Secure Service-Oriented Architecture for Mobile Transactions

Feng Zhang, Sead Muftic, Gernot Schmöelzer
Communication Systems
School of Information and Communication Technology
Royal Institute of Technology (KTH)
Stockholm, Sweden
fengz@kth.se, sead@kth.se, gernot.schmoelzer@setecs.com

Abstract

The paper describes secure service-oriented architecture for mobile transactions. The architecture comprises components, protocols, applications and interfaces and it provides various security services to various mobile applications: registration, certification, authentication, and authorization of users, secure messaging at an application–level (end–to–end security), protection of data in databases, and security services for protection of its own components. The architecture is modular, integrated, extendible and scalable. The paper describes design of the architecture, the status of its current implementation, and future research and development plans.

1. Introduction

During the last two decades mobile technology has achieved great progress and mobile phones today are one of the necessary accessories in people's everyday lives all over the World. According to the GSMA, an industry group, total number of mobile subscribers in the World will reach 6 billion by 2013 [1]. Therefore, in addition to standard communication services – simple calls and exchange of SMS messages, mobile commerce is becoming more and more popular, especially mobile financial transactions. Mobile technologies are considered an innovative approach to complement current, mainly web-based applications and transactions and to transform existing, still usually paper–based financial systems into cashless systems. Financial institutions and telecom companies are investing a lot of efforts to convert their payment transactions, such as air–time top up, money transfers or bill payments, into mobile electronic form. Due to significant decrease of the cost of mobile phones and mobile services, currently there are many initiatives to perform those transactions using mobile technology [2], [3], [4).

At the time when this paper was written, there are several systems in some countries supporting mobile financial transactions [5], [6]. But, all current systems are just "point-solutions". They are based on proprietary products and therefore not compliant to any standard. As such, current mobile transaction systems are not mutually compatible, they cannot scale, and they are not easily extendable with additional functions or services. All current implementations provide very limited scope of functions and generally have no security features. Security of these systems relies on features provided by the GSM network, which are not adequate, especially for financial environments or on use of simple PIN schemes. In December 2009, a German computer engineer announced that he had deciphered and published a code used to encrypt digital mobile messages, saying it was his attempt to expose weaknesses in the security of GSM systems [7]. There are also many security issues related to SMS services, such as SMS spam, flooding, SMS fraud, and impersonation of users. Another security issue in mobile Internet is weaknesses of the WTLS protocol, which does not provide end-to-end security [8].

Most of the current solutions and implementations of mobile financial systems comprise only two components: a simple mobile phone application and a corresponding mobile transactions server. The server understands (limited) set of messages coming from phones, uses background financial data to perform transactions, and returns the result. Such concept and systems cannot be easily extended with new functions, since in that case both client application and server must be modified. Those systems do not scale, meaning that phone application, designed to access and use one server, cannot access and use any other mobile financial server. Finally, these systems cannot be interconnected, so that users registered in one system cannot transfer funds to and use functions of other systems.

Therefore, what is needed in the current situation is a concept, a set of standards, and implementation

978-0-9564263-7/6/$25.00©2011 IEEE

tools for an architecture for mobile services. As recently suggested, "*The main challenges facing telecom operators are a lack of infrastructure, the need for cooperation between operators, retailers and banks, and the need to create clearly defined revenue models for all investing parties*" [9].

Based on all those motivations, this paper describes the concept, components and services of a large–scale, comprehensive architecture for secure mobile applications and transactions. The concept is

- *comprehensive*, i.e. many security services are provided by the architecture;
- *scalable*, it provides the possibility for interlinking of mutually independent deployments, if based on the described architecture;
- *modular*, i.e. new services, functions and components can be easily added to the architecture;
- *expandable*, i.e. mobile applications can easily be linked to the architecture and can utilize its services; and
- *open*, meaning that integration of new components is based on utilization of standard-based Web services and interfaces.

