetric key cryptography, hash function, digital certificates and digital signatures. There is a security protocol for mobile Internet, a lightweight version of SSL, called Wireless Transport Layer Security (WTLS). WTLS functions very similar to SSL, but with a number of additional characteristics, such as compact coding, datagram support, optimized handshakes, dynamic key refreshing, fast encryption and hashing algorithms, client-gateway rather than client-server coverage, etc [8].

Since it seems that WTLS covers many security issues of mobile Internet, maybe we could use it also for security of financial transactions. The answer is "NO" and the reason is that

WTLS provides only communication security between client devices and WAP gateway. However, most mobile Internet transactions, especially financial transactions, require also security between the WAP gateway and backend Web servers. In other words, for mobile financial transactions end-to-end security is needed. There are two possible approaches to achieve this goal:

a. SSL could be extended between the WAP gateway and the backend Web servers. In this way, client builds WTLS session with the WAP server and sends credential data (for example credit card information) to a WAP gateway in an encrypted format. Gateway decrypts the credential data and uses new SSL session to send it to Web servers. In this case, security relies on the administrative access to the WAP gateway, which is not suitable for financial transactions.
b. Alternatively, the gateway can be hosted by the Web service providers and therefore placed behind the service provider's firewall. This is also not a good solution, because Web service providers do not provide mobile Internet services to all their mobile users. This was the primary focus of our research activities.

Based on all the above, we may conclude that current security solutions at the communication layer in mobile environments are not adequate. Therefore, security at the application layer must be added in order to achieve end-to-end protection for mobile financial environments.

1.2 Related Works

C. Narendiran, S. Albert Rabara, "*Performance Evaluation on End-to-End Security Architecture for Mobile Banking System*" [9]. In this paper, the authors evaluated security issues in mobile banking system and proposed a framework by using PKI to provide end-to-end security. In their framework Online Certificate Status Protocol (OCSP) is used for mobile devices to validate certificates of other entities. However, their framework is designed and implemented only for GPRS networks. They also measured the impact of time on the performance of three-encryption algorithms: RSA, 3DES and AES used in Public Key Infrastructure for calculating time in mobile device for client functionality. From their results, it is shown that: (a) It could be difficult to encrypt the message digest using PIN by RSA based public key algorithm in the mobile phone, but AES works much faster; (b) RSA key algorithm needs more memory; (c) AES algorithm utilizes less computation time and memory for encrypting the user's data and it shows greater performance than the 3DES and RSA algorithms that use public key infrastructure.

Hany Harb, Hassan Farahat and Mohamed Ezz, "*SecureSMSPay: Secure SMS Mobile Payment Model*" [10]. Secure mobile payment model using SMS is introduced in this paper. This model can use symmetric and asymmetric cryptography without the need of trusted 3rd parties or even PKI complexity. It uses a pre-shared key between payer/payee and their banks to encrypt/decrypt SMS messages and it needs mobile devices supporting running J2ME application, which is used to encrypt/decrypt SMS messages. The proposed model involves a payment gateway to connect the payer's and the payee's banks. This payment gateway should store all mobile numbers, whether they belong to the payer's or payee's bank, in order to route transactions based on mobile phone number. Practically speaking, this model is not suitable, since banks usually do not supply SMS service. The most common case is that telecom operators supply SMS service and route the messages to different banks. However, in their proposed model the Gateway knows all the customers' transaction details, which is a serious security issue.

Shahriyar Mohammadi and Hediye Jahanshahi, "*A Study of major Mobile Payment Systems' Functionality in Europe*" [11]. This paper analyzes some of the major mobile payment systems in Europe based on five criteria: Scenarios, Security, Cost, Convenience, and Functionality Requirements. After surveying the mobile payment systems in Finland, Serbia and Germany, the paper gives a framework consisting of six criteria, which can be used for evaluating mobile payment system adoption by customers and merchants.

1.3 Motivations

Based on the problems illustrated in section 1.1, one of the main prerequisites for successful, large-scale and broad deployment of mobile financial applications is their security. Currently, several, mainly SIM chip vendors and banks, offer initial version of such applications for banking transactions either without security or based only on user PINs. These methods not only do not provide satisfactory level of security required for financial transactions, but also create false impression of their security, thus opening possibilities for hackers to exploit their vulnerabilities. When mobile financial transactions are performed internationally on a large scale without adequate security, it is certain that current financial losses due to on-line fraud will be much larger.

On the other hand, even though mobile handsets have achieved dramatic improvements, what makes them not only equipment for telephony, but also a small "computer" with much useful functionality integrated inside, there are still several limitations explained below. There are mainly four types of limitations [12]:

a. **Small screens and low resolutions:** Even though mobile phone vendors are trying to make the screen bigger and bigger, it anyhow cannot be large enough, since mobile device will not be portable or convenient. Screen resolution is another problem.
b. **Input limitations:** Current mobile phones input capabilities are not user-friendly, which leads to slow input, full of spelling errors and inconvenient input methods.
c. **Limitations when accessing Internet:** Due to differences between mobile phone wireless networks and cabled Internet networks and different coding methods, it is difficult to

access ordinary internet Web pages. Most ordinary Internet Web pages are distorted on mobile phone screens. Therefore, in order to enable mobile phones to browse websites, people have to design specific Web pages by using HDML, XHTML etc.

d. **Lack of standardization and compatibility:** There are no standards in terms of communication protocols, functionalities, etc. For example, some countries like US are using CDMA2000, Japan is using W-CDMA and China is trying to use TD-SCDMA. Lack of compatibility is also a big problem for design and deployment of mobile transaction systems. Some mobile phones support E-mail functions, some do not. Even SMS service is not compatible in some countries.

e. **Other limitations:** Some other limitations are limited storage and computing capabilities, limited length of short messages, disabled SSL, etc.

All the limitations listed above represent serious problems for designers of mobile transaction systems. Therefore, a reliable, secure, scalable, interoperable and energy-saving solution is needed for mobile financial transaction environments.

1.4 Objectives of Our Research

The focus of this research was to use mobile technology to solve the problems listed in section 1.1, since more and more people are using mobile financial transactions due to a widespread proliferation of mobile phones and wireless technologies.

Chapter 2:

Mobile Applications of the *SAFE* System

SAFE (Secure Applications for Financial Environment) is the system that performs various financial transactions using mobile phones and other mobile hand–held devices. Current initial versions of similar systems provide simple client–to–bank transactions [13-15]. *SAFE* system supports transactions with multiple banks, direct client–to–merchant payments, person–to–person transactions, and other non–banking mobile applications. In addition, the distinguished feature of the system is its strong security for users, their transactions and applications. This chapter illustrates the design details of the *SAFE* system.

One of the main features of the *SAFE* system is to manage and use mobile pre–paid accounts (PPAs). These accounts may be used to deposit and withdraw cash and also for various mobile payments. The system is based on secure servers for various other mobile services described below, so that subscribers with pre–paid accounts are able to use those accounts to pay for those services. *SAFE* system supports various types of transactions, which can be categorized into four groups: (1) mobile banking, (2) mobile commerce, (3) mobile ticketing and (4) mobile parking. Mobile banking and mobile commerce are mainly financial applications, while mobile parking and mobile ticketing are applications that use *SAFE* system for payments.

The objectives of the design of the *SAFE* system were:

a. to *establish* and *manage* pre–paid accounts (PPAs) for individuals (*SAFE* agents and customers) and for business entities (service providers and merchants);
b. *to use* those PPAs for financial transactions – Point–of–Sale (PoS) payments, cash deposits/withdrawals, and account transfers. PoS payment transactions are *purchases* of goods, services, and telecom air–time with merchants using *over–the–counter (OTC)* or *over–the–air (OTA)* transactions. *Cash deposits* and *withdrawals* (cash-in and cash-out) are transactions to/from PPAs or real bank accounts (RBA). Account transfers include debits or credits from own PPAs to/from other PPAs and also to/from own RBAs;
c. to *issue* and *manage* biometrics smart cards for system administrators, *SAFE* agents, customers, and merchants;
d. to use those cards for *authentication, authorization* and *payment* against PPAs.

The functions (a), (c) and (d) are described in Chapter 5. This chapter gives the details of various applications supported by the *SAFE* system.

2.1 Mobile Banking (m-Banking)

Mobile banking (m-Banking) involves use of a mobile phone or another mobile device to perform various financial transactions with a client's bank account. Mobile banking is one of the newest approaches to provision of financial services through GSM or wireless Internet network, made possible by the widespread adoption of mobile phones, even in low-income countries. The rollout and functional capabilities of mobile telephony have been rapid and have extended usage well beyond classical (telephone calls and short messaging) applications. There is mounting evidence of positive financial, economic and social impacts of those technologies all over the world.

2.1.1 Transactions and Players

Mobile banking supports broad range of financial transactions, such as:

- Management of accounts
  - Open account
  - List account status
  - List transactions
- Cash deposits and withdrawals using client's own account with "digital" ATMs,
- Cash deposits and withdrawals using client's own account based on the concept of "Mobile ATM" in developing countries,
- "Digital cash" deposits and withdrawals using client's own account with "digital" ATMs,
- Transfer of cash between user's own accounts in the same or in different banks,
- The ability for third parties to make deposits into a user's account (employer, family member, merchants, loan provider or a micro-finance organization in developing countries).

The participants in those transactions are the following:

Banks – perform registration and certification of individuals and provision of financial services

Clients – individuals initiating or receiving transfers as the result of financial transactions

2.1.2 Mobile Banking System Components

The system is organized in the form of a large–scale, federated security architecture. The components of that architecture are various types of servers and (static or mobile) workstations.

There are two types of servers in the mobile banking system:

> ***Gateway Servers*** – specialized servers that supports various secure communication functions, used as the "front–end" (proxies) to Bank Servers
>
> ***Bank Servers*** – internal servers in banks performing standard banking applications and transactions

The following stations are used in the *SAFE* system:

> ***Client Mobile Stations*** – those are mobile phones enhanced with secure applications
>
> ***Client Web Stations*** – those are standard PCs used by clients to perform financial transactions from static locations (home, offices, etc.)

The functions of these components and transactions between them for individual applications are described in the next section.

2.1.3 Usage and System Operations

This section contains diagrams and short description of various mobile transactions listed in section 2.1.1.

◆ Cash Dispensing: Mobile and Static ATM

Mobile and static ATM are two innovative approaches to dispensing of cash, especially suitable in regions where there are no standard banking ATMs. With "Mobile ATM", cash will be distributed by the specialized bank agents, located areas without standard ATMs. They will dispense cash upon receipt of the authorization messages from bank servers. The procedure is equivalent to static ATMs, where cash will be dispensed by post offices, eventually merchants, and other cash distribution agencies.

The sequence of steps and exchange of messages for this transaction are the following: Customer who needs cash comes to the location of the Mobile (Bank Agent) or Static ATM. Using his/her phone, the customer sends Cash_Request message to the specialized *SAFE* Server. The Server has direct connection into the banking network and verifies the status of the customer's account. If the confirmation is received from the bank, *SAFE* Server sends Cash_Confirmation message to the Bank Agent or corresponding cask dispensing agent (like Post Office). When the message is received, cash can be given to the customer. The sequence of messages is shown in Figure 1.

Transactions of the Mobile-ATM system are explained below. In order to perform a transaction, a customer with a mobile phone comes to the Mobile-ATM agent, who has another mobile phone. Figure 2 illustrates messages in the Mobile ATM system.

1. A customer visits a Mobile-ATM agent and sends a secure SMS message to the bank (withdrawal request) with Mobile-ATM agent's (Mobile-ATM) phone number and requested cash amount.
2. The bank verifies status of the customer's account and if OK sends an authorization SMS message to the customer together with a confirmation number (a random number).
3. At the same time, the bank sends a payment authorization SMS message to the Mobile-ATM agent (Mobile-ATM) together with a transaction number (a random number which is different from the confirmation number).
4. The customer tells the confirmation number to the Mobile-ATM agent (Mobile-ATM).
5. The Mobile-ATM agent (Mobile-ATM) sends a confirmation SMS message to the bank together with the transaction and the confirmation number.
6. The bank transfers the amount from the customer's account to the Mobile-ATM agent's (Mobile-ATM's) account and sends a transaction confirmation SMS to the Mobile-ATM agent.
7. The bank also sends a transaction confirmation SMS message to the customer.
8. Mobile-ATM agent hands in the money to the customer.

Two random numbers are used in all transactions to order to provide non-repudiation. Moreover, it is a strong evidence to confirm that the transaction has been fully completed.

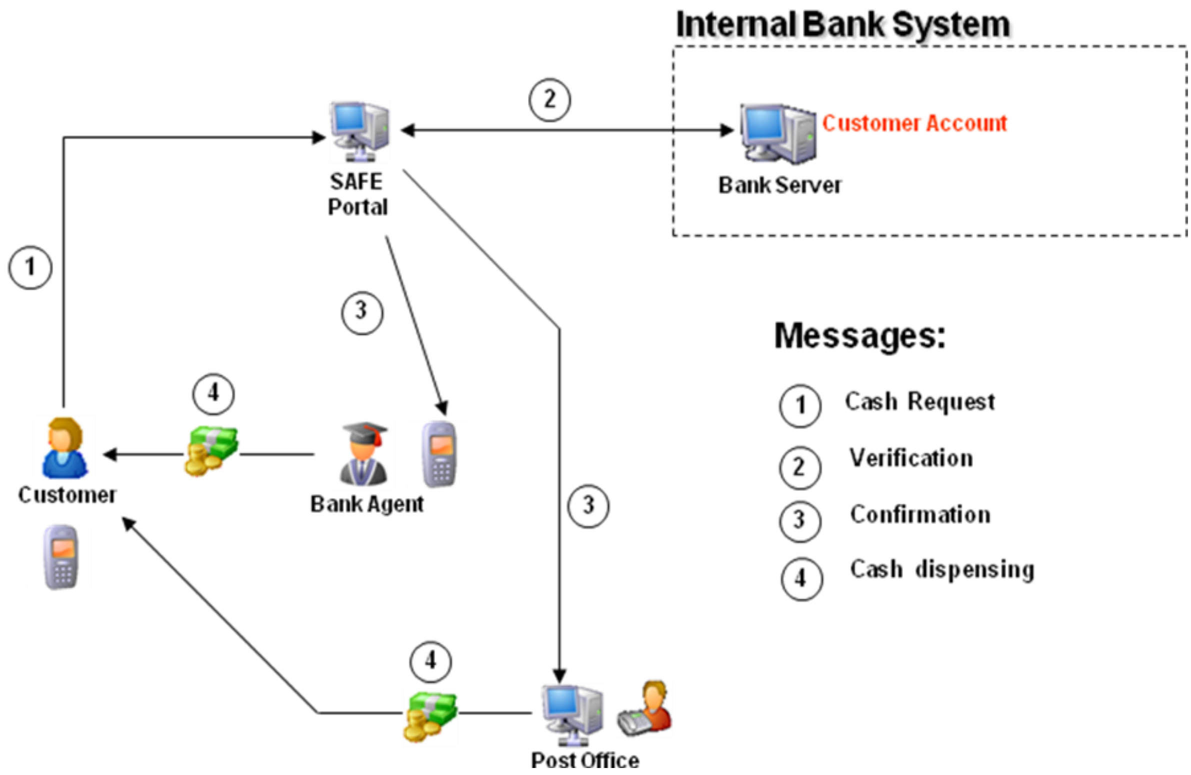


Figure 1. Cash Dispensing Transaction Messages: Mobile and Static ATM

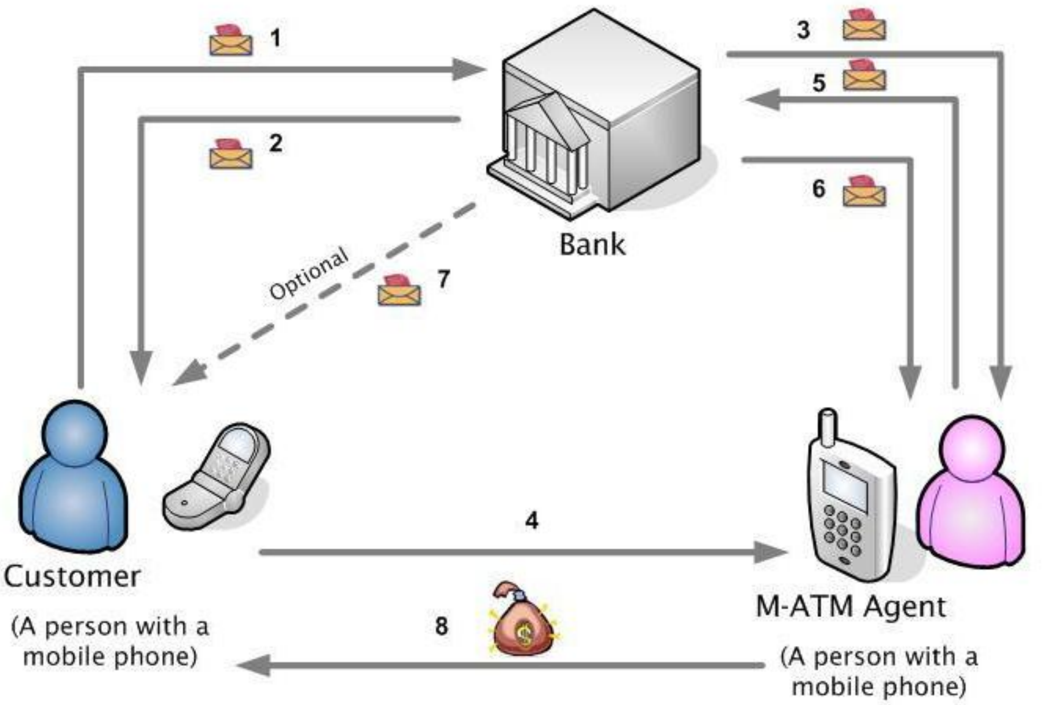

1
2
3
5
6
7
Optional
Bank
4
8
Customer
(A person with a mobile phone)
M-ATM Agent
(A person with a mobile phone)

Figure 2. Messages in the Mobile-ATM [13]

- Account-to-Account Transfers Transaction

This transaction may be performed between two personal accounts or between a personal and a corporate account. In both cases one customer is the sender (initiator of the transactions) and the other customer is the recipient. This transaction may be used for remittance, personal payments, bill payments, etc. It may be performed between two customers with accounts in the same bank or with accounts in different banks.

If the two customers have accounts in the same bank, then the sender initiates the transfer of certain amount of money from his/her account to the account of the recipient. Transfer_Request message is sent from the sender's mobile phone to the *SAFE* server, which, after verification and effective transfer performed by the bank, informs the recipient about the transfer.

If recipient's account is in another bank, then after receiving authorization for the transfer from the sender's bank, sender's *SAFE* server will inform recipient's *SAFE* server about the transfer. Recipient's *SAFE* server will notify recipient's bank and the recipient.

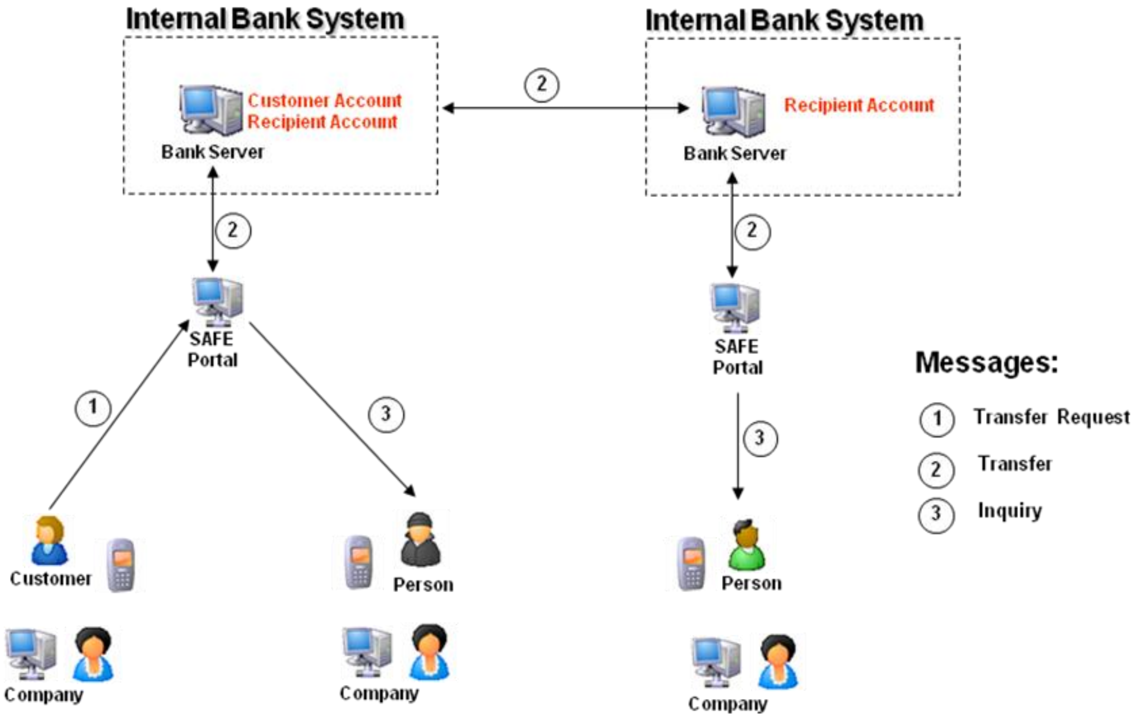


Figure 3. Personal Account-to-Account Transaction Messages

- Application and Administration of Loans

SAFE system also supports various transactions for administration of loans. Those could be mortgages, home equity loans, or micro–loans in developing countries. Applicants may apply for a loan and after approval, loan provider may transfer the amount to the applicant's account using account–to–account transaction, described in the previous section.

Applicants may also administer their loans, such as reviewing the status of the loan, payment schedule, initiating payments, etc. For this transaction, the messages are the following: applicant applies for a loan. Applicant's *SAFE* server will pass the application to the *SAFE* server of the loan provider. When approved, applicant's *SAFE* server and bank server will be notified and the loan will be activated. Finally, the applicant may also use various transactions with its *SAFE* server to administer the loan.

