GSM and GPRS Security

Chengyuan Peng

Telecommunications Software and Multimedia Laboratory

Helsinki University of Technology

`pcy@tml.hut.fi`

Abstract

Analog cellular phones and networks were designed with minimal security which soon turned out to be insufficient. The GSM system provides solutions to a few important aspects of security: subscriber authentication, subscriber identity confidentiality and confidentiality of voice and data over the radio path. This paper gives an overview of the security features provided in a GSM PLMN and GPRS network. Also the SIM module, which plays an important role in GSM security, is discussed.

1 Introduction

Cellular fraud is extensive in analog cellular systems since the voice and user data of the subscriber is sent to the network without encryption. Anyone with an all-band radio receiver can tune in and hear everything going on in a cell [11].

The GSM system provides security controls. The system operator wants to ensure that the subscriber requesting the service is valid (authentication). The subscriber, on the other hand, wants to have access to the services without compromising privacy (confidentiality of subscriber data). The GSM's security controls achieved using the four primary mechanisms [9], i.e., each subscriber is identified using a cryptographic security mechanism; the subscribers security information is stored in a secure computing platform called SIM (Subscriber Identity Module) module or smart card; the GSM operator maintains the secrecy of the cryptographic algorithms and the keys for authenticating the subscriber and providing voice privacy; the algorithms are stored in the SIM and Authentication Center (AUC); the cryptographic keys are not shared with other GSM administration.

GSM introduced powerful algorithms and encryption techniques on security controls. They are categorized into three functions according to ETSI standard specifications [3]. They are subscriber identity confidentiality, subscriber identity authentication, user data confidentiality on physical connections, connectionless user data confidentiality, and signaling information element.

The first function describes an identifying method used in location updating procedure. The second function introduces an authentication procedure when subscriber identity is triggered by the netwok to verify a valid identity. The third function introduces some ciphering and key setting methods used to protect user data and signaling information elements.

This paper presents these three security features provided in the GSM system in detail. The GPRS (General Packet Radio Service) security features are also addressed. In order to well understand the GSM and GPRS security, Section 2 and section 3 give a short introduction of GSM and GPRS system architectures and security-related components.

2   GSM system architecture

A GSM system has two major components: the fixed installed infrastructure (network) and the mobile stations (MS) [7]. The mobile subscribers use the services of the network and communicate over the radio interface. Fig. 1 illustrates the GSM system architecture.
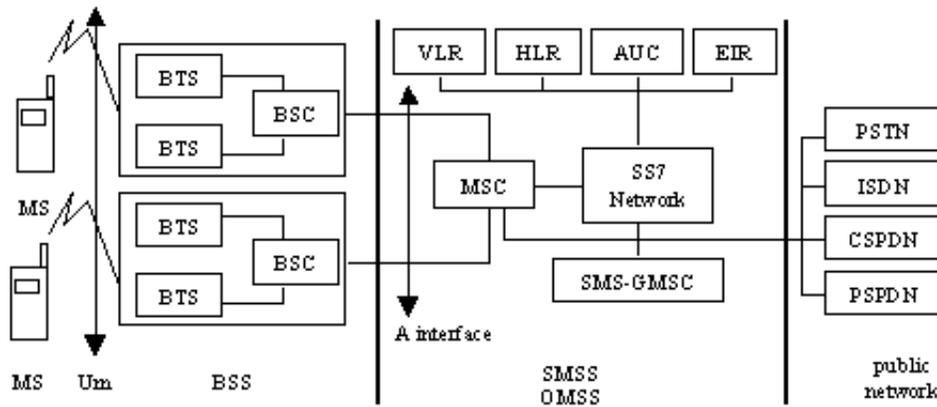

Figure 1: GSM system architecture

2.1   Mobile station (MS)

The MS consists of two major components: the Mobile Equipment (ME) and SIM module.

2.2   Fixed Network

The fixed installed GSM network can be subdivided into three subsystems: the BSS (Base Station Subsystem), the SMSS (Switching and Management Subsystem), and the OMSS (Operation and Maintenance Subsystem) [9].

