Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 81 (2003)

Heft: 10

Artikel: Secure SIM lifecycle management

Autor: Aebi, Paul / Oswald, Rudolf

DOI: https://doi.org/10.5169/seals-876692

Secure SIM Lifecycle Management

GSM, the Global System for Mobile Communication, is based on an initiative back in 1982 by the former European Post and Telecommunication Authorities (CEPT). Its success as a worldwide system is also the beginning of the lead of the European industry in wireless communication. GSM is in use by more than one in ten of the world's population and growth continues to soar with the number of subscribers worldwide expected to surpass one billion by the end of 2003.

PAUL AEBI AND RUDOLF OSWALD

A mobile station in any cellular network must be personalised, i. e. associated with a given subscription. This is needed since the identity of the subscriber is not in one-to-one correspondence with the physical medium used for access (unlike in wired networks). The approach taken in the precursor C network was to store the required information in the mobile equipment's permanent memory. The resulting fraudulent activities associated with this approach created a strong need for a more secure solution. Another driver for a Smart Card approach was mobility. In those days, when a mobile station had the size of a suitcase, it was the intention for travellers to carry just the SIM cards and use them in different mobile stations, for example equipment available within a taxi.

Secure SIM Life cycle management is a process that has three main aspects:

- The cryptological methods used: The algorithms used, and the associated attacks have been covered in many publications. We therefore do not examine this area any further.
- The card access mechanism, mainly PIN management: In announcements of successful broken SIM cards, it is usually assumed that the attacker already has the PIN and has full access to the card's functionality. In practice this is not the case as the PIN mechanism itself has not been broken and is a very important part of SIM security – provided the user has enabled the PIN.
- The processes within and between the manufacturers and the card issuer organisations (operators): This article discusses secure SIM management from a network operator's perspective.

GSM and the SIM Card

GSM is a cellular network in which each cell is served by a Base Station (BS) which provides its area with radio coverage. A BS is connected via a Base Station Controller (BSC) to the core network where the Mobile Switching Centre (MSC) is the controlling element. The MSC is responsible for the routing of calls. A central element is the Home Location Register (HLR) with its satellite, the Visitor Location Register (VLR). The HLR contains all the subscribers' relevant permanent and temporary data such as the International Mobile Subscriber Identity (IMSI), the Mobile Station International ISDN Number (MSISDN), the available services, and also the actual location of the subscriber. While the MSISDN is the telephone number of a subscriber, it is the IMSI that is used for internal network signalling. Once a subscriber has switched on his Mobile Equipment (ME) and entered the PIN correctly, the ME sets up communication with the VLR / HLR and requests network authentication; this is enabled by the SIM (Subscriber Identity Module) and the Authentication Centre (AuC). After successful authentication, instead of using the IMSI a temporary IMSI (TMSI) will be used on the radio link for security reasons. The system is now ready to set up and to receive calls.

The SIM was initially defined only as a security module to authenticate the user to the network provider. Today SIM is a secure platform for operator defined services allowing operator differentiation by exploiting the power of the microcomputer in the SIM. SIM features can be divided into four functional areas:

- Security: This includes keys, algorithms and access management (PIN/PUK).
- Network Parameters: These contain personalised files such as the list of preferred networks. They also contain files that are updated regularly during a network session (e. g. location information and the most recently used network).
- User Data: This includes the phone book and the SMS store.
- Application: This might be a browser that gives WAP access where the handset has no WAP functionality.

The SIM can be defined in two possible mechanical formats: ID1 (Credit card size) and ID-000, plug-in (Fig. 1).

Overview of the SIM Card Lifecycle

Ordering

SIM Profile definition

Before a card can be ordered by an operator, the profile has to be defined. In the terminology of the SIM, it contains not only the electrical profile, but also the graphical profile with the definition of all general and card individual printings.

