SAFE SYSTEM:  
SECURE APPLICATIONS FOR FINANCIAL ENVIRONMENTS USING MOBILE PHONES 

Sead Muftic¹, Feng Zhang¹  
1Department of Computer and System Sciences, Royal Institute of Technology, Stockholm, Sweden  
sead@dsv.su.se, fenge@dsv.su.se  

Kasun DeZoysa²  
2Department of Computer Science, School of Computing, University of Colombo, Sri Lanka  
kasun@ucsc.cmb.ac.lk

ABSTRACT

Mobile financial transactions are used by more and more people 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 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. Therefore, one of the main prerequisites for successful, large-scale and broad deployment of mobile financial applications is their security. This paper introduces the concept of SAFE system (Secure Applications for Financial Environment) that represents a secure, convenient and reliable infrastructure for mobile financial transactions. The infrastructure comprises Mobile Wallet, three servers: Gateway, IDMS and Bank servers, security protocols, and messages between all components.

KEYWORDS

SAFE, mobile transactions, security, wireless protocols, security infrastructure, mobile phone

1. INTRODUCTION

Mobile banking (m-banking) is based on the use of mobile phones or other mobile devices to perform various financial transactions, either directly with the recipient or indirectly, via a client’s bank account. m-banking is one of the newest approaches to the provision of financial services through wireless Internet network, made possible by the widespread adoption of mobile phones especially in developing countries. The rollout and functional capabilities of mobile telephony have been rapid and have extended usage well beyond classical mobile applications (telephone calls and short messaging). There is mounting evidence of positive financial, economic and social impact of those technologies all over the world.

One of the most important issues with mobile transactions 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 create false impression of their security, thus opening possibilities for hackers to explore 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.

SAFE (Secure Applications for Financial Environment) is the system that performs various financial transactions using mobile phones and other mobile hand–held devices. Contrary to the current initial versions of similar systems, which provide limited client–to–bank transactions, the system also supports 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.
2. APPLICATIONS AND PARTICIPANTS

SAFE system is designed to support broad range of secure financial transactions, which may be classified in three groups:

Financial transactions performed by individuals:
- Deposits and withdrawals of cash using client’s own account with “digital” ATMs,
- Deposits and withdrawals using client’s own account based on the concept of “Mobile ATM” in developing countries [1],
- Deposits and withdrawals of digital cash using client’s own account with “digital” ATMs,
- Transfer funds 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 ability to make retail purchases with m–Commerce enabled merchants using debit and credit card payments,
- The ability to make retail purchases with m–Commerce enabled merchants using micropayments,
- Provision for bill payments.

The second group is corporate financial transactions:
- Corporate–to–bank transactions (m–Banking),
- Corporate–to–Corporate transactions (quotes, purchase orders [2], invoices, payments, etc.),
- Corporate–to–individual transactions (payments, fees, various reimbursements etc.).

The third group is non–monetary transactions:
- Collecting and using bonus points,
- Collecting and using loyalty points,
- Using prepaid authorizations (gift cards, telephone air-time, etc.),
- Handling prepaid or purchased tickets.

The participants in those transactions are the following:

- **Banks** – perform registration and certification of individuals and provision of financial services,
- **Bank agents** – individuals who provide financial services on behalf of banks, locally at the banks’ locations or remotely as banks’ agents,
- **Financial Services Providers** – institutions providing financial services, like post offices, Western Union, currency exchange providers, etc,
- **Security Services Providers** – institutions providing security services in large, international networks, like identity (registration) services, certification services, smart cards services, etc,
- **Merchants** – companies selling goods and services and charging for those goods and services,
- **Clients** – individuals initiating or receiving transfers as the result of financial transactions.

3. SYSTEM COMPONENTS AND ARCHITECTURE

SAFE 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 five types of servers in the SAFE 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,
- **SAFE Gateway Servers** – specialized servers that support various secure financial transactions, used as the “front–end” (proxies) to Bank Servers,
- **Bank Servers** – interface servers in banks performing linking of the system to standard banking applications and transactions,
- **Merchant Servers** – servers located at merchants’ premises performing direct financial transactions with clients.
The following stations are used in the SAFE system:

- **Client Mobile Stations** – those are mobile phones loaded with secure applications,
- **Client Static Stations** – those are standard PCs used by clients to perform financial transactions from static locations (home, offices, etc.),
- **Agents Mobile Stations** – these stations are either smart phones or hand-held devices with smart card capabilities, used by mobile banks’ agents,
- **Registration Stations** – those stations are standard PCs enhanced with smart card capabilities and used by registration agents,
- **Financial Services Provider Stations** – those stations are also PCs with smart card and used by financial services providers,
- **Merchants Stations** – those are POS terminals, which are enhanced with smart card capabilities and used by merchants to perform direct financial transactions with clients.