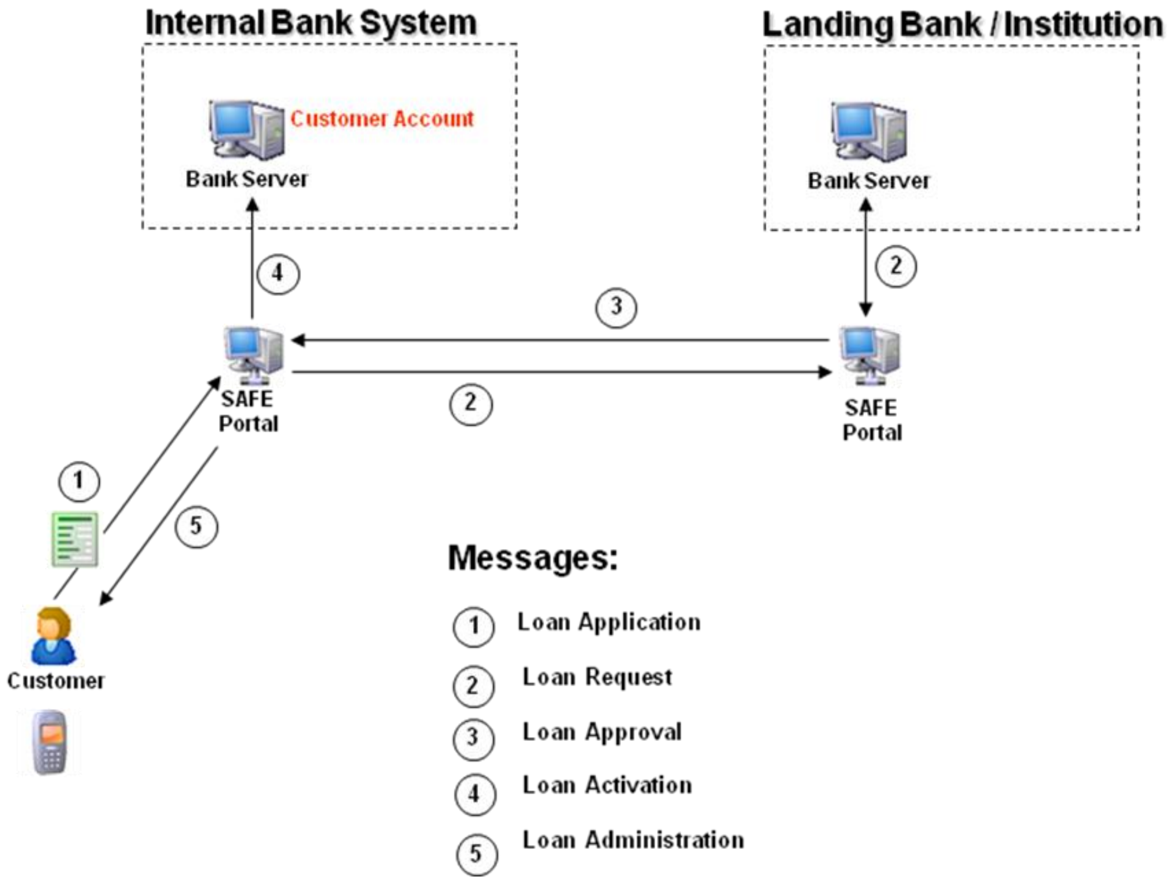


Figure 4. Loan Application and Administration Transaction Messages

2.2 Mobile Commerce (m-Commerce)

Mobile-Commerce is the latest concept of enabling financial transactions, such as mobile payments using mobile phones and hand-held devices. With the rapid development of the society, m-Commerce applications play a vital role. This section describes mobile commerce transactions supported by the *SAFE* system. m-Commerce are mainly payment transactions and digital cash dispense transaction (cash in/ cash out).

2.2.1 Transactions and Components

Mobile commerce supports broad range of financial transactions, such as:

- Registration of merchants and customers,
- Enrollment of merchants and customers for issuance of the *SAFE* smart card,
- Opening of merchant's and customer's PPAs associated with cards,
- Accepting OTC payment transactions using *SAFE* smart cards for authentication of customers,
- Accepting cash as deposits to customers' PPAs.

The components of *SAFE* m-Commerce system are shown in Figure 5.

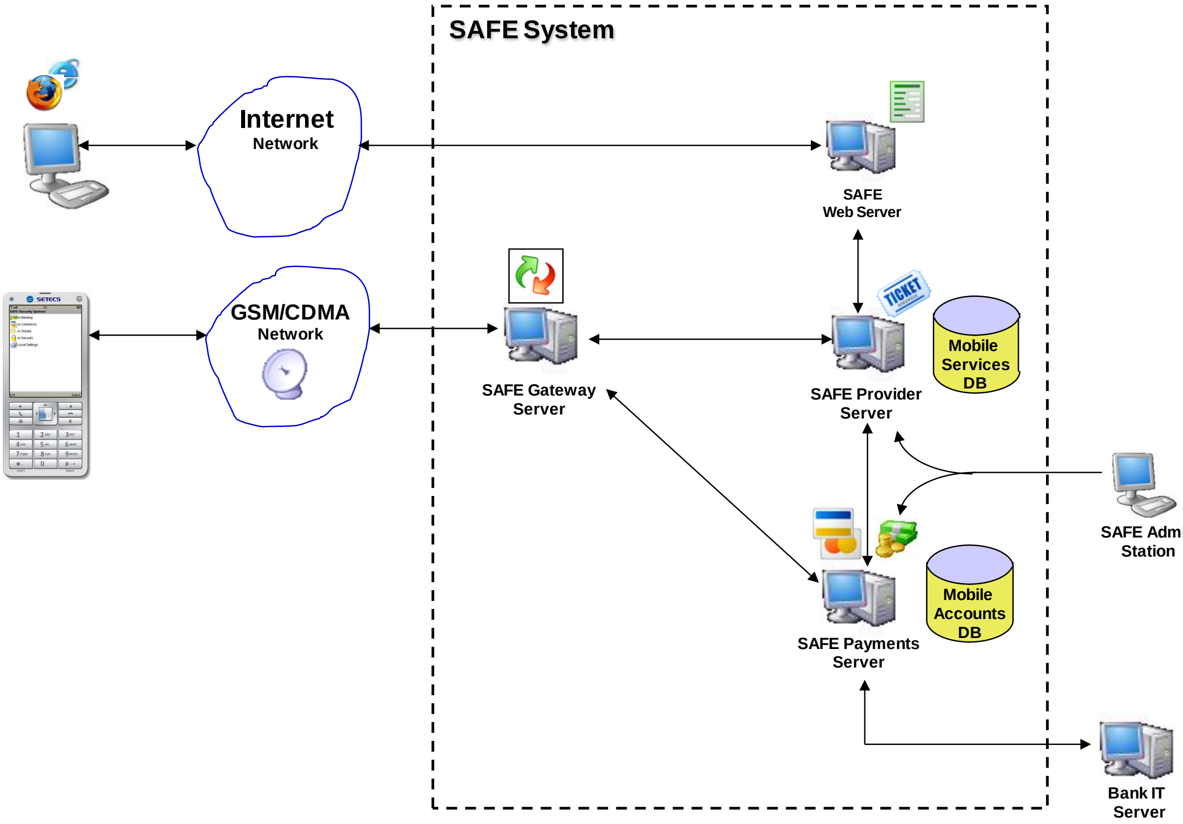


Figure 5. Components of SAFE m-Commerce System

2.2.1 Operations of m-Commerce System

Customers can perform mobile commerce transactions in two ways, one is Over-the-Counter (OTC) and the other is Over-the-Air (OTA). For OTC transactions, customers use biometrics chip cards and merchants use specialized PoS terminals capable of reading smart cards. For OTA transactions, both customers and merchants use mobile phones and a secure mobile wallet loaded into the phone. The cards used in the system are called *SAFE cards*. They are issued and managed by *SAFE* Smart Card Management System, appropriately modified to manage financial smart cards. On-line transactions using PPAs for customers, *SAFE* agents and merchants are handled as follows: when using *SAFE* cards, by *SAFE* PoS application extended with the *SAFE* Smart card client, and when using mobile phones, by the *SAFE* Secure Mobile Wallet loaded into the phone.

- Digital Cash Dispensing and Micropayments

Instead of cash, *SAFE* system can also distribute "digital cash" which is stored in mobile phone and later used for micro-payments. The prerequisite for this application is that merchants' Point–of–Sale (POS) terminal is equipped with hardware and software supporting appropriate proximity protocol and micro–payment application. If so, customers do not need cash, because they are using bank agents or cash dispensers described in the previous section. The sequence of steps and transactions is the following: Customer sends Cash_Request to the *SAFE* server. After validation as before, "digital cash" is debited from customer's account, transferred to and stored in his/her mobile phone. Thus, mobile phone becomes "digital wallet". When the customer comes to the POS, he/she performs payment transaction using mobile phone. The payment amount is reduced from the customer's "digital wallet" and transferred to the merchant's POS terminal. It sends Cash_Reclaim message to the *SAFE* server which contacts merchant's bank server to make deposit into the merchant's account.

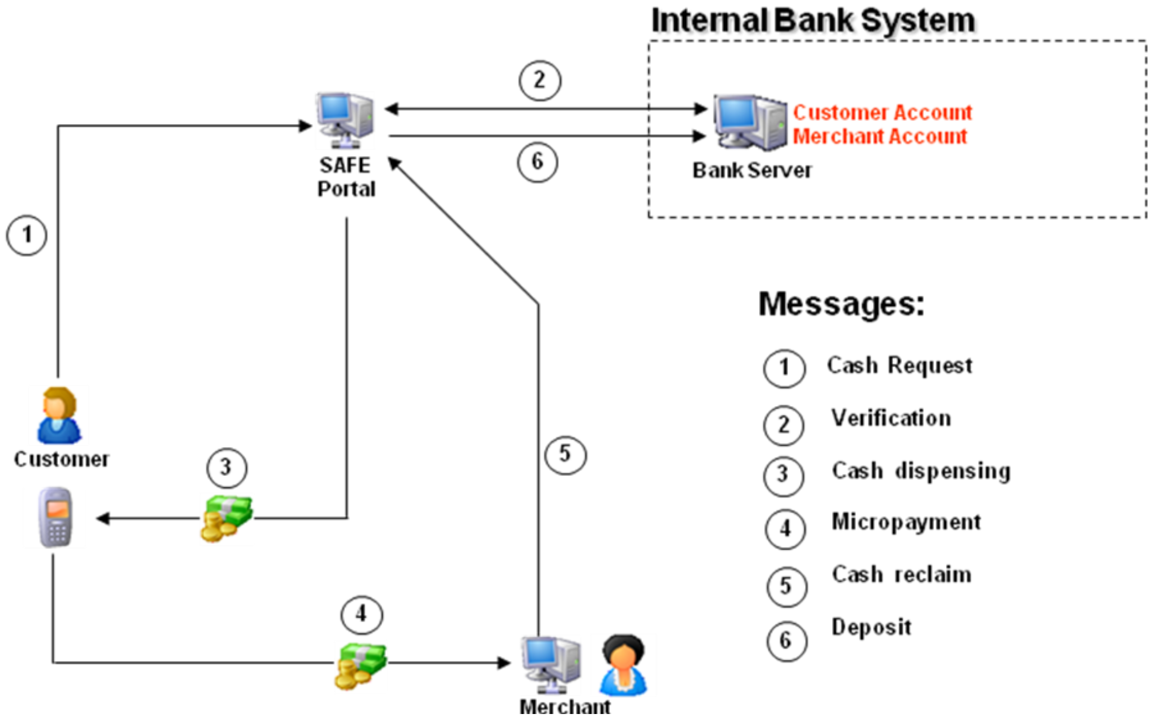


Figure 6. Digital Cash Dispensing and Micropayments

- Credit/Debit Card Payment

Standard debit and credit card payments are today performed using plastic debit/credit cards with magnetic stripe and somewhere with chips. In the *SAFE* system, magnetic stripe data (credit card number and other data) are stored in the mobile phone. Merchant's POS terminal must be capable to accept such data through proximity protocol. All other steps with this application are the same as in today's debit and credit card transactions. Debit/credit card data are entered into the customer's mobile phone either during registration or during the process equivalent to debit/credit card issuance.

The process is the following: customer uses his/her mobile phone to provide card number and other data to the merchant's POS terminal through the proximity protocol. Merchant either connects to the *SAFE* server to verify the authorization of the transaction or connects directly to the existing Card Payment Gateway. When the authorization is received, the payment transaction is completed. Later, merchant sends Credit_Request message to the *SAFE* server or Payment Gateway to request payment.

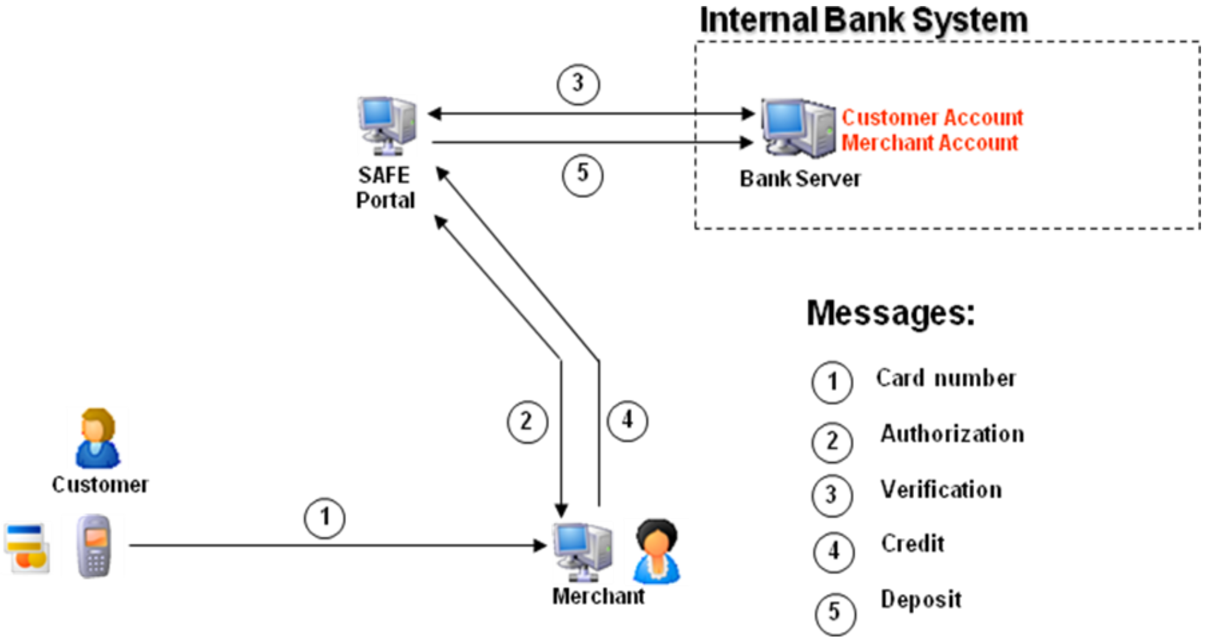


Figure 7. Debit/Credit Card Payment Transaction Messages

2.3 Mobile Parking (m-Parking)

Nowadays most parking systems work like this: customers estimate their parking time before parking and pay the parking fees in advance. This is not convenient, since customers have to remember their parking expiration time. *SAFE* system can be extended to support pay-by-cell phone parking transactions, where customers can send parking payment using SMS messages and the parking bill will be either paid using *SAFE* pre-paid account or later delivered with the mobile phone monthly fees. This approach reduces the cost of time during parking procedure. It also allows customers to park their cars as long as they want, without estimating the time before parking.

2.3.1 Transactions and Components

SAFE m-Parking system provides the following functions to three types of uses:

- For customers (drivers), registering their identification and financial data, paying parking using cell phones, sending warning messages, and inquiring regarding payment transactions and account status,
- For Parking Enforcement Staff, reviewing of payment status for individual parking spaces for issuance of parking tickets,
- For Parking Authorities, it provides a wide range of reporting, security, and financial services.

The following components are included in the *SAFE* parking system and the architecture is shown in Figure 8:

***SAFE* Gateway Server** - connects to various mobile operators. It receives SMS messages, recognizes them as messages for parking system, and passes those messages to the *SAFE* Parking Server.

***SAFE* Web Server** - provides a Web interface to drivers to register their first name/last name, address, phone numbers, and car’s license plate. It enters this registration data into the Drivers Database.

***SAFE* Parking Server** - accepts parking transactions (SMS message) and stores them in the Parking Database as active parking transactions. These database entries are used in combination with the *SAFE* Payments Server to perform payment transactions and, in combination with the Drivers Database, to create violation notifications to parking enforcement personnel.

***SAFE* Payment Server** - maintains payment data and credentials for drivers. This Server maintains the Payment Database and, in combination with the Parking Database, processes payments for parking transactions. The Payment Server is connected in the background with the Bank IT Server to process transactions based on pre-paid accounts and/or real-bank accounts, and with the Credit-Card Acquirer, to process credit-card payments.

***SAFE* Administrative Station -** performs administrative functions with the *SAFE* Parking Server and with the *SAFE* Payment Server in order to perform system monitoring and to create system reports.

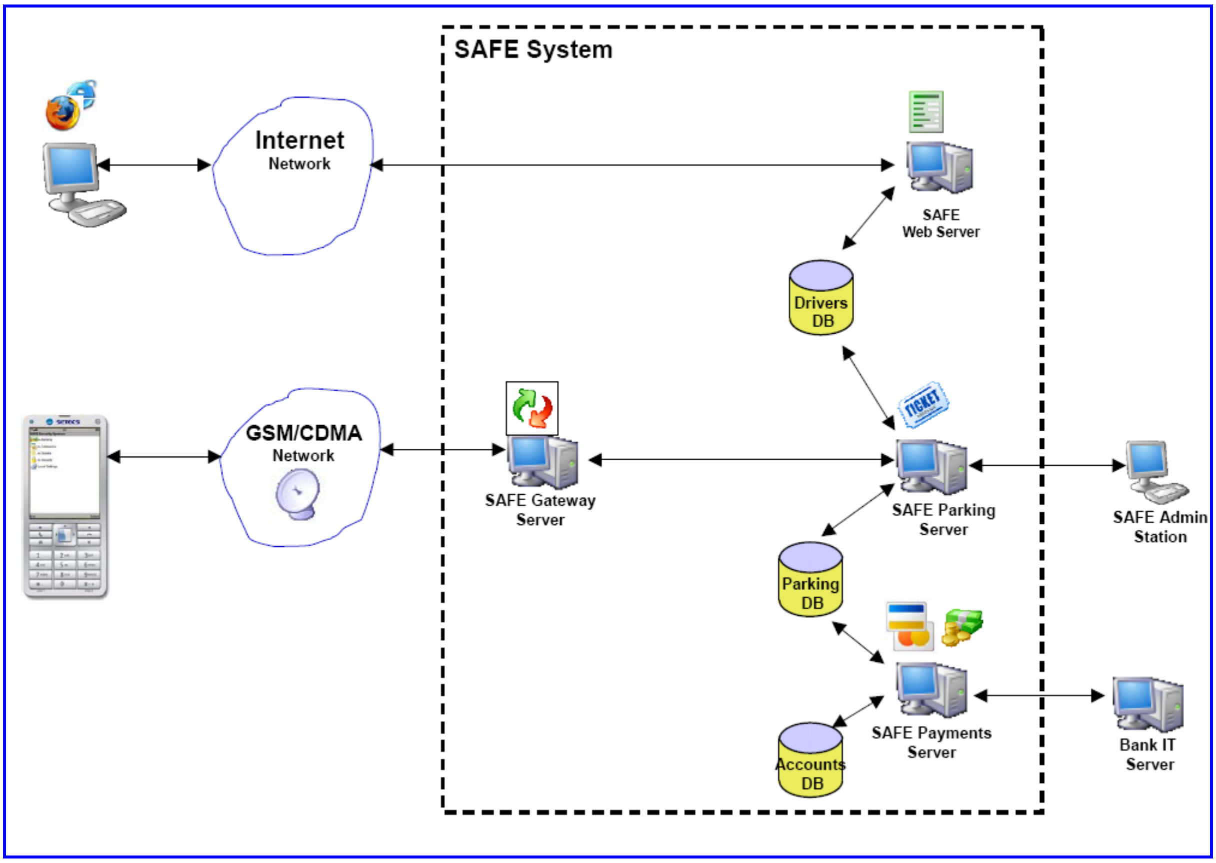


Figure 8. SAFE Parking System Architecture

2.3.2 Operations of m-Parking System

SAFE m-Parking system provides user-friendly experience that will gain rapid popularity and promote quick uptake. It enables the user to send parking space and selected parking time data directly using user's mobile phone with simple SMS messages. Registration data are entered on-line using *SAFE* website, where new users will enter basic driver and payment information necessary to link each user's virtual account to a payment method.

◆ Parking Pay

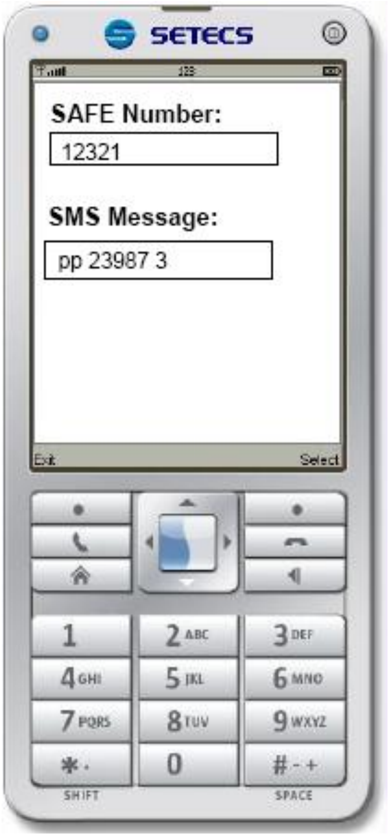
After parking in a public space, the driver selects the *SAFE* System mobile number and sends a SMS message to that number:

pp 23987 3

Interpretation: Parking pay, lot number: 23, meter number: 987, parking time: 3 hours (Figure 9)

When the system receives the message, it will recognize the mobile number of the phone from which the message is sent. It will link that number to the registration entry of the driver and from that entry it will select an authorized method of payment (credit card, pre–paid account, or checking account). The system will then record the data, including the time when the message arrived. The system will reply to the driver with a confirmation message (Figure 10).

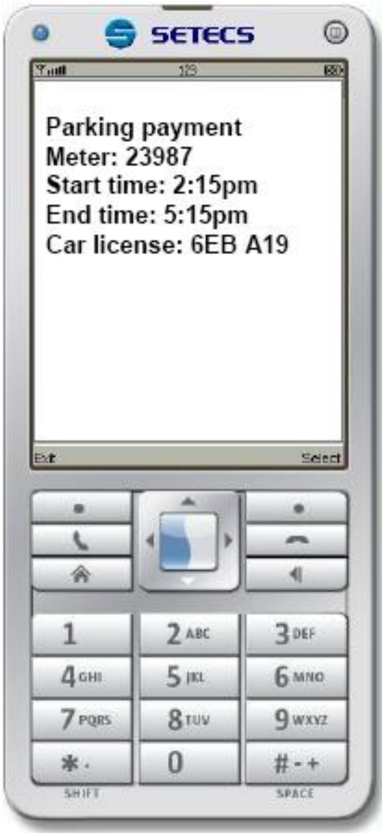
15 minutes before expiration, the system will send warning message to the driver that the allotted time is about to expire.



SAFE Number:
12321

SMS Message:
pp 23987 3

Figure 9. Parking Payment SMS Message



Parking payment
Meter: 23987
Start time: 2:15pm
End time: 5:15pm
Car license: 6EB A19

Figure 10. Parking Confirmation SMS Message

◆ Parking Inquiry

SAFE m-Parking System also supports parking inquiry by a driver:

pi

Interpretation: Parking inquiry (lot number, meter number, and parking time will be fetched from the parking transaction database).

◆ Parking Departure

pd

Interpretation: Parking departure.

