



Software for a mobile future



Valentina Vodnika 8/9
21000 Novi Sad, Serbia
Tel: +381 (0)21 472 15 48
Fax: +381 (0)21 472 15 49
E-mail: info_ns@zesium.com
Web: www.zesium.com

Basic Solution Concepts



Application for safe and secure transactions on mobile devices

1 Concept and justification of the solution

1.1 Aim and basic requirements

Recently, there has been an obvious rise in the tendency of introducing mobility into the business world which raises the question of identification of users and security of information being transferred in the digital (mobile) environment. Examples of such tendencies are m-Banking, m-Trading, among others, which are based on the idea of service availability any time any place. In such concepts, communication takes place in a client- server model between a service provider such as bank, shop, broker, etc., and distant mobile terminals such as mobile phones, PDA devices etc. Over here, security of communication and users is an absolute priority.

The aim of **Zesium mobile d.o.o.** is the development of such a system which has been named **Mobistel**.

Hence the main requirements of this project are:

- To design and implement a client application for mobile phones and other portable devices which provides services enabling secure and safe transactions via mobile devices. The user will have a user-friendly application installed on his/her mobile device, with available functionalities based on the specific service being provided for that is simple and clear to use and understand even for an average mobile phone user. The user is thus able to carry out necessary transactions using a mobile device relying on a secure solution that involves latest standardized cryptography methods. The transaction process includes the registration of the user as an owner of an electronic signature certificate, as well as generation, storage, publishing, recalling and suspension of the electronic certificate based on the requirements and constraints defined by the service provider.
- To design and implement a server application that will automatically receive and register requests from the client side, enabling secure and authorized access to private/secure data in the data base of the service provider. The server would be part of an existing network infrastructure of the bank using the services based on electronic signature certificates.

1.2 Main challenges of the project

The main challenges of the project can be broken into four aspects:

- The first aspect is related to the needs of the user and designing the architecture of a software system that will be successfully integrated into an existing software system of the service provider and that will function on different mobile devices.
- The second aspect is directly related to the technical solution and actual implementation of the design of the system, and integration of the corresponding software solution on mobile devices that will satisfy the needs of users.
- The third aspect is in the business logic/domain and is about ensuring quality of service which will enable simple and efficient use of the system for mobile transaction and enable signing and verification of the electronic signature by the user.

- The fourth aspect is a challenge which involves gaining the trust of clients concerning reliability of the system and security of transactions.

1.3 Business requirements

The server has to satisfy the following requirements:

- To enable all necessary functionalities for business communication between the user and the service provider.
- To ensure that received requests from a client have really been sent by the client whose integrity can be verified.
- To ensure and verify that all data received from clients is uncorrupted.
- To be able to check and verify specific requests/data received from the user and timestamps of the requests.
- To minimize the effect of such a solution on existing applications and transfer of data between server and clients.

The user of the service has the following requirements:

- To be certain that communication is with the server of the service provider.
- To be sure that data sent to the server is not compromised in any way during transfer to the server.
- To be guaranteed security of complete functionality of Mobistel.
- To be provided with a means of checking the content and timestamp of sent requests.
- To be assured that data privacy is guaranteed which is possible by minimizing the possibility of a third party cracking security and intercepting data during transactions.

2 Project Overview

2.1 Characteristics of the project

<i>Possibilities and benefits of m-banking services:</i>	
Mobistel	
<i>Application on mobile devices for secure transactions</i>	
Possibility:	Benefit:
1. New technology	m-Banking is the latest and technologically most advanced solution for providing remote mobile banking services. The realization of such a solution will enhance and strengthen the reputation of a bank as a leader in the implementation of high-tech banking solutions.
2. Facilitate transactions and reduce costs of branch offices	m-Banking services will reduce the need for clients of banks to be present at the banks to carry out transactions since these transactions can be performed anywhere anytime. This in turn will enable the banks cut down the number of necessary branch offices.
3. Reaching out to high profile clients	m-Banking solutions will enable banks satisfy the ever demanding needs and requirements of overworked and time strapped clients always on the move who require immediate services from banks.
4. Potentially new source of revenue	Banks have the option of billing the m-banking services.
5. Is installed and executes without the direct intervention of the GSM operator	All transactions and entire functionality is independent and does not involve the GSM operator since GPRS is used only as a carrier for communication performed on the IP level between the client and server.