2. Service-oriented architecture

Contrary to the current solution, our service-oriented architecture for secure mobile transactions solves all these issues and has all the properties listed at the end of the previous section. In order to achieve these goals and properties, our system is a 6–tier architecture, as shown in Figure 1 (organized vertically). The name of our system is *SAFE* (Secure Applications for Financial Environments). The components of the *SAFE* system are in two dotted frames. The others are external components to which the system connects for smooth exchange of data and messages.

The first tier (the first group of components) is various *SAFE* clients: browser access to the system, PC–based or device–based Point–of–Sale (PoS) applications, and finally our Wallet implemented as an application in mobile phones, as an UICC applet or as a smart card applet.

The second tier is various networks and corresponding communication protocols: large–area networks (based on Internet or GSM/3G protocols) and proximity networks (Bluetooth or NFC protocols).

The third tier is communication components of the *SAFE* system: there is one component for each of the communication protocols provided by communication networks. These components support communication services at the network level – sending and receiving messages. The next tier is *SAFE* Communication Server. It provides communication services at the application level – analyzing and dispatching *SAFE* messages to various *SAFE* Mobile Application Servers.

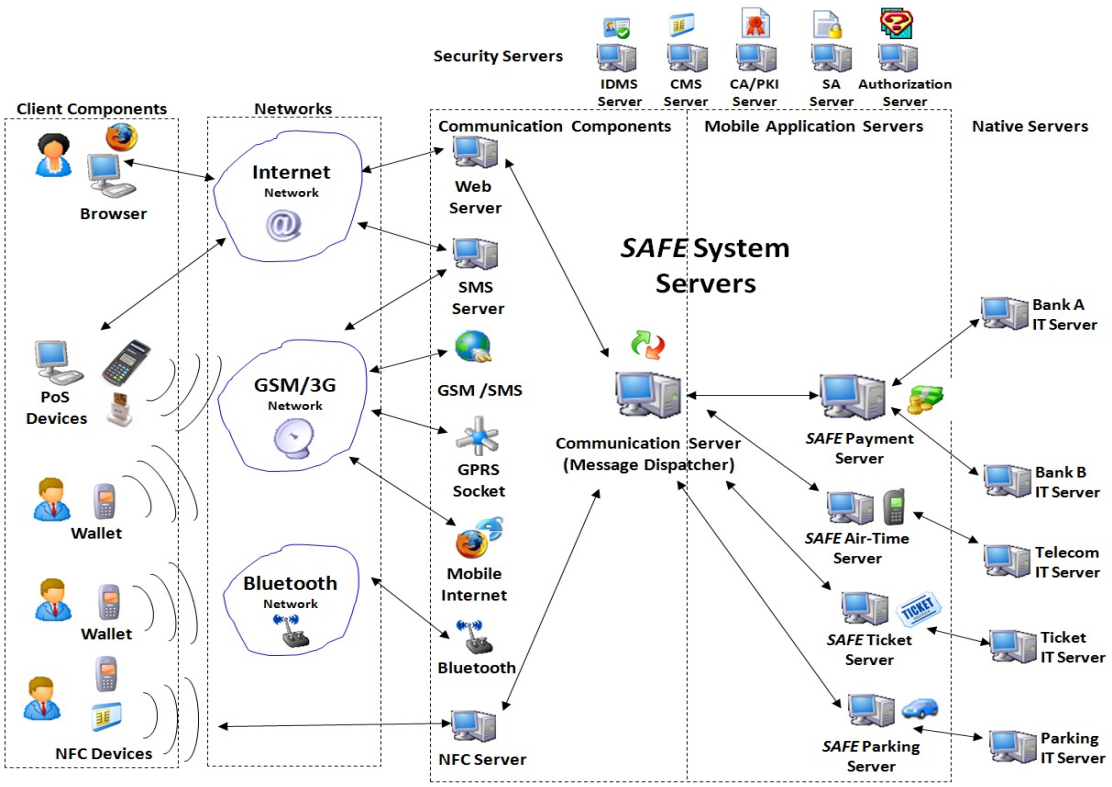

Figure 1. Secure service-oriented architecture for mobile transactions

Behind the Communication Server, as the fifth tier, are various *SAFE* Mobile Application Servers. Figure 1 shows four of them: *SAFE* Payments Server – supports mobile financial transactions, *SAFE* Air–Time Server – supports payments and management of air–time using mobile phones, *SAFE* Ticketing Server – supports inquiries, purchase and dispatching tickets using mobile phones, and *SAFE* Parking Server – supports payments for parking using mobile phones. Those four *SAFE* Mobile Application Servers are only examples, currently implemented in the *SAFE* system. Other *SAFE* Mobile Application Servers can be easily added to the architecture.