When this message is received, the system will recognize that a car has left location 23987. With this message, the system may provide additional services, like

- Inquiry about available parking spaces by drivers
- Crediting drivers with parking time
- Various statistics and analyses reports (average duration of parking, etc.)

2.4 Mobile Ticketing (m-Ticketing)

Mobile ticketing is an application that enables customers to inquire, order, pay for, obtain and validate tickets from any location and at any time using mobile phone or other mobile handsets. It reduces the production and distribution costs of traditional paper-based ticketing channels and increases customer convenience by providing new and simple ways to purchase tickets [16].

2.4.1 Transactions and Components

Nowadays, there are many websites selling tickets online. Using *SAFE* system, this service can be extended to provide secure mobile transactions – purchasing tickets using mobile phones. This system will provide inquiry about all shows for which tickets are available, inquiry about pricing of individual tickets, and ordering of tickets using mobile phones. The *SAFE* m-Ticketing system provides the following transactions to two types of users.

- For customers, registering their identification and financial data, booking and paying ticketing using cell phones, inquiring regarding tickets information and account status,
- For Tickets Distributors, publishing tickets information, manage customers' registration and tickets data, issuing electronic tickets to customer's mobile phone and verifying tickets.

The following components are included in mobile ticketing system:

***SAFE* Gateway Server** – connected to various mobile operators, it receives SMS messages, recognizes them as messages for *SAFE* Ticket Services and passes those messages to the *SAFE* Tickets or Payments Servers.

***SAFE* Tickets Server –** accepts tickets ordering transactions (SMS message) and stores them into Tickets Database, as active tickets transactions. These database entries are used in combination with the *SAFE* Payments Server to perform payment transactions

***SAFE* Payment Server** – maintains payment data and credentials for *SAFE* customers. This Server maintains Payment Database and in combination with Tickets Database processes payments for tickets transactions. Payment Server is connected in the background with the Bank IT Server to process transactions based on pre-paid accounts and/or real-bank accounts, and with Credit-Card Acquirer to process credit-card payments.

***SAFE* Administrative Station** – is used by administrators of the *SAFE* system to perform administrative functions with *SAFE* Tickets Server and with *SAFE* Payments Server and to review various system reports.

The architecture for mobile ticketing system is shown in Figure 11.

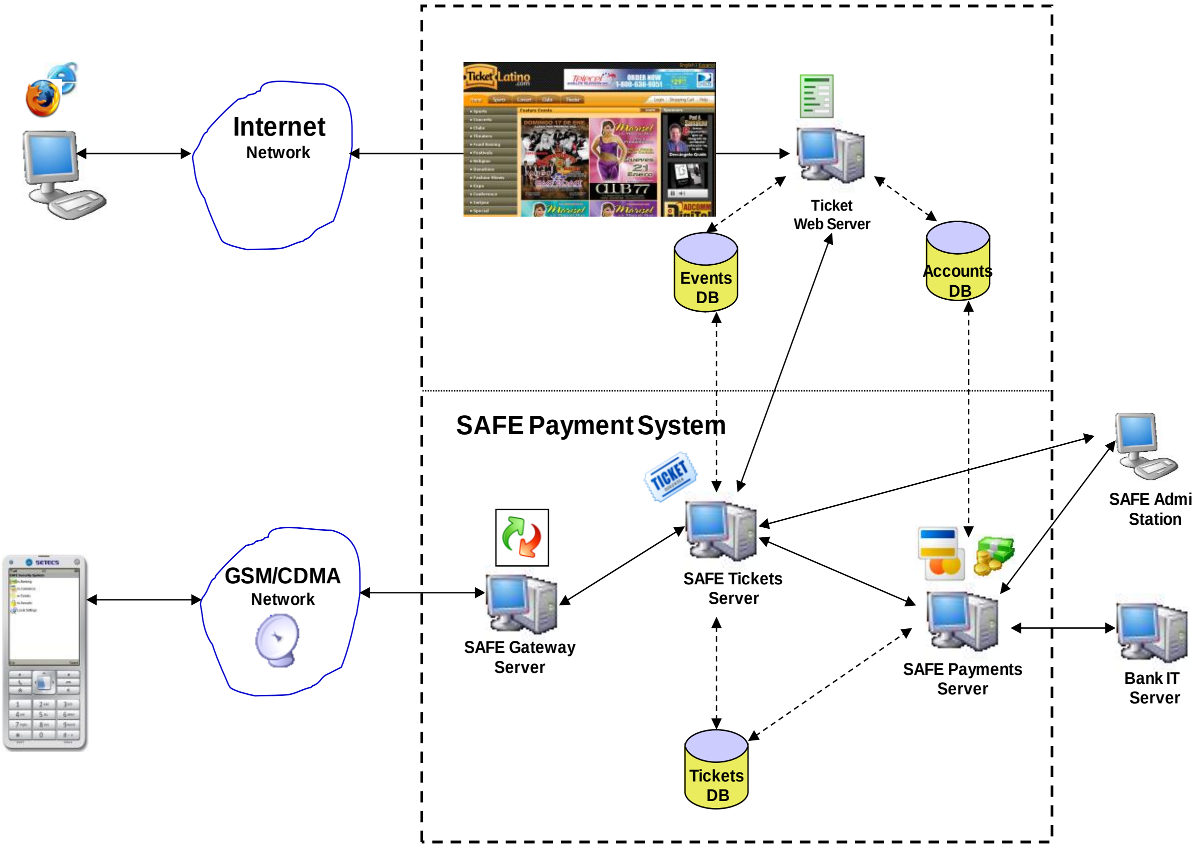


Figure 11. System Architecture for Mobile Ticketing

2.4.2 Operations of m-Ticketing System

- Ticket Buy

SAFE m-Ticketing system allows customers to buy tickets by sending the following SMS message to the *SAFE* Ticket Server:

tb 45467

Interpretation: Ticket Buying with ticket number 45467.

- Ticket Transfer

Customer can transfer ticket to other customer’s mobile phone by sending the command:

tt +12334367 45467

Interpretation: Ticket Transfer to destination mobile phone number +12334367 and ticket number 45467.

- ◆ Ticket Use

Customer can use ticket by sending the command:

tu 45467

Interpretation: Ticket Use with ticket number 45467.

- ◆ Ticket Distribute

Tickets may also be distributed to mobile phones, if venue booths are upgraded to perform their verification. The *SAFE* m-Ticketing system allows tickets distributors to distribute tickets to customers by sending the following command to customer's mobile phone:

td +12343455 45467

Interpretation: Ticket Distribute with customer's mobile phone number **+12343455** and ticket number **45467.**

After installing, configuring and activating all system components, Events and Accounts Database must be populated first. For that, Ticket Web Server must be modified to feed all those information to the *SAFE* Tickets Server and *SAFE* Payments Server. Events Database will contain one entry for each seat at each event. This database will be populated continuously as new events are announced and new customers are registered in the system using Ticket Web Server.

After that, ticketing and payment transactions may be performed. For each transaction, based on the mobile number of the incoming SMS message, the system recognizes the customer, the event, and the selected seat, and creates ticket purchase transaction in the Tickets Database. At the same time, the system triggers payment transaction by the *SAFE* Payment Server.

If tickets are sold over Web, Ticket Web server must be modified to provide on–line and in real–time two types of information to the *SAFE* System:

- Information about new events, seats, tickets, prices, etc., i.e. all information needed for mobile customers to select the desired tickets,
- Registration data for customers, including their payment options, bank accounts (if any), etc.

Chapter 3:

Analysis of System Requirements

Before designing security system, we start with analyzing two issues. The first is what applications are supported by the system and the second one is what are the requirements for designing the system. For mobile financial environments, security is one of the most important issues. This chapter lists the requirements for mobile financial applications provided by the *SAFE* system, described in Chapter 2. For the answer to the second question, considering the system's adaptability and extension ability, we chose to use standards created by international institutes. This chapter also overviews standards regarding secure mobile financial transactions.

3.1 Security Requirements

Based on the transactions illustrated in Chapter 2, there are various security threats because of the sensitivity of data and vulnerabilities of GSM networks, as presented in Chapter 1. These threats can be categorized into three groups:

a. Reveal of sensitive data – as presented in Chapter 2, most transactions provided by *SAFE* system deal with bank accounts, credit/debit card payments, etc. Therefore, many very sensitive financial data, such as credit card number or account status, should be kept secret both when stored locally and when transferred over the open networks. For example, a customer may store his/her credit card information locally in his/her mobile phone in order to conduct credit card payment. Data may be revealed to someone who can access that customer's mobile device or if the customer loses the mobile phone. It is also risky while exchanging these data via open networks when no extra protections are added, especially between mobile phone and the *SAFE* Gateway Server.

b. Unauthorized access – it is common that the customer lends his/her phone to someone else for a temporary use or just loses the mobile phone. Both of the cases may cause unauthorized access to the mobile device, especially applications and data stored in it.

c. Denial-of-Service attack– because *SAFE* Gateway Server acts as a proxy that transfers and routes all the messages and it integrates several kinds of wireless communication interfaces at the front end, it is easy to perform denial of service attack on the *SAFE* Gateway Server. The table indicates potential losses from Denial-of- Service attack.

Business type	*Brokerage firm*	*Credit card authorization company*	*Automated teller machines*	*Major online auction site*
Exposure/Hour	$6.5 million/hr	$2.6 million/hr	$14,500/hr in fees	$70,000/hr

Table 2. Potential Losses from a Denial-of-Service Attack [17]

d. Identity theft – refers to the case when a person pretends to be someone else in order to steal money or achieve other benefits. Identity theft is very common for electronic financial transactions. It is reported that identity theft is the number one crime in the United States. Reported incidents of identity theft are projected to more than double, from 700,000 in 2001 to 1.7 million in 2005, and the cost to U.S. financial institutions alone will increase 30 percent each year, to more than $8 billion in 2005. These numbers do not take into account wide range of social costs associated with this crime, such as litigation expenses or hours lost to redeem one's name or credit information. [17]

In m-Commerce applications, each party that participates in a particular transaction does not meet each other physically. However, in financial transactions trust should somehow be established between parties [26]. In addition, because of these security threats, the *SAFE* system is required to provide comprehensive security features in order to prevent these threats. For (a), sensitive data should be stored and transmitted in an encrypted format. For (b), every entity needs to authenticate each other before communication. For (c), more than one Gateway Server are needed in case any of them is down, and all these Gateway Servers should be well protected from both external and internal attacks. More details about security features provided by the *SAFE* system are given in Chapter 4, Chapter 5 and Chapter 7.

3.2 Social Requirements

Additionally there are some social requirements. For example, Mobile-ATM system targets rural communities [18] in developing countries and there are several constraints in developing community acceptable solutions. Poor computer literacy stands against successful deployment of such projects. Therefore, mobile user interface should guide users to perform transactions with very simple help steps.

Moreover, existing m-Banking systems use only electronic financial materials (like electronic coins) for transactions [19]. In most of the developing countries only very few facilities exist to perform transactions using electronic financial materials. Meanwhile, the survey that was conducted shows that most of the people in rural areas do not like to use electronic coins [20]. Therefore, m-Banking systems for developing countries should be capable to use actual notes and coins as the transaction medium. Therefore, our system should be able to deal with the actual coins and notes.

3.3 Related Standards

3.3.1 FIPS 196

Entity Authentication Using Public Key Cryptography standard (FIPS 196) is a specification of the mutual authentication protocol. The diagram of the Strong Authentication Protocol is illustrated in Figure 12.

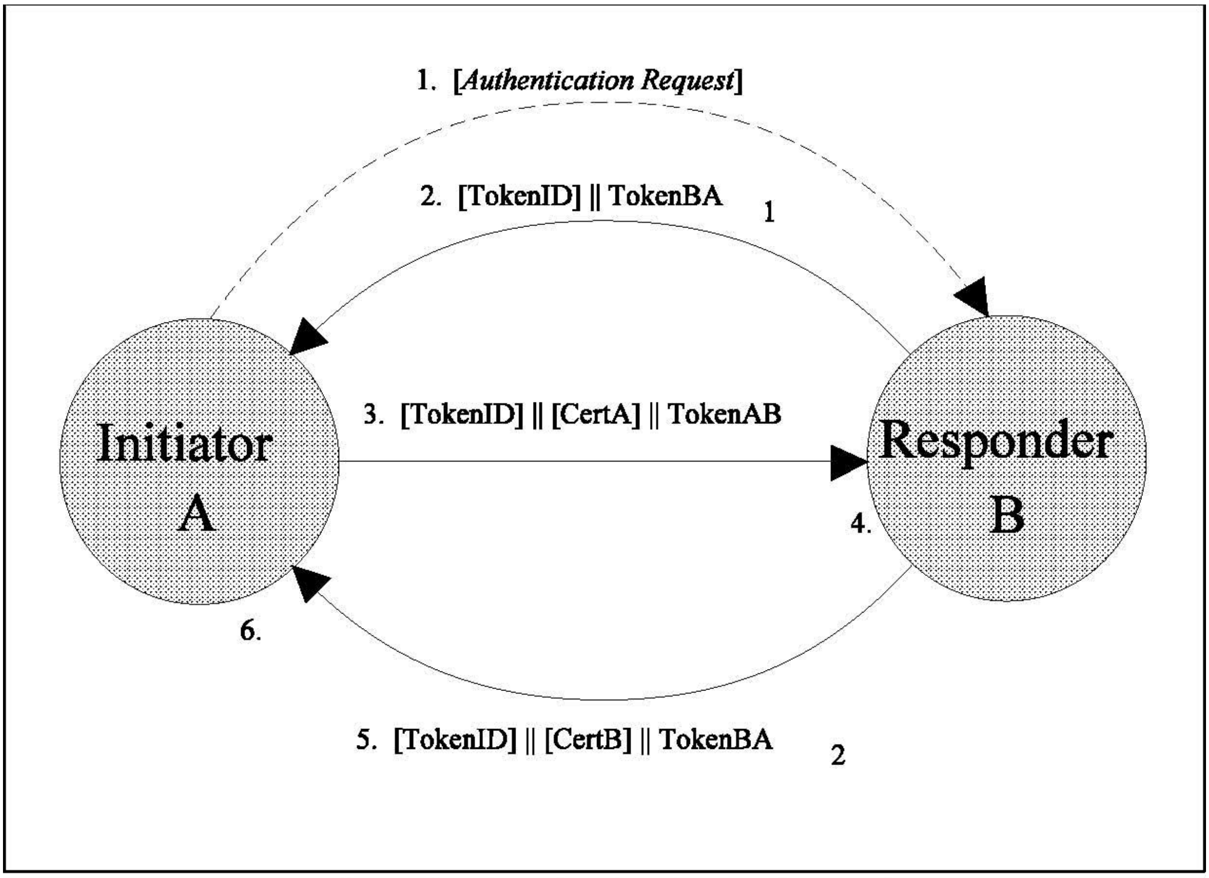

1. [*Authentication Request*]
2. [TokenID] || TokenBA
1
Initiator
A
3. [TokenID] || [CertA] || TokenAB
Responder
B
4.
6.
5. [TokenID] || [CertB] || TokenBA
2

Figure 12. Mutual Strong Authentication Protocol [21]

Description of Figure 12:

Authentication Request: a message is sent from an initiator to a responder that contains initiator's ID and a value indicating the request.

TokenID: Distinguished Name of the entity that sends the message

CertX: certificate of an entity X

TokenBA1: the responder determines if it will continue, initiate or terminate the authentication exchange. If responder agrees to continue, this token is sent from the responder to the initiator that contains a random number RB, generated by the responder, and an optional text. Responder will retain RB.

TokenAB: this token is sent from the initiator to the responder that contains a random number RA, generated by the initiator, and a signed data of RA. The data is signed by the initiator's private key. There can be also some optional text. All the signed data that are optional appear only when their corresponding values appear in the unsigned part. Although RB received from TokenBA1 does not have to be in an unsigned part, it must be in the signed data.

TokenBA2: when receiving TokenAB, the responder should first verify: a) RB and b) certificate of the initiator whether it is contained in the TokenAB. If verification succeeds, the responder will send this token to the initiator that contains a successful indicator, a signed data of RA and optional texts. Otherwise, the responder will send a token that contains a fail indicator and a new random number, which repeats from the step 2 or terminates exchange.

When receiving TokenBA2, the initiator should first verify a) RA and b) certificate of responder, whether it is contained in the TokenBA2. If verification is successful, the initiator will send a successful indicator back to the responder. Otherwise, the initiator will send a fail indicator and a new random number, which repeats from step 3 or terminates exchange.

For more details of the strong authentication standard, please see FIPS 196.

3.3.2 EMV

EMVCo is the organization currently responsible for maintenance and enhancements of the EMV® standards. It is co-owned by VISA, Master Card, JCB and American Express. EMV® is a global standard for credit and debit payment cards based on chip card technology. Transactions based on EMV standard are more capable to protect cardholders from fraud than those payments with traditional magnetic stripe cards, as EMV chip cards provides strong crypto algorithms, such as Triple-DES, RSA and SHA for card authentication to the merchant terminals and the transaction processing centre [22].

EMV standards are mainly designed for chip cards and the interoperations with POS and ATM. However, in recent years, with new applications EMV expanded usage of original EMV cards to other media for convenience of use. At present, official EMV standard documents for Integrated Circuit Card (ICC) have been published as Version 4.0 in the focus of four books:

- Book 1 - Application Independent ICC to Terminal Interface Requirement
- Book 2 - Security and Key Management
- Book 3 - Application Specification

- Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements

The most widely known implementations of EMV standard are:

- VSDC – VISA
- MChip - MasterCard (includes former Europay International SA)
- AEIPS - American Express
- J Smart - JCB (formerly Japan Credit Bureau)

For more details of EMV standard, please check related documents.

3.3.3 Wireless Communication Standards

The following communication protocols are used in the *SAFE* system:

SMS **–** stands for *Short Messaging Service* and all mobile phones support this function. Customers can type simple short messages according to the *SAFE* message formats for different types of transaction requests. The advantages of the SMS service is that it is cheap, easy, fast and simple to use and the disadvantage is its limitation of the number of characters per message (at most 140 characters/message).

USSD **–** stands for *Unstructured Supplementary Service Data* and it uses SMS technology, but functions in a different way. In order to provide USSD service, a USSD server is necessary [24]. When a user sends a USSD service request, USSD server sends back a menu listing several options based on user's request. Then, instead of typing specific transaction request, the user just needs to choose one from the menu and sends the option number to the USSD server. USSD server will handle the transaction by following user's choice.

Internet **–** there are two possibilities for the *SAFE* system to access Internet. The first is to use PC to connect to Internet and the other one is mobile Internet using mobile phone and WAP to access Internet.

GPRS **–** this is session-oriented communication protocol based on package switching technology. Mobile users need to open this service by applying to telecom companies. The advantages are that it can exchange large amount of data with high speed and the connection is stable. The disadvantages are its higher cost (counted by amount of flow of data) and it is not as common and acceptable as SMS service.

Bluetooth – this is communication protocol becoming more and more popular. The advantages are its high speed for exchanging large amounts of data (also supporting exchanging files) and it is completely free to use. The disadvantages are its short communication distance (within ten meters) and some security related issues (for example, sometimes people forget to turn off Bluetooth when they go to a public place, from where hackers can utilize that as the starting point of accessing or even controlling their mobile phones).

NFC – stands for Near Field Communication and *SAFE* system does not support it now, but it is planned for the next phase. Since mobile and chip technologies are developing so fast, soon the SIM chips inside mobile devices should be able to support contactless protocol. In that case, mobile phone can be used in the same way as a contactless card, where NFC is used.

Communication services architecture of the *SAFE* system is shown in Figure 13.

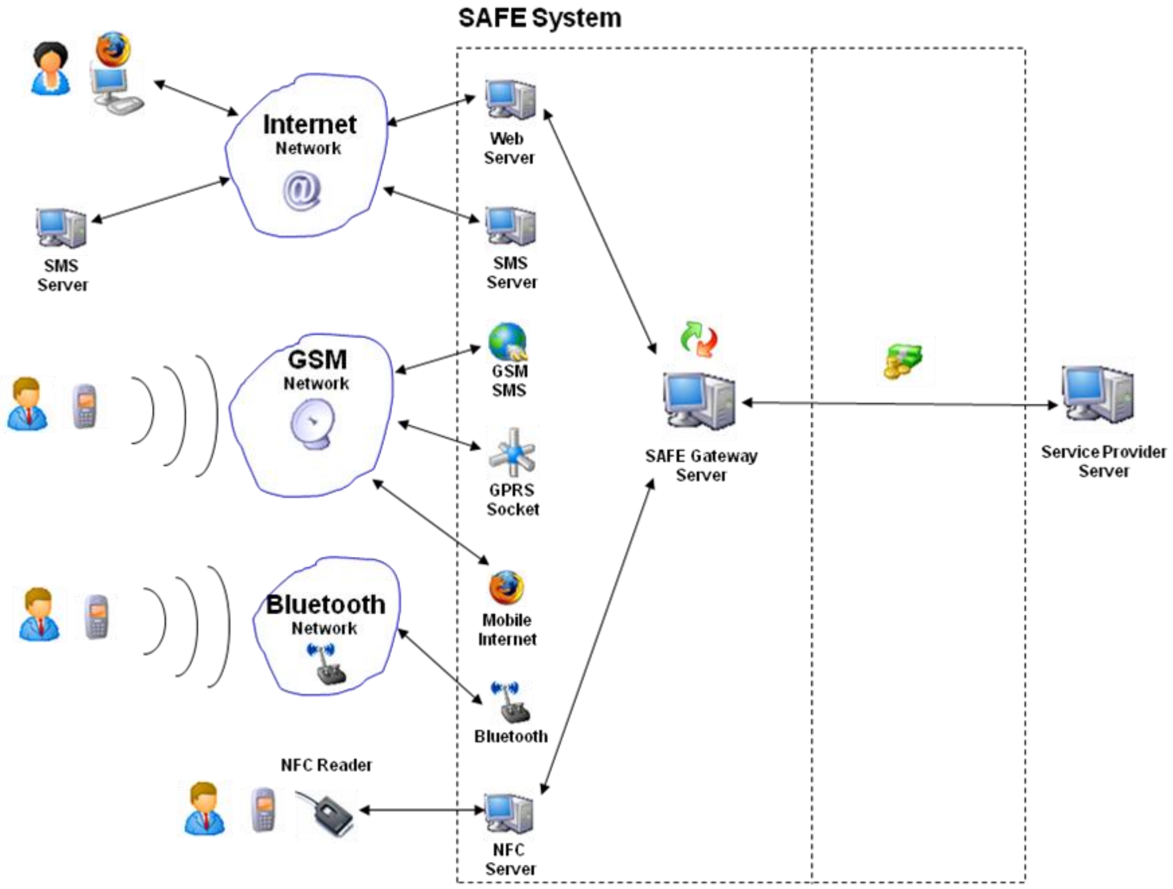


Figure 13. Communication Service Architecture of the SAFE System

Chapter 4:

Security Infrastructure of the *SAFE* System

As illustrated in Chapter 2, *SAFE* system supports various mobile applications. Since all the transactions are financial transactions, the main concern must be their safety. Therefore, one of the most distinguished features of the *SAFE* system is its comprehensive security. This chapter describes the security infrastructure of the *SAFE* system.