It is obvious that there is a need for a flexible and efficient software solution to enhance security of data transfer via GPRS which will further enable more secure communication on the IP network. This is precisely the idea behind the development of Mobistel: develop an application that ensures secure data transfer to/from mobile devices over the GPRS/IP network providing users a secure and safe means of carrying out financial transactions.

Generally, Zesium Mobile d.o.o. is capable of fully implementing the technical and business segments of the project:

- **Expertise** – Highly skilled IT engineers capable of delivering solutions to satisfy customer demands.

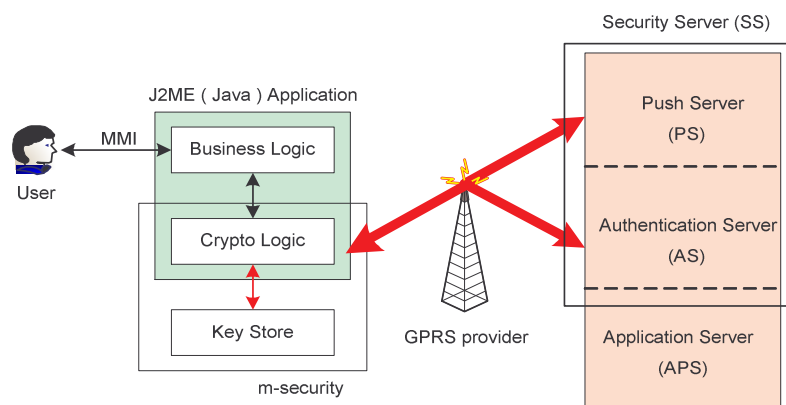
- **Resources** – Availability of software and hardware resources necessary for realization of the project.
- **Finance** – The financial aspect of the project is covered by the customer.
- **Cooperation with Faculty of Technical Sciences** – Availability of experts and new solutions in the field of cryptography.

2.2 Analysis of the solution

The problem of secure communication is quite a complex one and can be broken down into the following sub-problems among others:

- Am I communicating with the right party? Does that party have permission to communicate with me? How can I confirm my identity? (authentication and authorization)
- Is the information/data being transferred safe and secure from attacks in the sense that unauthorized parties cannot understand or change the content of the information? (data encryption and integrity)

The model of the solution being developed at Zesium Mobile d.o.o., which answers the questions above and satisfies the requirements regarding secure transfer of information and data, is based on the client-server model shown in the picture below.



The client side is a J2ME application consisting of the following entities:

- **Business Logic** – provides an interface to the user and is responsible for all operations on data which is sent and received via the secure channel.
- **Crypto Logic** – responsible for executing main procedures for establishing secure communication with the server side in such a way as to enable adjustment of security parameters, as well as establishment, monitoring and termination of connections.
- **Key store** – location (file system, RMS or SIM card) where all critical information used in establishing secure communication (private keys, identifiers, random sequences) is stored in encrypted form. Encryption of the location is achieved by key shared between user and server. By the request of key owner, the special procedure enables partially change of encryption key. Also, to achieve higher security, server shall alter its part of encryption key after each session.

The server side can be divided into two parts with the following two functionalities:

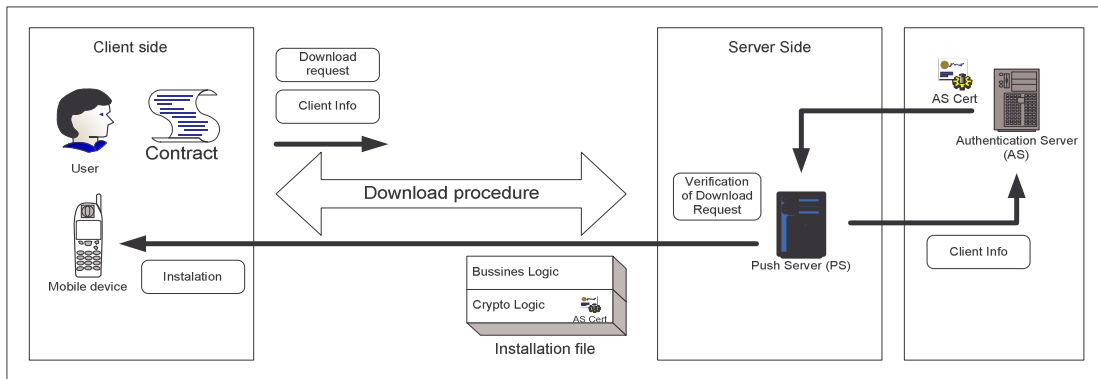
- **Push Server** – responsible for the distribution phase, i.e. download of application onto the mobile device.
- **Authentication Server** – responsible for the authentication and authorization of client applications and represents the other end point of the secure channel, which is actually part of the IT network infrastructure of the bank or service provider.
- **Application Server** – responsible for storing and exchanging of client data related to the business logic; always communicates with client application over secure channel (tunnel), established after authentication procedure.

