3.2 The Use of Smart Cards in GSM

Dr. Klaus Vedder
Chairman ETSI STC SMG9
Giesecke & Devrient GmbH
Prinzregentenstr. 159, 81607 München, Germany

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 role of the Subscriber Identity Module and security aspects related to network management.

1 Introduction

The specification of the Global System for Mobile communications (GSM) started in 1982 with the formation of the Groupe Spécial Mobile by CEPT, the European Conference of Postal and Telecommunica-tions Administrations. In 1989 GSM became a Technical Committee of the newly founded European Telecommunications Standards Institute (ETSI) and is now known under the name SMG (Special Mobile Group). The 9 Sub Technical Committees specify all aspects of this digital cellular telecommunications system from services and facilities (SMG1) to the interface between a mobile and a *S*ubscriber *I*dentity *M*odule (SMG9) and co-ordinate the Universal Mobile Telecommunications System (SMG5).

One of the fundamental features of GSM is the possibility to roam across networks and national boundaries. A user may utilise the facilities of any GSM network subject only to a roaming agreement between the operators of the home network and the visited network. The implications of this for network management, billing procedures and security services are manifold. Authentication and billing are done by the operator of the home network of the subscriber, the so-called Home Public Land Mobile Network (HPLMN). Every operator can run its own proprietary authentication algorithm subject to it satisfying the interface parameters. While the data needed for checking the authenticity of a user is usually generated centrally by the home network, the actual verification and thus the access control to the (visited) network are handled locally by the Visitor Location Register (VLR), where the subscriber is temporarily registered.

When travelling the subscriber need only take the subscriber card, the SIM, along and insert this into any mobile equipment (ME). The SIM contains all the necessary information about the subscription, such as the International Mobile Subscriber Identity (IMSI), as well as the network specific authentication algorithm and the secret, subscriber specific authentication key. No subscription related information is contained in an ME. This split of a mobile station (MS) into a radio part and a subscription part 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 the corresponding base station can hardly be prevented. How useful, if at all, the intercepted data are to the eavesdropper depends on the security services provided by the network. One of the novel features of GSM is the enciphering of the radio link to protect user and signalling data. Special ciphers have been developed for this purpose. They are integrated into the mobile equipment as a dedicated piece of silicon. The key for enciphering the data is derived by the SIM as part of the authentication process. The enciphering can thus only be activated after the identity of the SIM has been (successfully) verified. To run the authentication procedure the mobile station is, of course, required to send the identity of the SIM over the air interface. To counteract the threat of tracing the whereabouts of a user, temporary identities are issued by the VLR.

After the discussion of the security features and the security services provided in a GSM network, we look at the role played by the Subscriber Identity Module as a secure device for storing keys and algorithms. This is followed by key management issues and a list of definitions and abbreviations. For a general description and background information on the GSM system the reader is referred to [4,14,16].

The security services specified for the new Digital European Cordless Telephone system (DECT) are similar in nature to those provided by GSM. As roaming is not an integral part of this cordless system, the authentication process may have to be done by a visited network. For this reason a DECT Standard Authentication Algorithm (DSAA) has been specified by ETSI. This is mandatory to be contained in the DECT Authentication Module, which plays a role similar to that of the SIM [13]. A very detailed threat analysis of the DECT system, which applies to a large extent to any mobile communication system, as well as the specification of the authentication functions are contained in [12].

2 Security threats and features

The basic security threats to an operator and the user are the interception of data on the air interface and the illegitimate use of a service.

The interception of user data or signalling information related to the user may result in a loss of confidentiality of this data or the loss of the confidentiality of the user's identity with respect to the outside world. (There is no anonymity as for instance offered by a pre-paid telephone card. It would be comparatively easy to manipulate a mobile so that the charges are not deducted from the card. This would not be noticed by the network, as the signalling channel cannot be used to send an acknowledgement from the card to the network.) User data is transferred over traffic channels as well as over signalling channels. The signalling channel carries, apart from obvious user related signalling information elements such as the called and the calling telephone numbers, user data in form of short messages. This service allows the user to receive and send messages of up to 160 bytes over the radio link without activating a traffic channel.