Input File

The input file contains the card's individual data (as a minimum it will contain the card number [ICCID] and the IMSI). In many cases, the MSISDN is not known at this stage of the process and can therefore not be personalised. Many operators use transport keys to encrypt the secret data in the output file. In this case, the input file also contains an index that defines the transport key for the output. The input file usually contains no secret data and can be transported without much security being applied.

Production and Personalisation

During production and personalisation, the manufacturer creates all secret data and writes it into the card's memory.

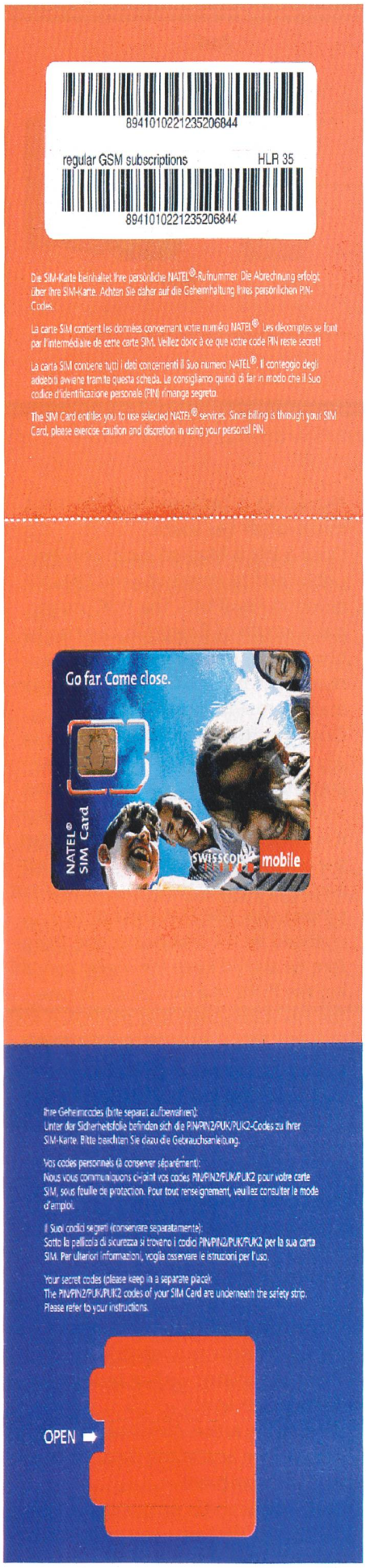

Fig. 1. Card holder with dual format SIM (Center) and PIN/PUK (below the sticker).

Usually the PIN is a randomly generated number. However, some operators prefer a simple PIN that is the same for every card (e. g. 0000) and ask the customer to change it immediately upon receipt. This is a dubious technique as many users do not perform the change.
The personalisation of the card holder, the PIN/PUK letter and the packaging are part of this process. Many operators have a combined card holder and PIN letter. The PIN is then printed on the card holder and covered with a sticker which has security features that are always visible once the sticker has been removed. It is not a security risk to have the card and PIN together because the cards are not active at this stage; this also saves logistical costs. The personalisation of the package is the card number printed on the package, often as a barcode (Fig. 1).

Logistics

The manufacturer supplies the cards and an output file to the operator. Throughout the logistical process from the supplier to the operator, and within the operator's organisation, the cards remain inactive and therefore there is only a low security risk during this process.
An exception to this is the prepaid card. In many countries the user expects to make calls immediately after purchasing the card without having to register, so there have to be active cards available in retail outlets. The exact date of activation of those cards in the logistic process is a well-kept secret of each operator. The output file contains the individual data for each card. This includes the PUK and Ki (the Key for network access). It is obvious that this data must be kept secret and therefore secure transport is essential.

Activation Process

The output file data has to be provided to the operators' IT systems in a secure manner. Even after this process the card is still not active. Many operators have a specific customer activation tool in their outlet that has an on-line connection to their customer management system, and which allows card activation once the subscriber has obtained the card.