4.1 Security Components and Architecture

In m-Commerce applications parties that participate in a particular transaction did not physically meet each other. However, in financial transactions trust should somehow be established between each party [23]. General cryptography concepts can be used to provide trust between participants. There are five types of security senices that are needed for establishing trust:

- *Authentication:* authentication is the process of proving user identification. One party involved in a transaction needs to make sure that counterparty is the one he/she is interested to communicate with. The information used for authentication is called authentication factor. Factors are generally classified into three categories:
  a. Ownership: something the user has, for example ID card or security token.
  b. Knowledge: something the user knows, for example password, PIN, answers to security questions.
  c. Inherence: something the user is or does, for example fingerprint, voice, biometric identifier, etc.

- *Integrity:* assuring the receiver that the received message has not been altered in any way from the original message. Usually the hash value of the original message is attached with the message for the recipient to verify the integrity. Hash function is the algorithm that has three characteristics:
  a. One-way function: by given the input, it is easy to calculate hash value, but by given the hash value, it is computationally infeasible to find out the input.
  b. One-to-one pairing: one input can only lead to one hash value. It is impossible to find two inputs that have the same hash value.
  c. Fixed length of output: the length of input could be arbitrary, but the length of hash value is fixed.

  These three characters guarantee the integrity of a message by computing its hash value and comparing with the hash value sent from the originator.

- *Confidentiality:* ensuring that no one else can read the message except the intended receiver. Encryption and decryption of data could achieve confidentiality. There are two kinds of crypto systems based on two types of keys: symmetric and asymmetric crypto system. If both the encryptor and decryptor share the same key, it is symmetric. Otherwise, it is asymmetric.

- *Non-repudiation:* a mechanism that prevents that the counter party denies the transaction. In other words, if A sends a message to B, A cannot deny that he/she sent the message.

- *Privacy:* ensuring that the message is not readable by unexpected third party between its source and its destination. This is very important over Internet, since any information transferred across the Internet has to go via several routers. Anyone with access to the routers is able to inspect or modify the data.

- *Availability:* system availability is whether (or how often) a system is available for use by its intended users. This is an integral component of security.

In order to achieve end-to-end security, besides establishing trust, protection is necessary for all the data stored both at a client side (mobile device) and at a server side. Especially, data in mobile phone need protection, since it is very easy to get mobile devices lost or stolen by someone else.

In addition to the components described in Chapter 2, there are three other components for security of the system:

Identity Provider (Registration) Servers – providing registration services and distribution of reliable identities

Certification Servers – providing certification of participants, issuance of their X.509 certificates, management and distribution of those certificates

Authorization Servers – providing authentication (single- sign–on) and authorization services for system authorities and consumers, based on secure web services

The complete security architecture of the *SAFE* system is shown in Figure 14.

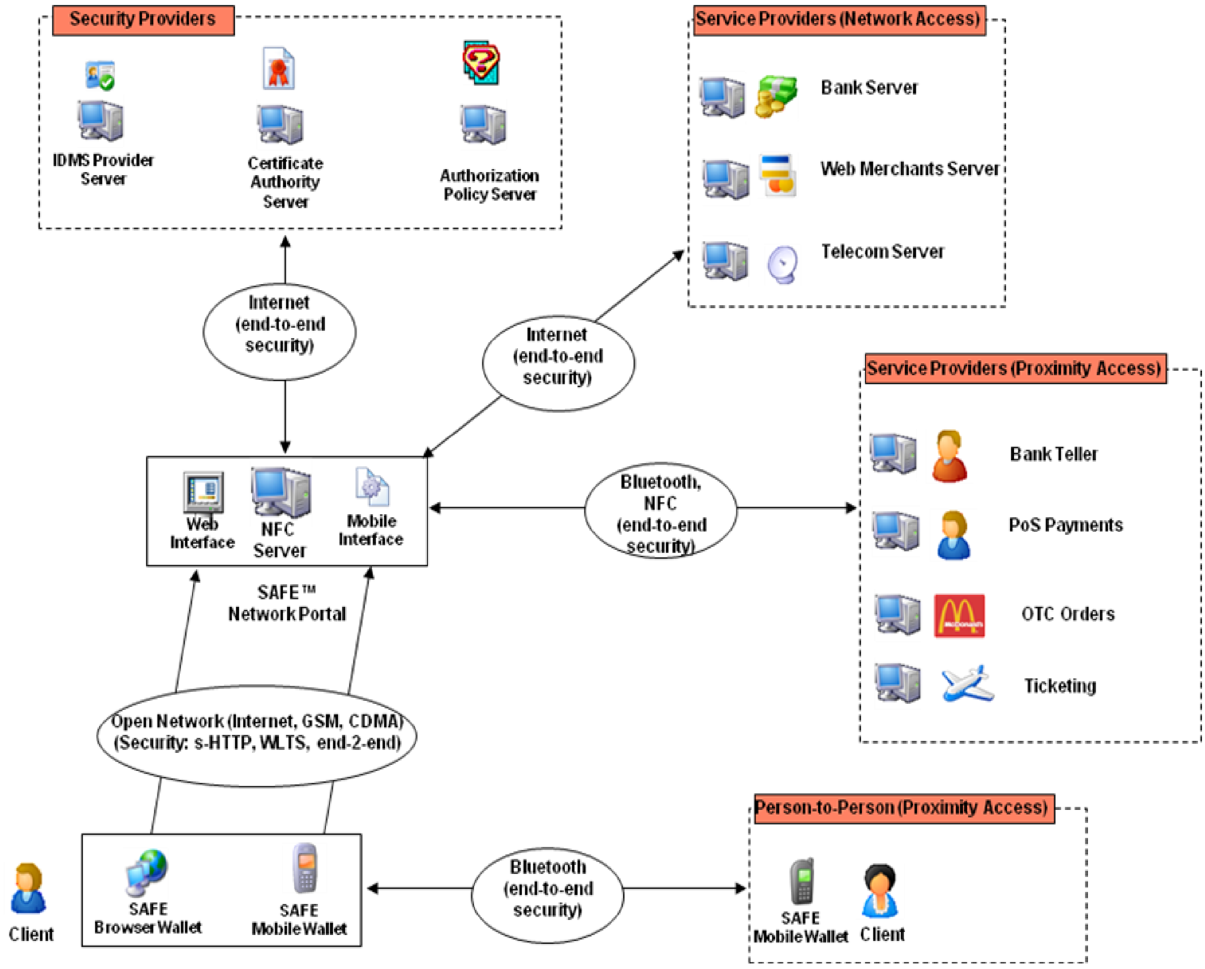

Security Providers
IDMS Provider Server
Certificate Authority Server
Authorization Policy Server
Service Providers (Network Access)
Bank Server
Web Merchants Server
Telecom Server
Internet (end-to-end security)
Internet (end-to-end security)
Service Providers (Proximity Access)
Bank Teller
PoS Payments
OTC Orders
Ticketing
Web Interface
NFC Server
Mobile Interface
SAFE™ Network Portal
Bluetooth, NFC (end-to-end security)
Open Network (Internet, GSM, CDMA) (Security: s-HTTP, WLTS, end-2-end)
Person-to-Person (Proximity Access)
Client
SAFE Browser Wallet
SAFE Mobile Wallet
Bluetooth (end-to-end security)
SAFE Mobile Wallet
Client

Figure 14. Secure Service-Oriented Infrastructure

Based on this architecture, clients conduct transaction both with other clients and with various service providers via *SAFE* Gateway Server. The *SAFE Gateway Server*, which is the core component of the *SAFE* system, communicates with the client at the front-end through several kinds of wireless communication protocols, described in Chapter 3 and connects with security providers and service providers at the back-end through stable TCP/IP connections. It receives various requests from clients, interprets them based on *SAFE* messages syntax and dispatches these request messages to different service providers. *SAFE* messages syntax is described in Chapter 5.

SAFE system includes application servers described in Chapter 2 for different service providers in order to utilize their services combined with the *SAFE* system. Application servers receive messages from the *SAFE* Gateway Server, create messages with specified syntax and send these messages to the real service providers. The syntax of messages is based on either international standard, such as ISO-8583 or specifications from service providers if they have such specifications. If there is no international standards for message syntax and service providers do not have their specifications, *SAFE* system will provide both communication service and message syntax.

4.2 Security Management Operations

In previous sections security components and architecture were presented. This section describes security management operations of the *SAFE* system.

4.2.1 Registration of Participants

All participants in the *SAFE* system must be registered. Figure 15 shows registration process performed by Registration Agents and registration data stored in the registration database of the IDMS server. This step may be performed by a bank, by a telecom operator or by any other independent ID services provider. All participants in the system have reliable and verifiable registrations data used for all *SAFE* transactions.

Registration progress consists of two phases. In the first phase, the customer can either send SMS message with his/her first name and last name to the *SAFE* Gateway Server for quick registration or he/she may fill the registration form on the *SAFE* Website for registration. Once the customers finishes the first phase, they can immediately use the *SAFE* system. They can open *SAFE a*ccount (pre-paid account), deposit money, withdraw money and transfer money. This feature is very useful in rural areas where customers want to use *SAFE* system to deposit, withdraw or transfer money.

The second phase is a face–to–face authentication procedure, when personal data and credentials are verified and completed. Registration Agents fill out registration form and data is stored in the registration database at the IDMS Server. At the same time, a password is either transferred on–line into mobile phones of customers and bank agents or given to other parties for later use.

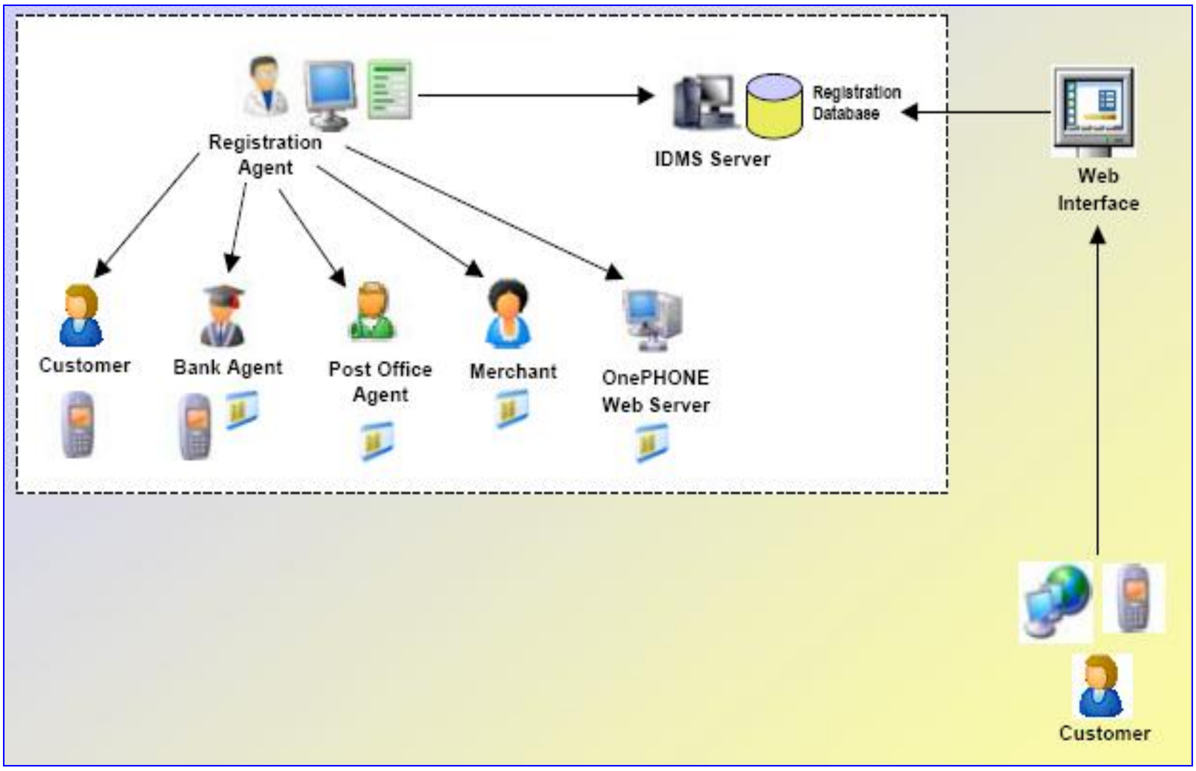


Figure 15. Registration of Participants

4.2.2 Issuing of Certificates and Smart Cards

In the *SAFE* system all participants have certificates. They are issued by the Certification Authority (CA) Server, based on registration data stored in the IDMS database. In addition, all participants performing high–value transactions are also issued smart cards. Only customers will not have their own smart cards, due to the high cost of mobile phones that can use smart cards. For customers, key pairs are generated in their mobile phones, while for those in possession of smart cards, key pairs are generated by their cards.

Certificates and smart cards may be issued by banks or by any other independent service providers.

Certificates, issued by the CA server, are stored in mobile phones and in smart cards. Therefore, security of all transactions is based on public key cryptography, supported either by software in mobile phones or by smart cards.

After reliable and verifiable registration, certification, and issuance of smart cards, an instance of the *SAFE* system is ready for its secure operation, supporting various secure financial transactions.

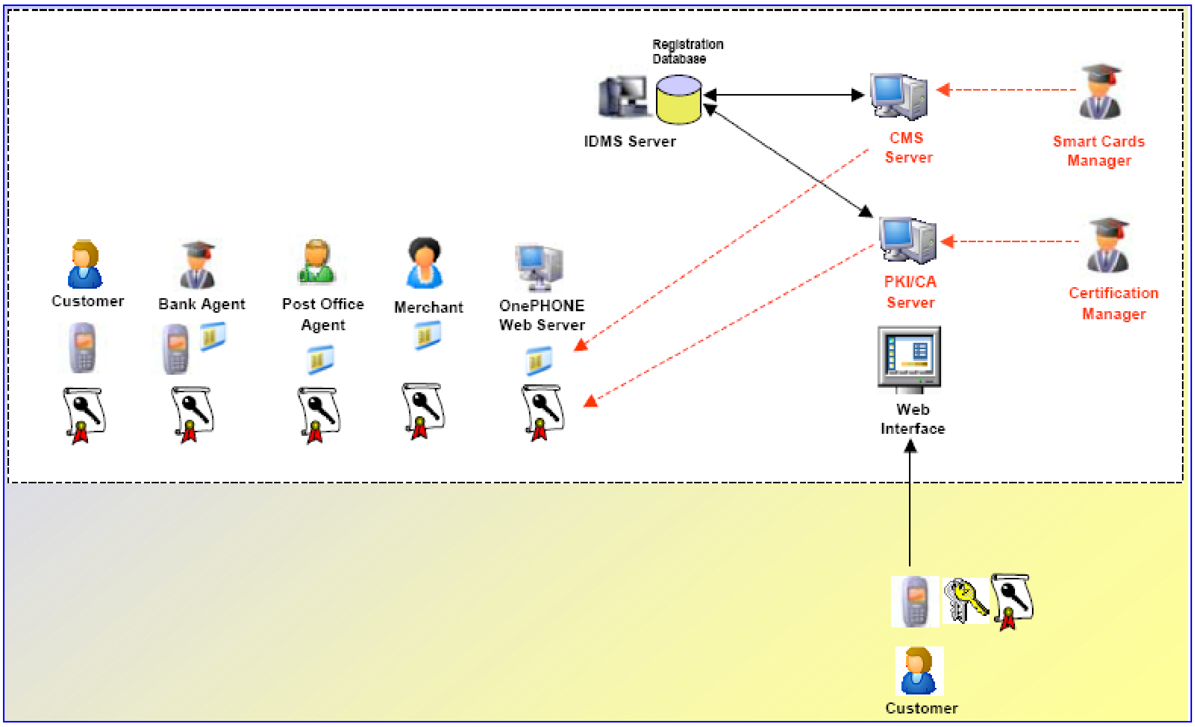


Figure 16. Issuing of Certificates and Smart Cards

Due to the limitations of mobile devices, mentioned in Chapter 2, normal PKI cannot work for mobile financial environments. Therefore we proposed our lightweight version of the PKI called mobile PKI. Figure 17 shows the certificate request progressing in the m-PKI:

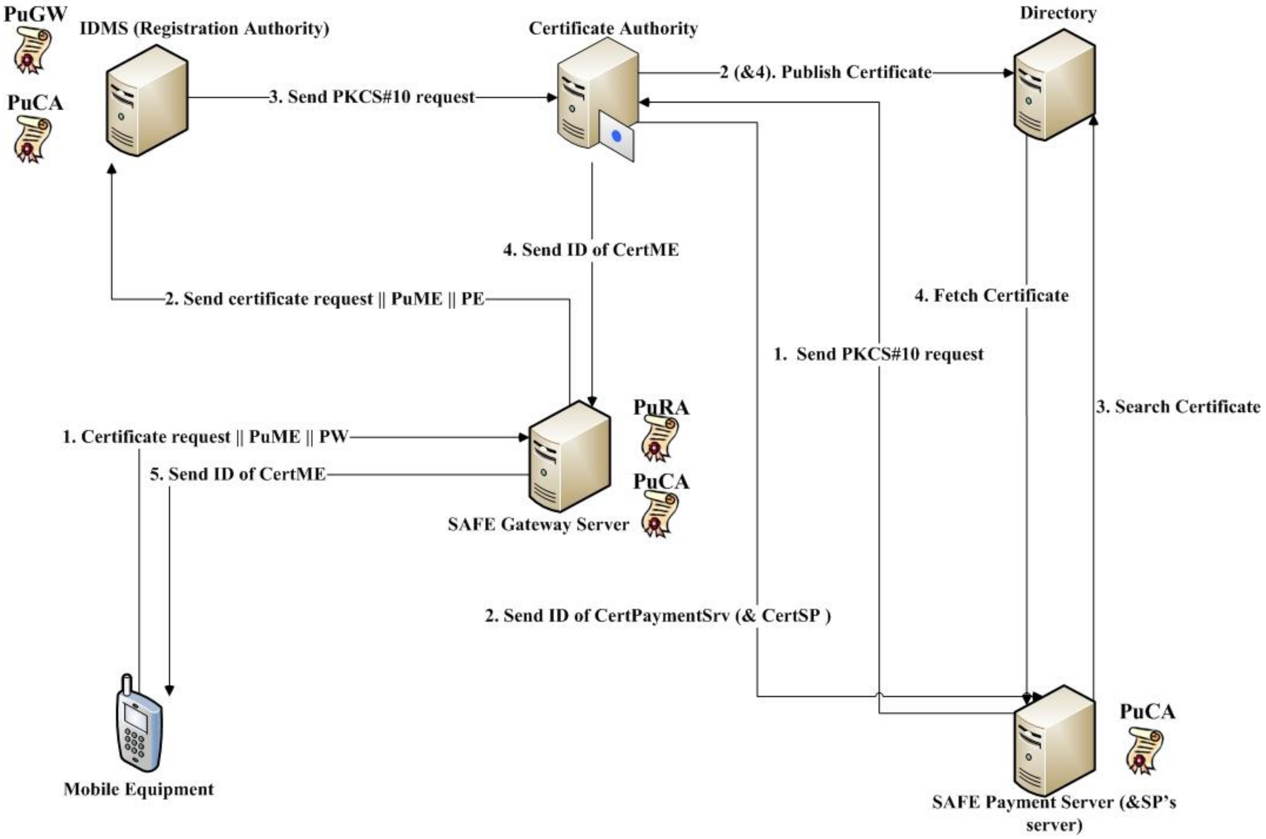


Figure 17. Certificate Request in the m-PKI

Interpretations of the figure above:

PuX – Public key of X
CertX – Certificate of X
PW – Password
SP – Service Provider

Preparations:

a. Every entity except the mobile customer has already fetched other entities' public key;
b. During registration progress, a password is generated for every customer;
c. The customer uses UICC in a mobile phone to generate 1024 bits RSA key pair.

1. The customer sends a message containing customer's public key, password and a certificate request indicator "mCertRequst" to the *SAFE* Gateway Server;
2. The SAFE Gateway Server encrypts customer's mobile phone number, public key and password with IDMS Server's public key and sends it to the IDMS Server;
3. IDMS Server verifies customer's identity by checking the password. If the verification is successful, the IDMS Server searches customer's registration information based on customer's mobile phone number. Then the IDMS Server creates PKCS#10 message based on the customer's registration data and public key and encrypts the message with CA's public key and sends the result to the CA;

4. The CA issues certificate and publishes it into the Directory Server. At the same time, the CA sends an ID linked to the customer who requested certificate to the *SAFE* Gateway Server;
5. *SAFE* Gateway Server sends the ID of the customer's certificate to the customer.

The certificate request progress for service providers is the same, but simpler. The SP can generate the key pair and create PKCS#10 request directly and send it to the CA. Instead of sending back the ID of the certificate, the CA sends back SP's certificate directly to the SP.

Chapter 5:

Secure Mobile Applications and Transactions

SAFE System supports communication interface with multiple telecom networks (front-end) and with multiple service provider systems (back-end). It supports multiple types of mobile applications: mobile banking, mobile commerce, mobile ticketing, mobile parking, etc. This chapter describes the details of security features of these applications.

5.1 Functions and Messages

As described in Chapter 3, *SAFE* system supports four types of applications: mobile banking, mobile commerce, mobile parking, and mobile ticketing. Every application supports several functions. Table 3 shows all the functions supported by the mobile applications. Client side of these applications is called Secure Mobile Wallet. The details of the Secure Mobile Wallet are presented in Chapter 6.