The illegitimate use of a service is not only of concern with respect to proper billing. It is clearly important that billing is always possible and that only the subscriber, who has caused the charge, is billed for it. The not so obvious illegitimate use is masquerading. Impersonating a subscriber and claiming afterwards that this subscriber (or to be more precise his subscriber card) must have been in a particular place at a particular time is certainly not a very widespread threat but one which could prove very serious indeed in certain circumstances. Due to the cell structure of the network and the constant updating of the location information in the SIM, which is necessary for a proper and timely delivery of mobile terminated calls, the network knows the location of an active subscriber card down to the cell. The area covered by a cell depends on the location of the cell and ranges from a few hundred metres to about a 35 km radius around the base station.

To protect network operators and users against such 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 confidentiality.

The functional description of these security features is given in the Technical Specification GSM 02.09 [7]. The protection of the mobile station itself, that is to say the SIM, against unauthorised usage is part of the functionality of the SIM [8]. A new specification [11] for security management is elaborated by SMG6 which deals with operation and maintenance of GSM networks.

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 network functions and the external specification for the cryptographic algorithms needed to provide the services for the security features listed above are contained in GSM 03.20 [9].

From a user point of view it is not relevant whether the user-related data to be protected is 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

Before a user can make, say a call, or go on standby for receiving calls, his identity has to be known to the network. Rather than sending the International Mobile Subscriber Identity (IMSI), which uniquely identifies the subscriber worldwide, a temporary identity is transmitted 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" and "should be used only when necessary" [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 his 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 TMSI is unknown to the VLR, the VLR will request the IMSI from the MS. It then assigns a TMSI to the subscriber and transmits this identifier (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. From then on this TMSI will be used by the MS instead of the IMSI until a new TMSI has been assigned to the subscriber.

Though the TMSI consists of only 5 digits, the subscriber is uniquely identifiable. For the TMSI is unique within the location area where the MS moves, and the location area identification (LAI) is always used in conjunction with the TMSI. To be able to identify and locate the subscriber, the TMSI is stored together with the IMSI and the LAI in the VLR and also in the SIM. A new TMSI is

to be assigned at each location update procedure. GSM 03.20 specifies six scenarios for the allocation of a new TMSI. If there is no malfunctioning in the system, the IMSI will never again be used for call set up. Even if the SIM has moved to a new VLR in a different network, the new VLR can and must obtain the IMSI from the old VLR by using the old TMSI and LAI which have been sent by the mobile station.

3.2 Authentication

Authentication is the corroboration that an entity is the one claimed or, in other words, the verification of the identity of the SIM. The purpose is "to protect the network against unauthorized use" [9] and thus to ensure correct billing and to prevent masquerading attacks.

3.2.1 The general procedure

Authentication is in the domain of the network operator and every operator may use its own algorithm(s). A proposal for a possible algorithm is available upon appropriate request [9]. However, to achieve interoperability the authentication protocol and its parameters have been specified.

The authentication algorithm (denoted by A3) is implemented in the Authentication Centre (AuC) of the operator and in the SIM. The method employed between the HLR/AuC and the SIM is a challenge-response mechanism using "non-predictable numbers". Figure 1 shows the authentication of the SIM by the network. To establish the common key Ki used in this protocol the network has to know the (temporary) identity of the subscriber. For the authentication key Ki is specific to the subscription.

The network transmits a non-predictable number RAND to the MS as a challenge. To compute the 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 transmitted to the network side. There it is compared with the value computed by the HomePLMN, which has used the same algorithm with the same RAND and the key associated with the identity claimed by the subscriber. The MS is granted access to the network only if the two values are equal. Only in this case it can be assumed that the SIM is in possession of the right subscriber key Ki and that, therefore, its identity is the one claimed.