The main procedures involved are:

- **Download of application onto the mobile device.** The user
 - signs a contract with the bank and provides necessary information such as name/surname, phone number, IMEI, etc.

- receives a download identifier and a user personal identifier (userID) which are IDs for initialization and starting up of the application.
- accesses the push server, enters the given download identifier and phone number, after which the push server checks whether the identifier corresponds to the phone number, and if so installs the application onto the mobile device.

The application at this moment consists of the Business and Crypto Logics only, with an identifier equal to the phone identifier and Server Certificate of the authentication server. User identifier shall be known by user only and also stored within Authentication Server in form that enables user identification, but not its value estimation. With purpose to increase integrity of the user, user identifier may be altered on user request.

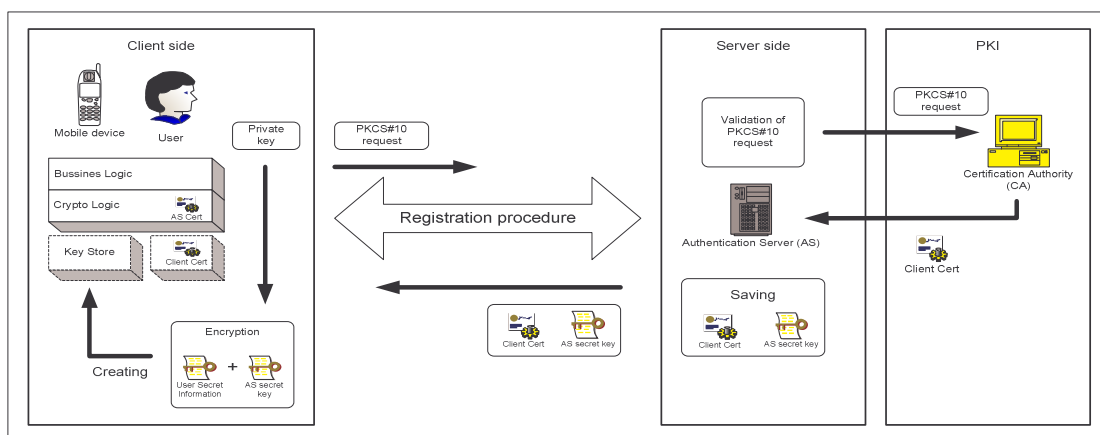


• **Initial registration.** The user

- enters the initialization identifier which is actually the user ID.

The application sends the application identifier (appl ID) together with the user ID and a random number RC0 (as a challenge) to the authentication server in the form of a *hello* request. This information is encrypted with the public key of the authentication server. After verifying the identifiers, the server responds with a new random number RS0 to challenge the client application and to avoid replay attacks. Moreover, data are verified by using *hash* algorithms.

After this, the application generates its private and public key pair and sends a request for a certificate (PKCS#10), together with the appl ID, user ID and received random number RS0, which are all encrypted using the authentication server public key. Based on the identifiers, the authentication server checks the validity of the request and forwards it to the Certificate Authority (CA) within the IT network infrastructure of the bank or service provider. After positive certification of the client application is performed, the client certificate (X.509v3) is sent to the client together with a new random number RS1, after which initial registration is complete. While client certificate doesn't exist, server sends data encrypted by random number RS0 (*one-time key* cryptography) and verified by using *hash* algorithms. After positive client certification, data shall be encrypted by user public key. The random number RS1 is kept on the server until next session establishing procedure.