The BTS (Base Transceiver Station) and the BSC (Base Station Controller) together form the BSS. A cell is formed by the radio coverage of a BTS. The BTS provides the radio channels for signaling and user data traffic in a cell. Several BTS can be controlled by one BSC.

The SMSS consists of the mobile switching centers (MSC) and the databases which store the data required for routing and service provision. The MSC performs all the switching functions of a fixed-network switching node. A GSM PLMN has several databases. The SMSS consists of two databases, i.e. the HLR (Home Location Register) and the VLR

(Visitor Location Register). The HLR stores all permanent subscriber data and the relevant temporary data of all subscribers permanently registered in the HLR. The IMSI (International Mobile Subscriber Identity) and authentication data are stored in it. The VLR stores the data of all MSs which are currently staying in the administrative area of the associated MSC [10].

The ongoing network operation is controlled and maintained by the OMSS. Network control functions are monitored and initiated from an OMC (Operation and Maintenance Center) [9]. Two more databases are defined in this subsystem. They are responsible for various aspects of system security. System security of GSM networks is based primarily on the verification of equipment and subscriber identity. These databases serve for subscriber identification and authentication and for equipment registration. Confidential data and keys are stored and generated in the AUC (Authentication Center). The EIR (Equipment Identity Register) stores the serials numbers (supplied by the manufacturer) of the terminals (IMEI).

2.3   SIM

A personal chip card SIM can be a fixed installed chip (plug-in SIM) or an exchangeable SIM module. The SIM is a secure microprocessor-based environment implemented on a credit-card-sized platform with on-board non-volatile memory [13]. Two types of SIM cards are used in GSM, i.e. ID-1 and plug-in card .

There are three types of memory, i.e., ROM, RAM, and EEPROM [13]. The ROM contains the operating system, the applications, and security algorithms A3 and A8, which implements important functions for the authentication and user data encryption based on the subscriber identity IMSI and secret kes. RAM is used to buffering transmission data and executing. The EEPROM consists of subscriber identification (IMSI, PIN), call number (IMSI and MSISDN), keys Ki, network-related information (TMSI, LAI), and the equipment identifier IMEI.

The security features supported by the SIM are authentication of the subscriber identity to the network, data confidentiality over the air interface, and file access conditions [5]. The first two features are presented in section 4. The SIM can support five access conditions [13, 5]. One of the access conditions is PIN which is used to control user access to the SIM. If the subsciber typed three incorrect PIN code, the SIM will be blocked. [13].

Therefore, use of the SIM, the whole of MS can be protected together with PIN against unauthorized access.

2.4   Identities

In this section, some identities related to GSM security are introduced. The association of the most important identifiers and their storage locations are summarized as follows: Subscriber is identified by IMSI, MSISDN, TMSI, MSRN; Mobile Equipment is identified by IMEI; IMSI, MSISDN, and MSRN are stored in HLR; The LMSI, MSRN, IMSI, TMSI, MSISDN, and LAI are stored in VLR; The IMSI, RAND, SRES, Ki, Kc are stored in AUC. IMEI isstored in EIR [6].

When registering for service with a mobile network operator, each subscriber receives a unique identifier, the **IMSI** (International Mobile Subscriber Identity). This IMSI is stored in the SIM. A mobile station can only be operated, if a SIM with a valid IMSI is inserted into equipment with a valid IMSI, since this is the only way to correctly bill the appropriate subscriber. The IMSI consists of several parts: mobile country code (MCC): 3 decimal digits, internationally standardized; mobile Network code (MNC): 2 decimal digits, for unique identification of mobile networks within a country; Mobile Subscriber Identification Number (MSIN): maximum 10 decimal digits, identification number of the subscriber in his mobile home network [10].

MSISDN: The real telephone number of MS is MSISDN (Mobile Subscriber ISDN Number) [6].

