13.2 THE GSM SYSTEM

The smart card used in GSM mobile telephones, which is called the 'subscriber identity module' (SIM), was and still is the pioneer in terms of functionality and memory capacity. This is in part due to the fact that smart cards used in mobile telephones, whose manufacturing costs are several hundred euros, are significantly less price sensitive than other types of smart cards, such as those used for electronic payments or medical applications. Another decisive factor with regard to smart card technology is the generally high rate of evolution of the entire telecommunications sector. The pioneering position with regard to technology and standardization that is presently held by the SIM, in comparison with all other smart card applications, is the reason why this topic is described here in such great detail.

GSM, which was commercially inaugurated in 1992, became the international standard for mobile telecommunications systems within only a few years. This includes transmitting not only voice but also data, which are presently still primarily transmitted in the form of 'short messages' using SMS. In mid-2001, there were a total of 400 mobile telecommunications networks in 171 countries based on the GSM standard, with more than 565 million subscribers. More than 20 billion short messages are transmitted every month.[4] Mobile telecommunications networks based on the GSM standard often have country-specific designations. In Germany, for instance, the four operational GSM networks are called the D-Netz (900-MHz and 1800-MHz GSM variants) and the E-Netz (1800-MHz variant), and in Austria the GSM network is in part also referred to as the A-Netz.

Specification of the GSM system started in 1982 under the auspices of the *Conférence Européenne des Postes et Télécommunications* (CEPT). The objective was to generate a specification for a transnational, interoperable mobile telecommunications network. In the course of time, these efforts led to the conclusion that it was possible to draft specifications for a transnational, interoperable and ISDN-compatible digital cellular mobile telecommunication system operating in the 900-MHz band. The Groupe Spécial Mobile was founded for this purpose, which gave rise to the original abbreviation 'GSM'. In 1986, the GSM Permanent Nucleus was established, with headquarters in Paris, to coordinate the generation of the specification. It was later also responsible for specifying a wide variety of tests for system components. From a technical perspective, it is interesting to note that a number of the technologies that were chosen for GSM at that time were fully new and untested in practice. For instance, the air interface using a combination of time-division multiple access with frequency-division multiple access and digital data transmission was totally unexplored territory for large-scale mobile telecommunication applications. These decisions led to many technical problems, particularly in the system development stage, but from the present perspective they can be regarded as a fortunate choice, since GSM proved to be an innovative system that was not burdened with the technical ballast of the early days of mobile telecommunications.

[4] A good overview of current statistical figures and network operators can be found at GSM World [GSM]

The common contractual basis for operators of GSM networks is the Memorandum of Understanding (MoU), which was first signed by 15 European network operators in 1987. The GSM Association is an internationally active body, with offices in Dublin and London, for the coordination of mobile telecommunications systems. It was founded in Copenhagen in 1987, and it is responsible for the development and application of the GSM standards. The GSM Association represents more than 500 network operators, manufacturers and suppliers in the GSM industry. In 1989, the specifications developed by the various working groups under the leadership of the GSM Permanent Nucleus were incorporated into the newly founded European Telecommunication Standards Institute (ETSI), where they have since been further developed. In 1990, all of the GSM Phase 1 specifications were complete in an acceptable form and were frozen.

In 1998, the Subscriber Identity Module Expert Group (SIMEG) started work on the specification for the GSM smart card, which is called the 'subscriber identity module' (SIM). This group was composed of representatives of card manufacturers, manufacturers of mobile telephones and network operators. Working under the auspices of the ETSI, the SIMEG generated the specification for the interface between the smart card and the mobile telephone. This specification bears the name 'GSM 11.11'. In 1994, the SIMEG was transformed into the newly founded Special Mobile Group 9 (SMG9), which retained the duties and authorities of the original group. The SMG9 was given the mandate of further developing and maintaining all of the SIM specifications up to 2000. In 2000, the SMG9 was dissolved, and its responsibilities were divided between two newly founded expert groups. The ETSI Project Smart Card Platform (EP SCP) expert group handles all generic issues in the area of smart cards for telecommunications, while the 3GPP expert group is responsible for the application-specific interface between the mobile telephone and the SIM or USIM.[5]

The first operating GSM network was demonstrated at the ITU Telecommunications Fair in Geneva in 1991. During the fair, approximately 11,000 calls were routed without any major problems. In 1992, the first GSM systems were put into regular service in several European countries (Denmark, Finland, France, Germany, Italy, Portugal and Sweden). At that time, there were approximately 250,000 subscribers. Also in that year, the first 'roaming agreement' between two network operators was signed, and the first non-European network operator signed the MoU, which meant that it officially decided to use the GSM system. Only one year later, at the end of 1993, the millionth subscriber was registered. In that year, the first GSM-1800 network began operation in Great Britain. In 1995, the first GSM-1900 network went into operation in the USA, and at the end of July 1998, the 100-millionth GSM subscriber was registered. In mid-2001, there were 500 million subscribers throughout the world, and it is anticipated that there will be 1 billion subscribers in 2005.

The GSM specifications were extended in 1991 and 1992. They now also cover the 1800-MHz frequency band (1710–1785 MHz uplink, 1805–1880 MHz downlink; wavelength approximately 16.6 cm) with GSM 1800 (previously called Digital Cellular System, or DCS) and the 1900-MHz band (1850–1910 MHz uplink, 1930–1990 MHz downlink; wavelength approximately 15.8 cm) with GSM 1900 (previously called Personal Communication System, or PCS). Since then, GSM in the original 900-MHz frequency band (880–915 MHz uplink,

[5] A comprehensive overview of the interesting history of the expert groups for the standardization of the SIM, USIM and UICC can be found in an article by Klauss Vedder entitled 'The Subscriber Identity Module: Past – Present – Future', in [Hillebrand 02]

925–960 MHz downlink; wavelength approximately 33.3 cm) is referred to as GSM 900. Due to the higher frequencies and lower levels of transmitted power, the maximum diameter of a cell in the higher-frequency systems is only 20 km. Consequently, they are primarily used in regions with high subscriber density, and less often in regions with low subscriber density. The principal difference between GSM 1800 and GSM 1900 is found in the transmitter and receiver components on either side of the air interface.