Usage

During the usage phase, an essential part of the security is in the hands of the customers. An activated PIN is not only the best protection against every attack on the card. The PIN also protects the users' data, the bulk of which is contained in the phonebook and the SMS store.
At all times, the operator has access to the card via OTA (Over The Air) which is a specific secure SMS protocol. This allows the download of data and applications, or in other words, a repersonalisation of the SIM at any time.

End of Life

The SIM has no validity period as for example a bank card. There are still cards from the first generation of the early '90s in use. Most operators worry about SIM swap because of logistical obstacles and because of low customer acceptance. The usual end of life of a SIM is therefore the case of lost or stolen cards and customer churn.

The SIM Profile

The SIM Profile is the customisation of a vendor's product. For a SIM it contains:

- The electrical profile: This describes how free non-volatile memory (EEPROM) is organised. It is made up of customer applications for example JAVA applets and the size of lists whose contents can be modified by the user. The most relevant of these are the number of SMSs, the size of the phonebook, the size of the list of last dialled numbers, and the number of preferred networks. Within the profile there is also the predefined content of the lists.
- Parameters that are common to all cards: A selection of the most important SIM parameters are:
  - *SIM Service Table.* Informs the handset which standardised services are supported by the card.
  - *Service Provider Name.* A text string to be displayed on the handset, usually in the first line.
  - *Preferred Language.* To tell the handset which languages the user prefers. This can be a list with more than one language, for example 4 in Switzerland.
  - *PLMN Selector (Preferred Network).* A list of networks which are to favour when there is more than one network available.

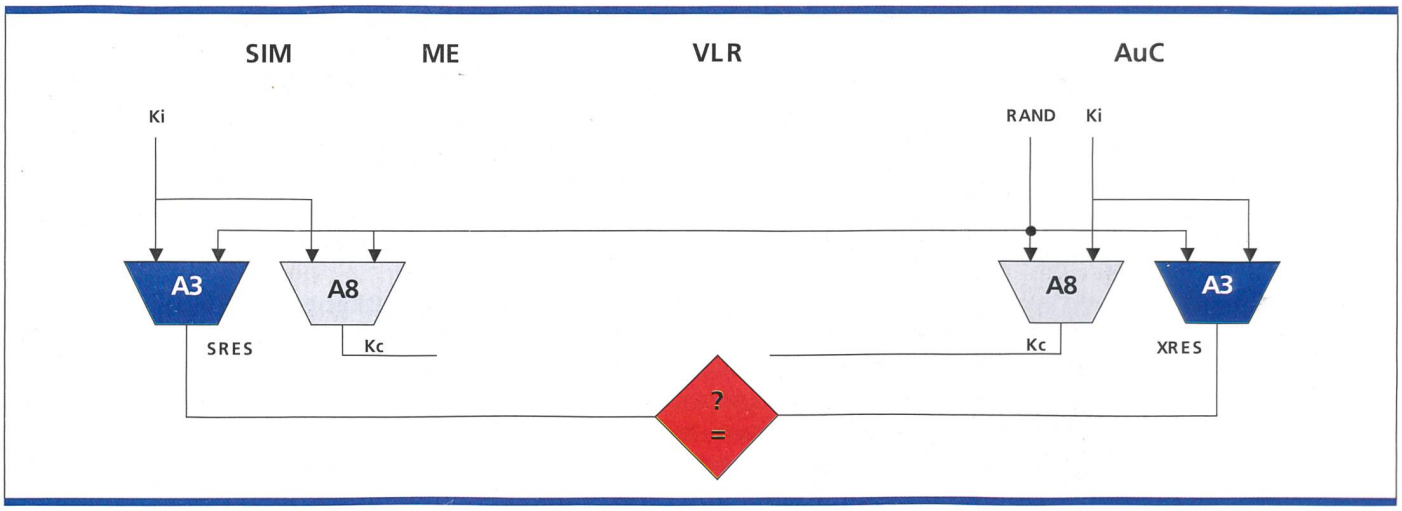

Fig. 2. Authentication and encryption key generation.