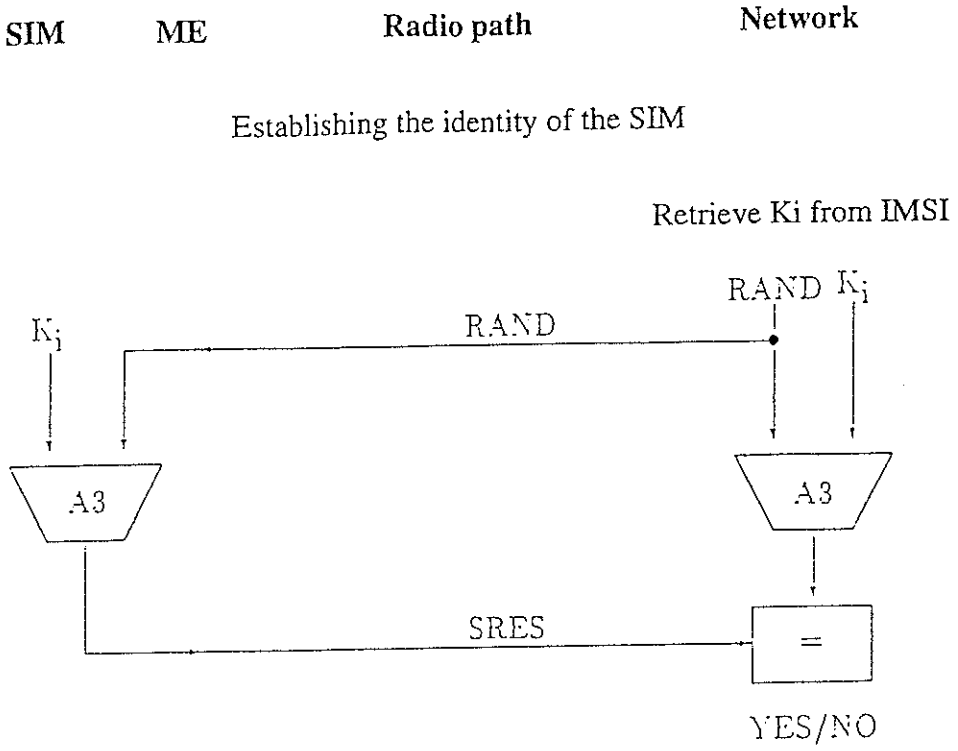


Figure 1: Authentication procedure

The network transmits a non-predictable number RAND to the MS as a challenge. To compute the 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 transmitted to the network side. There it is compared with the value computed by the HomePLMN, which has used the same algorithm with the same RAND and the key associated with the identity claimed by the subscriber. The MS is granted access to the network only if the two values are equal. Only in this case it can be assumed that the SIM is in possession of the right subscriber key Ki and that, therefore, its identity is the one claimed.

3.2.2 Handling of the parameters

The handling of the parameters is of importance with respect to both security and the efficient authentication of a subscriber. The parameters have the following lengths:

Ki: 128 bits; RAND: 128 bits; SRES: 32 bits, Kc: 64 bits,

where Kc is the cipher key used for the ciphering of the air interface.

The verification of SRES is done in the VLR where the MS is currently registered, while the computation is carried out in the HLR/AuC of the home network of the subscriber. The VLR obtains pairs consisting of RAND and the corresponding SRES from the HLR/AuC (of the home network) upon request for security related information using the IMSI of the subscriber who is to be authenticated. 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 3.3). The challenge RAND and the derived values SRES and Kc are called an authentication triplet or a set of security related information.

As the VLR and the HLR/AuC may be thousands of kilometers apart, the VLR may store five authentication triplets. Each authentication triplet is used only once and must be discarded after being used. Both restrictions will 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.

When the user has moved to a different VLR, this new VLR will normally request the IMSI from the previous VLR by sending the old TMSI and LAI (see 3.1). In either phase 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, of course, only send a request for triplets to the HLR/AuC after it has learned of the real identity of the subscriber which is through this request to the old VLR.