The VLR responsible for the current location of a subscriber can assign a **TMSI** (Temporary Mobile Subscriber Identity) which has only local significance in the area handled by the VLR. It is used in place of the IMSI for definite identification and addressing of the MS. This way nobody can determine the identity of the subscriber by listening to the radio channel, since this TMSI is only assigned during the mobile stations presence in the area of one VLR, and can even be changed during this period (ID hopping). The mobile station stores the TMSI on the SIM card. The TMSI is stored on the network side only in the VLR and is not passed to the HLR. It can consist of up to 32 bits. The association between IMSI and TMSI is stored in the VLR.

The **MSRN** (Mobile station Roaming Number) is a temporary location-dependent ISDN number which is assigned by the local VLR in its area. The **IMEI** (International Mobile Station Equipment Identity) uniquely identifies mobile equipment internationally. It is a kind of serial number. The IMEI is allocated by the equipment manufacture and registered by the network operator who stores it in EIR. By means of the IMEI one recognizes obsolete, stolen, or nonfunctional equipment. Each Location Area (LA) has its own identifier, i.e., the LAI (Location Area ID). It is structured hierarchically and internationally unique.

3   GPRS system architecture

GPRS as a new data service uses a packet-mode technique to transfer high-speed and low-speed data and signaling in an efficient manner. GPRS optimizes the use of network and radio resources. Strict separation between the radio subsystem and network subsystem is maintained, allowing the network subsystem to be reused with other radio access technologies. GPRS does not mandate changes to an installed MSC base [8].

GPRS network elements (cf. Fig. 2) are SGSN (Serving GPRS Support Node), GGSN (Gateway GPRS Support Node), Border Gateway (BG), Backbone network (intra-PLMN and Inter-PLMN), HLR, MSC/VLR, SMS-GSMC [8].

GPRS introduces two new network nodes SGSN and GGSN in the GSM PLMN [12]. The SGSN is at the same hierarchical level as the MSC. It is responsible for the delivery of packets to/from the MSs within its service area and communicates with the GGSN. The SGSN keeps track of the individual MSs' location within its service area and performs security functions and access control. The SGSN is connected to the BSS with Frame

Relay [12].

Figure 2: GPRS system architecture

The GGSN provides interworking with external packet-switched networks, such as the Internet, X.25 networks or private networks , and is connected with SGSNs via an IP-based GPRS backbone network. It maintains routing information used to tunnel Protocol Data Units (PDU) to the SGSN that is currently serving the MS. The HLR is enhanced with GPRS subscriber information, and the SMS-GMSCs and SMS-IWMSCs are upgraded to support SMS transmission via the SGSN.

GPRS security functionality is equivalent to the existing GSM security [8, 12]. The SGSN performs authentication and cipher setting procedures based on the same algorithms, keys, and criteria as in existing GSM. GPRS uses a new ciphering algorithm optimized for packet data transmission.

The GPRS phone communicates with GSM base stations, (but unlike circuit-switched data calls which are connected to voice networks by mobile switching center), GPRS packets are sent from BSS to a SGSN. When the mobile station sends packets of data, it is via the SGSN to the GGSN, which converts them for transmission over the desired networks (the Internet, X.25 networks or private networks). IP packets from the Internet addressed for mobile station are received by the GGSN, forwarded to the SGSN and then transmitted to the mobile station [12].

4   GSM and GPRS Security Functions

This section gives a detailed description of the three GSM and GPRS security functions.

4.1   Subscriber Identity Confidentiality

The purpose of this function is to avoid an intruder to identity a subscriber on the radio path (e.g. Traffic Channel or signaling resources) by listening to the signaling exchanges [7]. This function can be archieved by protecting the subscriber's IMSI and any signaling information elements. Therefore, a protected identifying method should be used to identify a mobile subscriber instead of the IMSI on the radio path. The signaling information elements that convey information about the mobile subscriber identity must be transmitted in ciphered form. And also a ciphering method is used.

Identifying method.