- *Service Dialling Number.* Prestored telephone numbers, for example helpdesk
- *Last Dialled Number.* The size of the list with the last dialled numbers.
- *SMS-Centre Number.* Used for sending SMS.
- *Fixed Dialling Numbers.* A handset with a SIM, and with fixed dialling numbers, can only set up calls to these predefined numbers. All other numbers are blocked. As an example, employees can only call their office, or children can only call their parents.

– The graphical profile: This is the artwork for the card, and also the definition of card-specific printing, for example the ICCID on the plug-in.

Access Conditions

General

In the SIM Profile section we have seen that different types of information are stored in the SIM's files. The confidentiality requirements will not be the same for all information types. Furthermore, not all information has the same owner. This is allowed for by having specific access conditions (AC) for each file. In the following we explain the concept of access conditions in more detail.

PIN Concept – Authentication

To grant access to information stored on the SIM the user needs to authenticate himself to the card. The authentication is usually done by presenting a number to the SIM. Different numbers (not values) are defined for different purposes. The most commonly used are:

– PIN1 [Personal Identification Number 1]: This number is known by the user of the card. In order to have access to the network it is necessary to present it to the SIM. Note that this particular PIN can be disabled. This little „convenience" can have a big price for the user if he loses the SIM and the finder is dishonest. The length of a PIN is 4...8 digits, for convenience 4 digits are usually used.

– PIN2 [Personal Identification Number 2]: This number is only known by the owner of the card. The purpose of it is to grant write access to files which can only be read after presenting PIN1. The following illustrates its use:

- After presenting PIN2, the owner of the SIM (e. g. parents) can store a list of phone numbers in a specific SIM file. Then the SIM is switched to fixed dialling number (FDN) mode. Subsequently, the SIM user (e. g. child) can only make calls to these stored numbers.

– ADM [Administrative key]: This number is known by the card issuer (normally the operator). It is not distributed to the customer but is securely stored by the operator. It is used in the rare cases when the operator needs to update the contents of the SIM. The length of ADM is usually 8 characters. In the OTA section we will see another method of updating SIM information.

In order to prevent brute force attacks on the different PINs, a PIN blocking mechanism is used. If a wrong PIN is presented a specified number of times, the corresponding PIN is blocked. For PIN1/2 this number is usually set to 3, and for ADM it is set to 10. The reason for allowing a larger number of incorrect ADMs is because the ADM has a much larger key space.

Once a PIN is blocked it can only be unblocked by presenting the PIN Unblocking Key (PUK). The PUK usually has a length of 8 digits. It can also be blocked if it is incorrectly entered a number of times (10 attempts are normally permitted).

Once the PUK is blocked there is usually no way to unblock it; the associated PIN and the whole card become useless. In order to avoid this situation, it is advisable that the owner changes the default PINs received from the operator to an easy to memorise (but not simple) one. The PUK can not be changed by the SIM owner and therefore he should keep the mailer containing the PUKs in a safe place. In case the PIN is forgotten and the PUK is lost one should not try to guess the PUK but contact the operator. After proving that a person is indeed the registered SIM owner, most operators disclose the PUK values.

File Access Condition

Each file has its own access condition which defines who has permission to perform specific actions on this file. Among others, the following actions can be performed on files: read, update (write), invalidate and rehabilitate. Each action is associated with at least one access condition level.

The following access condition levels exist:

– Always: The action can be performed without restrictions.

