GSM: Security, Services, and the SIM

Klaus Vedder

Giesecke & Devrient GmbH
Prinzregentenstr. 159, D-81677 München, Germany
klaus.vedder@gdm.de

Abstract. Security requirements and services of a mobile communication system differ, due to the radio communication between the user and the base station, extensively from those of a fixed network. There is no physical link in the form of a (fixed) telephone line between the user and the local exchange, which could serve to "identify" the user for routing and charging purposes. Authentication by means of cryptographic procedures is thus required to stop impostors from taking on the identity of somebody else and "transferring" calls and charges. Eavesdropping on the radio path, intercepting data or tracing the whereabouts of a user by listening to signalling data are other serious threats. This paper discusses countermeasures designed into the Global System for Mobile communications, the rôle of the Subscriber Identity Module as a security device and security aspects related to the management of the secret authentication keys.

1 Introduction

The specification of the *G*lobal *S*ystem for *M*obile communications (GSM) began in 1982 with the formation of the *G*roupe *S*pécial *M*obile (GSM) by the European Conference of Postal and Telecommunications Administrations (CEPT). In 1989 GSM became a Technical Committee of ETSI, the newly founded European Telecommunications Standards Institute. This allowed industry to take a more active rôle in the standardisation process through "direct" participation. The eleven SubTechnical Committees specify all aspects of this digital cellular system from services and facilities to the interface between a mobile and a subscriber card. They are also responsible for the *U*niversal *M*obile *T*elecommunications *S*ystem (UMTS). The incorporation of this next generation system into the scope and work of the Technical Committee GSM in 1992 also led to the change in the acronym for the committee from GSM to SMG (*S*pecial *M*obile *G*roup).

GSM offers the user the possibility to roam across networks and national boundaries. A roaming agreement between the two operators is the only real prerequisite. Though the implications of roaming for network management and billing procedures are manifold one could, from a security point of view, think of the

B. Preneel, V. Rijmen (Eds.): COSIC'97 Course, LNCS 1528, pp. 224-240, 1998.

foreign network as a remote part of the subscriber's home network. While the data needed for checking the authenticity of a user are generated by the home network, the verification of the data and thus the access control to the (visited) network are handled locally by the Visitor Location Register (VLR) where the (roaming) subscriber is temporarily registered.

All the necessary information about the subscription as well as the network specific authentication algorithm and the subscriber specific authentication key are contained in the subscriber card, the *S*ubscriber *I*dentity *M*odule (SIM). The split of a Mobile Station (MS) into a radio part, the Mobile Equipment (ME), which does normally not contain any subscription related information, and a subscription part, the SIM, gives the network operator, on whose behalf the SIM has been issued, the complete control over all subscription and security related data. The SIM is thus an integral part of the overall security system of each and, therefore, all networks and a token for the mobility of the subscriber.

Listening to the communication between a Mobile Station and a base station can hardly be prevented. One of the novel features of GSM is the enciphering of this link to protect user and signalling data against eavesdropping. Special ciphers have been developed for this purpose. They are integrated into the ME as a dedicated piece of silicon. The cipher key is derived by the SIM during the authentication process. To authenticate a SIM the network has to know its (claimed) identity. As this has to be sent over the air interface, temporary identities are used to counteract the threat of tracing the user's whereabouts.

After discussing security issues and the security services provided in a GSM network, we look at the rôle played by the Subscriber Identity Module as a secure device for storing keys and algorithms. This is followed by a consideration of aspects related to key management, a list of abbreviations with definitions, and the references. The article is based on the current GSM Phase 2 specifications with some particularities of Phase 1 being mentioned. For more information on the GSM system the reader is referred to [5,16].

Threat analysis and security services are similar in nature for most mobile communication systems. To obtain a deeper insight into these issues the interested reader is referred to [3] which contains a threat analysis as well as the specification of the security services for DECT, the Digital Enhanced Cordless Telecommunications. The second edition of [3] contains several annexes dealing with the security of the interworking between DECT and GSM. It also discusses the functionality of the SIM and the DAM [4] in such a system. The DECT Authentication Module (DAM) plays a rôle similar to that of the SIM.

2 Security Issues

The main security threats to a mobile communication system are probably the illegitimate use of a service and the interception of data on the air interface which could result in a variety of threats to the profitability of the system, the privacy of the user and the integrity of either.

It is clearly important that billing should always be possible and that only the subscriber, who has caused the charge, is billed for it. The purpose of a masquerading attack may, however, not just be to defraud the network by having the charges transferred to *any* subscriber but to impersonate a *specific* subscriber. This could then be used to "show" that that subscriber made a call from a particular place at a particular point in time. Authentication of the subscriber by cryptographic means and the use of a security device for storing data and algorithms needed for the authentication process are thus essential requirements.