The TMSI is used in the method. It's a local number and only valid in a given location area. The TMSI must be used together with the LAI to avoid ambiguities.

The network manages the databases (e.g. VLR) to keep the relation between TMSIs and IMSIs [7]. When a TMSI is received with an LAI that does not correspond to the current VLR, the IMSI of the MS must be requested from the VLR in charge of the indicated location area if its address is known; otherwise the IMSI is requested from the MS.

A new TMSI must be allocated in each location updating procedure. The allocation of a new TMSI corresponds implicitly for the mobile to the de-allocation of the previous one [7]. In the fixed part of the network, the cancellation of the record for an MS in VLR implies the de-allocation of the corresponding TMSI.

When a new TMSI is allocated to an MS, it is transmitted to the MS in a ciphered mode. The MS stores its current TMSI in a non-volatile memory together with the LAI so that these data are not lost when the MS is switched off.

Cases of Location updating procedure

The following paragraphs list several cases during the location updating to show how the identifying method works. The interested readers can find rest of cases in [7].

Location updating in the same MSC area. In this case, the original and new location area are controlled by the same MSC. The TMSI is issued by the VLR, at the latest, when the mobile station changes from one LA into another. When the MS entered a new location area, it reports to the new VLR with the old LAI and TMSI (i.e., LAI, TMSIold). The VLR then issues a new TMSI (TMSInew) for the MS (cf. Fig. 3). This TMSI is transmitted in encrypted form [7].

Location updating in a new MSCs area, within the same VLR area. This is the case when the original location area and the new one depend on different MSCs, but they are on the same VLR. The BSS/MSC/VLR indicates the location of the MS must be updated. Fig. 3 illustrates this procedure. *The management of means for new ciphering* in the figure means that the MS and BSS/MSC/VLR agree on the means for ciphering signaling information elements, especially for transmitting TMSInew [7].

Location updating in a new VLR, old VLR reachable. This case happens when the original location area and the new one depend on different VLRs. The MS is still registered in VLRold and requests registration in VLRnew. LAI and TMSiold are sent by MS as identifying fields during the location updating procedure. The MSC/VLRnew needs

some information for authentication and ciphering. This information is obtained from MSC/VLRold [7].

GPRS User Identity Confidentiality (stage 1).

GPRS network uses the similar identifying method with the distinction that the MS sends Temporary Logical Link Identity (TLLI) and Routing Area Identity (RAI) to the SGSN [12]. A TLLI (Temporary Logical Link Identity) is used to identify a GPRS user on the radio path instead of TMSI in GSM [7]. The SGSN handles the procedure instead of MSC. Location updating is combined with routing area updating.

The TLLI is still a local number and has a meaning only in a given RA (Routing Area). The TLLI must be accompanied by the Routing Area Identity (RAI) to avoid ambiguities. The SGSN manages suitable databases to keep the relation between TLLIs and IMSIs instead of VLR in GSM. The relationship between TLLI and IMSI is known only in the MS and in the SGSN (cf. Fig. 2).

When a TLLI and an RAI do not correspond to the current SGSN, the IMSI of the MS is requested from the SGSN in charge of the indicated routing area if its address is known; otherwise the IMSI is requested from the MS. A new TLLI may be allocated in each routing area updating procedure.

4.2   Subscriber Identity Authentication

This function can be triggered by the network whenever one of the following events happens [9]:

- Subscriber applies for a change of subscriber-related information element in the VLR or HLR [9]. The subscriber-related information element includes location updating involving change of VLR), registration, or erasure of a supplementary services).