The low data transmission rate of the GSM system, which is 9600 bit/s or 14,400 bit/s with an improved codec for the air interface, has relatively quickly proven to be a weakness of the system. The rapidly increasing demand of mobile subscribers for transferring large volumes of data has further exacerbated this shortcoming. Consequently, an evolution path leading to increased data transmission rates, and particularly packet-switched transport services, has been specified. The next stage in the development of GSM is the circuit-switched HSCSD (high-speed circuit-switched data) service. With HSCSD technology, a theoretical data transmission rate of up to 76,800 bit/s (8×9600 bit/s) for uplink or downlink can be achieved by using 'channel bundling' to combine several existing time slots in the air interface. Existing GSM networks can be extended to support HSCSD with relatively little effort by modifying the base stations and using special mobile telephones. However, the disadvantage of this approach is that the number of transmission channels can be increased by at most a factor of 8, so HSCSD will probably not become a major success.

The packet-switched General Packet Radio System (GPRS) service is the following step in the evolution of GSM. It provides a packet-switched connection with a data transmission rate of up to 115.2 kbit/s (downlink or uplink) by bundling the eight existing 14.4-kbit/s time slots. A mobile telephone with GPRS technology is constantly logged in to the network for data transport, and thus always available for data transmission. For this reason, GPRS is also quite suitable for discontinuous data transmission. A drawback is the relatively high cost of upgrading the base stations. GPRS is regarded as a G2.5 technology, and it has a good chance of becoming a significant factor in extending the lifetime of existing GSM systems.

The final planned stage of enhancement for GSM networks is EDGE ('Enhanced Data Rates for GSM and TDMA Evolution'). Using the existing network infrastructure, GSM mobile telephones with EDGE technology can be connected to base stations with a data transmission rate of up to 384 kbit/s by using a different modulation method for the air interface. The extent to which EDGE technology will play a significant role in the future, when it will have to compete with 3G systems such as UMTS that will then be available, cannot presently be foreseen.

The designated successor to GSM is UMTS, whose basic architecture is based on GSM. It thus does not represent a fundamentally new mobile telecommunications technology, as did GSM at the time it was developed.

13.2.1 Specifications

A large number of interrelated and mutually dependent specifications were necessary to fully describe the GSM system in technical terms. In total, there are approximately 130 individual specifications, with a total size of more than 6000 pages.

Particularly in connection with the GSM system, the terms 'specification' and 'standard' are often used interchangeably. In the case of GSM, both of these terms are actually justified.

Since they are published by the ETSI standardization organization, the specification documents formally have the status of standards. However, their technical descriptions are so strict that practically all implementations based on them are mutually compatible, which is a typical characteristic of a specification. For this reason, in this book we consistently refer to the GSM numbering scheme (e.g., GSM 11.11) that is commonly used in technical circles, rather than the corresponding ETSI standards (e.g., TS 100977), which are identical in content.

The course of development of the GSM system is characterized by a series of phases building on top of each other. The basic services (voice transmission, call forwarding, roaming and the SMS message service) were implemented in Phase 1, which began in 1992. In Phase 2, which began in 1996, supplementary services were added, including conference calls, call handover, call number negotiation and GSM in the 1800-MHz frequency band. This was followed by Phase 2+, in which these services were augmented with the functions of the SIM Application Toolkit, HSCSD and GPRS (among others).

As is usual with specifications, the GSM specifications employ their own technical vocabulary. This vocabulary is precisely defined in technical terms in various lists of abbreviations and glossaries, and is only applicable to the GSM field. A summary is provided by GSM 1.04 ('Abbreviations and acronyms'). Due to this technical vocabulary, it is generally relatively difficult for newcomers to become familiar with GSM, since it is constantly necessary to consult the explanations of the abbreviations in the appropriate places when studying the specifications.

The specification forming the basis for the GSM security module in the mobile telephone is designated GSM 02.17 ('SIM Functional Characteristics') and contains a relatively abstract description of the functional requirements for the SIM. The most important card-specific document in the GSM system, GMS 11.11 ('Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface'), is based on this specification. In more than 170 pages, GSM 11.11 precisely and unambiguously specifies the interface to the SIM. This is a pure interface specification that does not contain any details about the actual implementation.

The specifications of the electrical parameters of smart cards using 3-V and 1.8-V technology, which supplement GSM 11.11, are contained in GSM 11.12 ('Specification of the 3 Volt Subscriber Identity Module – Mobile Equipment (SIM – ME) interface') and GSM 11.18 ('Specification of the 1.8 Volt Subscriber Identity Module – Mobile Equipment (SIM – ME) interface').

Besides these specifications, which primarily describe the basic functionality of the SIM, there is also GSM 11.14 ('Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface'), which describes a platform for secure supplementary services in the SIM. These are referred to as the SIM Application Toolkit (SAT). This specification was published in 1996, and it primarily offers network operators the possibility of loading their own applications into the smart card for controlling the mobile telephone. GSM 11.14 specifies in detail how functions such as driving the display, polling the keypad, sending short messages (SMS) and other functions related to suitable value-added applications must be implemented in the SIM.

The requirements specifications GSM 02.48 ('Specification of security mechanisms for the SIM application toolkit, stage 1') and GSM 03.48 ('Specification of security mechanisms for the SIM application toolkit, stage 2'), which is based on GSM 02.48, introduce two important security mechanisms for the SIM. The first item that they address is specifying security mechanisms for end-to-end communications between the background system and the SIM

that are protected against eavesdropping and manipulation. In practice, these mechanisms are primarily used for secure data transmission via the air interface ('over the air', or OTA). The second item, which is addressed by GSM 03.48, is a description of the basic mechanism for remote file management (RFM) and remote applet management. This description is in principle bearer-independent, but in GSM 03.48 it is presented using transport via SMS as an example.

Particularly in the telecommunications environment, smart cards with Java have become established very quickly, which is why the effects of such cards were seen relatively early in the GSM specifications. The basis for all smart card operating systems with executable program code is formed by the GSM 02.19 specification. It contains a list of all basic services for a language-independent API for executable program code in the SIM. Based on this standard, GSM 03.19 specifies a detailed implementation of a Java Card API for SIMs based on the Java Card 2.1 specification. This standard is the key document for using Java Card with GSM. It is supplemented by GSM 11.13, which specifies the test environment, test applications, test procedures, test coverage and individual test cases. The described tests are aimed exclusively at the IT aspects of a Java Card implementation for GSM.