1. m-Banking a. List accounts b. Deposit cash c. Withdraw cash d. Transfer cash e. Stored cash f. Open account g. Apply for loan h. Review loan status i. Pay loan installment	**2. m-Commerce** a. Pay bills b. Pay (Credit Card) c. Pay (Debit Card) d. Pay (Stored Money) e. View (Stored Money) f. View transactions g. List credit cards	**3. m-Ticketing** a. Inquire distributors b. Inquire shows c. Inquire tickets d. Buy ticket e. List tickets
4. m-Parking a. Parking pay b. Parking inquiry c. Parking departure d. Parking extension	**5. m-Security** a. Security options b. Change PIN c. User registration d. Fetch registration data e. View registration data f. Update registration data g. Request certificate a. List certificates	**6. Local Settings** a. Configuration b. Thin Wallet c. USSD Wallet

Table 3. SAFE Mobile Wallet Functions

Based on these functions, we designed *SAFE* commands for every function. Every message has a simple format, so that customers can type fast and easily using mobile phone. Table 4 shows all the commands that may be used in the *SAFE* system:

Object	Function	Amount	Target	Sample	Description
Account (a)					
	Open (**o**)	N/A	[Currency]	**ao EUR**	Request to open an Euro account
	Status (**s**)	N/A		**as**	List status (balance) of an account
	List (**l**)	N/A		**al**	List transactions with the account
	Close (**c**)	N/A		**ac**	Request to close an account
	Transfer (**t**)	[Amount]	[Target ID]	**at 100 1122334455**	Transfer 100 units from R-Acc to another R-Acc
	Load (**l**)	[Amount]		**al 100**	Load 100 units from R-Acc to own V-Acc
	Return (**r**)	[Amount]	[Target ID]	**ar 100**	Return 100 units from V-Acc to own R-Acc
Air Time (at)					
	Buy (**b**)	[Amount]		**atb 100**	Buy 100 unit air time
	Transfer(**t**)	[Amount]	[Target ID]	**att 100 1122334455**	Transfer 100 unit air time to the target account
Bill (b)					
	List (**l**)	N/A		**bl**	List bills with the mobile phone number
	Pay (**p**)	N/A	Bill NO.	**bp 5832454**	Request to pay the bill with bill number
Card (c)					
	Pay (**p**)	[Amount]		**cp 100**	Pay 100 units by using debit/credit card
Loan (l)					
	Review (**r**)			**lr**	Request to review all loans
	Apply (**a**)		[Loan ID]	**la 75435454**	Request to apply for a new loan with loan ID
	Pay (**p**)		[Loan ID]	**lp 34545456**	Request to pay a loan with loan ID
Money (m)					
	Deposit (**d**)	[Amount]		**md 100**	Deposit 100 units in cash over the counter in R-Acc
	Withdraw (**w**)	[Amount]	[Target ID]	**mw 100**	Withdraw 100 units in cash over the counter from R-Acc
				mw 100 25	Withdraw 100 units in cash from Agent 25
				mw 100 33	Withdraw 100 units in cash from Merchant 33

				mw 100 55	Withdraw 100 units in cash from real ATM no. 55
	Load (**l**)	[Amount]		**ml 100**	Load 100 units as digital cash into Wallet
	Return (**r**)	[Amount]		**mr 100**	Return 100 units of digital cash from Wallet
	Pay (**p**)	[Amount]	[Target ID]	**mp 100 44**	Pay 100 units from V-Acc to Target No. 44
Parking (p)					
	Control (**c**)		[Location Number]	**pc 23**	Request to control the parking position
	Departure (**d**)			**pd**	Indicate system that the car is leaving the parking position
	Inquiry (**i**)			**pi**	Request to inquiry parking information (lot number, meter number, parking time, etc).
	Pay(**p**)		[Lot number], [meter number], [parking time]	**pp 23987 3**	Request to pay the parking fees on lot number:23, meter number:987, parking time:3 hours
	Violation (**v**)		[Lot number], [meter number]	**pv**	Indicate system parking violation
Ticket (t)					
	Buy (**b**)		[Ticket ID]	**tb 3433445**	Request to buy a ticket
	Transfer(**t**)		[Ticket ID], [Target ID]	**tt 6565656 1234343456**	Transfer a ticket to another account
	Use (**u**)		[Ticket ID]	**tu 5478348**	Use ticket with ticket ID

Table 4. SAFE Commands and Their Description

5.2 Secure Messages

SAFE system provides three options for security of messages, as shown in Figure 18.

a. *Basic security:* this option uses standard GSM security of messages and strong security only from the Gateway further into the system. End-to-end security is not provided. This is the case when people want to use standard SMS function in every mobile phone without loading and using any software. This case is very popular in rural areas, since advanced mobile phones, which support Java platform, Bluetooth, large storage capability, etc. are not commonly used in rural areas. In this case, data is encrypted by GSM A5/1 algorithm from a client to the *SAFE* Gateway Server, and then Gateway Server encrypts data by using RSA (asymmetric crypto algorithm) and sends to backend Bank server or other service providers' servers.
b. *Medium security:* with this option, end-to-end security is provided by sharing a secret key between client and service providers. In this case, the Gateway Server is just a passer between client and service providers. However, users' mobile phone must be able to support

Java platform, since secure mobile wallet has to be loaded in mobile phone and user should use Thin or USSD mobile wallet, mentioned in Chapter 6, to conduct the transactions instead of basic functions provided by every mobile phone.

c. *High security:* with this option, end-to-end security is provided by using asymmetric crypto functions. In this case, user needs not only to load secure mobile wallet, but also his/her certificate. In addition, user is able to prevent data from being revealed to the Gateway Server. It is working like this: user first encrypts sensitive data with randomly generated symmetric key, then envelops that key using the public key of service provider, attaches the encrypted result to the data that can be known by Gateway Server (IP address of service provider, user's mobile phone number etc.), sends the message to Gateway Server.

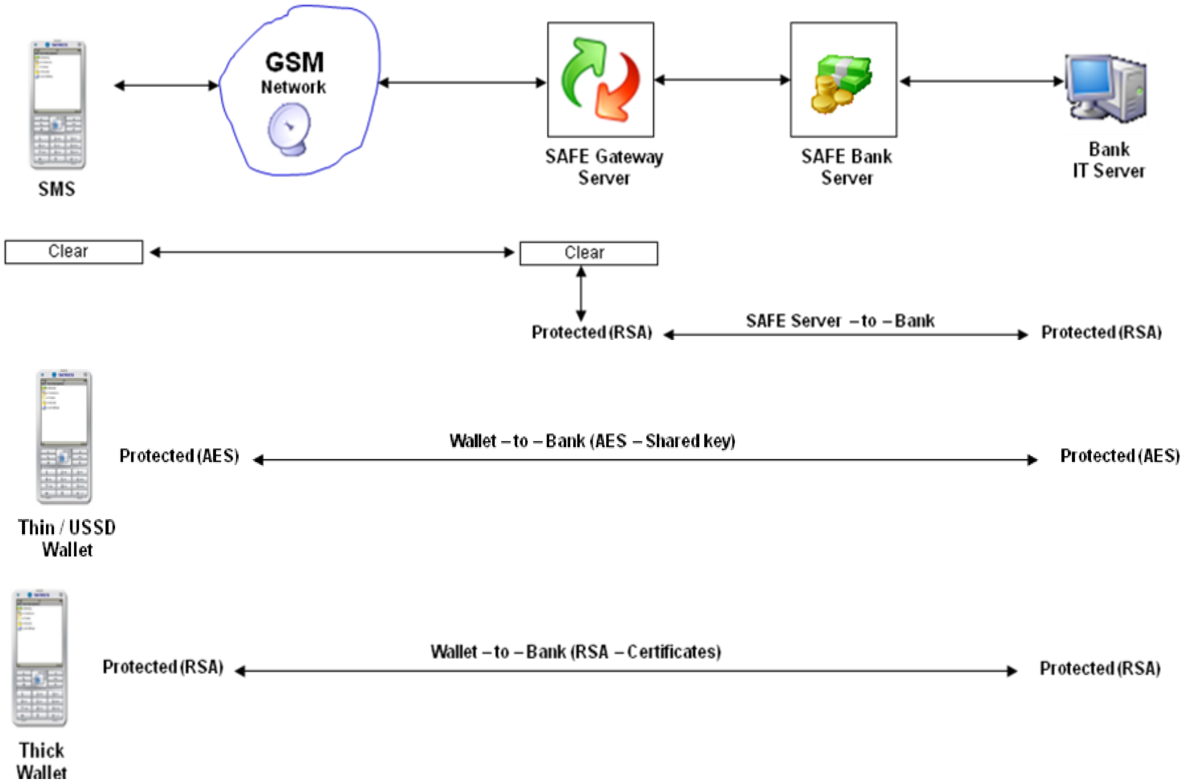
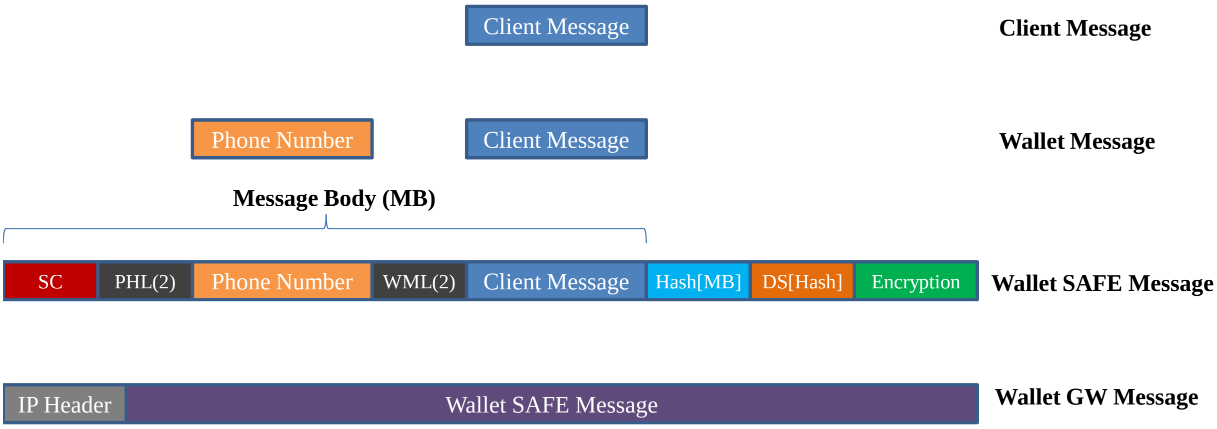


Figure 18. Security of Messages

If users want the highest level of security they should be registered through face–to–face procedure, so that all identities are strongly verified. Identification information stored in IDMS servers is encrypted, thus not vulnerable to the identity theft attack.

In order to achieve end-to-end security, *SAFE* system defines a comprehensive format for message enveloping. The message format is shown if Figure 19.



Client Message: ***transaction command***
Wallet Message: ***client message added with client's mobile phone number***
SAFE Message: ***wallet message added with security fields***
GW Message: ***Gateway Message that is SAFE message added IP header, which is ready to send to Gateway Server***
Phone Number: ***client's mobile phone number***
SC: ***Security Option(a. No Security b. Hash c. Encryption d. Both Hash & Encryption)***
DS[Hash]: ***Digital Signature of the hash value***
PHL (2): ***phone number length (2 bytes)***
WML (2): ***wallet message length (2 bytes)***

Figure 19. SAFE Message Format

There are three security options:

a. ***Encryption*** – security option is set to ENCRYPTIOIN in the security header. Message encryption key (MEK) is randomly generated and used to encrypt message content for message confidentiality. MEK is then encrypted with recipient's public key and combined with the encrypted content. Finally, secure message is packaged which contains encrypted message and encrypted MEK.

At the receiving end, recipient will inspect security header to check which "*security option*" was selected. If it is ENCRYPTION, recipient decrypts MEK with his private key and thereafter decrypts encrypted message using the MEK. The progress is shown in Figure 20.

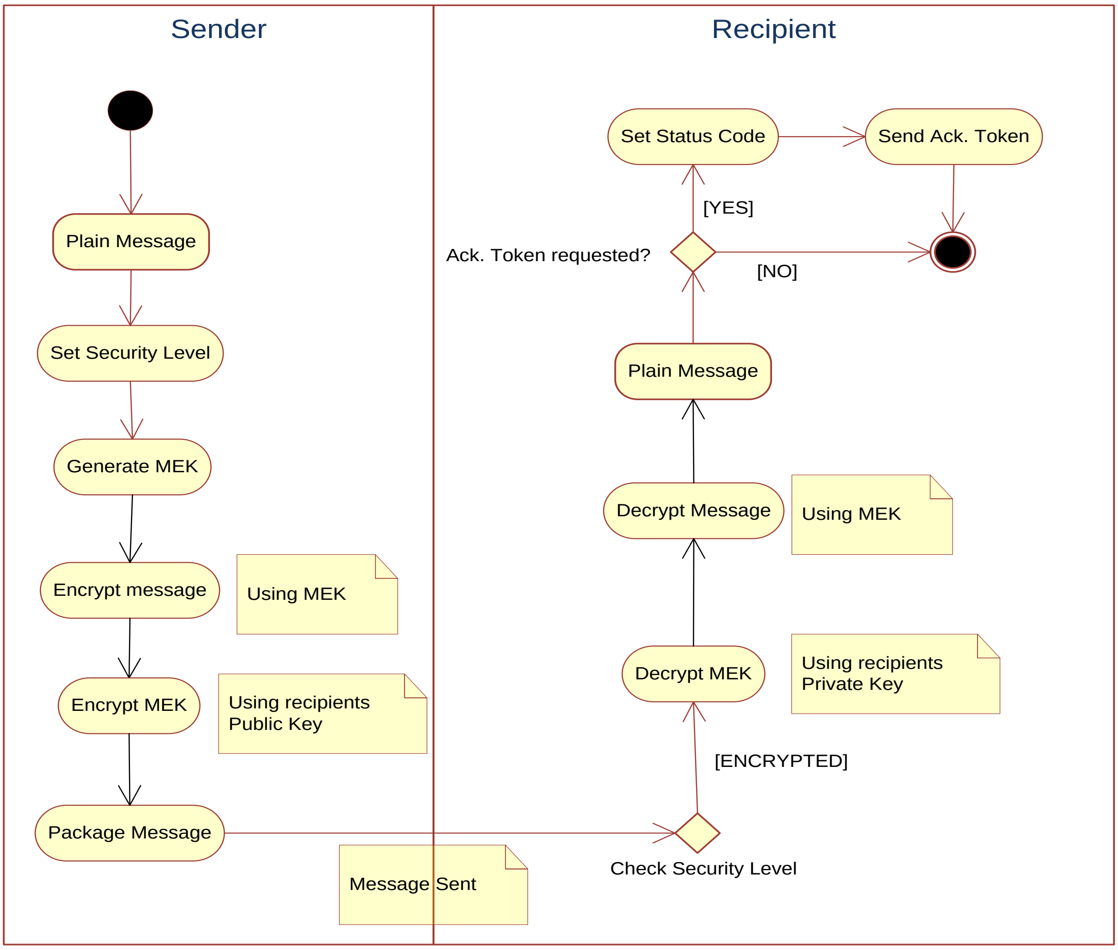


Figure 20. Message Confidentiality Protection

b. ***Integrity*** – security option in the security header is set to INTEGRITY. Hash of the message is calculated using SHA-1 to get Message Digest. This Message Digest is signed with the sender's private key. Message is packaged and ready to be sent using any transport protocol.

At the receiving end, the recipient will inspect security header to check "*security option*". Recipient independently calculates Message Digest using SHA-1 and compares it with the received "digital signature" after decrypting it with sender's public key. The progress is shown in Figure 21.

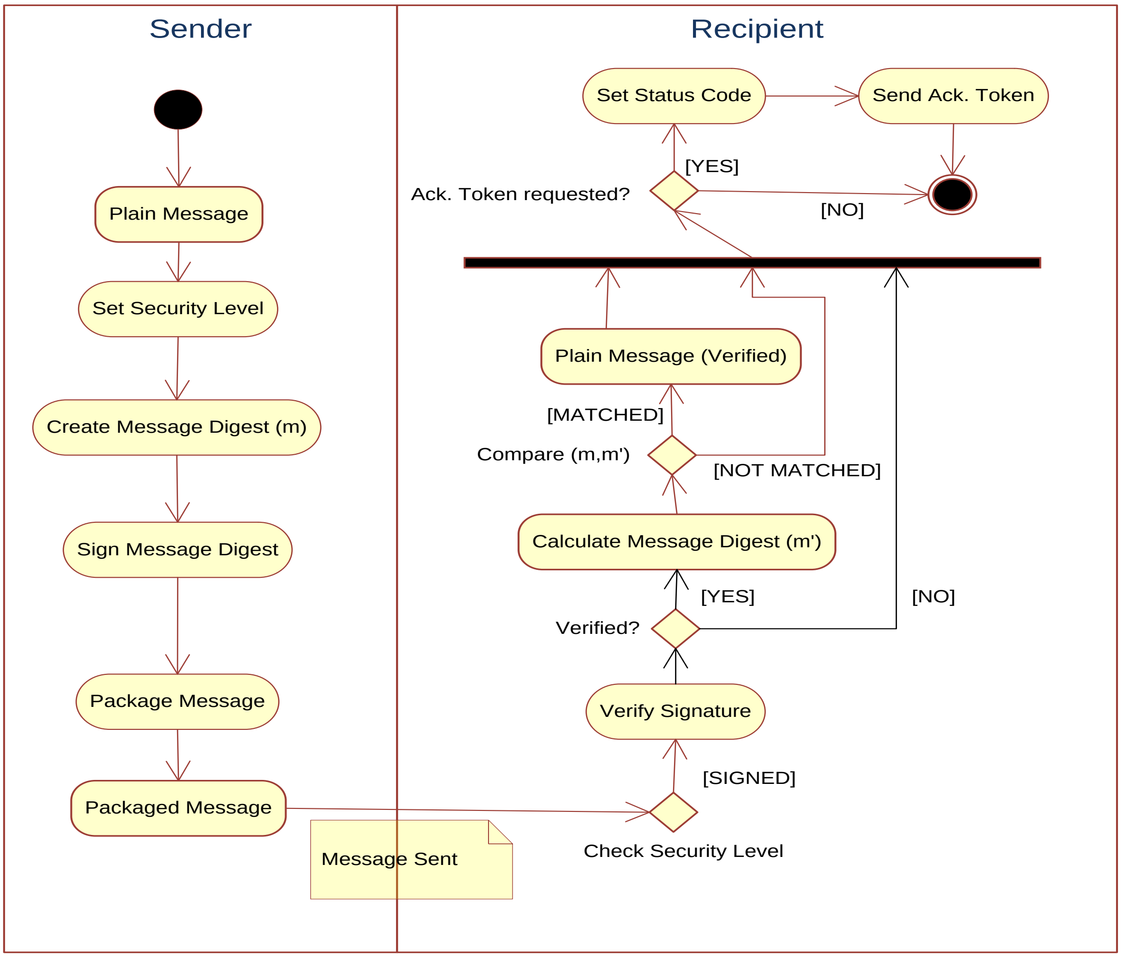


Figure 21. Message Integrity Protection

c. ***Encryption and Integrity*** – security option in the security header is set to SIGNED_ENCRYPTED. To sign and envelop a message, the steps required for signing and encrypting are performed one after the other. In the first step, message is signed by calculating Message Digest and then signing it to get Digital Signature, and in the second step, Message Encryption Key (MEK) is generated to encrypt message content along with digital signature. MEK is then encrypted with recipient's public key and packaged.

At the receiving end, recipient checks security header for "*security option*". Recipient decrypts MEK using his private key, and using MEK decrypts the received message which contains digital signature of the sender and actual message content. Recipient verifies digital signature to confirm message integrity and secure authentication. The progress is shown in Figure 22.

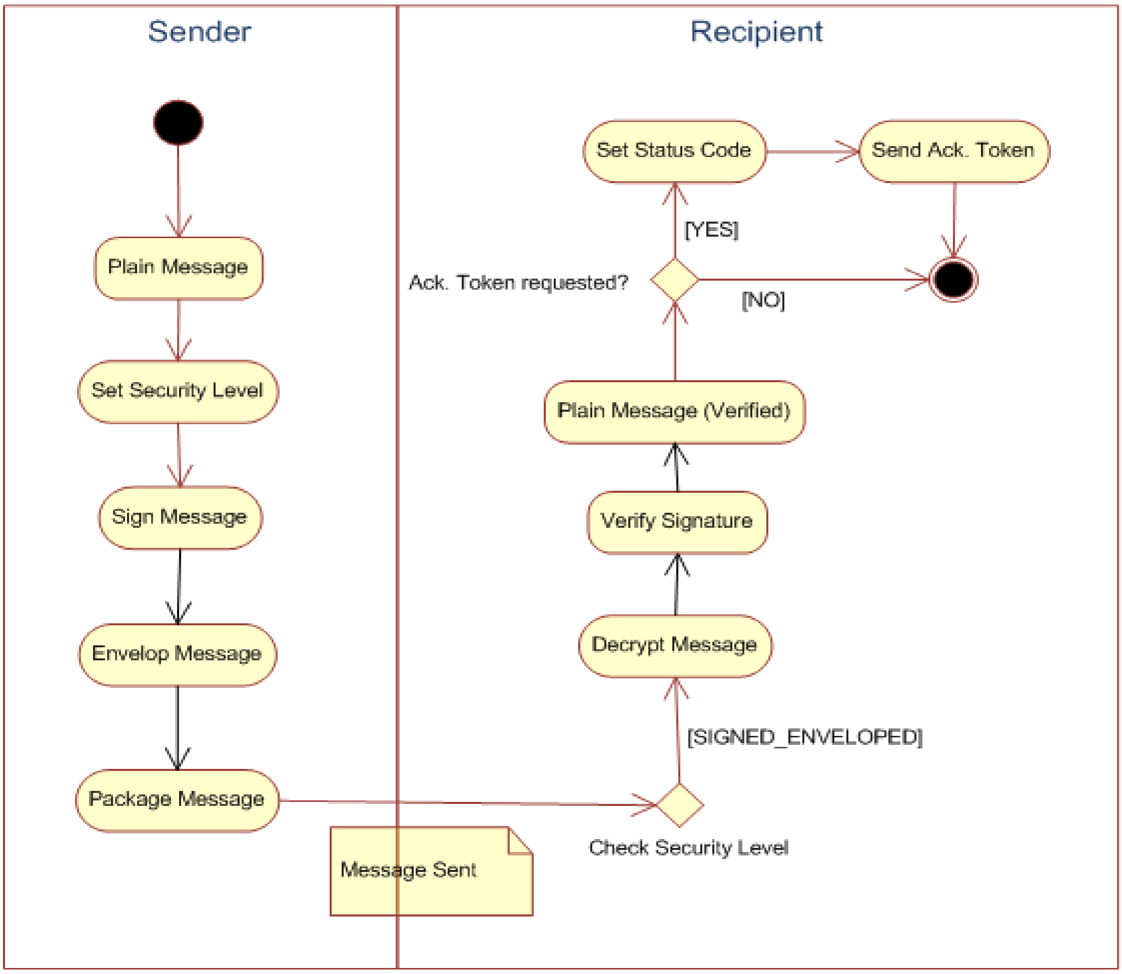


Figure 22. Message Confidentiality and Integrity Protections

Chapter 6:

Implementation and Demonstration

All servers of the *SAFE* system are running on standard OS platforms – various versions of Windows, using Java Run–Time Environment, SQL–compliant database servers, and TCP/IP protocols. Deployment of client mobile stations, especially secure mobile wallet, deserves additional attention and considerations. Namely, the development goal was that the wallet should be portable to different types of mobile phones and in different environments (developed and developing countries).

Considering those limitations, there are several versions of the Mobile Wallet. The simplest version is based on SMS messages, sent over a network to the *SAFE* Gateway Server, without the need of preloading of any software. The next version is "Thin" Wallet, software that provides only GUI for SMS messages. The third one is called USSD Wallet, software that provides USSD service for mobile customers. The most comprehensive version is "Thick" Wallet that must be pre–loaded into a phone. The full Wallet provides all security features described in this report. If the Wallet is loaded into the phone, then there are two versions of the Wallet: one that can be downloaded through mobile Internet and the other that is pre–loaded in the UICC of mobile phone. Thus, *SAFE* wallet supports a variety of mobile phones, with alternative capabilities, and wireless communication protocols. More details about *SAFE* Secure Mobile Wallet are given in this chapter.