- Subscriber accesses to a service. The service may be setting up mobile originated or terminated calls, activation or deactivation of a supplementary service.
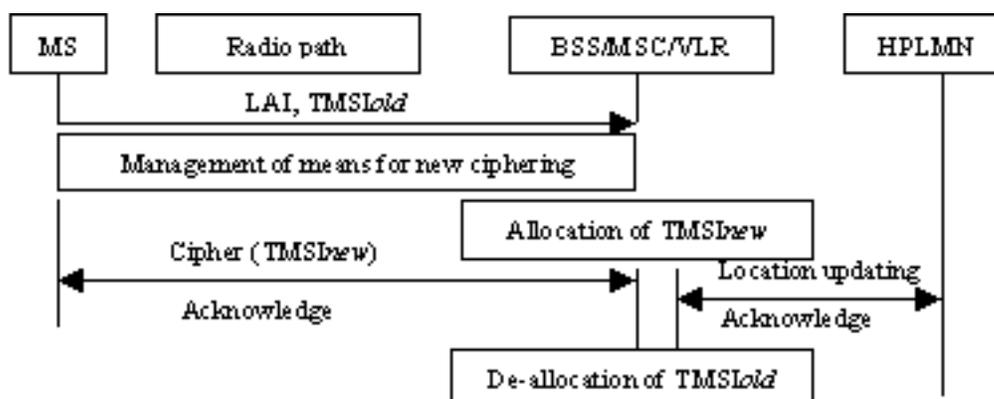

Figure 3: Location updating in a new MSCs area, within the same VLR area [7]

- Subscriber accesses to the network for the first time after restarting of MSC/VLR.

- The cipher key sequence number mismatch.

When a subscriber is added to a home network for the first time, a Subscriber Authentication Key (Ki) is assigned in addition to the IMSI to enable the authentication [10]. At the network side, the key Ki is stored in the AUC of the home PLMN. A PLMN may contains one or more AUC [9]. At the subscriber side, the Ki must be stored in the SIM. This function must complete an authentication procedure including management of the keys inside the fixed network subsystem.

The authentication procedure is based on the A3 algorithm [7, 4]. The A3 algorithm is implemented at both the network side and the MS side. This algorithm calculates independently on both sides the Signature Response (SRES) from the Ki and a Random Number (RAND) offered by the network (cf. Fig. 4) (i.e., SRES=A3(Ki, RAND)) [4]. The Ki and IMSI are allocated at subscription time. The MS transmits its SRES value to the network that compares it with its calculated value. If both values agree, the authentication is successful. Each execution of the algorithm A3 is performed with a new value of the RAND which cannot be predetermined; in this way recording the channel transmission and playing it back cannot be used to fake an identity. The operators may free to design their own A3 algorithm [14].
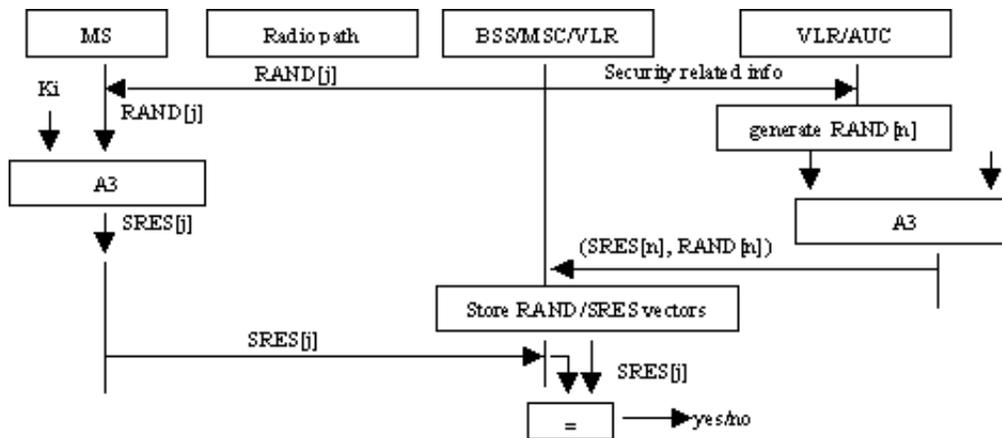

Figure 4: General authentication procedure

Fig. 4 shows a general authentication procedure. At the network side, the 2-tuple (RAND, SRES) need not be calculated each time when authentication has to be done. Rather the AUC can calculate a set of (RAND, SRES) 2-tuples in advance by applying A3 algorithm, store them in the HLR, and send them on demand to the requesting VLR [4]. The VLR stores this set (RAND[n], SRES[n]) and uses a new 2-tuple from this set for each authentication procedure. Each 2-tuple is used only once; so new 2-tuples continue to be requested from the HLR/AUC [9]

Several special cases may happen When performing the authentication procedure. The following paragraphs describe some cases. Others can be found in [4].