The GSM specifications related to the SIM are not being developed any further, since the functionality of the SIM is fully adequate for the current needs of the GSM system. The only modifications that are still routinely made to the relevant specifications involve clarifications of passages that are subject to interpretation. Since 1999, the focus has been on standardizing

Table 13.2 The most important standards for the SIM and SIM-related services[6]

GSM 02.09	Security Aspects
GSM 02.17	SIM Functional Characteristics
GSM 02.19	Subscriber Identity Module Application Programming Interface (SIM API); Service description; Stage 1
GSM 02.48	Specification of security mechanisms for the SIM application toolkit, Stage 1
GSM 03.19	Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card; Stage 2
GSM 03.48	Specification of security mechanisms for the SIM application toolkit, Stage 2
GSM 09.91	Interworking aspects of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface between Phase 1 and Phase 2
GSM 11.11	Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface
GSM 11.12	Specification of the 3 Volt Subscriber Identity Module – Mobile Equipment (SIM – ME) interface
GSM 11.13	Test specification for SIM API for Java card
GSM 11.14	Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface
GSM 11.17	Subscriber Identity Module (SIM) conformance test specification
GSM 11.18	Specification of the 1.8 Volt Subscriber Identity Module – Mobile Equipment (SIM – ME) interface

[6] A general list of all GSM standards related to the SIM is provided in the directory of standards in Chapter 16. All of the GSM standards can also be obtained free of charge from the ETSI web server [ETSI]

the UICC ('universal integrated circuit card') with the USIM ('universal subscriber identity module') application, which is primarily being pursued under the auspices of the 3GPP.

13.2.2 System architecture and components

Every GSM network can be divided into three general subsystems, which are described in general terms in the GSM 01.02 specification ('General description of a GSM Public Land Mobile Network (PLMN)'). These three subsystems are the radio subsystem (RSS), the network and switching subsystem (NSS) and the operation subsystem (OSS).

The radio subsystem is composed of the mobile telephone, which is called the mobile station (MS), and the base station subsystem (BSS). The mobile station consists of two physically and logically separate components, which are called the mobile equipment (ME) and the subscriber identity module (SIM). The mobile equipment is the radio and encryption component with the user interface, while the SIM is the correct designation (in GSM nomenclature) for a GSM-specific smart card. These two components together form the operational mobile telephone.

As a rule, the base station subsystem is formed by the base stations located at the center of each cell. The functions of the base station subsystem are to establish contact with the mobile telephones via the air interface and to supply data to the higher-level components of the network. A base station consists of one or more base transceiver stations (BSTs) and a base station controller (BSC). The base station transceiver, with its aerial and associated radio-frequency components, is the actual transmission and reception component. A typical receiver module for a base station transceiver has eight 200-kHz channels, so in theory it can concurrently maintain eight active links to mobile stations. In practice, only seven active links are usually used, since one channel is usually reserved for administrative communications. One, three or six receiver modules are usually fitted in each base transceiver station. One or more base transceiver stations are in turn managed by a base station controller. A typical setup consists of three base station transceivers arranged at 120 degrees to each other, all connected to a base station controller. If a mobile station moves from the send/receive region of one base transceiver station into that of another base transceiver station, and both base transceiver stations are assigned to the same base station controller, the base station controller can independently initiate the handover after signaling this to the responsible mobile switching center.

Data transmission via the air interface is encrypted and has a net transmission rate of 13 kbit/s in full-rate mode. It employs a lossless compression method with technically sophisticated error correction mechanisms, such as frequency hopping, convolutional coding and interleaving.

The network and switching subsystem essentially consists of the mobile switching center and the visitor location register (VLR). A mobile switching center (MSC) manages multiple base station subsystems. It forms the link between the base station subsystems connected to it, other mobile switching centers and, of course, the public switched telephone network. The mobile switching center is responsible for setting up, managing and shutting down connections, handling call charges and supervising supplementary services, such as call forwarding, call blocking and conference calling. The visitor location register (VLR) contains information about all mobile stations currently within range of the associated mobile switching center. This information is needed for functions such as routing a call to a particular mobile telephone via the proper base station subsystem and radio cell. The VLR also maintains a list of mobile

stations belonging to subscribers of other networks that have logged into the network of the associated mobile switching center via roaming.

The topmost hierarchical level in a GSM system is the operation subsystem. It consists of the operation and maintenance center (OMC), the authentication center (AuC), the home location register (HLR) and the equipment identity register (EIR). The operation and maintenance center is responsible for regular network operation, subscriber administration and call billing. The authentication center is the security component on the network side, and in a manner of speaking it is the counterpart to the SIM on the mobile side. It generates and manages all keys and algorithms needed for operating the system, especially for authentication of the mobile stations (i.e., the SIMs). Another central component is the home location register, which contains all of the subscriber data as well as the localization data for each of the mobile stations. The equipment identification register is the complement to the HLR for mobile stations instead of subscribers. It contains essential data, such as the serial numbers of all mobile stations represented in the network.

13.2.3 Important data elements

This section describes a selection of important data elements that are primarily related to the SIM and its functions. The coding of the described data elements can be found in the descriptions of the typical data of a SIM.

Coding of alphanumeric characters

In the original middle-European GSM system, alphanumeric characters were and still are coded using a 7-bit code derived from the ASCII code. This code is defined in the GSM 03.08 specification. However, the spread of the GSM to other countries made it necessary to extend the character set. Consequently, the UCS-2 16-bit subvariant of the Universal Character Set (UCS) is used for characters that cannot be represented using the west-European character set as defined by GSM 03.38. The UCS-2 character set allows the most important characters of all living languages to be represented.[7]

Three different schemes are defined for character coding using the USC-2 character set, in the interest of minimizing memory space. The preferred scheme (Scheme 1), which, however, requires the most memory, is identified by having a value of '80' for the first byte. This is followed by the 16-bit USC-2 character code, with the most significant byte first. Unused bytes are set to 'FF'.