The application then creates the key store and generates a unique key store identifier as well as a key for encrypting and decrypting the store based on the data entered into the key store and the random number RS1 received from the

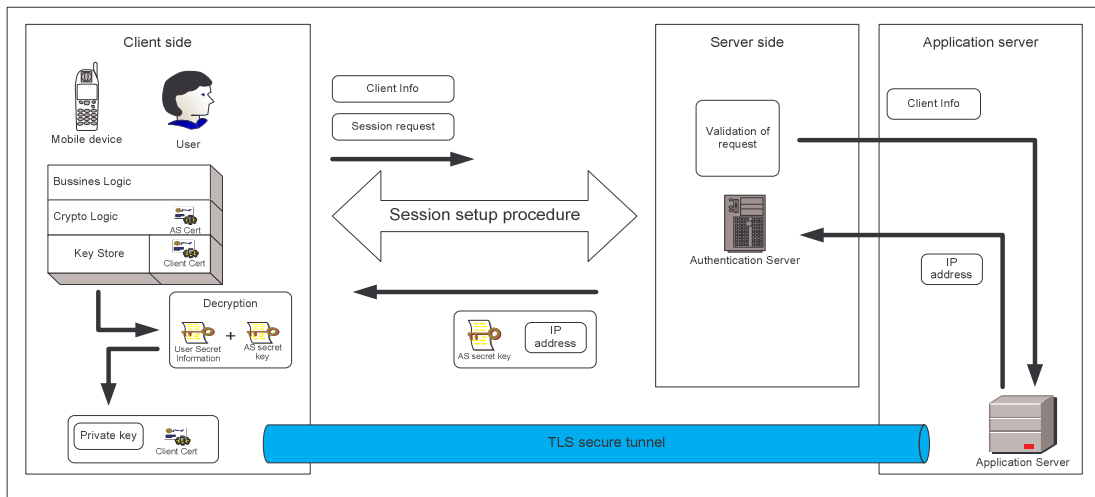
server. Once created, the key store is used to store critical information. At the end or interruption of ongoing session, the client application shall delete random sequence RS1 used for Key Store encryption, which shall prevent unauthorized access to Key Store.

After the initialization process is completed, the user has the option to change the user ID since it is used only to access the key store.

- **Establishing secure connections.** The user
 - enters the user ID.

The *hello* request procedure is similar to the initial registration procedure, with the difference being the random numbers RCn and RSn. As response on *hello* request, the server sends random number RS[n-1] generated in previous session or initialization procedure. The application decrypts the key store using the user ID and random number RSn received from the server. It then retrieves and uses its private key and its certificate in authentication and establishing a secure TLS connection with the authentication server. A temporary key is generated in the process which is used for encryption during the session. After completion of this process, all business information transferred between the user/client and bank is done via the established secure tunnel.

For terminating the session, the server sends a new random number RSn+1 which is used by the client to decrypt the key store using a new key.



2.3 Security

- **User Identification**

User identification model is designed based on the two-factor authentication model using a parameter which the user knows (user ID) and another parameter which the user possesses (appl ID). UserID is a secret parameter shared between the user and the service provider and represents a password or PIN code. On the other hand, the appl ID corresponds to hardware parameters of the mobile device such as SIM card, IMEI, and IMSI which makes copying of the application to another mobile device more difficult. In addition, to enable direct access to the service, the private and public keys generated by the client application are verified/certified by the service provider using the client certificate.

On the server side, the service provider is identified by its certificate which is located in the application.

- **Important information**

Only a necessary subset of information relevant for authentication and establishment of secure communication is stored on the mobile device. Private keys and initial values of pseudo-random sequences, which are examples of this information, are stored in encrypted form on SIM cards or RMS (Record Management System). The secret keys of participants (client and server private key) never leave equipment that has generated them. Each valuable information (pseudo random sequences) exchanged over radio link is transferred in encryption form.

- **Access regulations**

Authentication Server (AS), based on received information from the client, authenticates the client and verifies whether the client is authorized to access the intranet network of the bank or service provider. Random number

generators which are synchronized on both the client and server prevent replay attacks and limit the number attempts in a brute-force attack.

After the client gains access to the intranet network of the service provider, available services granted by the service provider to the client are defined in the client certificate.

- **Privacy**

For the purpose of securing information that is transferred between the client and server, standard cryptography algorithms are used (TLS, 3DES, AES, MD5, SHA-1). MD5 and SHA-1 algorithms shall be used as standard algorithms for generating *hash* results and TLS, 3DES and AES as standard mechanisms for data encryption.