The final sixth tier is various back–end ("native") servers supporting appropriate mobile applications: payment servers support mobile financial transactions for banked users, telecom servers support administration and use of air–time, ticketing and parking servers support corresponding mobile applications and transactions.

3. Communication components and services

Communication subsystem comprises multiple service providers at the network level, called Communication Modules, and one provider at an application level, called Message Dispatcher. These Communication Modules are shown in Figure 1. Communication Modules communicate with users at the front-end and with Message Dispatcher at the back-end. They support various communication protocols, such as SMS, GPRS, Bluetooth, Internet, NFC, etc, and provide connection interfaces for mobile phones. Each Communication Module supports two services: establishment of secure session and secure exchange of messages. Communication Modules receive service requests through various communication channels, create uniform *SAFE* request messages, whose formats are pre-defined and agreed between Communication Modules and Message Dispatcher, and send messages to the Message Dispatcher. Message Dispatcher connects with various Communication Modules at the front-end and with different *SAFE* Mobile Application Servers, such as *SAFE* Payment Server or *SAFE* Ticketing Server, at the back-end. When it receives uniform service requests from Communication Modules, it parses the requests by analyzing the headers of messages (the details of message syntax is explained in [10]). After parsing the request, it dispatches it to different *SAFE* Mobile Application Servers, based on the type of transactions. *SAFE* Mobile Application Servers receive messages from the Message Dispatcher, create messages with specified syntax and send these messages to the back-end service providers' servers. The syntax of such messages is based either on some international standard, such as ISO-8583, or on specifications from native service providers, if they have such specifications. If there are 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. Security components and services

SAFE System is complemented with five security servers that provide the full scope of security services to users, transactions, applications and data stored in the database. These security servers are: IDMS Server, Certificate Server, Card Management System (CMS) Server, Strong Authentication (SA) Server, and Authorization Server. They provide security services to mobile transactions. There are four groups of those security services: registration and identity management services, certification and certificates management services, smart cards management services, and authorization services. This section describes the details of each of these groups of services.

4.1 Registration and identity management services

All entities involved in mobile financial transactions must be registered. This is performed as the first step after installation of the system. For subscribers, *SAFE* System provides two types of registration services: *quick registration* and *comprehensive registration*.

Quick registration service is based on use of SMS messages and it is especially useful for the areas without any other communication networks except GSM network is available. It works as follows: client sends `Registration_Request` SMS message containing client's first name and last name to the *SAFE* SMS Communication Module. SMS Communication Module creates `SAFE_Registration` message in an XML format based on the `Registration_Request` data received from a client and sends it to the Message Dispatcher through a stable and secure channel. Message Dispatcher checks message type, which is in this case `Customer_Quick_Registration` and forwards the message to IDMS Server. This server stores client's data, generates a *SAFE* ID and a *SAFE* PIN and returns them to Message Dispatcher, which delivers `Registration_Response` to the SMS Communication Module as an XML file containing data received from the IDMS Server. SMS Communication Module sends SMS message including the *SAFE* ID and *SAFE* PIN to client's mobile phone. At that time, client's registration status is "Pending" and the client is not able to perform any mobile transaction until his/her

registration data is verified, when registration status becomes "Completed". Client completes registration with additional `SAFE_Registration_Confirm` message.

