# Secure Architectures for Mobile Applications

Cristian TOMA, Bucharest, Romania, cristian.toma@ie.ase.ro

*The paper presents security issues and architectures for mobile applications and GSM infrastructure. The article also introduces the idea of a new secure architecture for an inter-sector electronic wallet used in payments – STP4EW (Secure Transmission Protocol for Electronic Wallet).*

***Keywords:*** *secure architecture, m-application, smart-cards, 3G Mobile.*

## GSM Overview

The basic GSM network architecture is presented in fig. 1. The main components involved in voice and data transmission are the following:

- BSS – Base Station Subsystem. It controls the quality of the links from GSM radio interface and contains BTS and BCS.
- BTS – Base Transceiver Station. Controls the "antennas" and maintains the communication through a duplex radio channel. It supports configurations for: electro-magnetic power, radio channel used for broadcasting, BSIC – Base Station Identity Code. Its main functionalities are: message encryption, channel coding and modularization.
- BCS – Base Station Controller. Administrates and controls base stations and radio channels. It provides the coding implementation for voices messages and manages the data localization.
- NSS – Network Sub System. It contains MSCs, Databases such as VLR, HLR, EIR and AuC and adaptation modules such as XC, IWF, EC. NSS provides the following functionalities: management of communication link with other mobiles, land and satellite networks, management of mobile subscribers from other BSCs, and the management of the subscribers using data from AuC, EIR, VLR and HLR databases
- MSC – Mobile Switching Center. Contains switching subsystems (e.g. for PBX signaling and for communication signaling over SS7 with other MSCs) and control subsystems
- HLR – Home Location Register. Stores the subscribers' parameters including the MSISDN and the service type (e.g. 10 SMS, 80 minutes for 1 month).
- VLR – Visitors Location Register. It is a mirroring database of HLR for temporary subscribers of another VLR area.
- EIR – Equipment Identity Register. It is the centralized database with IMEI (unique number for each provider-device) for each mobile device.
- AuC – Authentication Center. The following functionalities and responsibilities are included: authorization process for the subscriber access into mobile network for encrypting transmission on radio path and for assign of the temporary identity - TMSI (Temporary Mobile Subscriber).

Fig. 2 presents the main concept used in GSM for end-user device: the mobile is a 2 in 1 computer. The first computer is represented by the SIM – Subscriber Identity Module. Actually, the SIM is a smart card with a microcontroller, three types of memory area (ROM, EEPROM and RAM) and I/O ports for outside communication (usually in half duplex mode). The mobile device itself is the second computer. It also includes a microprocessor, different types of memory areas and an operating system.

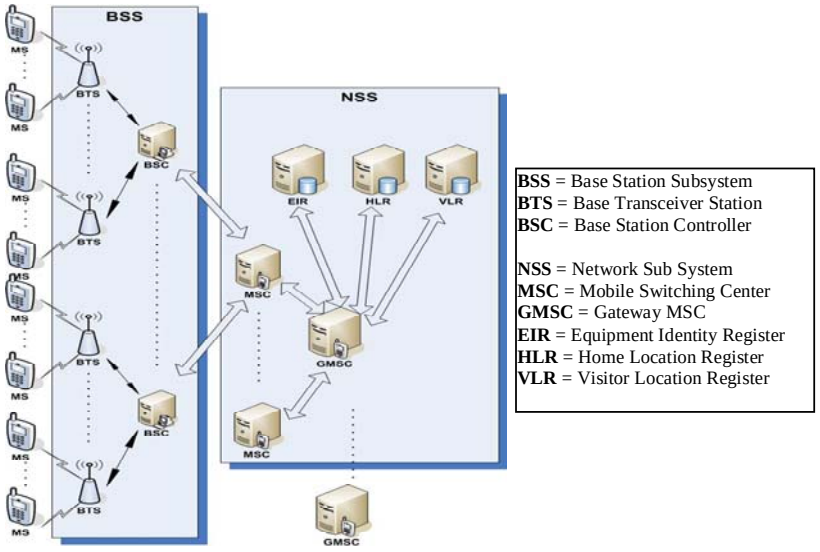


Fig. 1. GSM Network Architecture

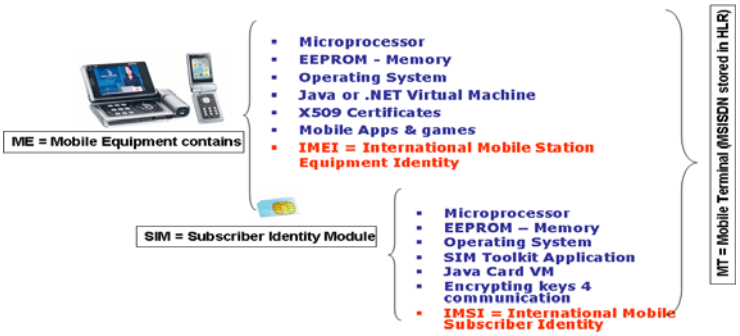


Fig. 2. GSM Mobile Equipment Structure

The GSM evolution is based on this infrastructure and the security of the entire system depends on many factors.