At the set up of a session the identity of the subscriber has to be sent to the network by the MS. Furthermore, due to the constant update of the location of an MS, which is necessary for a proper and timely delivery of mobile terminated calls, the network has to know the location of the subscriber card down to the cell in which the MS containing this card is active, that is, switched on. (The area covered by a cell may range from a few hundred metres to about 35 km.) Measures need thus be taken to the protect the confidentiality of the identity of the subscriber.

The interception of user data or user related signalling information may result in a loss of confidentiality of this data or of the user's identity with respect to the outside world. User data are transferred over traffic channels as well as over signalling channels. The signalling channels carry, apart from obvious user related signalling information elements such as the called and the calling telephone numbers and user data in form of short messages. These allow the user to receive and send messages of up to 160 bytes over the radio link without activating a traffic channel.

To protect network operators and users against attacks inherent in any unprotected radio link, the *implementation* of the following security features is mandatory:

- subscriber identity confidentiality;
- subscriber identity authentication;
- user data confidentiality;
- signalling information element confidentiality.

The functional description of these security features is contained in GSM 02.09 [7]. A standard on the secure management of networks [12] has been elaborated by SMG6 which deals with operation and maintenance issues.

3 The Security Services

A functional description is by its very nature not sufficient to ensure interoperability between networks and the same level of security being achieved throughout the system. The specification of the security related network functions and the parameters for the cryptographic algorithms needed to provide above services are contained in GSM 03.20 [9] which forms the basis for the implementation of these features.

From a user point of view it is not relevant whether the user-related data to be protected are contained in a traffic or a signalling channel. We may therefore say that GSM provides three security services:

- *temporary identities* for the confidentiality of the user identity;
- *authentication* for the corroboration of the identity of the user;
- *enciphering* for the confidentiality of user-related data.

3.1 Temporary Identities

When a user logs into a network the identity of the subscriber has to be made known to the network. Rather than sending the International Mobile Subscriber Identity (IMSI), which uniquely identifies the subscriber world-wide, a temporary identity is transmitted by the MS in most instances.

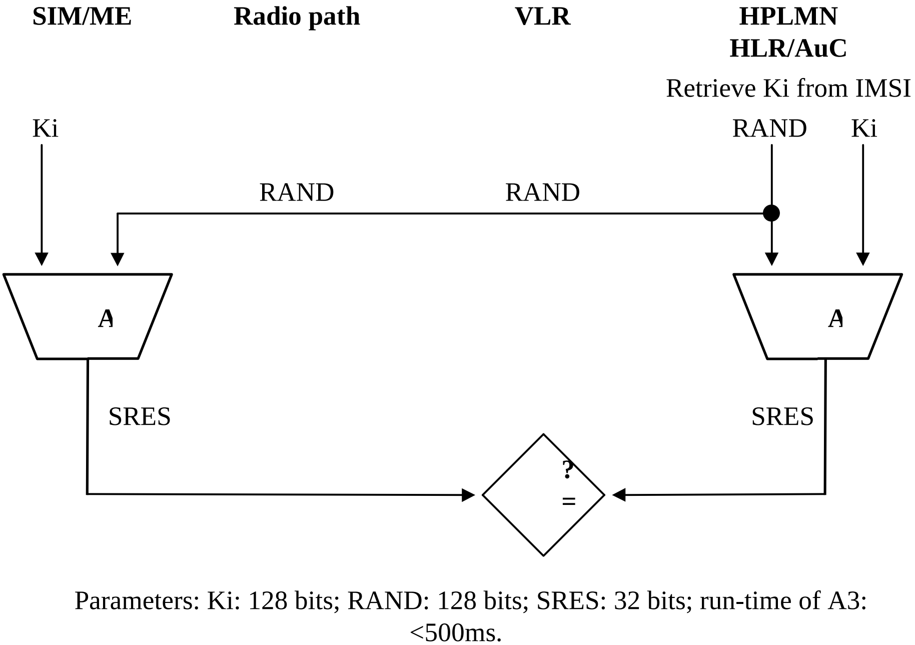
The purpose of temporary identities is to deny an intruder the possibility of gaining information on the resources used by a subscriber, preventing the tracing of the user's location and matching user and data transmitted. To achieve this "the IMSI is not normally used as an addressing means on the radio path" [9]. Clearly, the IMSI has to be used for the set up of a session if there are no other means to identify a mobile subscriber. This is, for instance, the case when the subscriber uses the SIM for the first time or at a data loss in the VLR where the subscriber is temporarily registered. When the SIM is used for the first time, the MS will read the default Temporary Mobile Subscriber Identity (TMSI) stored in the SIM at pre-personalisation (see 5.3) and send this value to the VLR. As this is a default value, the VLR will request the IMSI from the MS. It then assigns a TMSI to the subscriber and transmits this (after a successful authentication and the activation of the cipher) in an enciphered form to the MS. The MS deciphers the data and stores the TMSI and information about the present location in the SIM. At the next log-in the TMSI will be sent in clear to the network, a new TMSI will be assigned by the VLR and sent to the MS as enciphered data. Enciphered TMSIs can thus not be matched against TMSIs in clear text. Furthermore, the TMSI must be updated at every location update and will be changed several times during a session.