Comprehensive registration service is more complex, but provides higher level of security than quick registration. The complete process consists of two phases: the first phase is submitting registration form and the second phase is a face-to-face verification process preformed by authorized Registration Agent (referred as RA). This role has been certified by the Certification Authority, such as banks, post offices, etc. The first phase is almost the same as for quick registration. The only difference is that instead of just sending first name and last name, a client accesses *SAFE* Web Server either through computer or mobile phone and fills in complete registration form. After submitting the form to the *SAFE* Web Server, the sequence of steps is the same as with quick registration. In the second phase, client needs to go to a RA and tell his/her *SAFE* ID to RA, who fetches registration information from the registration database in the IDMS Server based on client's *SAFE* ID and verifies client's information by checking valid proofs of client's identity. If client is successfully verified, RA can update client's data and send complete client's registration data to the IDMS Server. Figure 2 shows comprehensive registration process.

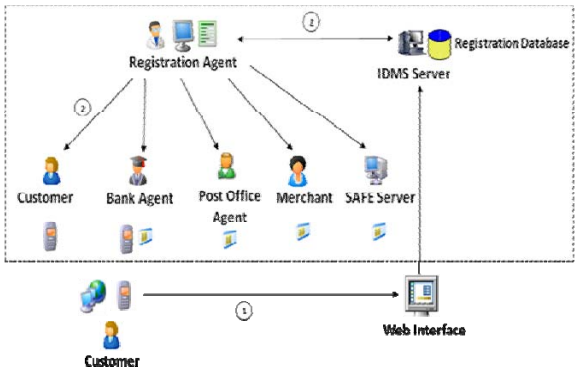

Figure 2. Registration of subscribers

IDMS Server is responsible for managing identity verification, validation, issuance and storage process. It provides 10 digits unique ID for every registered entity, which is compliant with Personal Identity Verification (PIV) of Federated Employees and Contractors standard [11].

4.2 Smart cards management services

Smart card is a secure and reliable media for storing credentials and sensitive data in financial environments. All the entities performing high value transactions are issued smart cards. For compatibility purpose, *SAFE* System issues PIV standard-based smart cards, so that *SAFE* cards can be used with multiple applications. All smart cards are issued and managed by the *SAFE* Card Management System (CMS) comprising CMS Server and CMS Station. The sequence of steps for issuance of smart cards is the followings: client sends `SmartCard_Apply` request containing client's *SAFE* ID to *SAFE* Web Server either by computer or mobile phone. Web Server creates `SAFE_SC_Request` message and sends to Card Management System (CMS) Server. CMS Server fetches client's information from the request containing client's *SAFE* ID to *SAFE* Web Server either by computer or mobile phone. Web Server creates `SAFE_SC_Request` message and sends to Card Management System (CMS) Server. CMS Server fetches client's information from the IDMS Sever based on client's *SAFE* ID and issues the card (load applet, personalize data and print the card). In this step, PIN has default value (for example, 11112222). When the card owner receives the card, he/she uses CMS Station, with smart card management client software, to select his/her own PIN, which is updated in the card. At the same time, the card is triggered four times. Each time, it (internally) generates two keys, public key is read, and certificate request (PKCS #10) is created and sent to the CA Server. CA server then issues certificate for each request and returns it to the CMS Station, which writes each certificate in the card. After that, the card is activated. Since the card is based on the PIV standard, the four certificates are:

a. PIV Authentication Certificate
b. Key Exchange Certificate
c. Digital Signature Certificate
d. Card Management Certificate

Smart card management system is shown in Figure 3.

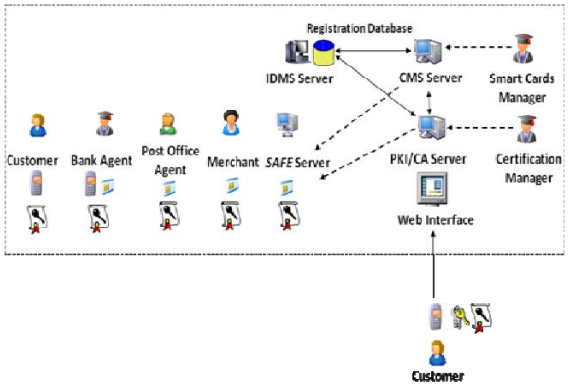

Figure 3. Smart cards management system

4.3 Certificates Management

Certification is very important services since trust must be built among entities involved in financial transactions and in most cases don't know one another. The certification process is more complex in