System components and the architecture are shown in the following Figure:

![SAFE System: Secure Service-Oriented Architecture](image)

**Figure 1.** Components and the Architecture of the SAFE System

### 4. USAGE AND SYSTEM OPERATIONS

#### 4.1 Registration of Participants

As the first step all participants in the SAFE system are registered. Registration is performed by Registration Agents. Registration data are stored in the Registration database of the IDMS server (see Figure 1). This step may be performed by the bank, by telecom operator or by any other independent ID services provider. Thus all participants in the system have reliable and verifiable registrations data used for all SAFE transactions.

Registration is performed as the face-to-face procedure, where personal data and credentials are verified before being entered in the system. Registration Agents fill out registration form and data are stored in the
Registration database at the IDMS Server. At the same time registration data is transferred on-line into mobile phones of customers and bank agents and also transferred to other parties for later use.

4.2 Certificates and Smart Cards

In the SAFE system all participants have X.509 certificates. They are issued by the Certification Authority (CA) Server, based on registration data stored in the IDMS Server. In addition, all agents who perform security management or high-value transactions are issued smart cards. Customers do not use their own smart cards, due to the high cost of mobile phones that support 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 are issued by banks and by all 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 applications.

4.3 Cash Dispensing: Mobile and Static ATM

Mobile and static ATM are two innovative approaches for dispensing of cash, especially suitable in regions where there are no standard banking ATMs. With “Mobile ATM”, cash is distributed by the specialized bank agents, who visit areas without standard ATMs. They dispense cash to customers upon receipt of the authorization messages from banks based on customer cash requests. The procedure is equivalent with static ATMs, where cash is dispensed by post offices, eventually merchants, and other cash distribution agencies.

The sequence of steps and exchange of messages for this function 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 cash dispensing agent (like Post Office). When the message is received, cash is given to the customer.

4.4 Stored Money and Micropayment Transactions

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, therefore 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 approves 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_Reclalm message to the SAFE server which contacts merchant’s bank server to make deposit into the merchant’s account.

4.5 Debit and Credit Card Payments

These are standard debit and credit card payments, which today are performed using plastic debit/credit cards. 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.

4.6 Account-to-Account Transactions

These transactions are 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. These types of transactions are suitable for remittance, personal payments, bill payments, etc. They are 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 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.

4.7 Loans: Applications and Administration

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

Applicants may also administer their loans, reviewing the status of the loan, payment schedule, initiating payments, etc. For this application, the messages are the following: applicant applies for the 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.

5. SECURITY PROPERTIES OF THE SAFE SYSTEM

One of the distinguished features of the SAFE system, which makes it different from any other similar system, is its security. All participants in the SAFE system are 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.

All participants in the system have personal security credentials: key pairs, certificates and other security tokens. For customers, they are safely stored in 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.

Using those cryptographic credentials, all SAFE transactions are strongly protected. Each participant is authenticated before performing any transaction. All transactions are digitally signed, encrypted and enveloped for the targeted recipient. The system supports authorization based on identities and roles, 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, the system provides non-repudiation of its transactions and data.

6. CONCLUSIONS

SAFE system provides comprehensive protection for transactions in wireless environment, which includes not only strong authentication of every registered entity, but also confidentiality, integrity and availability of all sensitive data. Through federation of SAFE servers, the system can scale smoothly to global, international environments. It is compatible with all existing security features for Web transactions: SSL, SAML, secure XML, FIPS201 (PIV) smart cards and currently deployed proprietary banking security systems. With all those strong security features and advanced security technologies, SAFE system may be used not only for the financial transactions described in this paper, but also as security extension for any on-line banking system, based on Web technologies and services. Using SAFE system security features would greatly reduce identity theft and financial losses in banking and financial transactions.

ACKNOWLEDGEMENT

This research is sponsored by the “Mobile ATM” project supported by SPIDER (www.spidercentre.org) and by the “Models of transnational e-finance services” project supported by Vinnova.

REFERENCES