In this case, the authentication is done during location updating in a new VLR and identification is done using TMSI. The pairs for authentication as part of security related information are given by the old VLR. The old VLR sends those pairs that have not been used to the new VLR.

Still the authentication is done during location updating in a new VLR, but IMSI is used for identification, or more generally when the old VLR is not reachable. In this case, the pairs of (RAND,SRES) contained in the security related information are requested directly from HPLMN.
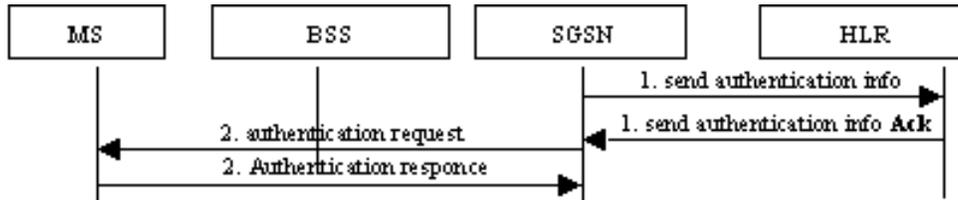

Figure 5: GPRS Authentication procedure [12]

GPRS Authentication

The GPRS authentication procedure is handled in the same way as in GSM with the distinction that the procedures are executed in the SGSN [12]. Fig. 5 shows a general GPRS authentication procedure. In some cases, the SGSN requests the pairs for a MS from the HLR/AUC corresponding to the IMSI of the MS.

4.3 Confidentiality of Signaling information elements, connectionless user data, and user information on Physical Connections

GSM confidentiality

The signaling information elements related to the user, such as IMEI, IMSI, and Calling subscriber directory number (mobile terminated or originated calls) need to be protected after connection establishment [4]. The user information such as short messages, is transferred in a connectionless packet mode over a signaling channel. It should be protected. And also User information on Physical Connections (voice and non-voice communications) on traffic channels over the radio interface should be protected. In order to archieve those confidentiality, a ciphering method, key setting, the starting of the enciphering and deciphering processes, and a synchronization are needed [4].

A ciphering method A5 is used to encrypt voice and signaling data [7]. It is a stream cipher based on three clock-controlled LFSR's using a ciphering key Kc. The layer 1 data flow (transmitted on Dedicated Control Channel (DCCH) or Traffic Channel (TCH)) is obtained by the bit per bit binary addition of the user data flow and a ciphering bit stream. The detailed ciphering can be found in [7].

A key setting completes a process that allows the MS and the network to agree on the key Kc using in the ciphering and deciphering algorithms A5 [7]. It is triggered by the authentication procedure and initiated by the network. Key setting must occur on a DCCH

not yet encrypted and soon after the identity of the mobile subscriber is known by the network.

The transmission of Kc to the MS is indirect. A Kc is generated on both sides using the key generator algorithm A8 and the RAND of the authentication process. At the network side, the values of Kc are calculated in the AUC/HLR simultaneously with the values for SRES. At the MS side, the Kc is stored by the mobile station until it is updated at the next authentication.

The encryption of signaling and user data is performed at the MS as well as at the BSS. This is a case called symmetric encryption, i.e. ciphering and deciphering are performed with the same Kc and the A5 algorithm and start on DCCH and TCH. [7]. This process can be described as follows: First, the newtwork (i.e. BSS) requests the MS to start its(de)ciphering process and starts its own deciphering process. The MS then starts its ciphering and deciphering.The first ciphered message from the MS, which reaches the network and is correctly ciphered leads to the start of the ciphering process on the network side [7].