Though the TMSI consists of only five digits, the subscriber is uniquely identifiable. For the TMSI is unique within the location area where the MS moves, and the location area identity (LAI) is always used in conjunction with the TMSI. As TMSI, IMSI and LAI are stored in the VLR the identity of a subscriber moving to a different VLR can easily be established by the new VLR. It knows the "old" VLR from the LAI which the MS has sent together with the TMSI at log-in and it then obtains the subscriber's IMSI from the old VLR. If there is no malfunctioning of the system the IMSI will not be used (over the air) for call set up after the initial session. GSM 03.20 [9] specifies eight procedures for the allocation of a new TMSI depending on the structure of the network(s) and possible data losses.

3.2 Authentication of the Subscriber

Authentication is the corroboration that an entity is the one claimed or, in this context, the verification of the identity of the SIM. The purpose is "to protect the network against unauthorised use" [7] and thus to ensure correct billing and to prevent masquerading attacks. Subscriber authentication is of major interest to each operator and all management issues not affecting the interoperabilty of GSM are left to the sole discretion of the operator.

The authentication algorithm (denoted by A3) is implemented in the Authentication Centre (AuC) of the home network, the Home Public Lands Mobile Network (HPLMN), and in the SIM. For operators not using a proprietary algorithm a proposal for an authentication algorithm is available upon appropriate request [9]. To achieve interoperability between all the networks and compatibility of the suppliers the parameters to be satisfied by the algorithm A3 and the authentication protocol have been specified by SMG [9]. The method employed between the HLR/AuC and the SIM is a Challenge-Response mechanism using "non-predictable numbers".



Parameters: Ki: 128 bits; RAND: 128 bits; SRES: 32 bits; run-time of A3: <500ms.

Figure 1: Authentication procedure

Figure 1 shows the basic procedure for the authentication of the SIM by the network. It should be noted that the rôle of the VLR is in [9] attributed, more generally, to the BSS/MSC/VLR parts of the system.

After establishing the identity of the SIM (see above) the VLR sends an authentication request to the HPLMN. This request contains the IMSI which is needed to retrieve the secret, individual subscriber authentication key Ki used in the protocol. The HPLMN then generates a non-predictable number RAND which is sent to the MS as a challenge (via the VLR). To compute the "Signed RESponse" SRES to the challenge RAND the SIM uses the algorithm A3 with RAND and the key Ki stored in the SIM as input data. SRES is then transmitted to the VLR which may be in a foreign network. There it is compared with the value SRES computed by and received from the AuC of the HomePLMN. The AuC has used the operator specific algorithm A3 with the same RAND and the key Ki which is associated with the identity claimed by the subscriber. The MS is granted access to the network by the VLR only if the value for SRES received from the MS equals the value received for SRES from the HLR/AuC. Only in this case it can be assumed that the SIM is in possession of the right subscriber key Ki and that its identity is the one claimed.

Upon request for security related information the VLR usually receives from the HLR/AuC a set of pairs consisting of RAND and the corresponding SRES. Accompanying these pairs is always a new cipher key Kc which has been computed using Ki and the same non-predictable number RAND with an algorithm called A8 (see 3.4). The challenge RAND and the derived values SRES and Kc are called an authentication triplet or a set of security related information.

When a user has moved to a new VLR, the new VLR will normally establish the subscriber's identity by requesting the IMSI from the old VLR (see 3.1). In both Phase 1 and Phase 2 the old VLR transfers, together with the IMSI, any unused triplets to the new VLR. This speeds up the authentication procedure as the new VLR can only send a request for triplets to the subscriber's HLR/AuC after it has learned of the "real" identity of the subscriber which is through this request to the old VLR.

In Phase 1 each triplet is used only once and must be discarded after being used. Both restrictions do not apply to Phase 2. The re-use of security related information in failure situations such as a breakdown of the link to the HLR is considered to improve the security level. In Phase 1 the VLR may in such a situation permit outgoing calls without further authentication if the MS has been successfully registered and authentication triplets cannot be obtained from the HLR.

Another Phase 1 option which has been deleted from the Phase 2 specifications is that the HLR/AuC may transmit, upon request for security related information, the secret subscriber key Ki to the VLR for the local generation of the triplets. It is however recommended to restrict this procedure to the HPLMN (clause 3.3.2 of GSM 03.20 Phase 1). Using this option would certainly reduce the traffic with the HLR and improve the availability of the service in situations where the link between the HLR and the VLR is unreliable. The security implications are, however, severe. The (secret) algorithms A3 and A8, which are used to generate SRES and Kc, need to be implemented in the VLR in a secured environment and secret keys have to be sent from the HLR to the VLR. The cryptographic protection of these links, which are natural places for an attacker to collect IMSIs and corresponding keys, may not always be possible. In the case that this method was used for roaming the home network would have to disclose algorithms and keys to the other operator or to supply black boxes and sending the keys enciphered.