– PIN1: The action is only possible after the correct PIN1 was presented to the SIM. If PIN1 is deactivated the action

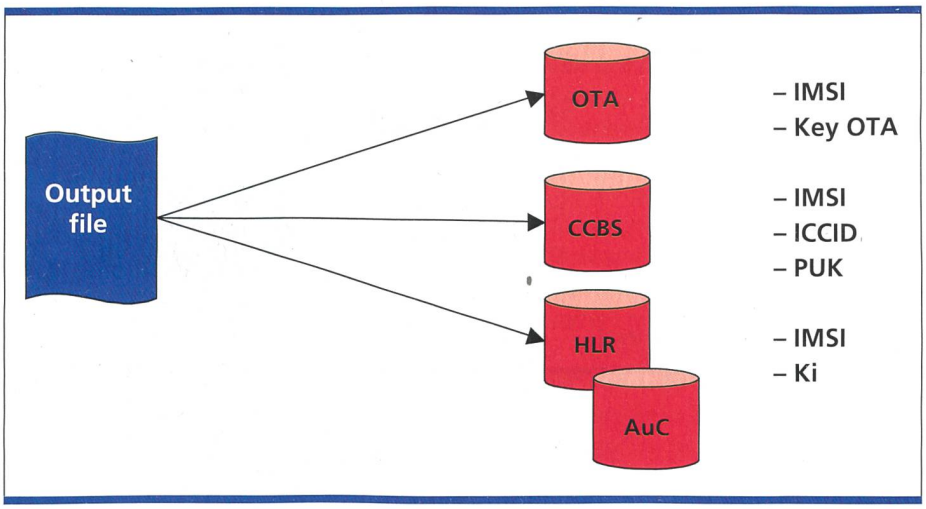

Fig. 3. Provisioning of IT systems with SIM Data.

can be performed without any restriction.
- PIN2: The action is only possible after the correct PIN2 was presented to the SIM.
- ADM: The action is only possible after the correct ADM was presented to the SIM.
- Never: The action can not be performed over the SIM-Handset interface. However, the SIM operating system has permission to perform this action.

The access condition levels are not hierarchical. This means that after presentation of ADM one does not necessarily have the access rights which are granted to the PIN.

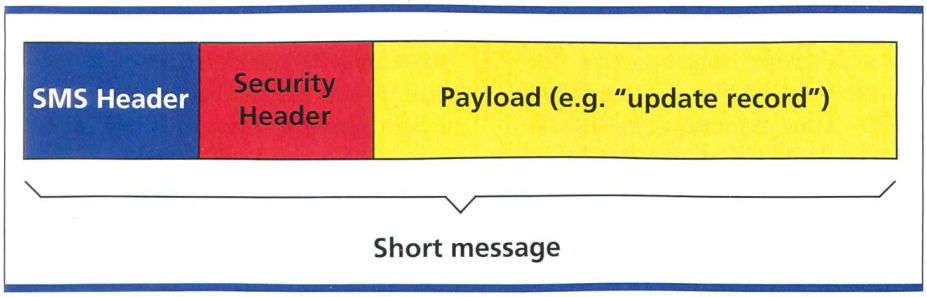

Fig. 4. Short message with security header.

The following example shows a typical personalisation of access rights for the file „SMS" which contains the short messages on the SIM:
- Read: PIN1
- Update: PIN1, ADM
- Invalidate: ADM
- Rehabilitate: ADM

After presenting PIN1, one can read and update the SMS file while after presenting the ADM key one can update, invalidate and rehabilitate it.

Network Access

Security Features

A mobile network is potentially less secure than a fixed one because everybody can send and receive radio waves without intercepting operators equipment. In GSM this thread is addressed with different countermeasures which are all related to the SIM functionality:
- Authentication of the user towards the network[1]
- Encryption of the radio path
- Protection of subscriber's identity

Authentication requires three networks elements: the Authentication Centre (AuC), the Visitor Location Register (VLR) and the SIM. The AuC contains for each subscriber its identity, the so-called IMSI (International Mobile Subscriber Identity) and an individual secret key (Ki). Additionally the AuC knows the authentication algorithm A3 and the cipher key generation algorithm A8. This information is also stored in the SIM.