6.1 *SAFE* Administrative Station

6.1.1 Registration of Entities

All the entities must be first registered. *SAFE* system provides Administration Station for administrator to register and manage entity data.

- Registration of Banks

Each bank connected to the *SAFE* Bank Server must be registered. Registration of individual banks and the listing of registered Bank Servers may be obtained using "Banks" drop–down menu:

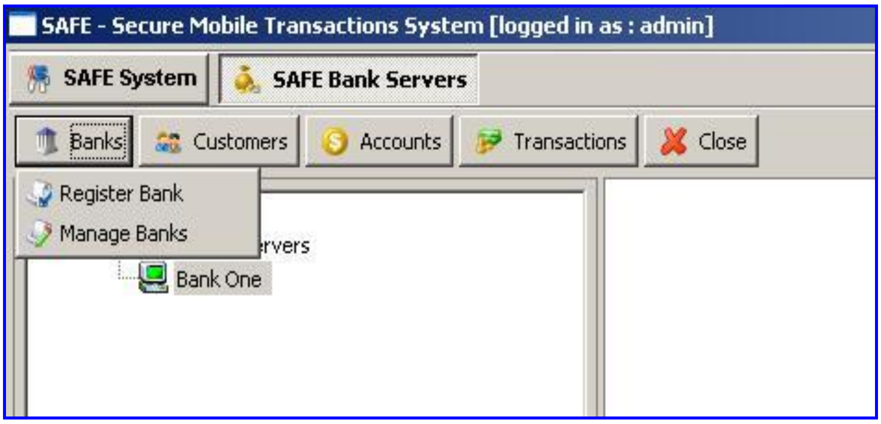
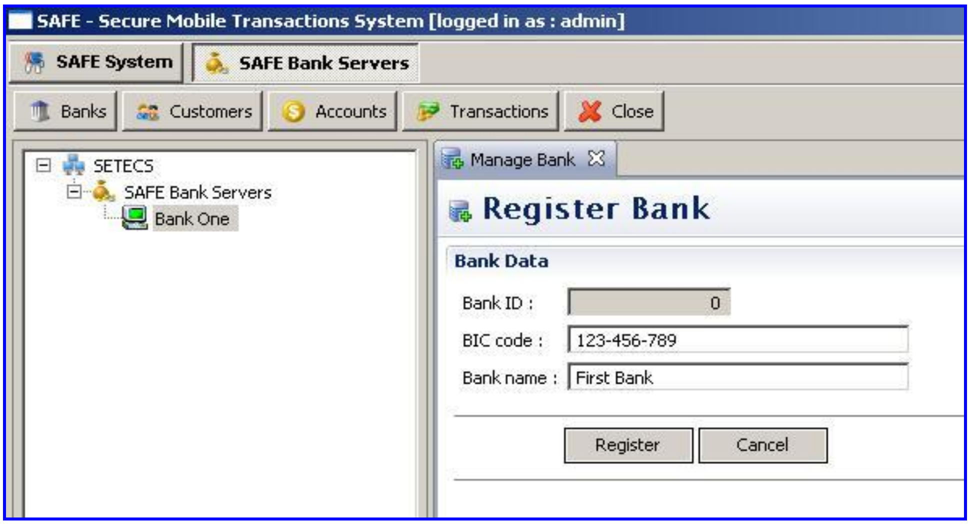


Figure 23. "Banks" Drop-Down Menu

To register a bank, press "*Banks*" drop–down menu, and select "*Register Bank*" drop–down option. The following form will be displayed:



Bank Data

Bank ID : 0

BIC code : 123-456-789

Bank name : First Bank

Figure 24. The Form to Register Bank

- Registration of Customers and Accounts

Depending on the type of services it provides for a particular deployment, *SAFE* system may have two types of customers: *banked customers*, those with real bank accounts, and *SAFE customers*, either un–banked customers who have only *SAFE* pre–paid accounts or even banked customers who for various m–services open their *SAFE* accounts. Procedures for registration of customers and their accounts are slightly different in the two cases.

a. Banked Customers and Real Bank Accounts

Each banked customer must be registered in the system. To register customers, press "Customers" drop–down menu and select "Register Customer" option.

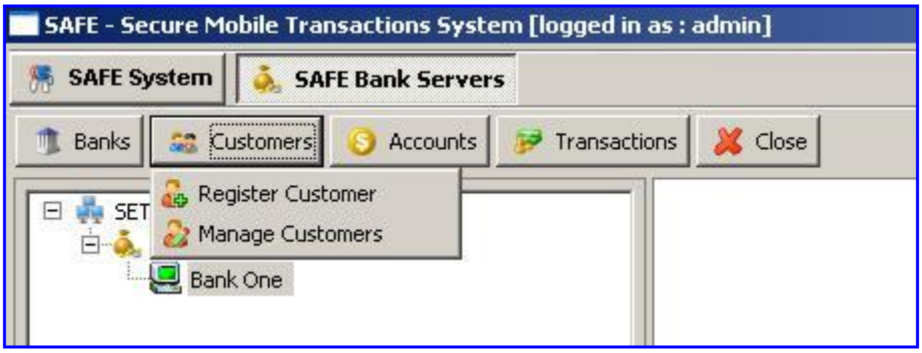
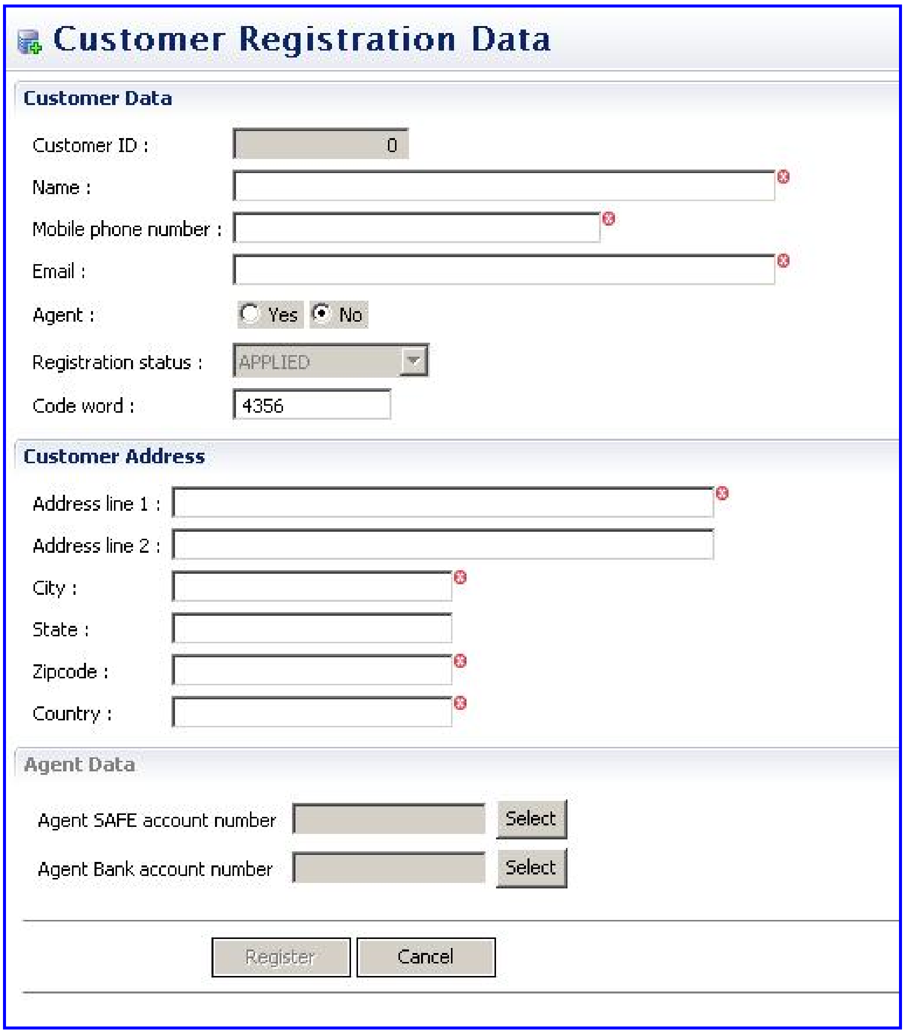


Figure 25. The Functions for Administration of Customers

The following form will be displayed:



Customer Registration Data

Customer Data

Customer ID : 0

Name :

Mobile phone number :

Email :

Agent : ○ Yes ● No

Registration status : APPLIED

Code word : 4356

Customer Address

Address line 1 :

Address line 2 :

City :

State :

Zipcode :

Country :

Agent Data

Agent SAFE account number Select

Agent Bank account number Select

Register Cancel

Figure 26. The Form to Register Customers

For banked customers only “Customer Data” and “Customer Address” sections should be populated. Customer ID is automatically assigned. Mobile Phone Number must be entered with the full int’l exchange sign (+), country code and the mobile number, without any blanks. Example: +11234567000. “Agent” option should be left to “No”. Code word is randomly generated customer’s password.

Registration data can be updated, using “Manage Customers” function (see Figure 25). When a banked customer is registered, the next step is to register his/her bank account. For that and other functions with accounts, “Accounts” drop–down menu should be used.

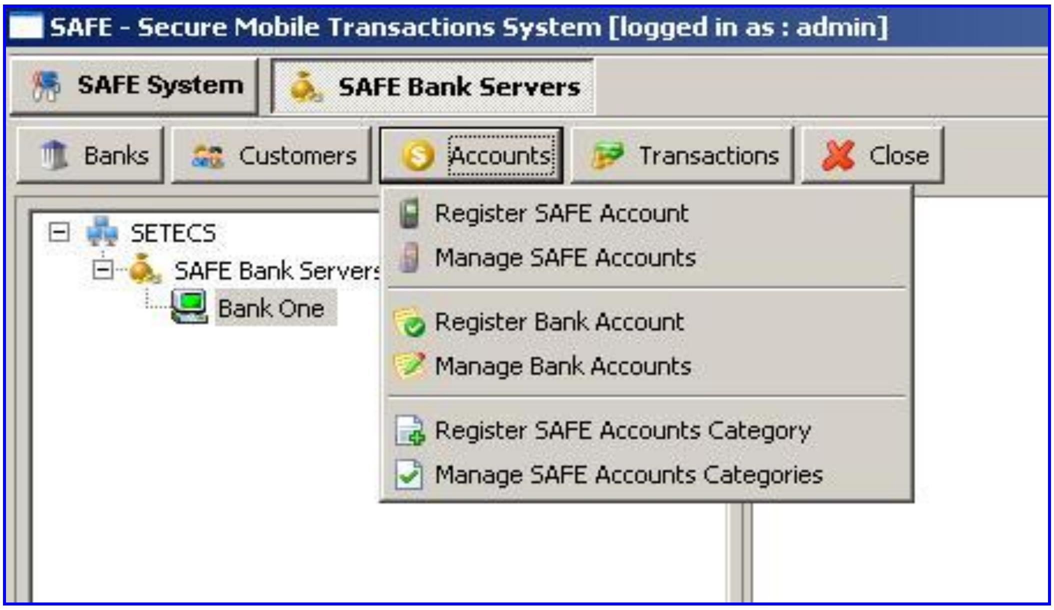
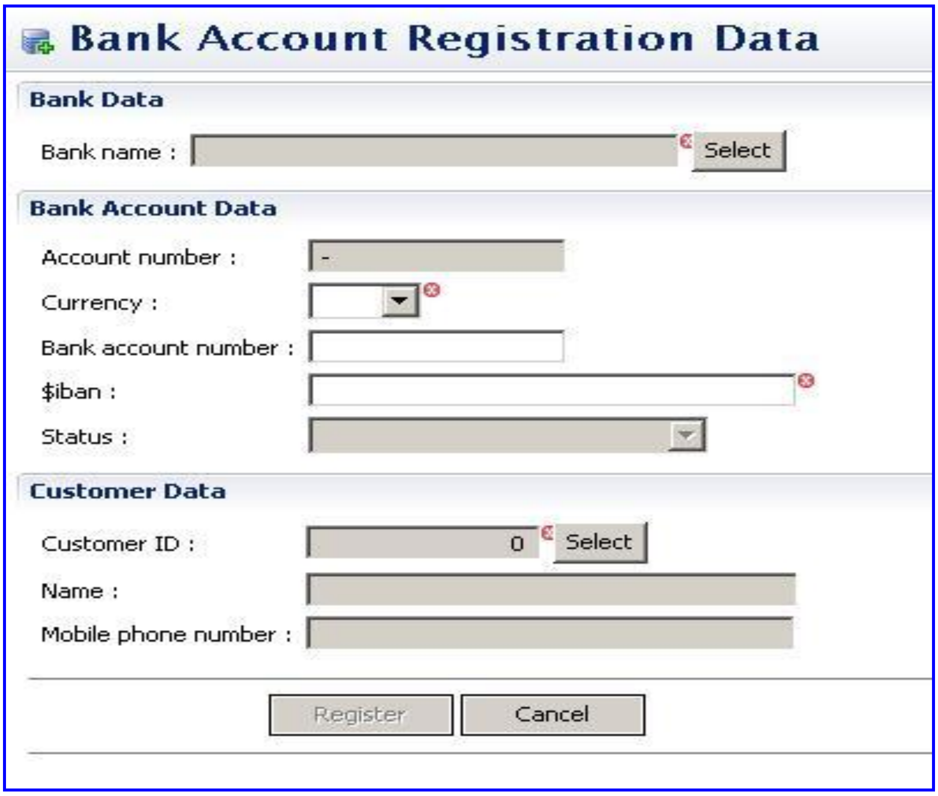


Figure 27. The Functions to Manage Accounts

To register bank account, “Register Bank Account” option is used. It displays the following form:



Bank Account Registration Data

Bank Data

Bank name : Select

Bank Account Data

Account number : -

Currency :

Bank account number :

$iban :

Status :

Customer Data

Customer ID : 0 Select

Name :

Mobile phone number :

Register Cancel

Figure 28. Registration of a Bank Account

“Bank name” should be selected from previously registered banks. “Customer Data” should be selected from previously registered customers.

Data for accounts can be updated using *“Manage Bank Accounts*” function (see Figure 27).

When bank customer and his/her bank account are registered, the customer may start using the system for various m–banking services.

b. Un-banked Customers and *SAFE* Pre-Paid Accounts

For un–banked customers, registration procedure is a bit different than for banked customers. First, pre–paid amounts must be deposited in some real bank account. Therefore, the first “customer” that needs to be registered is service provider itself. That is the entity/company/bank providing m–payment services based on pre–paid accounts. It must have real bank account, which is used as collective (escrow) account to keep all pre–paid amounts.

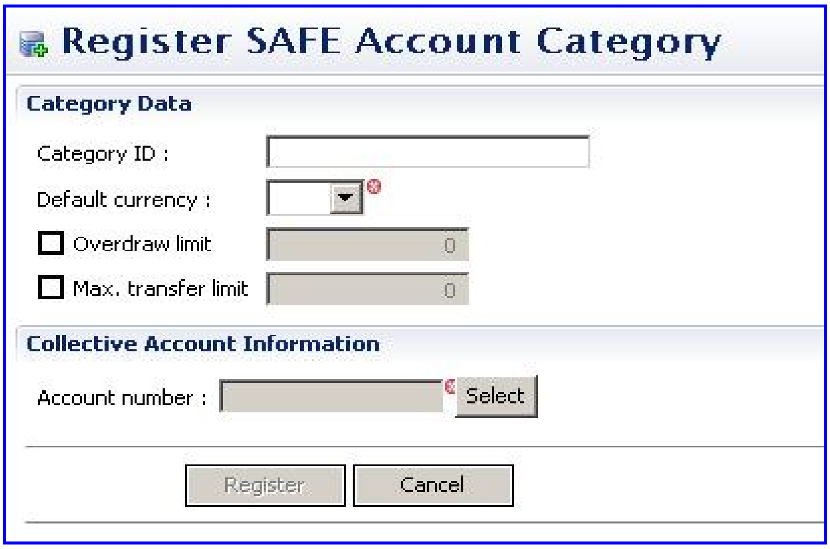
Next, since *SAFE* pre–paid accounts are not real bank accounts, they are not regulated or controlled by any restrictions and/or regulations, as bank accounts. Therefore, *SAFE* system uses the concept of account categories. Categories impose certain restrictions on use of *SAFE* accounts. Each *SAFE* account is linked to one of the categories and restrictions for that category apply to all those *SAFE* accounts. In the current version, account categories have “Overdraw limit” and “Max transfer limit”, but other restrictions may be introduced.

Finally, besides services provider, *SAFE* system with *SAFE* pre–paid accounts has another special category of users: *agents*. They are also customers of the system, but they can assist other customers with registration, cash–in and cash–out transactions. If some customer in the system is also an agent, than he/she must be explicitly declared as such.

With all these additional features and properties of the *SAFE* system when handling un–banked customers and *SAFE* pre–paid accounts, the procedure for registration of customers and their accounts is the following:

The first step is to register service provider and its real bank account that will be used as a collective account for *SAFE* pre–paid accounts. The procedure for that is the same as for banked customers, described in section 6.1.1 a. Real bank account registered for the service provider will be the collective account in the system.

The next step is to register account categories. For that, “*Register SAFE Accounts Category*” function is used (see Figure 29). When selected, the following form is displayed:



Register SAFE Account Category

Category Data

Category ID :

Default currency :

□ Overdraw limit 0

□ Max. transfer limit 0

Collective Account Information

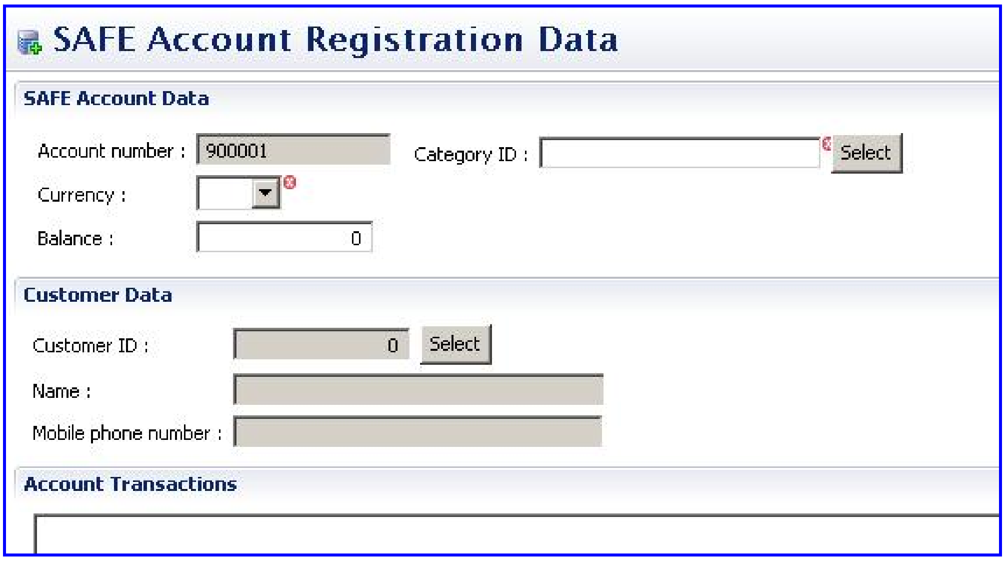
Account number :

Figure 29. Registration of the SAFE Accounts Category

Category ID as arbitrary designation of the category. The first category to be registered is used as a default category, but for subsequent categories, "*Default category*" indicator should be selected. "Account number" is real bank account, which is used as a collective account for this category. All *SAFE* pre–paid accounts are linked to some category and therefore indirectly, via the category, to the collective real bank account.

The next step is to register customers with *SAFE* pre–paid accounts. The procedure is the same as with banked customers. In addition, the same form (Figure 26) can now be used to declare some of the registered customers as *SAFE* agents. For that, customer registration data should be displayed and option "*Agent*" should be set to "*Yes*". In that case "*Agent SAFE account number*" and "*Agent Bank account number*" categories will be activated, so that through "*Select*" buttons their account numbers can be declared. Agents may use *SAFE* pre–paid or their real bank accounts.

For registration of *SAFE* pre–paid accounts, the function "*Register SAFE Account*" (Figure 27) is used. It displays the following form:



SAFE Account Registration Data

SAFE Account Data

Account number : 900001

Category ID :

Currency :

Balance : 0

Customer Data

Customer ID : 0

Name :

Mobile phone number :

Account Transactions

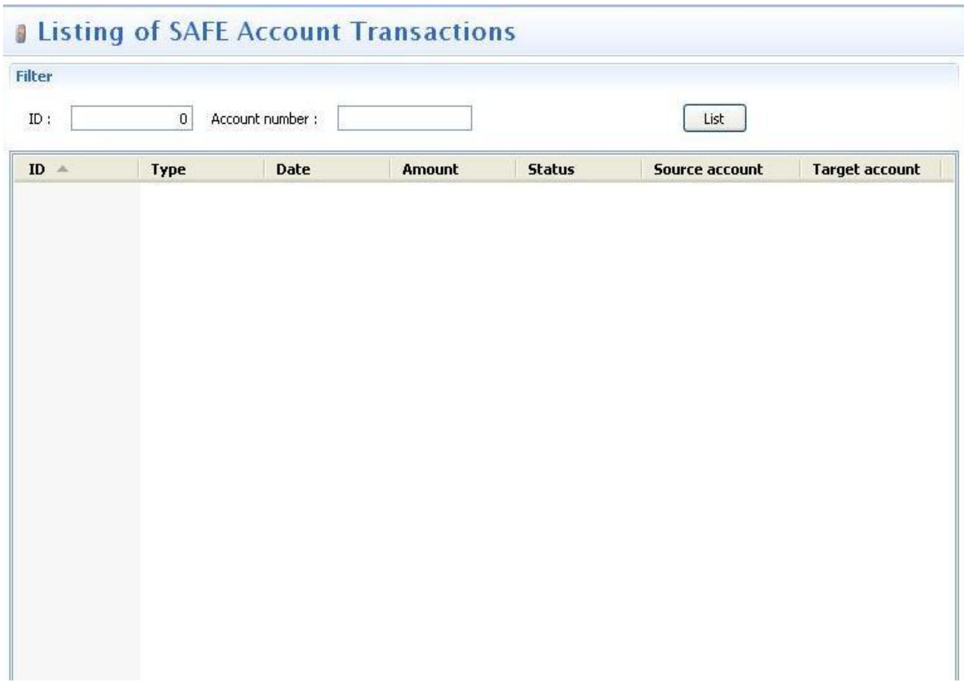
Figure 30. The Form to Register SAFE Accounts

"*Account number*" is automatically generated. "*Category ID*" should be selected from the registered categories and "*Customer Data*" should be selected from registered customers.

After registration of the service provider, categories, agents, customers and their *SAFE* accounts, the system can be used by un–banked customers.

6.1.2 Transactions Management

SAFE Administrative Station supports transactions management function that keeps the logs of all customers' transactions and messages. Figure 31 shows the management of all transactions. As it is shown, administrator types in customer's account number and then system shows the log of all the transactions for that account. This is useful for bank administrators to audit and trace customers' transactions. Figure 32 shows the form to list messages. When administrator types in customer's mobile phone number, system shows all SMS messages sent out/received to/from that customer. This is useful for telecom operator administrators to trace all the message flows.