The enciphering stream at one end and deciphering stream at the other end must be synchronized.

GPRS confidentiality GPRS network still needs this security feature. However the ciphering scope is different. The scope of GSM is between BTS and MS. The scope of GPRS is from the SGSN to the MS. A new ciphering algorithm GPRS-A5 is used because of the nature of GPRS traffic. The ciphering is done in the Logical Link Control (LLC) layer. The GPRS-Kc is handled by the SGSN independently from MSC [12].

5   Conclusions

This paper described the securty issues of GSM and GPRS. In particular, the more technical functions in each feature and SIM about security are introduced. However, the GSM system defined in the standard is not perfect. There are still some potential threats posed.

In subsciber authentication procedure, a collision attack on the A3 or A8 algorithm (i.e., single algorithm) is one example [14]. In order to avoid the attack, the operators should replace the weak A3/A8 algorithm with a strong one. The microwave links to the BSSs are extensively used when the operator opens its service. The voice and cipher keys Kc can be intercepted on these links. From the standard introduced, we know that the encryption of voice and use data is only on the radio interface between the MS and the BTS. It does not provide any protection method on the user traffic and signaling data transferred through the fixed parts of network. The ciphering keys should also be protected when transferred between and with networks on ss7 signaling links [14].

The paper didn't address the lawful interception in GSM and GPRS. It can be found in [12, 14].

6   Acknowledgment

I would like to deeply thank my tutor kaisa nyberg for her guide. It is invaluable for improving the paper and my future studies and work.

I would also like to thank my opponent Catharina Candolin for her valuable comments.

References

[1] ETS 300 501. European Digital Cellular Telecommunication System (Phase 2); Bearer Services (BS) Supported by a GSM Public Land Mobile Network (PLMN). *European Telecommunications Standards Institute.*, September 1994.

[2] ETS 300 502. European Digital Cellular Telecommunication System (Phase 2); Tele-services Supported by a GSM Public Land Mobile Network (PLMN). *European Telecommunications Standards Institute.*, September 1994.

[3] ETS 300 506. Digital Cellular Telecommunication System (Phase 2); Security Aspects. *European Telecommunications Standards Institute.*, August 2000.

[4] ETS 300 534. Digital Cellular Telecommunication System (Phase 2); Security Related Network Functions. *European Telecommunications Standards Institute.*, August 1997.

[5] ETS 300 608. Digital Cellular Telecommunication System (Phase 2); Specification of the Subscriber Identity Module-Mobile Equipment (SIM-ME) Interface. *European Telecommunications Standards Institute.*, May 1998.

[6] ETR 100. European Digital Cellular Telecommunication System (Phase 2); Abbreviations and Acronyms. *European Telecommunications Standards Institute.*, April 1995.

[7] ETSI TS 100 929. Digital Cellular Telecommunication System (Phase 2); Security related network functions. *European Telecommunications Standards Institute.*, November 1999.

[8] ETSI EN 301 344. Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2. *European Telecommunications Standards Institute.*, September 2000.

[9] Jörg Eberspächer and Hans-Jörg Vögel. *GSM switching, services and Protocols*. John Wiley and Sons, 1999.

[10] Garg, Vijay K. *Principles and applications of GSM*. Upper Saddle River (NJ) Prentice Hall PTR, 1999.

[11] Tanenbaum, Andrew S. *Computer networks*. Upper Saddle River (NJ) Prentice-Hall 1996.

[12] Hannu H. Kari. http://www.cs.hut.fi/ hhk/GPRS/.

[13] Klaus Vedder GSM: Security, Services, and SIM. State of the art in Applied Cryptography. *Course on Computer Security and Industrial Cryptography*. Leuven, Belgium, June 3-6, 1997.

[14] Fred Piper and Michael Walker. Cryptographic Solutions for Voice Telephony and GSM. *Network Security*. December 1998.