## 2. Architectures for Voice and Data Security in GSM

This chapter focuses on the security mechanisms involved within mobile data and voice transmissions. Fig. 3. presents the overall processes for authentication and confidentiality of mobile communication.

Fig. 4 and 5 present a more detailed technical view of the systems' security process. Fig. 4 shows the main network items involved in voice and data security, and fig. 5 presents the logical flow of the data.

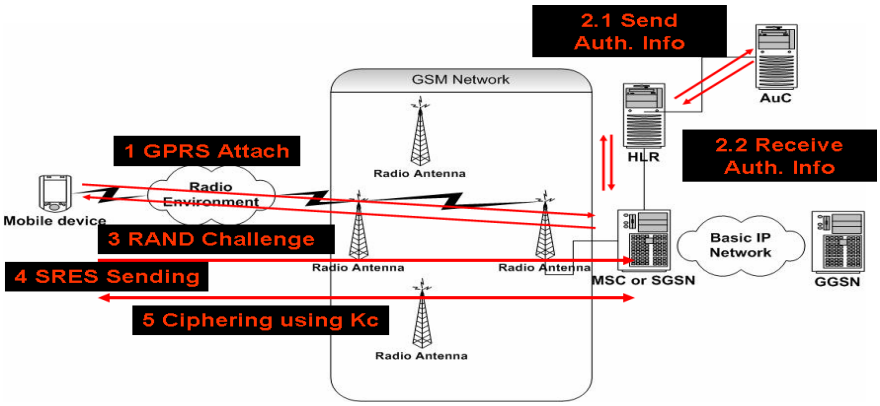


Fig. 3. Processes for authentication and confidentiality of mobile voice and data transmission

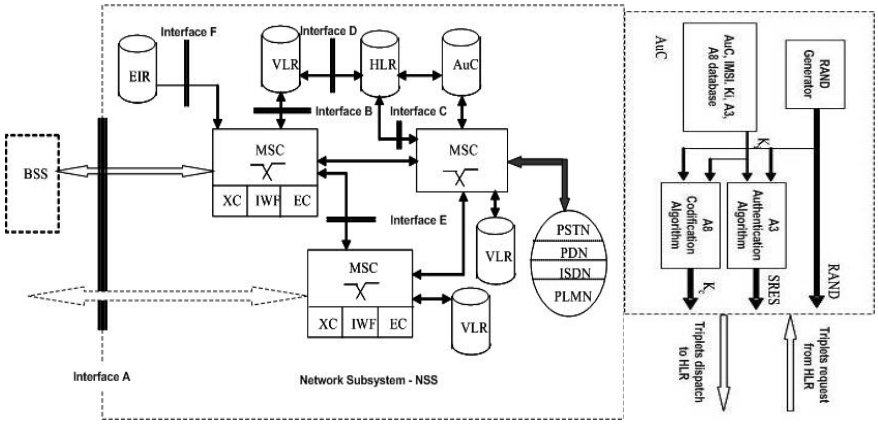


Fig. 4. The details of the security mechanisms

AuC – Authentication Center plays the main part in voice and data authentication and integrity. Its main functionalities and responsibilities consist in: authorizing the subscribers' access into the mobile network; encrypting transmission on radio path and assign of the temporary identity - TMSI (Temporary Mobile Subscriber Identity). The authentication process of the mobile subscriber is described as it follows:

- The mobile station sends the SIM's IMEI to the HLR through the "Net Attach" (or GPRS Attach).
- A triplets request is sent to the AuC from HLR (all HLR, AuC and SIM suppose to store same Ki) through the "Send Auth. Info" message (contains SIM's IMSI)
- The AuC generates a response that contains:
- RAND (random number – challenge)
- Kc – encryption key that is a result of the A8 algorithm. The A8 algorithm uses the stored identity key – Ki from AuC corresponding to the received IMEI.
- SRES – Signed RESponse generated through A3 Authentication Algorithm with RAND and Ki as input
- The HLR receives the triplets and sends to the mobile only RAND
- The mobile device must be enabled using Ki from SIM, A3 and A8 algorithms in order to reconstruct Kc and SRES. It then sends the SRES to the HLR via MSC or SGSN (in GPRS only).
- If the SRES received by the HLR from the mobile device is the same with the one that is received from the AuC, then the authentication is done and Kc will be used for ENCRYPTION.