Scheme 2 is identified by having a value of '81' in the first byte. The second byte contains the number of characters in the character string. The two following bytes represent a 16-bit pointer to the UCS character set, which is used to select a language-specific character within the UCS. Bits 1–7 and bit 16 of this pointer are set to '0'. If bit 8 of one of the following bytes has a value of °1°, bits 1–7 of that byte are added to the pointer value, with the resulting pointer value then indicating the actual character in the UCS character set. If bit 8 has a value of °0°, the character in question is a member of the 7-bit character set defined by GSM 03.38.

[7] See also Section 4.2, 'Coding Alphanumeric Data'

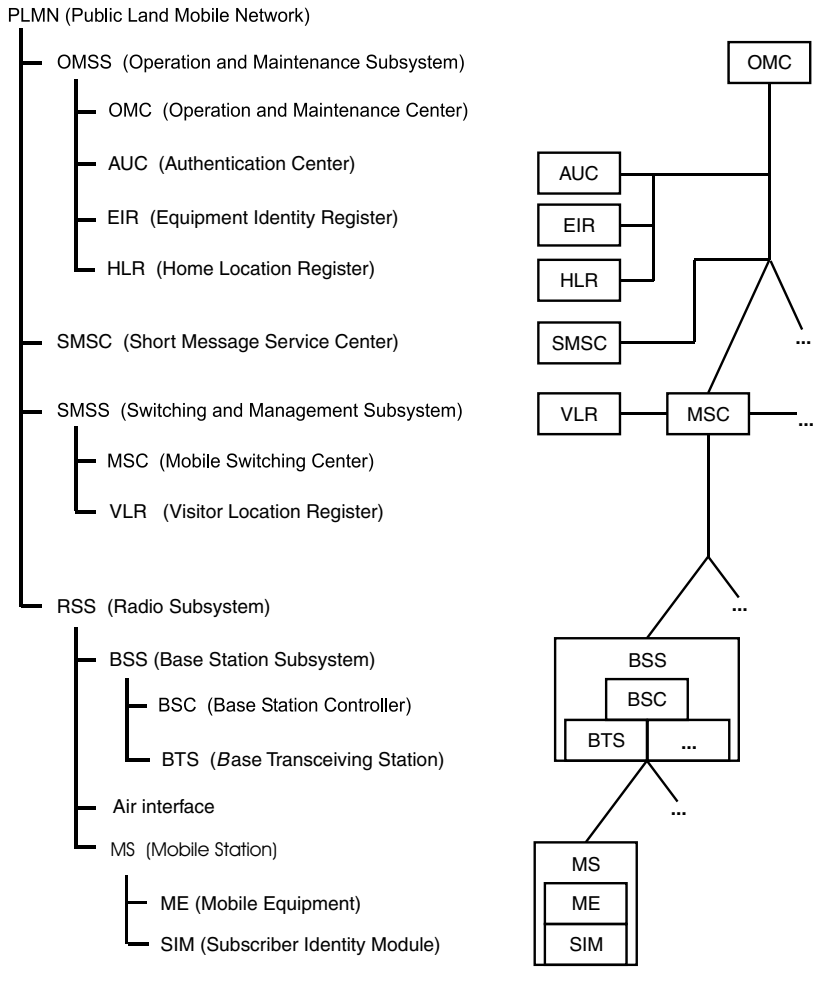

Figure 13.9 Basic architecture of a typical mobile telecommunications system compliant with the GSM 01.02 specification. In this example, the EIR and HLR databases are centralized. Since many aspects of the PLMN configuration are left to the operator of a particular network, the databases may be decentralized and distributed among several MSCs if necessary (e.g., due to high network loading). For ease of understanding, a link to a short message service center (SMSC) is also shown here, although this is not a direct GSM system component. One or more radio subsystems may be combined to form a location area (LA), and one or more network and switching subsystems may be combined to form a service area (SA)

Scheme 3 is identified by having an initial byte value of '82'. As with Scheme 2, the second byte contains the length of the character string, while the third and fourth bytes represent a complete 16-bit pointer to the USC character set table. If bit 8 of the following byte has a value of °1°, the following seven bits must be added to the pointer value to uniquely determine the UCS character. If bit 8 has a value of °0°, the character in question is a member of the 7-bit character set defined by GSM 03.38.

Table 13.3 The databases essential to the operation of a GSM system, and the most important data elements in these databases

Database	Data elements
HLR (home location register)	Subscriber information IMSI (international mobile subscriber identity) MSISDN (mobile station ISDN number) Service restrictions (e.g. roaming not allowed) Subscribed services Parameters for supplementary services Information about the subscriber's equipment Authentication data (i.e. RAND, SRES, Kc triplet) (implementation-dependent) Localization data (mobile location information) MSRN (mobile station roaming number) Address of current VLR (if available) Address of current MSC (if available) TMSI (if available)
VLR (visitor location register)	Subscriber information IMSI (international mobile subscriber identity) MSISDN (mobile station ISDN number) Parameters for supplementary services Information about the subscriber's equipment Authentication data (i.e. RAND, SRES, tuple) (implementation-dependent) Localization data (mobile location information) TMSI (temporary mobile subscriber identity) MSRN (mobile station roaming number) LAI (location area information) TMSI (if available)
EIR (equipment identity register)	IMEI (international mobile equipment identity) of all mobile stations (white list) IMEI of mobile stations to be reported (graylist) IMEI of blocked mobile stations (blacklist)

SIM service table (SST)

The SST contains a table of services that can be used with or enabled in addition to voice service, such as short message service or fixed dialing number service.

Fixed dialing numbers (FDN)

Fixed dialing numbers are a special type of dialing numbers that can be selected even when all other dialing numbers are blocked in the mobile telephone.

ICC identification (ICCID)

The ICCID is a unique identification number for the smart card. It is BCD-coded and 10 bytes long, and it can be right-padded with 'F' as necessary.

International mobile equipment identity (IMEI)

The IMEI is a unique device number for the mobile station. It contains 15 digits and thus usually occupies eight bytes. It is composed of the six-digit type approval code, two manufacturer code digits, a six-digit serial number and a check digit. The IMEI is stored in the mobile telephone and in the equipment identification register (EIR) in a central location.