3.3 Authentication of the Network

Unlike DECT, the security features of which have been specified only in the early 90s, GSM does not provide the means for the SIM to authenticate the "network". When specifying the security features of GSM this functionality was considered to be of limited use and the idea of administrating data in the SIM over the air interface had not been of widespread interest. The latter has changed considerably during the last few years and the finalisation of the so-called SIM Application Toolkit [11] has led to a revival of this dormant topic.

The SIM Application Toolkit offers a platform for new operator specific services such as the downloading of data into the SIM by use of the short message service. A typical example would be the update of service numbers or the creation of new data-fields in the SIM. The downloading of the data would be transparent for the Mobile Equipment. The SIM would "unwrap" the short message and execute the command internally without the request by its master, the ME. Depending on the data to be updated and the commands to be executed, the SIM has to be sure that the sender of the short message as well as its contents are genuine and have not been altered in an unauthorised manner. An obvious way of achieving both is to protect the contents of the short message by means of a message authentication code (MAC) [14]. The MAC is sent as part of the short message and verified by the SIM prior to any action coded in the short message. As calculation and verification of the MAC require a secret key known only to the sender (network) and the receiver (SIM), the SIM can also indirectly authenticate the network. If the verification of the MAC is positive the SIM can assume that the sender is the one claimed.

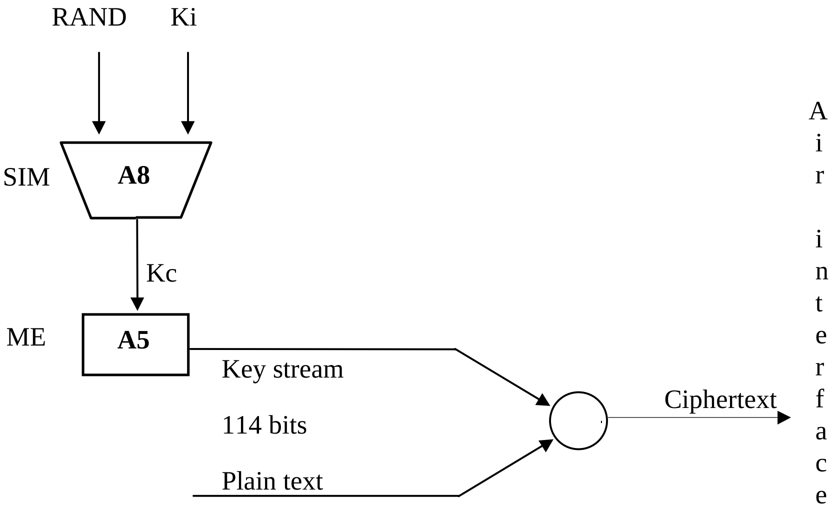
The authentication of sender and data are clearly not the only security relevant questions one has to discuss when using the short message service for the administration of SIMs. Other issues are, for instance, replay attacks and problems which might arise if commands and data are contained in more than one short message. As the SIM Application Toolkit is part of the GSM Phase 2+ programme and thus optional, one could argue that the security of these features is up to the specific operator and its suppliers. On the other hand, security holes in one network may have an effect on the system in general, even if it is "only" from an image point of view. Work has now started on providing a security standard for the short message service as part of the SIM Application toolkit.

3.4 Enciphering

The purpose of this security service is to ensure the privacy of the user information carried in both traffic and signalling channels and of user-related signalling elements on the radio path. The activation of this service is controlled by the network. It is started by the base station by sending a "start cipher" command to the MS. A standard cipher algorithm A5, now denoted by A5/1, is contained as a dedicated piece of silicon in mobile equipment and base stations. This algorithm can be implemented using about 3,000 transistors [2]. Since March 1993 a second cipher called A5/2 is available. Not more than seven version of the A5 will however be defined [9].

A form of stream cipher is used to encipher the layer 1 data. The plain text is organised into blocks of 114 bits as this is the amount of data which is transmitted during a time slot. The key stream, which is the sequence of bits to be XORed (modulo 2 addition) with the data block, is produced by the algorithm A5 as an output block of 114 bits. For synchronisation and other implementation details the reader is referred to [9].

Figure 2 below also shows the generation of the cipher key Kc, which controls the generation of the key stream by the algorithm A5. This key is derived in the SIM as part of the authentication process using the network operator specific cipher key generator A8 and the same RAND and Ki as in A3.



Parameters: Ki: 128 bits; RAND: 128 bits; Kc: 64 bits.

Figure 2: Cipher key generation and enciphering

Binding the generation of Kc to the authentication process has several advantages. No additional input data are required. Bypassing the authentication procedure by, say, manipulating the comparison of SRES in the VLR will, in general, not allow a fraudulent use of a service. The MS and the base station would use different cipher keys resulting in an indecipherable garbled message.