3.2.3 Option

In phase 1 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 used for authentication and enciphering. It is however recommended to restrict this procedure to the HomePLMN [9, clause 3.3.2]. 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 not available. 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 over insecure channels 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 network operator would have to disclose both algorithms and keys to the other operator or to supply him with black boxes and sending the keys enciphered.

Because of the sensitive nature of Ki this option has been deleted from phase 2.

3.3 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 [3]. Since March 1993 a second cipher called A5/2 is available. Up to 8 ciphers, including a mode in which no enciphering takes place, are catered for in phase 2.

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]. Security aspects of speech communication in general are extensively discussed in [2].

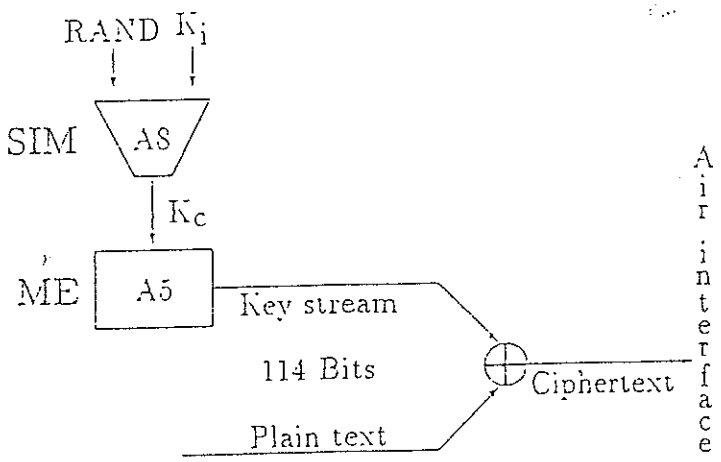


Figure 2: Cipher key generation and enciphering

Figure 2 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.

Binding the generation of Kc to the authentication process has several advantages. No additional input data is 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 undecipherable garbled message.

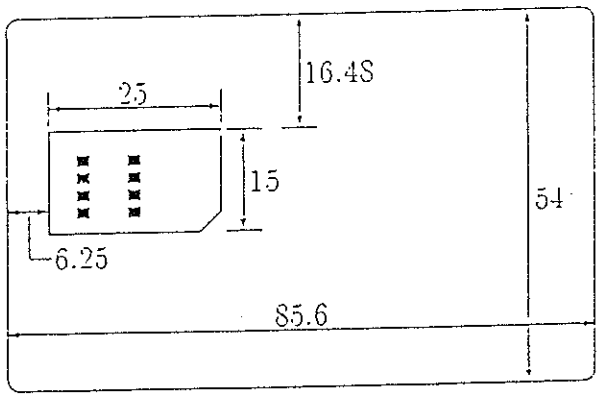
It is worth noting that the authentication algorithm A3 as well as the cipher key generator A8 compress the non-constant input data RAND from 128 bits to 32 and 64 bits, respectively. Even if A3 and A8 are one and the same algorithm, a compression takes place. This implies that the

challenge RAND can not be derived just from the output Kc, SRES of the SIM. This means 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 it 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 [10].

To achieve its main task of authenticating the subscriber to the network side, 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 intended to be used mainly with handheld mobiles which are 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 25mm by 15mm (see figure 3). For the exact dimensions and the location of the contacts the reader is referred to [10] and [15, part 2]. The electrical and mechanical interfaces are, with the obvious exception of the Plug-in SIM, in line with the relevant International Standards for IC cards [15]. In some instances, however, more stringent conditions were agreed upon to cater for the needs of the environment the SIMs are used in. These include, for instance, the temperature range the card has to satisfy and the power consumption of the microcomputer.



	typical	maximum
ROM	6 kByte	16 kByte
RAM	128 Byte	256 Byte
EEPROM	3 kByte	8 kByte

Figure 3: SIM formats and memory provided

The microcomputer consists of a CPU and three types of memory. The masked programmed ROM usually contains the operating system of the card and the security algorithms A3 and A8. The RAM 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, and network and subscriber related information, such as TMSI, LAI, abbreviated dialling numbers and short messages which are updated frequently

or have to be changeable by the subscriber, are stored in non-volatile erasable memory (EEPROM, Electrically Erasable 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 [19]. Basic security aspects of microcomputers and their manufacture can be found in [17].