Before a handset can access a GSM network it sends the IMSI stored on the SIM to the VLR. The VLR requests from the AuC an Authentication Vector which consist of a random number (RAND) an expected response (XRES) and an encryption key (Kc). XRES is calculated within the AuC with RAND and Ki as input to A3, whereas Kc is calculated with the same input parameters but A8 as the algorithm. The three parameters (=triplets) RAND, XRES and Kc are then sent to the VLR. The VLR sends RAND to the handset and requests it to authenticate itself. On the SIM, SRES and Kc are calculated and SRES is sent back to the VLR. If XRES = SRES the VLR grants access to this handset and uses Kc to encrypt/decrypt the radio link. In figure 2 this simplified procedure is illustrated.

The interesting and important features are that no secrets are transmitted over the network and that the algorithms A3 and A8 can be specific to each operator. This is important because GSM is designed to allow national and international roaming.

The fact that the Ki is specific to each SIM is the reason why it is not possible to breach the security of the GSM system by merely obtaining the Ki from one SIM. The illegal action of trying to obtain a SIM's Ki and use this information to produce SIM copies is often referred to as „SIM cloning". However, this is a much abused term for several reasons:
- SIM cloning is not an easy thing if the SIM manufacturer and the operator are vigilant; this means that they implement state-of-the-art algorithms and countermeasures against attacks and review them regularly.
- SIM cloning is only possible if one has physical access to the SIM.
- Most SIM cloning approaches require the PIN to work at least theoretically.

This leads to the conclusion that the owner of the SIM is the one most likely to clone his SIM. A situation not frightening at all for the owner and for the vigilant operator.

Card Activation

Card activation is a process in two steps. In the preactivation phase the data of the output file will be provided to all related IT systems in a batch processes called „provisioning". In the activation phase the card becomes active for net-

[1] If PIN1 is deactivated it is only an authentication of the SIM towards the network

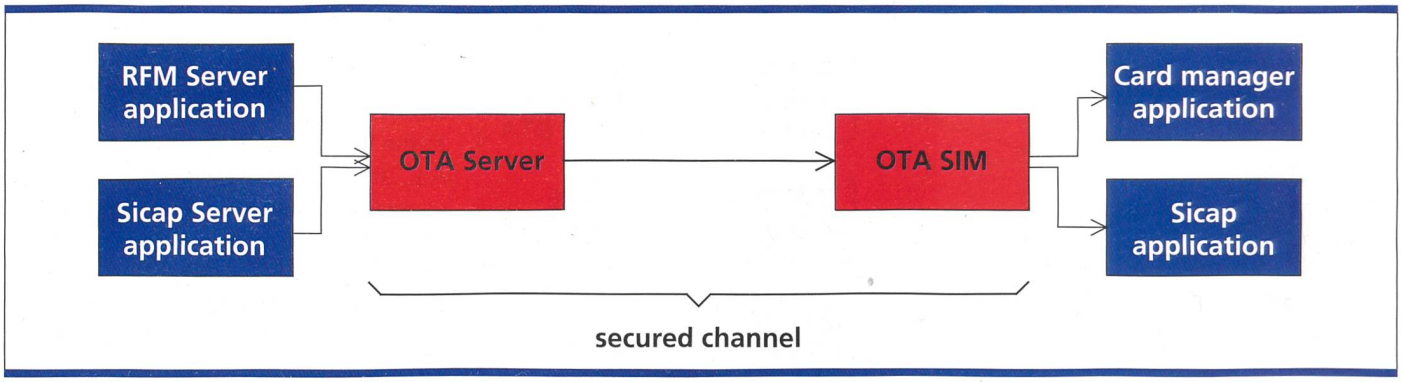

Fig. 5. OTA system with two application using it.

work access in an individual card-by-card process. The provisioning includes the following systems (fig. 3):