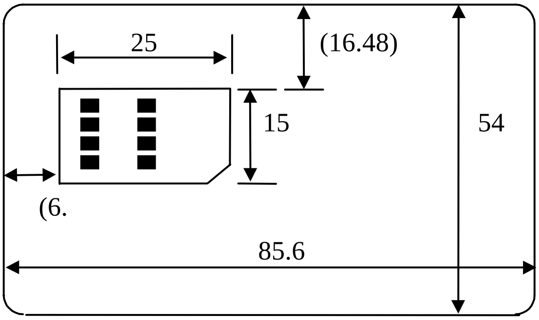
It is also worth noting that the authentication algorithm A3 as well as the cipher key generator A8 compress the non-constant input data RAND from 128 bits to 32 bits (SRES) and 64 bits (Kc), respectively. Even if A3 and A8 are one and the same algorithm (denoted by A38), a compression takes place. This implies that the challenge RAND can not be derived just from the output data (Kc, SRES) and that the SIM can not be used for enciphering or deciphering data.

4 The Subscriber Identity Module

The Subscriber Identity Module (SIM) is a security device which contains all the necessary information and algorithms to authenticate the subscriber to the network. It also adds a new dimension of mobility to the subscription as it is a removable module and may be used in any mobile equipment (subject to the SIM having the right format). The functionality of the SIM is described in GSM 02.17 [8] while its interface to the ME is specified in GSM 11.11 [10a,b] (reference [10b] contains additional features and services which are part of the optional GSM Phase 2+ enhancements).

4.1 General Properties

To achieve its main task of authenticating the subscriber to the network, the SIM contains a microcomputer with on-board non-volatile memory. The SIM is a smart card which comes in two formats. The ID-1 SIM has the size of a credit card. The Plug-in SIM, which is used mainly with mobiles too small to support an ID-1 SIM, may be "obtained" from the latter by cutting away excessive plastic and thus reducing the size to 25 mm by 15 mm (see figure 3). The electrical and mechanical interfaces are, with the obvious exception of the size of the Plug-in SIM, in line with the relevant International Standards for *I*ntegrated *C*ircuit (IC) cards [10, 13]. In some instances more stringent conditions were agreed upon to cater for the needs of the environment the SIMs are used in. These include the temperature range the card has to satisfy and the power consumption of the microcomputer.



ROM	up to 20 kByte
RAM	up to 512 Byte
EEPROM	up to 16 kByte

Figure 3: SIM formats and memory provided

The microcomputer consists of a CPU and three types of memory. The masked programmed ROM (Read Only Memory) usually contains the operating system of the card, the code for the GSM application and the security algorithms A3 and A8. The RAM (Random Access Memory) is used for the execution of the algorithms and as a buffer for the transmission of data. Subscription specific data such as Ki and IMSI, network related information such as TMSI and LAI, which need to be updated by the network, and subscriber related information such as abbreviated dialling numbers, which have to be changeable by the subscriber, are stored in non-volatile erasable memory (EEPROM, Electrically Erasable Programmable Read Only Memory). The memory space offered by present day smart card chips is given in figure 3. For more information on smart cards the reader is referred to [17].

4.2 Access to the SIM

The operating system of the card controls the access by the outside world, which may be an ME or any other interface device, to all data stored in the card. Access is mainly by reading or updating the respective memory cells. GSM has specified five (independent) access conditions. These are NEVER, ALWAYS, ADM, PIN and PIN2. The access condition ALWAYS means that no security restriction holds. The IC Card Identification number, which identifies the SIM and is also printed on the card itself, may ALWAYS be read over the interface but will NEVER be permitted to be updated. The definition and use of ADM is up to the discretion of the operator. This may be one of the five access conditions or a specific procedure which can only be executed by an appropriate administrative authority. PIN and PIN2 are discussed in the following section.

The interface to the outside world consists of eight contacts two of which are reserved for future use [13]. One of the remaining six contacts is needed for cards requiring an external Programming Voltage. For the GSM application this is not connected to the microcomputer as all SIMs have to derive the programming voltage from the Supply Voltage (Vcc) by means of an internal charge pump. Apart from the Vcc contact there are thus only four contacts to access the microcomputer electrically by "normal" ways. These are used for the Reset of the chip, the Clock to drive the chip, Ground and the Input/Output of data. Having only one I/O channel certainly restricts the data throughput but is of an advantage from a security point of view. At a Baudrate of 9,600 bits/sec the (theoretical) upper bound for the card throughput is 3,200 bits/sec. This is due to the half duplex transmission protocol and other overhead.