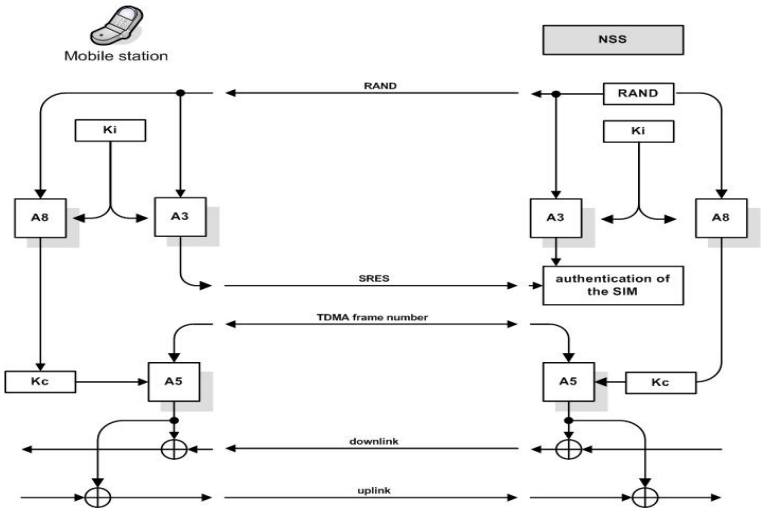


Fig. 5. Overview of data workflow for authentication and confidentiality

The described architecture had been considered at the beginnings of the GSM and has been used since (including in GPRS, EDGE, UMTS networks) [WOLF04].

## 3. A new proposed architecture for inter-sector electronic wallet

According to EN 1546 of CCE [EN 1546] an inter-sector electronic wallet for payments in retail business and e-commerce can be implemented. The standard provides specifications for a series of data elements (in bold), which allow the data used in the electronic wallet system to be referred unambiguously. All **files** that are necessary for proper operation are contained by a DF – dedicated file – within the smart card. The files and the **commands** used by the electronic wallet belong to the ISO/IEC 7816-4 standard. The commands are: SELECT FILE, READ BINARY and READ RECORD. The specific commands used for electronic wallets are defined in EN 1546: INITIALIZE IEP – initializes a subsequent purse command; LOAD IEP – loads the purse, cancels the previous payment and provides error recovery; DEBIT IEP – provides the payment using the wallet and confirms payment; CONVERT IEP CURRENCY – converts currencies; UPDATE IEP PARAMETER – modifies general parameters of the wallet. **State** diagrams are used to define the necessary states and state transitions within the application, corresponding to a sequence of commands. Depending on its current state, the card will accept or reject various commands. The **cryptographic algorithms** create the context for the entire security of the system. They represent the only message protection. Some of the most commonly used algorithms are DES and Rijndael for symmetric key encryption and RSA or DSS for asymmetric key algorithms. The standard also describes in the detailed manner the **procedures** representing the main functions of the wallet.

The new proposed architecture for an electronic purse improves the standard, binding **the smart card nature of the SIM** with a new transmission protocol – STP4EW (Secure Transmission Protocol for Electronic Wallet) – for the message exchange [TOMA06b].

## 4. Conclusions

Part of the STP4EW (Secure Transmission Protocol for Electronic Wallet) is in development phase within mSQE (Evaluation System for the Quality of Services Generated by the Mobile Applications in the Field of E-Business – Contract 104 between Academy of Economic Studies and MATNANTECH) and eServEval (Quality Evaluation System for Online Public Services used within the Business Environment and by the Citizens) excellence research projects (CEEX). Also, some parts of the STP4EW are developed by the Software Development Department that organizes the Informatics Security Master. The proposed secure architecture for electronic wallet relays on GSM security mechanisms and on the author's personal ideas. The main references for the secure architecture used in inter-sector electronic wallet for payments are [WOLF04], [EN 1546] and [TOMA06b].

## References

[EN1546], BS EN 1546-3:2000 – Identification Card Systems. Inter-sector Electronic Purse. Data Elements and Interchanges. http://www.standardsdirect.org

[TOMA06a], Cristian TOMA, "Tutorial on Java Smart Card electronic Wallet Application", Informatics Security Handbook, AES Publishing House, Romania 2006

[TOMA06b], Cristian TOMA, "Secure Patterns and Smart-card Technologies used in e-Commerce, e-Payment and e-Government", Informatics Security Handbook, AES Publishing House, Romania 2006

[WOLF04], Wolfgang Rankl & Effing, "Smart Card Handbook 3rd Edition", John Wiley & Sons Publishing House, USA 2004

[ZHIQ04], Zhiqun Chen, "Java Card Technology for Smart Cards – Architectures and Programmer's Guide", Addison Wesley, 2004