mobile financial environments than for other applications due to limitations of mobile phones, such as limited ability to process, store and display data. Besides traditional certification services, *SAFE* also provides mobile certification services for mobile clients. There are some prerequisites for mobile certification:

a. Mobile user can use mobile phone to generate RSA key pair
b. Mobile phone is capable to digitally sign messages by using user's private key
c. PIN is generated by *SAFE* system during user registration phase and securely stored on mobile user's device

Certificate request works as follows: client generates key pair, reads out public key and sends it to Message Dispatcher together with a Lightweight Certificate Request Message (LCRM), shown as step 1 in Figure 4. LCRM contains a message header "mCertReq" and a signed value, which consists of user's *SAFE* ID, first name, last name and hash value of user's PIN. Message header indicates mobile certificate request and is used by the Message Dispatcher to route messages to the correct application server, based on the message header. The signed value is used as a proof of possession. Message Dispatcher fetches client's registration information from the IDMS Server based on client's *SAFE* ID and creates PKCS#10 message, shown as step 2 in Figure 4. Then Message Dispatcher delivers the message together with the LCRM to the Certificate Authority (CA) Server based on the message type, which is in this case Certificate Request. CA issues certificate if all the data are successfully verified. Instead of sending a X.509 certificate to the client, the CA sends serial number of the certificate to the client, shown as step 3 in Figure 4. Later, serial number of the certificate is used to identify mobile client's certificate in validation and revocation processes. For other entities, which are not mobile clients, the process is standardized so that client sends PKCS#10 request message to the CA Server and receives X.509 certificate, shown as step 4 in Figure 4.

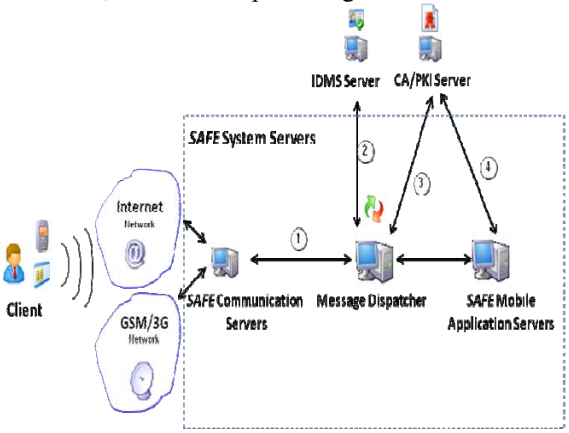

Figure 4. Certificates management service

4.4 Authorization Service

Various entities, such as customer, agent, merchant, system administrator, service providers, etc. communicate with each other to perform mobile transactions. However, each entity must be able to authenticate and access authorized resources. To achieve authentication between communicating entitles, a Strong Authentication (SA) Server is used to perform Strong Authentication based on FIPS-196 standard [12]. For authorization services in the *SAFE* System an Authorization Server (also acts a Policy Decision Point) is introduced to manage the authorization policies based on the XACML standard.

Initially the client performs strong authentication with the SA Server, shown as step 1 in Figure 5. Upon successful authentication, the SA Server returns a SAML_Ticket to client. The SAML_Ticket is generated and signed by the Authorization Server.

When a client wants to access a resource, it sends request for specific resource to *SAFE* Mobile Application Server. The request comprises: SAML_Ticket (Subject), name of the resource (Object) and action (such as read, write, modify, etc.). *SAFE* Mobile Application Server receives the request and activates Policy Enforcement Point (PEP), which is a component of *SAFE* Mobile Application Server. PEP creates `SAML_Authorization_Request` and sends it to the Authorization Server. Authorization Server evaluates the request against the policies and sends a decision back to PEP in the form of `SAML_Authorization_Response`. The PEP receives the response and acts accordingly.