4.3 User Access to the SIM

User access to the SIM is controlled by a *P*ersonal *I*dentification *N*umber (PIN). The PIN, which can be freely chosen within the range of 4 to 8 digits, may be changed by the user as often as felt necessary. This is possible since the PIN is stored in the EEPROM of the chip and the comparison of the value presented by the user with the PIN stored is done by the microcomputer of the SIM; the PIN does not leave the chip. To protect the user against trial and error attacks, the microcomputer controls the number of consecutive false PIN entries. After three such entries the card will be blocked and refuse to work, even if it has been removed in between attempts or a different ME is used. A blocked SIM does not even send its identity in form of the TMSI or IMSI to the ME as these data-fields are protected against reading by the security level PIN. The user can only "unblock" a SIM by presenting the so-called PIN Unblocking Key (PUK) to the card together with a new PIN. The PUK is simply another identification number consisting of eight digits. After 10 consecutive wrong PUK entries the SIM is permanently blocked. As the PUK cannot be changed by the user it could also be stored in the home network and given to the user if the necessity arises (subject to certain security conditions being satisfied). It should also be recalled that the access of a SIM to a mobile service can easily be suspended by blacklisting the subscription in the HLR/AuC.

Another novel feature is the option to disable the PIN check. The network operator or the service provider, if the network operator so decides, may set a flag in the card which allows the user to switch off (and on) the PIN check. If the PIN check has been disabled by the user, the SIM will not request the presentation of a PIN at the beginning of a session and access control to the SIM and thus the network (if the card is not blacklisted in the HLR/AuC) is based merely on the possession of the card.

The introduction of certain new services in Phase 2 has changed the rôle of the PIN. A SIM supporting the fixed dialling number service will not allow the user to call numbers other than those stored in the SIM. Advice of Charge may in certain scenarios used not only as an advice to the customer about the number of units spent but also for limiting the amount of money spent by the user. Typical examples for such applications would be SIMs issued to drivers of a fleet of lorries or to children. Changing the fixed dialling numbers or resetting the charge counter should clearly not be under the control of the user (though it may be under the control of the subscriber) and thus not under the control of the PIN. For the update of the contents of these and other data-fields independently of the normal PIN, PIN2 and the accompanying PUK2 have been introduced. Due to the nature of PIN2 as a means to protect data-fields the user should not have access to, it is not possible to disable the check of PIN2 though its value may, of course, be set to a trivial one or equal to the one of the PIN.

It should be mentioned that using the Advice of Charge service for charging purposes or the issue of pre-paid SIMs is, from a security point of view, not advisable. As the interface between the ME and the SIM is not secure it would be comparatively easy to manipulate the interface so that the charges do not reach the SIM. This would not be noticed by the network as the system does not provide the means that the card can acknowledge the receipt of the information. Though this could be achieved with a short message being generated by the SIM using the SIM Application Toolkit platform it is doubtful that effort and overhead would justify the purpose.

5 Key Management

In this section we consider some of the aspects concerning the authentication centre (AuC) and the handling of the individual subscriber authentication keys.

5.1 The Authentication Centre

The specific security and administrative requirements for an Authentication Centre are not standardised but left to each network operator as security matters are up to the discretion of the operator. GSM 03.20 [9] only states that the individual subscriber authentication keys Ki are stored in an AuC and that the AuC also contains the authentication algorithm(s) A3 and the cipher key generating algorithm(s) A8.

A malfunction or a temporary loss of the information contained in an AuC would have severe consequences for the security as it affects the generation of the authentication triplets. Since other information about the subscriptions, including possibly black lists of barred subscriptions, is contained in the HLR, it is only logical to "integrate" the AuC into the HLR. In networks with more than one HLR the back-up and overload facilities could be distributed over several HLR/AuCs.

Key management is a major issue when designing an AuC. The method used for generating and storing potentially several million individual subscriber authentication keys and the handling of the authentication requests are of importance for both the secure and the smooth running of the network.

5.2 Key Generation

There are two standard methods to generate keys. They may be generated by using a random number generator or by deriving them from user related data with the help of an algorithm under the control of a master key. Both methods have their advantages and disadvantages which we will briefly discuss in the light of the boundary conditions given in GSM 03.20 [9].

Deriving a key. The main advantage of deriving a key from non-secret (subscription) data under a master key MK is that such derivable keys need not be stored and that the back-up of the subscriber keys is reduced to the back-up of the master key. No data banks containing secret information are thus required in the AuC nor at the back-up facility. When an authentication request comes from the VLR, the AuC would just load the relevant data, say the IMSI, into the algorithm and derive the individual subscriber authentication key Ki from this data using the top secret master key MK. Ki would then be loaded with the random number into A3 and A8 for the generation of SRES and Kc.