The operating system of the card controls the access of the outside world, which may be a mobile equipment 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 a PIN2 (only used in phase 2). 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. One of the remaining six contacts is needed for cards requiring an external Programming Voltage. All SIMs derive this voltage from the Supply Voltage (Vcc) by means of an internal charge pump. The remaining contacts are used for the Reset of the chip, the Clock to drive the chip, Ground and only one contact for Input and Output. The latter 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 in particular due to the half duplex transmission protocol and other overhead.

4.1 User access to the SIM

Similar to some banking cards, user access to the SIM is controlled by a Personal Identification Number (PIN). A major difference is, however, that the PIN can be freely chosen by the user within the range of 4 to 8 digits and that the user may change the PIN as often as he/she feels necessary. This is possible since the reference PIN is stored in the EEPROM of the chip and the comparison of the value presented by the user with the reference PIN is done in the CPU 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 mobile equipment 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 may "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. As the PUK cannot be changed by the user it could also be stored in the home network and given, if the necessity arises, to the user

under mutually agreed security conditions such as the delivery of a special password by the user. It should be recalled that the access of a SIM to a mobile service can easily be suspended by blacklisting the subscription in the HLR/AuC. After 10 consecutive wrong PUK entries the SIM is permanently blocked.

Another novel feature is the disabling of 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 access control to the SIM and thus the network (if the card is not blacklisted) is based merely on the possession of the card.

With the introduction of new services in phase 2 the PIN will be the means to control user access to the actual GSM operation instead of the GSM application, while certain optional data fields may be protected by a second PIN and PUK. For instance, Advice of Charge is intended not only as an advice to the customer about the number of units spent but may also be used for billing purposes. 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 resetting the contents of this and other data fields independently of the normal PIN, PIN2 and the accompanying PUK2 have been introduced for phase 2.

5 Key management

In this section we consider some of the aspects concerning the authentication centre (AuC) and the handling of subscriber authentication keys. The keys Ki have to be very well protected to avoid charging the wrong subscriber and to counteract other threats posed by impostors.

5.1 The Authentication Centre

GSM 03.20 states that the individual subscriber authentication key Ki is allocated, together with the IMSI, at subscription time and that Ki is stored in an Authentication Centre (AuC). The AuC also contains the authentication algorithm(s) A3 and the cipher key generating algorithm(s) A8. The AuC is thus at the heart of the security of any network and the specific security and administrative requirements are not standardised but left to each operator.

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 is of importance for both the secure and the smooth running of the network.

5.2 Key generation

There are two standard methods for generating keys. This may be done by using a random number generator or by means of an algorithm which is used to derive the key from user related data under the control of a master key. Which of the two methods or variation thereof the designer of the security system chooses depends on the local circumstances. Both methods have their advantages and disadvantages which we will briefly discuss in the light of the boundary conditions given in the Technical Specification 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. A potential problem is however that, if the same IMSI has been issued by mistake to two subscribers, both subscribers would also have the same authentication key.

The main problem is of course to keep the very secret key MK secret. Anybody coming into possession of this key could, if he also knows 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 selection of the algorithm, which is used for deriving Ki, 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] 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 one could first reduce the length of the IMSI to 10 digits by removing the 5 digits which are identical for all IMSIs in the HPLM 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 as follows, where "||" denotes the concatenation of the two terms:

(i) $Ki = DEA_{MKleft}(UD) \,||\, DEA_{MKright}(UD)$, and

(ii) $Ki = DEA_{MK}(UD) \,||\, DEA_{MK}(DEA_{MK}(UD))$.