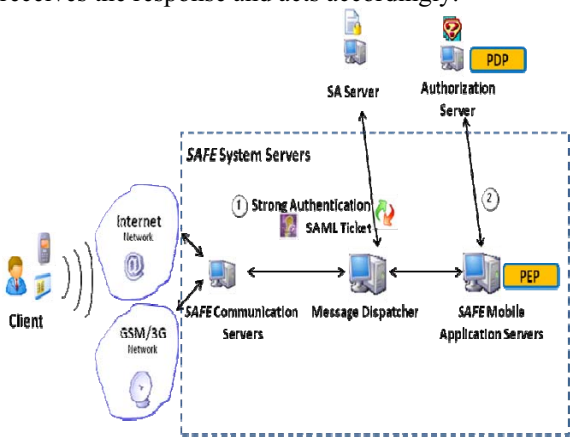

Figure 5. Authorization service

5. Current Implementation

The implementation of the described *SAFE* System is based on Java, which means the system is able to run on multiple platforms. *SAFE* Mobile Application Servers expose to service providers as Web Services, to make it easier to manage and extend. Plus, the plug-ins being developed and used

for servers are in encrypted form and these encrypted plug-ins can be loaded by using specially designed Secure Class Loader, which decrypts and verifies each plug-in before loading it into memory.

On the mobile phone, there is mobile client software named *SAFE* Mobile Wallet. It consists of three parts: UI, middleware and applets in UICC. UI is developed as Midlet by using J2ME. Applet is developed by using JCOP and middleware is used to build communicate between UI and applet.

6. Conclusions and Future Work

This paper explains design and current implementations of security system for mobile transactions, which supports communication services, registration and identity management services, certification and certificates management services, smart cards management services, and authorization services. The objective of the *SAFE* system is to provide secure, reliable, scalable and comprehensive mobile transactions, so that customers can perform mobile transactions anytime, anywhere if GSM network is available. What's more, it is very easy and convenient for service providers to manage and extend their services with *SAFE* System, since the system is compliant with several international standards. Future works will focus on two aspects: the first is to design and implement federated and scalable architecture and the second is the design and implementations of security protocols and messages for mobile transactions.

7. References

[1] "A Special Report on Telecoms in Emerging Markets*", The Economist*, September, 2009.

[2] Cardinal Bank, *Cardinal Mobile Banking* [Online]. Available:http://www.cardinalbank.com/PersonalBanking Mobile.asp (Access date: 22nd, November 2010).

[3] SunTrust, *Mobile Banking* [Online]. Available: https://www.suntrust.com/portal/server.pt/community/mobile_banking/1783 (Access date: 22nd, November 2010).

[4] AfriBank, *M-Banking* [Online]. Available: http://www.afribank.com/dynamicdata/mobilebanking.aspx (Access date: 22nd, November 2010).

[5] Mendes, Sh., Alampay, E., Soriano, E. and Soriano, Ch., "*The innovative use of mobile applications in the Philippines – lessons for Africa*", www.sida.se, September 2007.

[6] "*Micro-Payment Systems and Their Applications to Mobile Networks*", InfoDev Report, http://ww.infodev.org, 2006.

[7] O'Brien, Kevin J, "Cellphone Encryption Code Is Divulged", *New York Times.* December 28, 2009.

[8] "*Guide to Mobile Internet Security"* [Online]. Available: http://www.kannel.org/download/kannel-wtls-snapshot/wtls.html (Access date: 22nd, November 2010).

[9] "*O2 reveals mobile payment strategy*" [Online]. Available: http://www.nfcnews.com/2010/05/27/o2-reveals-mobile-payment-strategy (Access date: 22nd, November 2010).

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

[11] NIST, "*Federal Information Processing Standard (FIPS 201): Personal Identity Verification (PIV) System*", www.nist.gov

[12] NIST, "*Federal Information Processing Standard (FIPS 196): Entity Authentication Using Public Key Cryptography", www.nist.gov*