International mobile subscriber identity (IMSI)

The IMSI is the unique subscriber identity within the GSM system. It is BCD-coded and has a length of nine bytes, which may be right-padded with 'F' as necessary. It consists of the mobile country code (MCC), the mobile network code (MNC) and a serial number assigned by the network operator. The IMSI is normally never transmitted over the air interface in cleartext, in order to prevent the location of a mobile station from being illicitly traced. Instead of the IMSI, the TMSI is normally used together with the LAI for identification purposes.

Individual key (Ki) and cipher key (Kc)

The keys Ki and Kc are secret keys for symmetric cryptographic algorithms. Ki is the card-specific key for the cryptographic computation of the authenticity of the SIM, and Kc is used for encrypting data transmitted between the mobile station and the base station via the air interface.

Short message service (SMS)

The short message service allows messages with a maximum length of 160 alphanumeric characters to be transmitted between the network and the mobile station via the signaling channel. SMS service is used not only for conveying short messages for subscribers, but also as a bearer service for transmitting data to the mobile telephone or the SIM, for instance for the WAP and OTA services.

Abbreviated dialing numbers (ADN)

Abbreviated dialing number are dialing numbers stored in the mobile telephone or the SIM along with supplementary information, which can be easily and quickly selected using a menu or special buttons.

Location area information (LAI)

The LAI is the unique position information of the mobile station. It is used in combination with the TMSI to generate a unique subscriber identity. The LAI consists of a three-digit country code (CC), a two-digit mobile network code (MNC) and a location area code (LAC), which has a maximum length of five digits.

Mobile station ISDN number (MSISDN)

The MSISDN is the dialing number of the mobile station. It is independent of the subscriber identity (IMSI).

Temporary mobile subscriber identity (TMSI)

The TMSI is a temporally and spatially limited subscriber identity with a length of four bytes. It is used to protect the true subscriber identity. The TMSI is only unique in combination with the location area information (LAI). The TMSI is assigned by the VLR, where it is also stored.

13.2.4 The subscriber identity module (SIM)

The SIM is a mandatory security module located in the mobile telephone of a GSM system as an exchangeable component. It is defined as follows in the GSM 02.17 specification: 'The SIM is an entity that contains the identity of the subscriber. The primary function of the SIM is to secure the authenticity of the mobile station with respect to the network'.

Besides its primary functions of holding the identity of the subscriber, which is realized using a PIN, and authenticating the mobile station with respect to the network, the SIM also performs a number of other functions. It allows program execution to be protected against manipulation, and it makes it possible to store data such as dialing numbers, short messages and personal configuration settings for the mobile telephone. In addition, it is the bearer for secure supplementary services used with mobile telecommunications.

Two different SIM formats are used in the GSM system. In mobile telephones designed to allow the SIM to be exchanged relatively often, the ID-1 format is used. This is based on the idea of a company or family telephone with a separate card for each user. Mobile telephones with small dimensions, whose SIMs are intended to be exchanged only rarely, use plug-in SIMs in the ID-000 format. However, the only difference between the two types of SIMs is the physical size of the card. Their logical and physical characteristics are otherwise fully identical. Since the mid-1990s, mobile telephones have become more or less personal accessories. This has had an effect of the size of card used, since it is no longer necessary to exchange the card depending on who is using the telephone. Already in 1995, half of all ID-1 cards sold were punched to allow a card in ID-000 format to be broken loose, and since 1998 practically all cards have this feature.

Communications between the mobile equipment and the SIM use the $T = 0$ protocol with the standard parameters, as specified in ISO/IEC 7816-3. The data transmission convention can

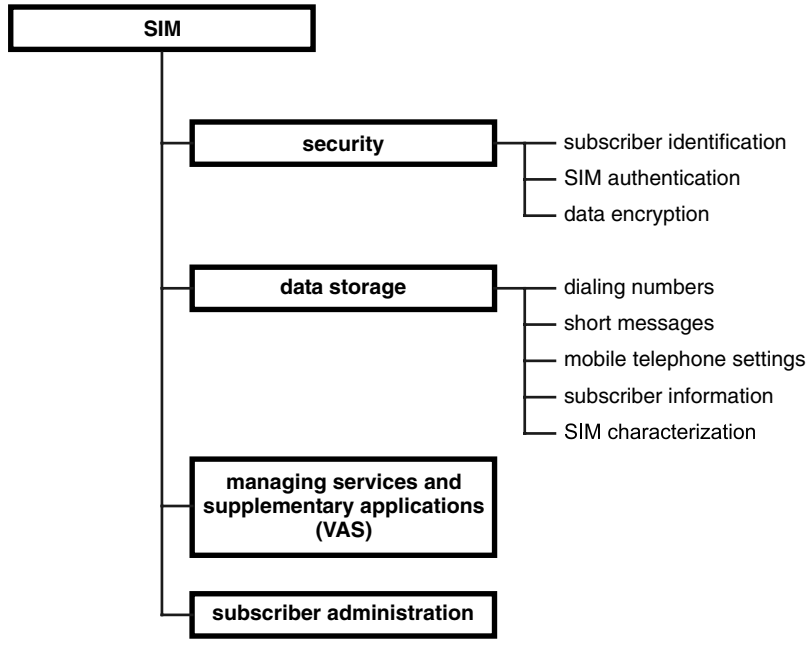

Figure 13.10 Classification of the basic functions of the SIM in the GSM system

be freely selected by the card via the ATR. There is provision for a PPS, and this capability is frequently used to increase the data transmission rate. The divider value (clock rate conversion factor) typically used by many mobile telephones is 64, which yields a data transmission rate of 78 kbit/s with a 5-MHz clock rate. In isolated cases, a value of 31 (≈156 kbit/s at a 5-MHz clock rate) is even used. For historical reasons, the T = 0 communications command GET RESPONSE is incompatible with ISO/IEC in two regards.[8] If data can be fetched from the terminal using GET RESPONSE, the SIM indicates this by putting '9F' in the SW1 byte, rather than '61' as specified in ISO/IEC 7816-3. GET RESPONSE also has another special feature. According to GSM 11.11, the data provided by the SIM can be fetched a byte at a time using GET RESPONSE, and a transmit buffer pointer is maintained in the SIM for this purpose. This is not possible with ISO/IEC 7816-3, which specifies that the data to be fetched using GET RESPONSE can only be requested starting with the first byte or as an entire block. However, these two incompatibilities do not lead to any problems in practice.