The selection of the algorithm and the input data to go into this algorithm depend on several boundary conditions. These include the length of the key Ki (128 bits) and whether one of the algorithm(s) already available in the AuC is suitable or whether a specific algorithm should be employed. Considering the number of authentication requests the algorithm has to be fast if one wants to avoid "queues" or having too many secured boxes running in parallel. A natural candidate for the input data would be the IMSI which consists, however, of only 15 digits each one coded on half a byte [10]. A natural candidate for the algorithm is the DEA [1], often referred to as DES, which is also available in hardware. As the key Ki consists of 128 bits and the DEA has an input block of 64 bits one has to "expand" the IMSI to 16 digits and apply the DEA twice. To improve the distribution of the derived keys (with respect to the set of strings having 128 bits) one could first reduce the length of the IMSI to 10 digits by removing the 5 digits which are identical for all IMSIs of the HPLMN and use parts of other subscription related data for the remaining 6 digits. Two possibilities to obtain Ki from this value UD representing the user data are given below, where "||" denotes the concatenation of the two terms and UD' (user) data which is different from UD:

(i) $\mathrm{Ki} = \mathrm{DEA}_{\mathrm{MKleft}}(\mathrm{UD}) \,||\, \mathrm{DEA}_{\mathrm{MKright}}(\mathrm{UD})$, and

(ii) $\mathrm{Ki} = \mathrm{DEA}_{\mathrm{MK}}(\mathrm{UD}) \,||\, \mathrm{DEA}_{\mathrm{MK}}(\mathrm{UD'})$.

In the first case the master key consists of two parts of 64 bits each, while in the second case the same 64 bit key is used for the calculation of the both parts.

Though this method may look very elegantly at first glance it has a few undesirable effects if it is not managed with extreme care from both an administrative as well as a security point of view.

The main problem is of course to keep the very secret key MK secret. Anybody coming into possession of this key could, if he/she also knows the method of deriving Ki and the secret algorithms A3 and A8, compromise every card issued under MK. One could reduce the potential damage by replacing the master key periodically. As a consequence, more secret keys have to be maintained and a logical link has to be established between the respective master key and the subscription (this could be done by coding the key number as part of the IMSI). The number of master keys being used at the same time depends on the length of time each one of them has been employed for generating subscriber authentication keys as well as on the validity period of those SIMs.

The method can also lead to the production of "identical" SIMs. If the same IMSI has been used by mistake to generate the keys for two SIMs, these SIMs will be identical from a security point of view. They contain the same IMSI and Ki. Though this should normally be noticed at the activation of the "second" SIM the implications are such that it puts a big question mark against the whole method.

One can avoid the risk of producing identical SIMs by combining subscription data with random data. In this variation the input data UD would consist of the IMSI or parts thereof together with a string of random bits. This is however somewhat counterproductive to the main reason for choosing the method in the first place. For this random data has to be stored, though not enciphered, against the IMSI (or other identification data) in a data bank in the AuC. On the other hand, this variation has the advantage that the random data is not publicly available and not related to the subscription. A compromise of the master key does, therefore, not automatically impair the security of the whole system. One could even go a step further and use only random data for the input to the algorithm.

The key as a random number. Using a random number generator to produce the subscriber authentication keys insures that all strings consisting of 128 bits are equally likely. This is another advantage which cannot be achieved by an algorithm using IMSIs as an input. As there is no "natural" link between the subscription and the authentication key, all keys have to be stored against some subscription specific data in a data bank of the AuC and have to be backed-up at a physically different location. As the authentication request involves the IMSI this would again be a natural choice. To protect the keys against unauthorised reading in the AuC they have to be stored in an enciphered form. The key (or keys) used for deciphering the subscriber authentication keys is clearly very sensitive. A compromise of such a key is in itself not as much a security breach as a compromise of the master key used to derive the authentication keys from subscription data. The attacker also needs a listing of the entries of the data bank.

Similar things as before can be said about the choice of this algorithm. Assuming this to be the DEA in electronic code book mode [15], we can also see that the times required for providing a key for the authentication request are about the same for both methods (assuming that access to the data bank causes no significant overhead). In both instances the DEA has to be executed twice.

5.3 Pre-personalisation

Pre-personalisation usually refers to assigning and loading a SIM with authentication key and IMSI and all other subscription relevant data. In general, no subscriber related information is required in the SIM for the access of a GSM service. A pre-personalised SIM may thus contain all information necessary for the GSM operational phase and be ready for use subject only to its 'release' in the HLR/AuC.

Which of the methods described in section 5.2 is employed for the generation of the subscriber keys depends also on the administrative environment of the pre-personalisation. Deriving Ki from subscription data, which is known prior to the pre-personalisation of the SIM, allows the computation of Ki independently in the HLR/AuC and at pre-personalisation time. Ki need, therefore, not be transmitted between the two places. If Ki is a random number or depends partially on random data, then it may be generated either in the HLR/AuC or at the place of pre-personalisation. In this case Ki or the random data have to be transmitted in a secure way between the two entities. Both solutions have their advantages and disadvantages and a decision for one or the other should take all security and administrative boundary conditions into account.

Abbreviations

This section contains the abbreviations used in this paper together with a brief explanation. For a more elaborate description and the precise definition of all the terms the reader is referred to [5] and [6].