In the first case the master key consists of two parts of 64 bits each, while it has only 64 bits in the second case.

A variation of this method would be to use as the input data UD 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 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 cannot be achieved by an algorithm using IMSIs as an input. The main difference is, however, that there is no natural link between the subscription and the authentication key. This requires all keys to be stored against some subscription specific data in a data bank of the AuC and 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 dump 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, we can also see that the times required for providing a key for the authentication request are about the same (assuming that access to the data bank causes no significant overhead). In both instances two DEA encipherments or decipherments have to be executed.

5.3 Prepersonalisation

Prepersonalisation 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 prepersonalised 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. This certainly facilitates the handling of SIMs and the corresponding PIN- and PUK-mailers.

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 prepersonalisation. Deriving Ki from subscription data, which is known prior to the prepersonalisation of the SIM, allows the computation of Ki independently in the HLR/AuC and at prepersonalisation 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 prepersonalisation. 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 is meant to give the reader a quick look-up table containing the abbreviations used in this paper together with a brief explanation. For a more elaborate description and the precise definition of all the terms used the reader is referred to [4] and [5].

A3:	Algorithm 3, authentication algorithm used for authenticating the subscriber
A5:	Algorithm 5, cipher algorithm; used for enciphering/deciphering data
A8:	Algorithm 8, cipher key generator; used to generate Kc
AuC:	Authentication Centre; used to store the keys Ki, A3 and A8 are implemented in the AuC
DECT:	Digital European Cordless Telephone
ETSI:	European Telecommunications Standards Institute
HLR:	Home Location Register; a register in the HPLMN of the subscriber where (all) information related to the location and the subscription are stored
HPLMN:	or Home PLMN; the network with which a subscriber is registered
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:	the cipher key; used in A5 to generate the key stream
Ki:	the individual subscriber authentication key; used in A3 and A8
LAI:	Location Area Identification; 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
PIN:	Personal Identification Number; used by the SIM for the verification of the identity of the user
PLMN:	Public Land 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:	a non-predictable 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 by the network side to verify the identity of the SIM in the authentication process

TMSI: Temporary Mobile Subscriber Identity; the temporary identity 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] H.J. Beker and F.C. Piper, *Secure Speech Communications*, Academic Press, London, 1985.

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

[4] ETSI, GSM 01.02 (ETR), *General Description of a GSM PLMN.*

[5] ETSI, GSM 01.04 (ETR), *Abbreviations and acronyms.*

[6] ETSI, GSM 01.05 (ETR), Abbreviations and acronyms.

[7] ETSI, TS GSM 02.09, *Security Aspects.*

[8] ETSI, TS GSM 02.17, *Subscriber Identity Modules, Functional Characteristics.*

[9] ETSI, TS GSM 03.20, *Security Related Network Functions.*

[10] ETSI, TS GSM 11.11, *Specifications of the SIM-ME Interface.*

[11] ETSI, GSM 12.03, *Security Management.*

[12] ETSI, ETS 300 175-7, *Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common interface Part 7: Security features*, October 1992.

[13] ETSI, DRAFT prETS 300 331, *Radio Equipment and Systems (RES); Digital European Cordless Telecommunications (DECT) Common interface DECT Authentication Module*, September 1993.

[14] F. Hillebrand (ed.), *GSM, Digital Cellular Mobile Communications Seminar*, Budapest, 1990.

[15] 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.*

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

[17] M. Paterson, *Secure Single Chip Microcomputer Manufacture*, in: *Smart Card 2000* (ed. D. Chaum), North Holland, Amsterdam, 1991, 29-37.

[18] G. Simmons, *Contemporary Cryptology, The Science of Information Integrity*, IEEE Press, Piscataway, NJ, 1992.

[19] K. Vedder, *Smart Cards*, Proceedings CompEuro 92, IEEE Computer Society Press, Los Alamitos, 1992, 630-635.