In 1998, on the occasion of the tenth anniversary of the standards for the SIM, the SMG9 published the slogan shown in Figure 13.11. This was the first statement to quite clearly show the significance and size already achieved by the GSM system at that time, as well as the pride felt for one of the essential components of the system, the SIM.

The specifications for the SIM formed the basis for many other specifications for smart cards used in the field of mobile telecommunications. The most important of these specifications are briefly described below.

[8] Strictly speaking, in this case the ISO/IEC 7816-3 standard is *de facto* incompatible with GSM 11.11, since the latter was chronologically first. However, in terms of standardization, an ISO/IEC standard has a higher rank, so GSM is *de jure* incompatible

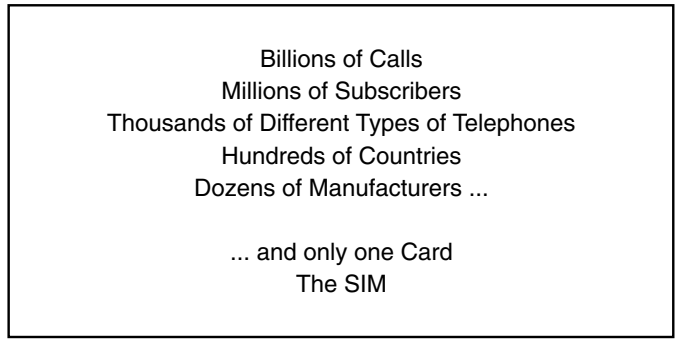

Figure 13.11 The slogan of the SIM standardization group SMG9 for its tenth anniversary in 1998

In 1992, as part of the European standardization of 'digital enhanced cordless telecommunications' (DECT) by ETSI (DECT is a standard for cordless telephones using cellular technology operating in the 1.9-GHz band), the first version of a specification for the DECT authentication module (DAM) was published. This specification was frozen in 1995 under the ETSI number ETS 300 331. Unfortunately, the DAM is specified as being optional, with the result that it was never converted into an actual product; it fell victim to the cost reduction programs of all manufacturers of cordless telephones.

The digital terrestrial trunked radio system TETRA [TETRA] also has provision for an optional smart card called the TETRA-SIM, whose specifications are based on the SIM for GSM mobile telephones. The EN 300 812 specification for the TETRA-SIM also allows it to be implemented as an application in the UICC if so desired. Since the TETRA-SIM is optional, it can also exist as a software implementation in the terminal device.

Another type of smart card whose specification is based on the SIM is the R-UIM (removable user identity module) in 3G mobile telecommunications systems, which was defined by the Third Generation Partnership Project 2 (3GPP2). The R-UIM is envisaged as an optional component of the associated terminals, and its functionality is similar to that of the SIM. It is specified in the TIA/EIA/IS-820 and TIA/EIA/IS-839 standards. A significant difference between the R-UIM and the SIM is that the former includes the CAVE ('cellular authentication, voice privacy and encryption') cryptographic algorithm, which as its full name suggests, can be used in the R-UIM for a wide variety of cryptographically secured functions. A UIM application toolkit (UATK), which borrows heavily from the SIM application toolkit, has also been specified for the R-UIM.

In the satellite-based Inmarsat mobile telephone network [Inmarsat], which has been in operation since the early 1989s, modified GSM cards are also used now as a means of establishing subscriber identity. Another extension of the SIM, which features a few additional files and a special cryptographic algorithm, is the smart card for the international Iridium mobile telecommunications system [Iridium]. In its ultimate form, this system is intended to consist of 66 satellites orbiting at a height of 780 km that are equivalent to GSM base stations. The frequency used for the air interface between the mobile stations and the satellites is 1616 MHz. The medium- to long-term survival of this technically interesting and unquestionably sophisticated mobile telecommunications system depends on the somewhat precarious financial situation of its operating consortium.

SIM commands

The GSM 11.11 specification defines 22 operational commands for the SIM, which are identified by a class byte value of 'A0'.[9] The commands can be classified into commands related to security, commands for operations on files and commands belonging to the SIM Application Toolkit. Table 13.4 contains a summary of these commands.[10]

Table 13.4 The commands specified for the SIM in GSM 11.11

Command	Brief description
Security commands	
CHANGE CHV	Change the PIN
DISABLE CHV	Disable PIN queries
ENABLE CHV	Enable PIN queries
RUN GSM ALGORITHM	Execute the GSM-specific cryptographic algorithm
UNBLOCK CHV	Reset the PIN retry counter from its terminal count
VERIFY CHV	Verify the PIN
Commands for operations on files	
INCREASE	Increase the value of a counter in a file
INVALIDATE	Reversibly block a file
READ BINARY	Read from a file with a transparent structure
READ RECORD	Read from a file with a record-oriented structure
REHABILITATE	Unblock a file
SEEK	Seek a text string in a file with a record-oriented structure
SELECT	Select a file
STATUS	Read various data from the currently selected file
UPDATE BINARY	Write to a file with a transparent structure
UPDATE RECORD	Write to a file with a record-oriented structure
SIM Application Toolkit commands	
ENVELOPE	Pass data to a value-added service of the SIM forming part of the SIM Application Toolkit
FETCH	Retrieve a SIM Application Toolkit command from the SIM in the mobile equipment
TERMINAL PROFILE	List all functions of the mobile equipment with respect to the SIM Application Toolkit
TERMINAL RESPONSE	Convey the response of the mobile equipment to a previous SIM Application Toolkit command of the SIM
Miscellaneous commands	
GET RESPONSE	Command specific to T = 0 for requesting data from the smart card
SLEEP	Obsolete command for putting the smart card into a low-power state

There is a special feature with regard to entering the four-digit PIN, which incidentally is designated 'cardholder verification' (CHV) in GSM. The user can disable further queries for the user PIN by using a special command (DISABLE CHV) together with the proper PIN,

[9] See Section 6.5.1, 'Structure of the command APDU', for a description of the command structure
[10] See Chapter 7, 'Smart Card Commands', for descriptions of typical smart card commands

thus making it unnecessary to enter the PIN before logging in to a mobile telecommunications network. The disadvantage of this, which is that a lost card can be used illicitly for telephoning until it has been blocked by the network operator, falls under the responsibility of the user. Another command (ENABLE CHV) can be used as desired to again enable PIN queries.