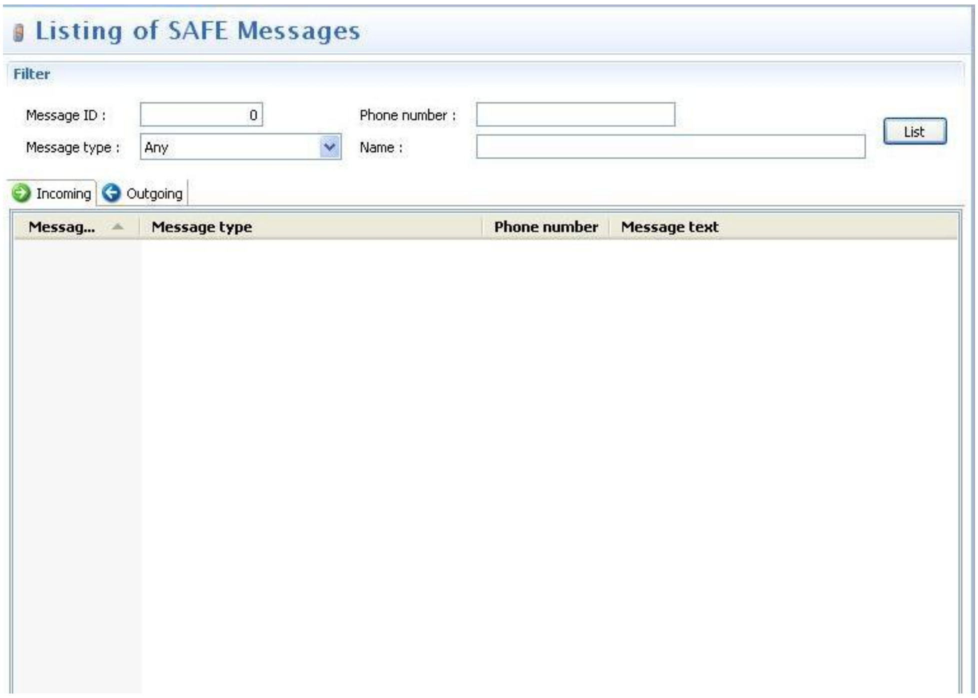
Listing of SAFE Account Transactions

Filter

ID : 0 Account number :

ID	Type	Date	Amount	Status	Source account	Target account

Figure 31. The Form to List SAFE Account Transactions



Listing of SAFE Messages

Filter

Message ID : 0 Phone number :

Message type : Any Name :

Messag...	Message type	Phone number	Message text

Figure 32. The Form to List SAFE Messages

6.2 Secure Mobile Wallet

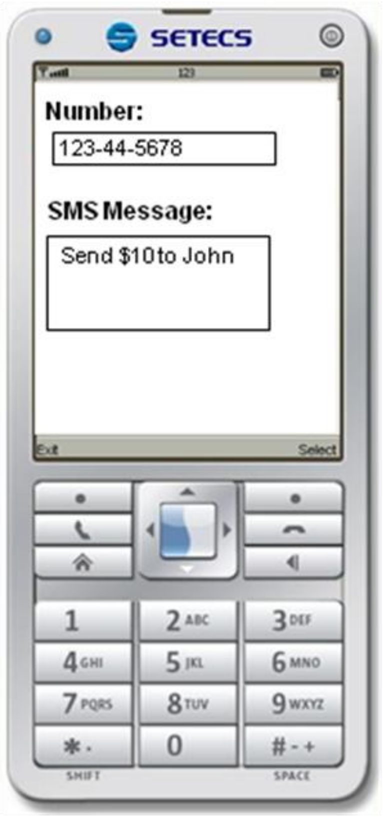
As one of the components of the *SAFE* system, secure mobile wallet represents secure, stable, convenient and easy-operational application, which is pre-loaded into customer's mobile device. This section describes design, implementation and demonstration of *SAFE* secure mobile wallet.

6.2.1 Versions of the Secure Mobile Wallet

SAFE system provides four versions of secure mobile wallets: SMS Wallet, Thin Wallet, USSD Wallet, and Thick Wallet. The section gives overviews of these four versions of the wallet.

SMS Wallet

SMS wallet is based on usage of the standard SMS messages. Since all mobile phones support this function, it will be the most widely spread version of secure mobile wallet. It has the least requirements for customer's mobile device. The disadvantage of this version is that it could not use other communication protocols, such as Bluetooth or GPRS. Therefore, there is no session created during transaction process, which directly influences the speed of the transaction process. Figure 33 shows an example of the SMS Wallet.



Number:

123-44-5678

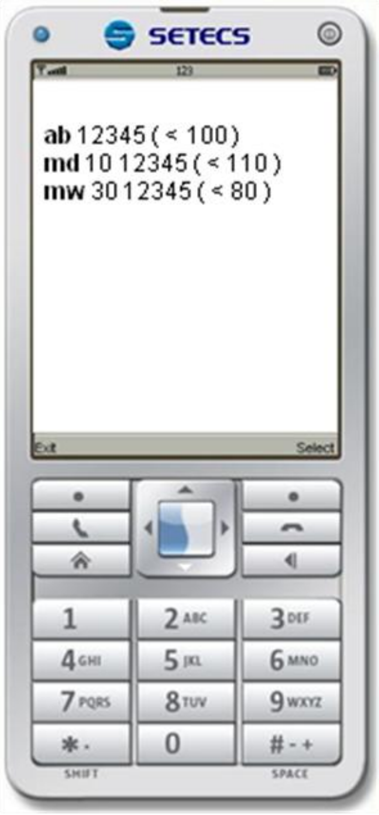
SMS Message:

Send $10to John

Figure 33. Example of the SMS Wallet

Thin Wallet

The concept of a Thin Wallet comes from the "Command Prompt" function in most operating systems. It supports text-based (command-line) function. It is easier and faster to perform transactions, besides it could use Bluetooth and GPRS to build a session with *SAFE* Gateway server. In Thin Wallet, there is a text box, whose size is as large as the mobile phone's screen. From the text box customer can enter *SAFE* command, which is illustrated in Chapter 5, as transaction request. After user clicks "Enter", transaction request is sent out to the Server through available communication protocol and Thin Wallet receives the response from the Server. The response is shown in the same text box, but one line below the first line. Then user can keep entering the next command on the first line and will get the response at the same position as the previous response. Previous response will be deleted from the text box. The example of Thin Wallet is shown in Figure 34.

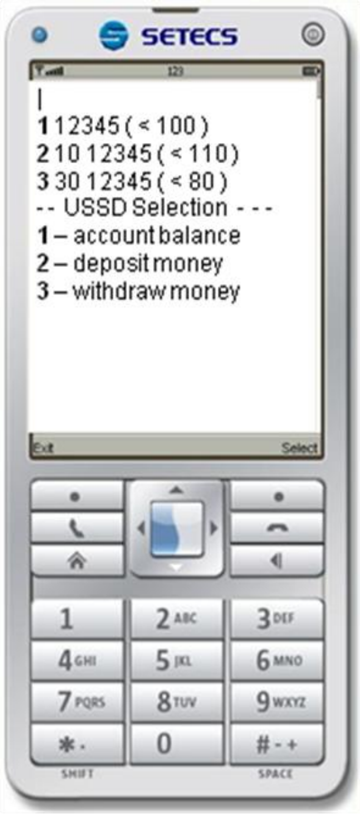


```
ab 12345 ( < 100)
md 10 12345 ( < 110 )
mw 30 12345 ( < 80 )
```

Figure 34. Example of the Mobile Thin Wallet

USSD Wallet

USSD (Unstructured Supplementary Service Data) is a capability of all GSM phones. It is generally associated with real-time or instant messaging type phone services. There is no store-and-forward capability, typical of other short-message protocols (in other words, an SMSC is not present in the processing path). Response times for interactive USSD-based services are generally quicker than those used for SMS. USSD Wallet is based on the combination of USSD and Thin Wallet. USSD Wallet has also one big text box for user entering command, except that USSD code instead of text command is entered. The menu is sent back from the Server and shown in the text box. Customer could choose from the menu by entering the number in front of the item. The usage example of USSD Wallet is shown in Figure 35.



```
1 12345 ( < 100 )
2 10 12345 ( < 110 )
3 30 12345 ( < 80 )
-- USSD Selection - - -
1 – account balance
2 – deposit money
3 – withdraw money
```

Figure 35. Example of the Mobile USSD Wallet

Thick Wallet

Thick Wallet provides the most comprehensive set of functions and support for customers out of the four versions. It gives full GUI that contains drop-down selections and data entry forms. Therefore, the requirements of running this version are relatively higher than the other three versions. All kinds of communication protocols, such as SMS, Bluetooth, GPRS, etc., are supported by the Thick Wallet. Customers may choose the most proper one for transactions based on different environment situation and contexts. Fox example, when user is sitting at home and wants to buy a ticket, SMS or GPRS are more suitable, since the distance from a client to the server is too far to use Bluetooth connection. However, if the user goes into a shop to buy over the counter, Bluetooth is the most convenient and fastest protocol to use it. The example of the main interface is shown in Figure 36.

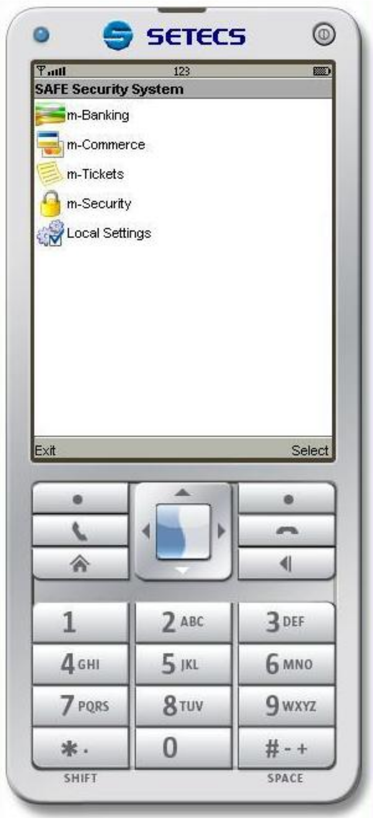


Figure 36. Example of the Mobile Thick Wallet

UICC Wallet

All the versions listed above are based on the use of memory card of a mobile device. We also have the version that is loaded inside the UICC (Universal Integrated Circuit Card) of the mobile phone called UICC Wallet, which stores data in a UICC. The UICC is the smart card used in mobile phone in GSM or UMTS networks. Since it is a smart card, it inherits all the security features of smart cards. It provides a secure storage of data. The functionalities and applications are the same as SMS Wallet except that user interface of the UICC Wallet is simpler than that of SMS Wallet due to the limitations of storage and process ability of a UICC.

For the implementation of UICC wallet, we created a middleware located between upper layer application and lower layer smart card applet. The middleware receives requests from upper layer, transfers them into APDUs, and sends the APDUs to the applets in the UICC. Then the middleware transfers the responses from UICC to the desired format and sends the response to the upper layer application. The example of the UICC wallet is shown in Figure 37

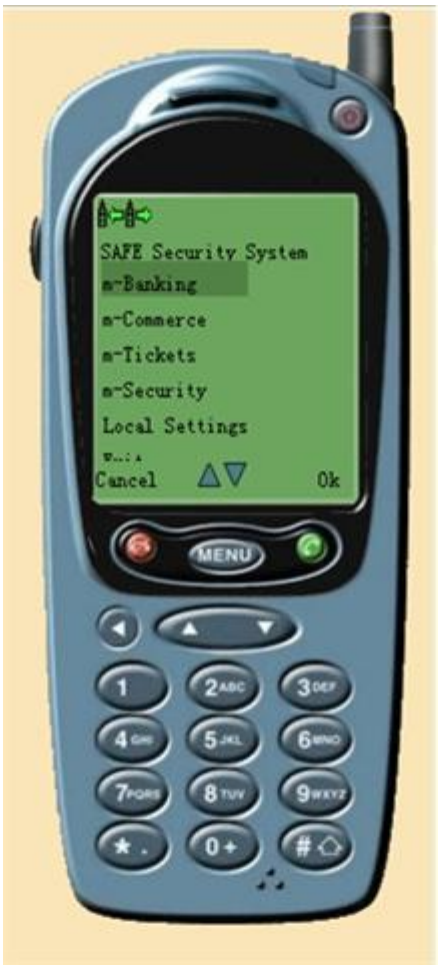


Figure 37. Example of the Mobile UICC Wallet

6.2.2 Design and Implementation

SAFE Secure Mobile Wallet as an application is developed using Java (J2ME), while as an applet it is developed using JavaCard framework. Its internal structure comprises four groups of modules:

a. GUI module – responsible for creating all user interface, related objects, such as forms, text editors, choice boxes etc.
b. Communication module – responsible for creating communication interfaces for all supported protocols between client and server,
c. Business logic module – responsible for creating transaction request messages and processing responses messages,
d. Security module – a "black box" that takes responsibility to utilize and combine security mechanisms providing security features, such as authentication, confidentiality, integrity for transactions and operations.

The internal structure and components of the Secure Mobile Wallet are shown in Figure 38.

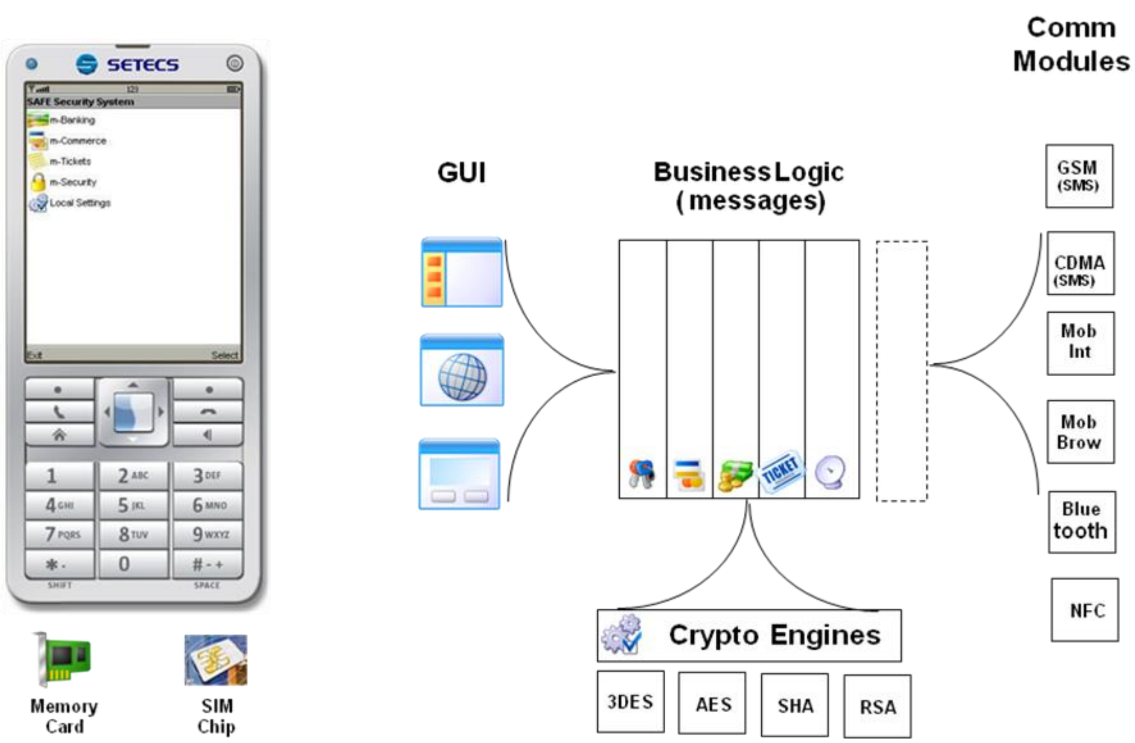
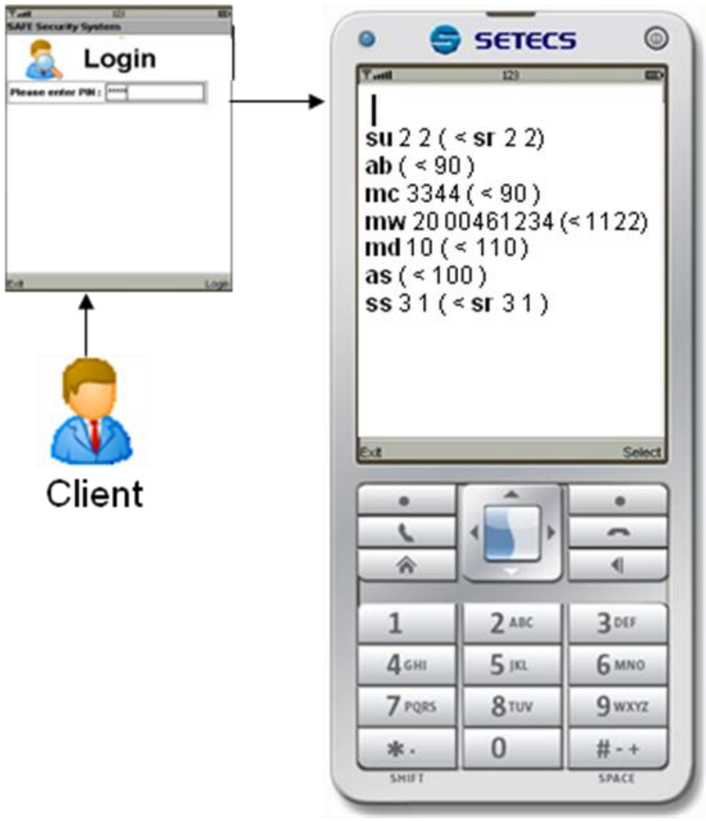


Figure 38. Internal Structure and Components of the Secure Mobile Wallet

One usage scenario of Secure Mobile Wallet is shown in Figure 39.



Please enter PIN : ****

```
su 2 2 ( < sr 2 2)
ab ( < 90 )
mc 3344 ( < 90 )
mw 20 00461234 (< 1122)
md 10 ( < 110)
as ( < 100 )
ss 3 1 ( < sr 3 1 )
```

Figure 39. Usage Scenario of Secure Mobile Wallet

Client starts by activating Wallet and giving PIN. The convention is: if four-digit PIN is given, then Thin Wallet is used; five-digit PIN – USSD Wallet; and six-digit PIN – Thick Wallet. We use a Thin Wallet in the example (commands are listed bottom-up, the most recent command is on the top).

Client starts by initiating session: (**ss 3 1**): session start (**ss**), security level (Enc + Hash, Level **3**) and wallet type – Thin Wallet (**1**). *SAFE* server responds with session response (**sr 3 1**). Client inquires account status (**as**), the response is 100 units.

Client deposits 10 units (**md 10**), new account status is now 110 units.

Client initiates money withdrawal (using "Mobile ATM – bank's agent) giving the amount and agent's mobile phone number (**mw 20 00461234**). *SAFE* Server responds by returning confirmation number (1122) to the client. At the same time, *SAFE* Server sends another confirmation number to the agent (3344).

Client confirms the receipt of money by returning agent's confirmation number (**mc 3344**). At the same time, the agent confirms transaction my returning client's confirmation number (**mc 1122**). The Server returns new client's account balance (90).

When the client inquires again account balance (**ab**), it is confirmed as 90 units.

Client may switch security level and Wallet type during the session: client updates the session to use security level 2 (encryption only) and USSD Wallet (**su 2 2**). *SAFE* Server confirms new session (**sr 2 2**).

Chapter 7:

Thesis Research Contributions

In this Chapter we summarize research contributions of this thesis. First, we give the list of publications that were produced during this work. Then, we provide the summary of the contributions for the problems we worked on.

7.1 List of Publications

1. Amila Karunanayake, Kasun De Zoysa, Sead Muftic, ***Feng Zhang***. ”*Experiences on Mobile-ATM Deployment in a Developing Country*”. Proceedings of the 1st International Conference on M4D Mobile Communication Technology For Development (M4D 2008, General Tracks): 11-12 December, 2008, Karlstad University, Sweden.
2. ***Feng Zhang***, Sead Muftic, Kasun DeZoysa, “*SAFE System: Applications for Financial Environments Using Mobile Phones*”, Proceedings of IADIS International Conference IADIS e-Society, February 2009, Barcelona, Spain.
3. Amila Karunanayake, Kasun De Zoysa, Sead Muftic, ***Feng Zhang***. ”*Mobile ATM for Developing Countries*”, Demonstration of the 7th ACM/USENIX International Conference on Mobile Systems, Applications, and Services, ACM, June 2009, Kraków, Poland.

7.2 Security Features of The *SAFE* System

One of the distinguished features of the *SAFE* system, which makes it different from any other similar system, is its strong security. The security services architecture is shown in Figure 40. There is IDMS Server for secure identification, CA Server for issuing and managing certificates of every entity, and Authorization Server for managing access control and different authorities for different entities.

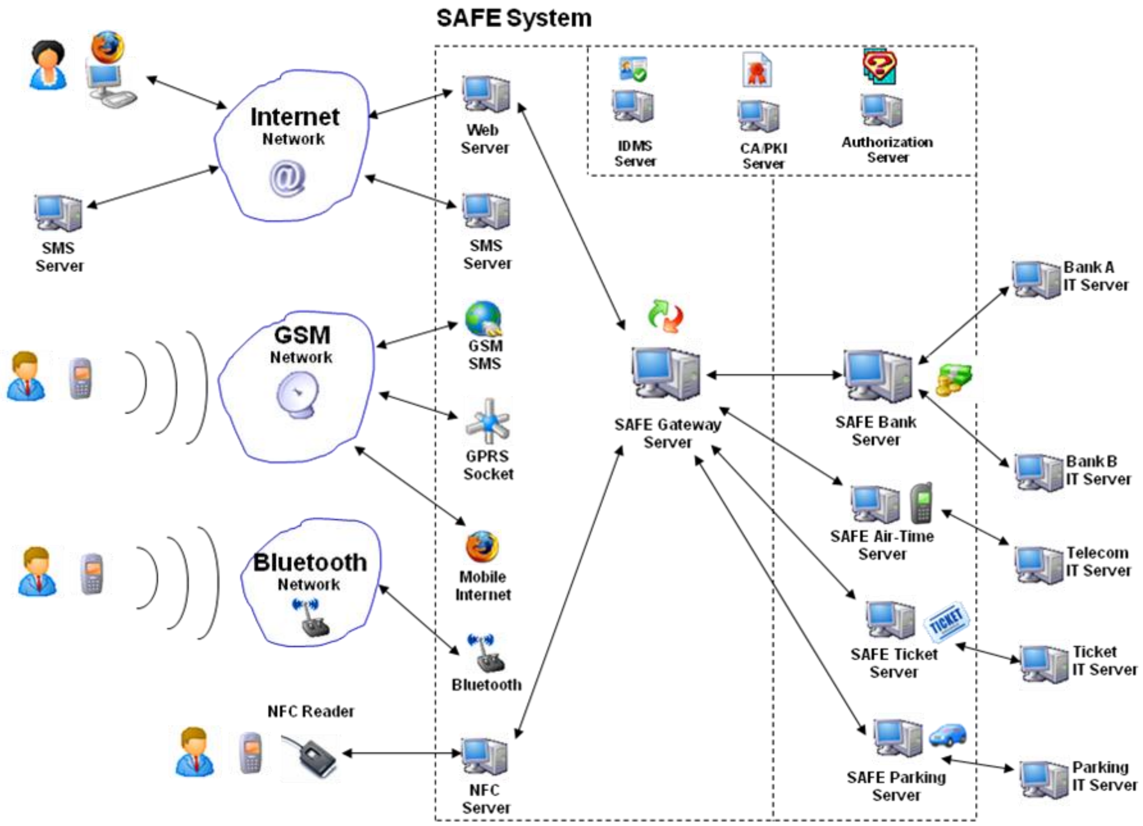


Figure 40. Security Service Architecture of The SAFE System

All participants in the system have personal security credentials: key pairs, certificates and other security tokens. For customers, they are safely stored in the UICC of their mobile phones, encrypted and accessible only after personal authentication. Participants in the system who perform sensitive and high–value transactions have cryptographic smart cards, which store their personal data and security credentials and perform all cryptographic operations. Each participant is authenticated before performing any transaction by verifying the PIN assigned to each user during registration.