A3	Authentication algorithm A3; used for authenticating the subscriber
A38	A single algorithm performing the functions of A3 and A8
A5	Encryption algorithm A5; used for enciphering/deciphering data
A8	Ciphering key generating algorithm A8 (cipher key generator); used to generate Kc
AuC	Authentication Centre; used to generate authentication data (thus containing individual subscriber keys Ki as well as A3 and A8)
BSS	Base Station System
DECT	Digital Enhanced Cordless Telecommunications (formerly: Digital *European* Cordless Telecommunications)
ETS	European Telecommunications Standard
ETSI	European Telecommunications Standards Institute
HLR	Home Location Register; a register in the HPLMN of the subscriber where information related to the location and the subscription is stored
HPLMN	or HomePLMN: the network with which a subscriber is registered
IC	Integrated Circuit

IMSI	International Mobile Subscriber Identity; the identity which uniquely identifies the subscriber in all GSM networks, used for routing in GSM (not to be confused with the subscriber's mobile telephone number)
Kc	Ciphering key; used in A5 to generate the key stream
Ki	Individual subscriber authentication key; used in A3 and A8
LAI	Location Area Identity; information indicating the location of a cell or a set of cells
ME	Mobile Equipment; the MS without the SIM
MS	Mobile Station; the equipment used to access GSM
MSC	Mobile Switching Centre
PIN	Personal Identification Number; used by the SIM for the verification of the identity of the user
PLMN	Public Lands Mobile Network; a network providing communication possibilities for mobile users
PUK	PIN Unblocking Key; used to unblock the GSM application which occurred as a result of three consecutive wrong PIN entries
RAND	RANDom number; used as a challenge in the authentication process
SIM	Subscriber Identity Module; the subscriber card containing security and other subscription as well as network related information
SRES	Signed RESponse; used to verify the identity of the SIM in the authentication process
TMSI	Temporary Mobile Subscriber Identity; the temporary identity of a SIM issued by a VLR to provide subscriber identity confidentiality
VLR	Visitor Location Register; the register where the user is (temporarily) registered while in a location controlled by this register

References

[1] ANSI X3.92: 1981, *Data Encryption Algorithm*. American National Standards Institute.

[2] C. Brookson, *GSM Security: A Description of the Services*, in F. Hillebrand (ed.): *GSM, Digital Cellular Mobile Communications Seminar*, Budapest, 1990, 4.5/1-4.5/5.

[3] ETS 300 175-7, *Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features*, 1996 (2nd edition).

[4] ETS 300 331, *Digital European Cordless Telecommunications (DECT); DECT Authentication Module*, 1995.

[5] GSM 01.02 (ETR 099), *Digital cellular telecommunications system (Phase 2); General description of a GSM Public Land Mobile Network (PLMN).*

[6] GSM 01.04 (ETR 100), *Digital cellular telecommunications system (Phase 2); Abbreviations and acronyms.*

[7] GSM 02.09 (ETS 300 506), *Digital cellular telecommunications system (Phase 2); Security aspects.*

[8] GSM 02.17 (ETS 300 509), *Digital cellular telecommunications system (Phase 2); Subscriber Identity Modules (SIM), Functional characteristics.*

[9] GSM 03.20 (ETS 300 534), *Digital cellular telecommunications system (Phase 2); Security related network functions.*

[10a] GSM 11.11 (ETS 300 608), *Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface.*

[10b] GSM 11.11 (ETS 300 977), *Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface.*

[11] GSM 11.14, *Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface.*

[12] GSM 12.03 (ETS 300 614), *Digital cellular telecommunications system (Phase 2); Security management.*

[13] ISO/IEC 7816, *Identification cards-Integrated circuit(s) cards with contacts.*
Part 1: 1987, Physical characteristics.
Part 2: 1988, Dimensions and location of the contacts.
Part 3: 1989, Electronic signals and transmission protocols.

[14] ISO/IEC 9797: 1994 (2nd edition), *Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.*

[15] ISO/IEC 10116: 1997 (2nd edition), *Information technology - Security techniques - Modes of operation for an n-bit block cipher algorithm.*

[16] M. Mouly and M.-B. Pautet, *The GSM system for mobile communications,* ISBN 2-9507190-0-7, Palaiseau, 1992.

[17] K. Vedder and F. Weikmann, *Smart Cards*, this volume, pp. 311-336.

The author has been a member of the SIM Expert Group (SIMEG) since early 1988 when this group was formed. In April 1993 he became chairman of this group. Presently he is the chairman of the ETSI committee SMG9 "SIM aspects" which took over the work of SIMEG as the custodian of the interface between the SIM and the mobile equipment. SMG9 is also responsible for all smart card activities of GSM and UMTS, the Universal Mobile Telecommunications System. Apart from his work on the subscriber card for GSM he has been the founding chairman of the ETSI working party RES3/DAM which produced the European Telecommunications Standard ETS 300 331 "DECT Authentication Module". This specifies the use of a smart card as an authentication device for DECT, the Digital Enhanced Cordless Telecommunications.