A SIM usually has two CHVs. The idea behind this is to differentiate between the card user and the cardholder, in order to distinguish the functions that can be used or allow only the cardholder to use certain functions. This can be briefly explained using the EF_{FDN} file holding the fixed dialing numbers as an example. The card user only knows CHV 1, which is sufficient for dialing the numbers stored in EF_{FDN}. However, the cardholder also knows CHV 2, so he or she can alter the entries in EF_{FDN}, since the access conditions for UPDATE RECORD require successful verification of CHV 2. One example of how this feature can be used is restricting the numbers that children can call with the mobile telephone to the numbers stored in EF_{FDN}, since they only need to know CHV 1 in order to use the telephone. Their parents, who also know CHV 2, can edit the numbers stored in EF_{FDN}.

For reasons of compatibility, all SIMs also support the SLEEP command, although it has been obsolete for many years. Its original function, which was to save energy in terminal equipment, has now been taken over by the hardware of the smart card microcontroller or the operating system.

The STATUS command is used for two purposes. The first is requesting information about the currently selected file, while the second is verifying that a SIM is present. The mobile equipment periodically sends a STATUS command to the SIM at an interval of approximately 30 seconds, in order to confirm that the SIM is present. If no response to the STATUS command is received from the SIM within five seconds, the SIM is deactivated and the call is terminated. In addition, there is usually some sort of mechanical contact present to detect or prevent exchanging the SIM while the mobile telephone is in use.

The relevant GSM specifications do not specify any administrative commands for file management. Such commands were originally not necessary, since for a long time smart card operating systems did not support creating or deleting files, due to a lack of memory space. However, this situation has fundamentally changed, with the result that these file management functions, which in principle are very important, are now available. They can be used to download files into SIMs at any desired time using remote file management functions, assuming sufficient free memory space is available. The administrative commands are described in the TS 102.222 specification, which originates from the 3GPP environment and was originally conceived for the USIM. However, since the administrative commands for smart card file systems do not exhibit any fundamental differences between SIM and USIM, in practice this standard has also become firmly established in the SIM environment.

SIM files

The SIM has a hierarchical file system, with an MF and two DFs directly below the MF. EFs containing data for the application are located under the MF and in the DFs. The EFs may have transparent, linear fixed or cyclic file structures.

The file identifiers (FIDs) of the SIM files have a special feature, which is that the first byte of each DF under the MF always has the value '7F', DFs directly below the GSM DF have the value '5F' and EFs have the value '5F'. EFs directly below the MF must have the value

Table 13.5 Smart card file management commands specified in TS 102.222

Command	Brief description
ACTIVATE FILE	Unblock a file
CREATE FILE	Create a new file
DEACTIVATE FILE	Reversibly block a file
DELETE FILE	Delete a file
TERMINATE CARD USAGE	Irreversibly block a smart card
TERMINATE DF	Irreversibly block a DF
TERMINATE EF	Irreversibly block an EF

'2F' in the first byte of their FIDs, EFs under the TELECOM DF must have the value '6F' and EFs in an MExE EF must have the value '4F'. These conventions are largely a remnant of the early days of smart card microcontrollers, and they have long since ceased to have any practical significance.

The access conditions for all files are state-oriented and are individually specified for the four file access commands READ, UPDATE, INVALIDATE and REHABILITATE for each file. There are 16 different states for file access, which are numbered from 0 to 15 in increasing order of security. State 0 as an access condition means **always**, which means that the file may always be accessed using the associated command. State 15 represents the other extreme, which is that the file may **never** be accessed using the associated command. State 1 means that access is allowed following successful verification of CHV 1, which means PIN number 1. Similarly, State 2 requires successful verification of CHV 2 prior to access to the file. State 3 is not presently used and is reserved for future use. States 4 through 14 are reserved for administrative use, which means that the network operator can access files using these access conditions with special PINs or authentications.

All EFs containing general information about the smart card, such as a unique card serial number (ICCID), are located directly below the MF. All EFs relevant to the GSM system are located in the TELECOM DF. A typical example of such EFs is the EF containing the abbreviated dialing numbers. The GSM DF, by contrast, contains all EFs holding information specific to the network operator, such as the IMSI.

In total, 70 different EFs are defined in the GSM 11.11 specification, of which only 12 (with a total content of approximately 110 bytes of data) are obligatory. The rest of the EFs are optional, so their presence in the file system of the SIM depends on the network operator and the services that are provided. In addition to the files defined in the specification, the network operator can place its own files in the SIM file tree for maintenance or administrative purposes. In practice, intensive use is made of this possibility, with the result that typically around 40 files containing approximately 12 kB of user data are present in the SIM.

Some of the EFs in the file tree of the SIM must be written especially often. One example is the LOCI (location information) EF. This file stores the currently valid temporary mobile subscriber identity (TMSI) along with the supplementary location area information (LAI). The data in this file must be modified for each change in base station and each new call. Consequently, a SIM operating system must support a special file attribute called ‘high update activity’. The technical implementation of this involves storing several file bodies under a