Using those cryptographic credentials, all *SAFE* transactions are strongly protected with end–to–end security protocol. All transactions are digitally signed, encrypted and enveloped for the targeted recipient. The system supports authorization based on identities and account categories, thus all applications can be accessed and used only by authorized individuals.

Finally, identification, financial and authorization data are stored in databases in the encrypted form. Therefore, they cannot be illegally accessed by hackers or other unauthorized individuals.

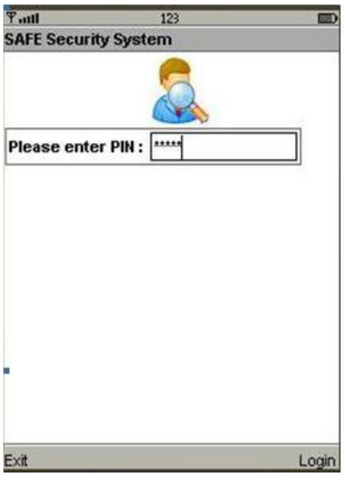
The system keeps encrypted logs of all its operations, so all transactions can be undeniably traced to their originators. Thus, in authentication with digital signatures and verification of certificates, the system provides non–repudiation of its transactions and data.

In the current version, security of the system is justified based on application of advanced security technologies, while in the near future system security will be tested through practical deployments in several countries.

This chapter will analyze the security features of the *SAFE* system based on five aspects: authenticity, integrity, confidentiality, non-repudiation, and availability. These five aspects are the basic security requirements of electronic financial system, indicated in Chapter 3.

7.2.1 Authentication of Users

SAFE system provides two types of authentication protocols: local authentication and remote authentication. Local authentication is based on PIN (Personal Identity Number) to verify the user. Once user opens Secure Mobile Wallet, PIN is required to use the application, shown in Figure 41.



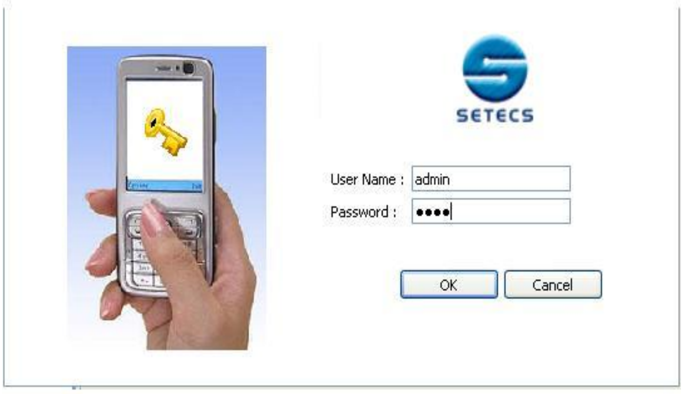
Please enter PIN : *****

Figure 41. Login to the Secure Mobile Wallet

Secure Mobile Wallet first calculates hash value of the PIN entered by a user by using SHA-1 algorithm. Then Wallet takes the hash value as AES (Advanced Encryption Standard) key and encrypts the entered PIN by AES, and stored it locally on a mobile phone. There are two advantages of this approach:

a. The PIN is encrypted by using a strong enough algorithm AES;
b. The Wallet does not need to store the key for the AES, so that the key can not be revealed unless user’s PIN is revealed.

User can modify PIN only if he/she enters the application (authentication successful). The same mechanism is utilized at the server side. The *SAFE* Administrative Station is using either “User Name-Password” authentication or authentication based on smart cards. The picture shows “Username/Password” authentication in Figure 42.



User Name : admin

Password : ●●●●

Figure 42. Login Panel of the SAFE System

Authentication information is also encrypted and stored at the server. Remote authentication is based on Strong Authentication Protocol specified in the Federal Information Processing Standard (FIPS) 196, described in Chapter 3. It provides mutual authentication based on digital signature. All entities apply for and fetch their authentication certificate first, which is illustrated in Chapter 4. OCSP (Online Certificate Status Protocol) is used to verify certificate. After getting certificate, it is ready to conduct mobile financial transactions by using PKI. The following Figure 43 shows one example of transaction messages flow using PKI:

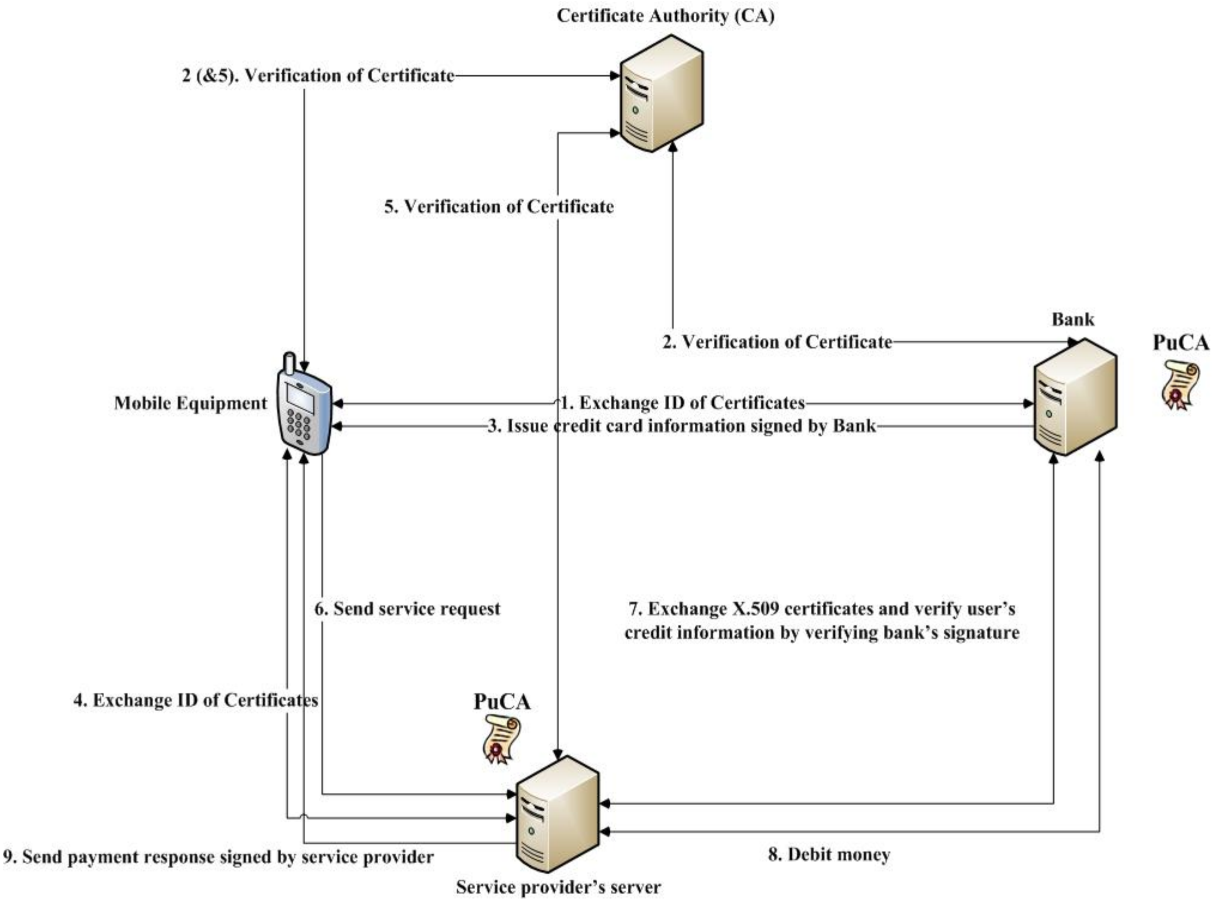
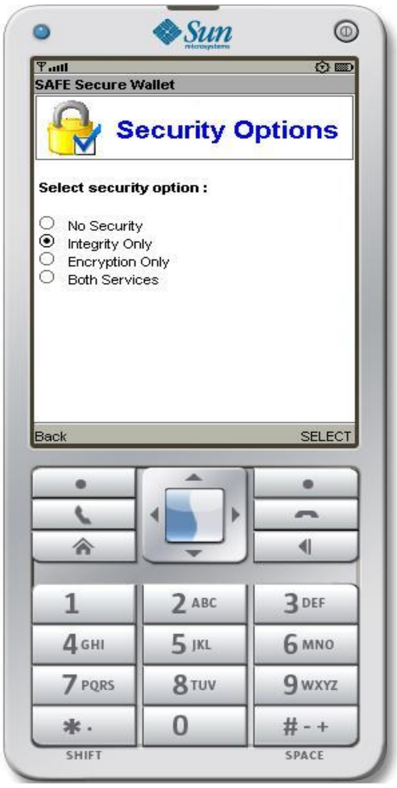

Certificate Authority (CA)
2 (&5). Verification of Certificate
5. Verification of Certificate
2. Verification of Certificate
Bank
PuCA
Mobile Equipment
1. Exchange ID of Certificates
3. Issue credit card information signed by Bank
6. Send service request
7. Exchange X.509 certificates and verify user's credit information by verifying bank's signature
4. Exchange ID of Certificates
PuCA
9. Send payment response signed by service provider
8. Debit money
Service provider's server

Figure 43. Example of Transaction Messages Flow Using PKI

a. Mobile user and bank exchange IDs of their certificates;
b. Both the mobile user and the bank send OCSP requests to CA to verify the other one's certificate;
c. Bank signs the credit card data and sends it to the mobile user;
d. Mobile user and service provider exchange IDs of their certificates for strong authentication;
e. Both mobile user and service provider verify each other's certificate by sending OCSP request to the CA;
f. After strong authentication, mobile user sends service request to service provider and service provider sends back payment data;
g. Mobile user creates payment confirmation message with the credit card data, signs the message with digital signature and sends it to service provider;
h. Service provider and bank exchange certificates for strong authentication and service provider verifies mobile user's credit card data by verifying bank's signature;
i. Bank debits money from mobile user's account and service provider signs payment response (e.g. receipts) and sends it to the mobile user;
j. Mobile user stores the payment response. Transaction completes.

7.2.2 Integrity of Messages

In order to provide integrity for the data during the progress of financial transaction, *SAFE* system utilizes SHA-1 as the algorithm to compute hash value. It provides users the option to use hash for integrity of messages. The details of applying integrity protection is shown in Chapter 5. The security setting is show in Figure 44.



SAFE Secure Wallet

Security Options

Select security option :

○ No Security
● Integrity Only
○ Encryption Only
○ Both Services

Back SELECT

Figure 44. Security Settings of the Secure Mobile Wallet

7.2.3 Confidentiality of Messages

All the information, both at the client side (Secure Mobile Wallet) and the server side (*SAFE* Administrative Station) is encrypted by AES. At the client side, customer must enter PIN into the customer side application and the application itself gets the customer mobile phone number and application ID to generate a secure hash code. The generated hash code is used as the key for the AES encryption algorithm to encrypt customer related information at the client side. This information includes mobile-ATM agent's phone number and the amount to be withdrawn. Then, this encrypted information is sent to the relevant bank. According to the assumption mentioned above, the bank generates a hash code using customer PIN, phone number and application ID and keeps it in bank's database, and uses the generated hash key to attempt decrypting the received encrypted message from the customer. If this is successful, it means that the hash key stored in bank’s database is equal to the hash key generated by the customer. Therefore, bank can authenticate the customer. In addition, encrypted version of the customer message provides the integrity and the confidentiality of the customer information.

The details of applying confidentiality protection is shown in Chapter 5. The diagram of customer side security is shown in Figure 45.

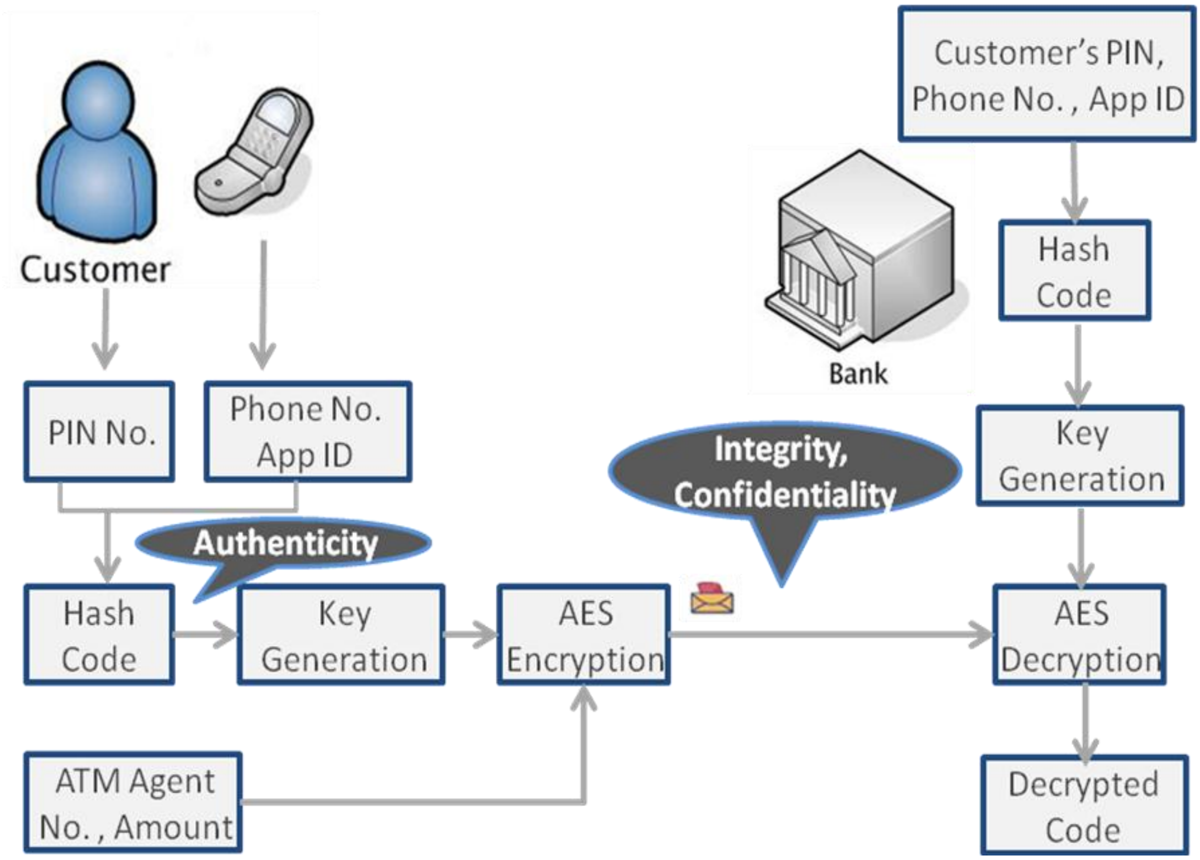


Figure 45. Security Features – Customers Side

7.2.4 Non-repudiation of Transactions

SAFE Administrative Station keeps logs of every operation and all the transactions. All the logs are encrypted and stored at the server's computer. Therefore, it provides non-repudiation, i.e. no one can repudiate or refuse the validity of an operation or transaction. Besides that, an initiator digitally signs all the important steps during transactions, which is shown in Chapter 5.

7.2.5 Availability of Services

All the components of the *SAFE* system are based on a Java platform. *SAFE* system also supplies four versions of the Secure Mobile Wallet, which covers nearly all the mobile customers to use the application. Using extendibility of *SAFE* Gateway Servers and their federation, the system can scale smoothly to global, international environments. Once an instance of the system is established, additional service providers (banks, merchants, etc.) may be easily added simply by registering them with the *SAFE* Gateway Server [20]. For international transactions, between two countries of between two instances of the *SAFE* system, scaling is provided by federating two or more *SAFE* Gateway Servers [25].

Chapter 8:

Conclusions and Future Work

Previous chapters represent the complete thesis work from different aspects. This chapter summarizes the thesis work. “Rome was not built in one day”, the success of the *SAFE* system needs some more efforts. In this Chapter, some planed future work is presented.

8.1 Security Architecture

In order to solve the problems, the thesis first studied current existing mobile financial systems and analyzed security requirements based on some related standards, and then composed a comprehensive architecture for Secure Applications for Financial Environments (*SAFE*) system. Based on the architecture we proposed, *SAFE* system provides a comprehensive protection of mobile financial transactions. In addition, it provides several combinations of solutions, so that it could satisfy different usage scenarios. During the process of implementing the system, a number of issues came out, which sometimes require modifications or extensions of the system architecture.

Based on the architecture, there are several components in the *SAFE* system including: *SAFE* portal server, service providers’ servers, security servers, and secure mobile wallet.

8.2 Security Features

As illustrated in Chapter 4, the most important feature of the *SAFE* system is that it provides sophisticated and comprehensive security services. There are three levels of security for different requirements and based on that, symmetric and asymmetric crypto functions are integrated in the *SAFE* system. All these together guarantee a safe and reliable environment for mobile financial transactions.

8.3 Future Research Activities

Even though we have *SAFE* system working for mobile banking with symmetric crypto functions, there is a lot of work needed to do in the future. First, we will extend the functionalities of the *SAFE* system to support credit/debit card payments, mobile ticketing transactions and maybe other mobile transactions, such as micro-loans, mobile healthcare service, etc. Second, we will extend security features to support full authorization of Public Key Infrastructure including digital signatures, certificates, etc. Third, we will extend Secure Mobile Wallet in a SIM card, so that it could run without requiring customers to use Java supported mobile phones or loading any software in mobile phone before using *SAFE* system. Finally, we will integrate contactless protocols, such as NFC into Secure Mobile Wallet, so that the mobile phone can be used like a contactless card, which will bring great convenience to many uses of standard mobile phones. The ultimate goal of the next phase of our research is design and (partial) implementation of a service-oriented architecture for secure mobile transactions and applications in a large scale, federated, international environments.

REFERENCES:

[1] Annual report, *Central Bank of Democratic Socialist Republic of Sri Lanka*, pages 71–74, 2007.

[2] Tiwari, R and Buse. S, *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Setor*. Hamburg : Hamburg University Press, 2007, p. page 33.

[3] A special report on telecoms in emerging marckets. *s.l. : The Economist*, September 26th 2009.

[4] Gadiax, Emmanuel, GSM and 3G Security. *s.l. : Black Hat Conference Singapore*, April 2001.

[5] O'Brien, Kevin J, Cellphone Encryption Code Is Divulged, *New York Times*. [Online] December 28, 2009. [Cited: 10th, January 2010.]

[6] Wezel, Markus Jakobsson and Susane, *Security Weaknesses in Bluetooth.*

[7] "RSA Laboratories Frequently Asked Questions about Today's Cryptography, Version 4.1", *www.rsasecurity.com/rsalabs/faq*

[8] Guide to Mobile Internet Security, *http://www.kannel.org/download/kannel-wtls-snapshort/wtls.html.* [Online] [Cited: 10th, January 2010].

[9] C. Narendiran, S. Albert Rabara, *Performance Evaluation on End-to-End Security Architecture for Mobile Banking System*, 1st IFIP, Wireless Days 2008. Dubai, UAE.

[10] Hany Harb, Hassan Farahat and Mohamed Ezz, SecureSMSPay: *Secure SMS Mobile Payment Model*, Anti-counterfeiting, Security and Identification, 2008. ASID 2008. 2nd International Conference.

[11] Shahriyar Mohammadi and Hediye Jahanshahi, *A Study of Major Mobile Payment Systems' Functionality in Europe*, Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference.

[12] Michale, HiggWang and Shudong, *Limitations of Mobile Phone Learning*. 832-4215, s.l. : JALT SIG, 2006, The JALT CALL, Vol. 2, pp. 3-14.

[13] *http://www.bankofamerica.com/onlinebanking/* [Online] [Cited: 31st, January 2010]

[14]*https://www.cardinalbank.com/PersonalBankingMobile.asp* [Online] [Cited: 31st, January 2010]

[15] *http://www.wachovia.com*. [Online] [Cited: 31st, January 2010]

[16] *Mobile Ticketing*, Wikipedia. http://en.wikipedia.org/wiki/Mobile_ticketing. [Online] August 2008. [Cited: 15th, January 2010.]

[17] Thomas Glaessner, Tom Kellermann, Valerie McNevin, *Electronic Security: Risk Mitigation in Financial Transactions Public Policy Issues*. World Bank Policy Working Paper 2870, July 2002.

[18] A.Karunanayake, K.Zoysa and S.Muftic, *Mobile-ATM for developing countries*. Seattle : Proceedings of the 3rd ACM International Workshop on Mobility in the Evolving Internet Architecture (Mobiarch'08), SIGCOMM, 2008.

[19] N. Wishart, *Micro-payment systems and their application to mobile networks*, Washington, DC: infoDev / World Bank. Available at: http://www.infodev.org/en/Publication.43.html 2006.

[20] Amila Karunanayake, Kasun De Zoysa, Feng Zhang, Sead Muftic, *Experiences on Mobile-ATM Deployment in a Developing Country*, Karlstad : Proceedings of 1st M4D Conference, Dec 10-11, 2008.

[21] *Entity Authentication Using Public Key Cryptography*, The Federal Information Processing Standards Publication Series of National Institute of Standards and Technology (NIST), February, 1997.

[22] EMVCo Website, April 2009: *http://www.emvco.com/*

[23] *D.V.Thanh. Security Issues in Mobile e-Commerce*, First International Conference on Electronic Commerce and Web Technologies, 2000. pp. 467-476.

[24] *Unstructured Supplementary Service Data*, Wikipedia, http://en.wikipedia.org/wiki/Unstructured_Supplementary_Service_Data, [Online] July 2008. [Cited: 16th, January 2010]

[25] Sead Muftic, *The Concept and Operations of the SAFE System.* Kampala, Uganda : MobileActive 08 Conference, November 4-6, 2009.

[26] D. V. Thanh. *Security issues in mobile e-commerce.* First International Conference on Electronic Commerce and Web Technologies, pages 467 – 476, 2000.