- CCBS (Customer Care and Billing System). This is the administrative system for customer management. It also usually contains the resource management; this means that there is a database of all available SIMs. Many operators store the PUK just in case customers (who have not kept their PUK) request their PUK.
- HLR. This is the heart of the network. It contains all the network numbering and settings of each subscriber. Each HLR is only capable of storing a range of IMSIs (big operators have more than 100 HLRs). This means that the allocation of SIM batches to HLRs has to be decided during the ordering phase. Preactivation means that just the IMSIs will be entered into the database. The MSISDN will usually be allocated during the activation phase. An exception to this is prepaid where the MSISDNs are already allocated during the ordering phase.
- AuC (Authentication Centre). The AuC is the counterpart to the SIM. It contains the same IMSI and Ki for the authentication. Therefore data at the AuC must be provided and stored using security mechanisms. The AuC is usually a part of the HLR equipment.
- OTA server (Over The Air). OTA provides a mechanism for communicating with the SIM via SMS (see section „Over the Air Management"). OTA needs a specific Key, which is stored on the SIM and in the OTA server. The provisioning of the data to the OTA is similar to AuC provisioning.

The individual card activation for standard, post paid customers is a part of the customer administration process. The network operator or service provider has a front end application for the shops. During the compilation of a new customer's data in the shop, the card number of a currently inactive SIM must be added by reading the barcode on the package. The system now has a range of free MSISDNs, from which the customer can select one. After the completion of this process, the CCBS provides the HLR (via a mediation device) with IMSI, MSISDN and services which are accessible for this customer. Now the SIM is active.

Over the Air Management

General

In section „Access Conditions" we examined the PIN mechanism. For this, we assumed that we have physical access to the card in order to get the required access condition level to be allowed to perform an action on a SIM file.
In practice it would be a big advantage to gain access to files without having physical possession of the card. This is especially the case for operators because they have stored a lot of information on the SIM which may change over time. The change of the SIM file «Service Provider Name» is one example where such a mechanism would be a great help – since today rebranding is not an unlikely event. With the Over The Air (OTA) mechanism this flexibility is achieved in a secure way.

OTA Functionality

Remote SIM management is usually built on the Short Message Service (SMS). The short messages (SM) act as bearer of the information, where the information itself is a command like „Update File ‚Service Provider Name' with ‚Swisscom Mobile'". Since the SMS has no built-in security it is necessary to add this to the standard SM with a so-called security header. A security header is illustrated in figure 4.
The different security threats are addressed with several countermeasures. The security features and how they are achieved in the OTA system are summarised in the following:

- Confidentiality: The payload is encrypted. The algorithm used and the key index is indicated in the security header. A commonly used algorithm is 3DES.
- Authenticity and integrity: A cryptographic checksum is calculated over the whole message and transmitted in the security header.
- Freshness: With each message a counter is transmitted within the security header. The counter is incremented for each new message.

Using the above security features a secure channel can be established between the operator and the SIM. The channel can be used by different applications such as remote file management, remote application management and secure messaging. Depending on the application the security features may vary; for example, confidentiality is not required for remote file management of the „Service Provider Name" field.
Figure 5 gives an overview of an OTA system with two applications.
The following chapters describe possible applications based on the secure channel provided by an OTA system.

Remote File Management

As already seen in the previous paragraphs, Remote File Management is an application that can be built on top of the OTA system. In order to keep track of the changes made to a SIM it is necessary to store all changes in a database. This database is fed initially with the profile information of each SIM and then updated when a SIM file is updated remotely. As an example the file „Service Provider Name" could have contained initially the value „Swiss Telecom" and

then be changed to the value „Swisscom Mobile".

Sicap Prepaid

Sicap is an abbreviation for SIM Card Application Platform[2]. It is used to build a mobile prepaid system which relies on GSM features and an application running on the SIM. It requires a secure channel as discussed above. A simplified description of Sicap functionality follows.
One building block is the GSM feature Advice of Charge (AoC). The aim of AoC is to inform the user about the cost of a call. The total cost of each call is added to a file on the SIM with the name Accumulated Call Meter (ACM). As long as the value of ACM is lower than the content of a second file, ACMmax, the phone functions normally. As soon as ACM ≥ ACMmax no more calls can be made with this SIM. This is where the Sicap SIM Application comes into play; to „reactivate" this SIM a new value of ACM is written to the SIM by means of a Sicap OTA message. This specific OTA message is referred to as a Reload message.
It is obvious that security is required for Reload:

- only the operator is allowed to perform such a Reload -> authentication required
- the message must not be changed in transit -> integrity required
- resending the same message must not lead to additional Reloads -> freshness required

Encryption is optional for this case. [3]

[2] Sicap is also the name of the company supplying such a prepaid system – see www.sicap.com

Paul Aebi *graduated in 1976 as an electrical engineer. After obtaining some indusry experience in the development of telephone switching equipment, he joined the former Swiss PTT with responsibility for long distance switching systems. Throughout this period he held a number of different positions in the headquarters of the now called Swiss Telecom. In particular he was responsible for projects in Network Management and Switched Broadband Systems. After joining Swisscom Mobile in 1994 he introduced one of the world's first Prepaid Solutions for Mobile Telephony and was the head of International Product Management. Today he is responsible for SIM aspects and related systems. From 1997 to 2002 he chaired the Smart Card Group of the GSM Association.*

Rudolf Oswald *received his engineering diploma in 1991. After spending several years in the development and engineering of electronic equipment, he joined Unisource (now Swisscom) where he was responsible for projects in the IP environment. He now works for Swisscom Mobile as a consultant in SIM Technology and Security. He is an active member of 3GPP and GSM Association and the Vice-Chairman of the Smart Card Forum Switzerland.*

Erstveröffentlichung des Artikels in «Elsevier Report».

Zusammenfassung

Das Schlüsselelement für die Sicherheit im GSM-System ist die SIM Karte. Sie dient zur Identifizierung des Benutzers gegenüber dem Netz und zur Generierung von Schlüsseln, die für die Sicherung der Luftschnittstelle benötigt werden. Damit diese Aufgaben wahrgenommen werden können, werden PINs und kryptografische Verfahren eingesetzt. Um die Systemsicherheit zu gewährleisten, reicht es allerdings nicht, die SIM als ein Bauelement zu betrachten. Es ist nötig, ihren gesamten Lebenszyklus zu berücksichtigen. Dieser Lebenszyklus beginnt bei der Herstellung der Karte, beinhaltet aber auch die Logistik und Distribution der Karte.
Ein interessantes Feature der SIM ist die Möglichkeit, Einstellungen über die Luftschnittstelle zu aktualisieren. Eine Anwendung, die auf diese Möglichkeit zurückgreift, ist das von der Firma Sicap entwickelte «prepaid-System».

Wissenschaftler finden neuen Baustein für optische Chips

Professor Dr. Ted Sargent von der Universität Toronto hat ein optisches Polymer entwickelt, das mit winzigen Quantendots (mit Kristallen von etwa 5 nm Grösse) «bestückt» ist. Diese Quantendots können Elektronen in Photonen wandeln und eröffnen damit eine neue Möglichkeit für optische Datenverarbeitung auf Chips. Die Nanokristalle sind aus Bleisulfid, das sich bei normalem Luftdruck und Temperaturen unter 150 °C verarbeiten lässt. Die Kristalle werden mit einem halbleitenden Polymer beschichtet. Da die Oberfläche dieser Nanokristalle instabil ist, legen die Forscher eine spezielle Molekülschicht darüber, sodass schliesslich ein dünner hybrider Polymerfilm entsteht. Bisher wurden Lichtwellen im Bereich zwischen 1,3 µm und 1,6 µm generiert. Zusammen mit schnellen Transistoren und Detektoren, Lichtmodulatoren und optischen Wellenleitern rückt damit der Aufbau von optischen Chips in den Bereich des Möglichen.

Info:
http://www.newsandevents.utoronto.ca/bin4/030428a.asp
Für Wissenschaftler bei
Prof. Dr. Ted Sargent
Tel. +1-416-946 5051
E-Mail: ted.sargent@utoronto.ca