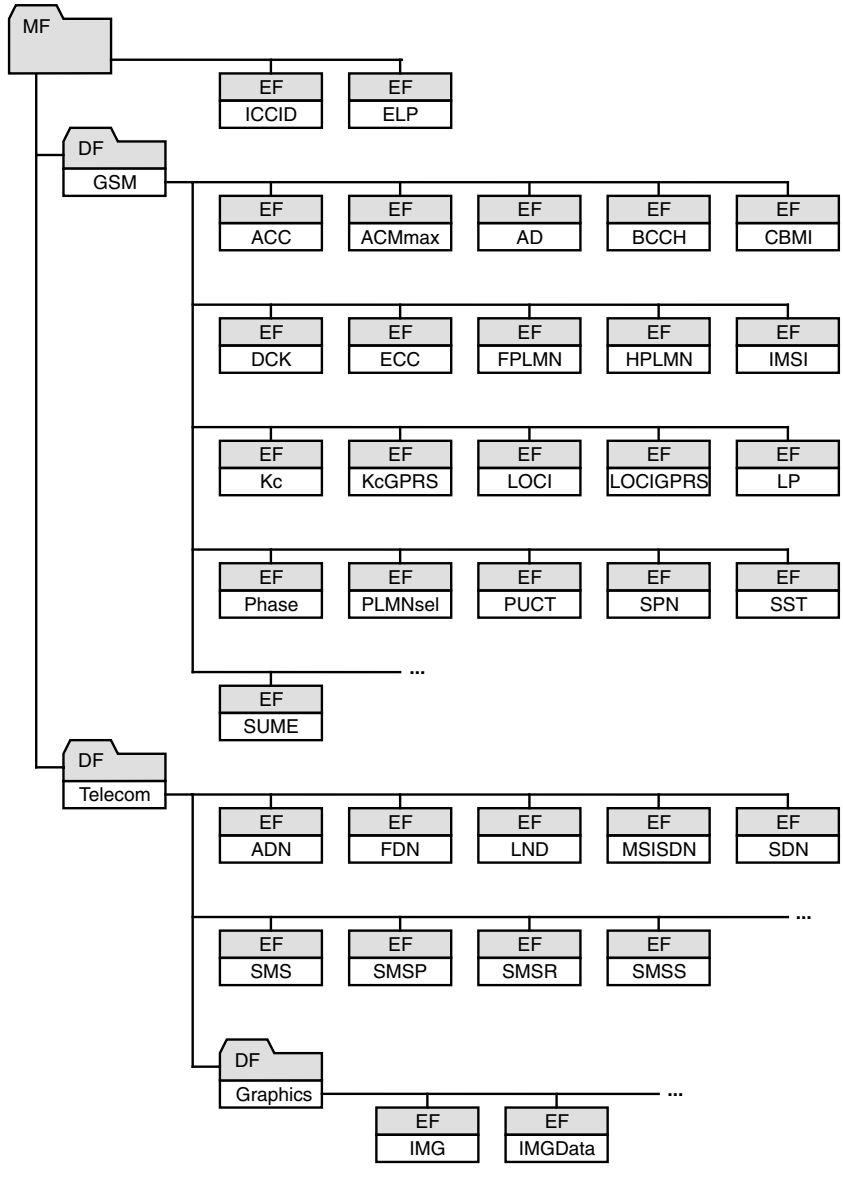

Figure 13.12 Overview of the most important SIM files

single file header. If an error occurs in a file body, the operating system automatically switches to a replacement file body. This file attribute came into existence at a time when EEPROM pages had only 10,000 guaranteed write/erase cycles. However, technical refinements have increased the number of cycles to around half a million, which means that this attribute has effectively become obsolete. Nevertheless, it is still present in the GSM specification, although

Table 13.6 Typical SIM files according to GSM 11.11, with the coding of the data elements and illustrative decoded examples

MF		**Root directory**
	Description:	This is the source directory for the entire SIM.
	File:	FID = '3F00'
$DF_{TELECOM}$		**Telecom directory**
	Description:	This directory holds all files specific to the services.
	File:	FID = '7F10'
DF_{GSM}		**GSM directory**
	Description:	This directory holds all files specific to the GSM network.
	File:	FID = '7F20' (or '7F21' for compatibility with older-model GSM 1800 mobile telephones)
$DF_{GRAPHICS}$		**Graphics directory**
	Description:	This directory holds all files containing graphics information.
	File:	FID = '5F50'
$MF.EF_{ELP}$		**Extended language preference (ELP)**
	Description:	This file holds an extended list of the preferred languages for the user interface.
	File:	FID = '2F05'; structure: transparent, file size: $2n$ bytes; accesses: READ: always, UPDATE: CHV 1
	Coding:	Each country code consists of two alphanumeric characters according to ISO 639, using the GSM 03.38 alphabet. bytes 1& 2: highest-priority language ... bytes 2 (n – 1) & $2n$: lowest-priority language
	Example:	'64 65' ⇒ highest-priority language: German '65 6E' ⇒ second highest-priority language: English '66 72' ⇒ third highest-priority language: French '65 73' ⇒ lowest-priority language: Spanish

Table 13.6 (*Cont.*)

MF.EF$_{ICCID}$	**ICC identification (ICCID)**
Description:	This file holds a unique identification number for the smart card.
File:	FID = '2FE2'; structure: transparent, file size: 10 bytes; accesses: READ: always, UPDATE: never
Coding:	sequential number, BCD-coded, left-justified and padded with 'F' as necessary byte 1, bits 1– 4: digit 1 byte 1, bits 5–8: digit 2 byte 2, bits 1–4: digit 3 etc.
Example:	'98 94 20 00 00 10 81 85 39 11' ⇒ 89 49 02 00 00 01 18 58 93 11
DF$_{GSM}$.EF$_{ACM}$	**Accumulated call meter (ACM)**
Description:	This file holds the number of call charge units accumulated since a particular starting time.
File:	FID = '6F39'; structure: cyclic, 3*n* bytes; accesses: READ: CHV 1; UPDATE: CHV 2
Coding:	bytes 1–3: accumulated number of call charge units
DF$_{GSM}$.EF$_{ACMmax}$	**Accumulated call meter maximum (ACM)**
Description:	This file holds the maximum amount of call charge units.
File:	FID = '6F37'; structure: transparent, 3 bytes; accesses: READ: CHV 1; UPDATE: CHV 2
Coding:	bytes 1 –3: maximum amount of call charge units
DF$_{GSM}$.EF$_{FPLMN}$	**Forbidden public land mobile network (FPLMN)**
Description:	This file holds a list of forbidden network operators.
File:	FID = '6F7B'; structure: transparent, 12 bytes; accesses: READ: CHV 1; UPDATE: CHV 1
Coding:	bytes 1–3: forbidden PLMN no. 1 bytes 4–6: forbidden PLMN no. 2; etc. See EF$_{PLMNsel}$ for the data structure and an example.

(*Cont.*)

Table 13.6 (*Cont.*)

Example:	'FF FF FF FF FF FF FF FF FF 62 F2 20' '62 F2' ⇒ MCC ⇒ '262' ⇒ Germany '10' ⇒ MNC ⇒ '01' ⇒ Germany D1
$DF_{GSM}.EF_{HPLMN}$	**Home public land mobile network search period (HPLMN)**
Description:	This file holds a time interval for searching for the home network.
File:	FID = '6F31'; structure: transparent, 1 byte; accesses: READ: CHV 1; UPDATE: ADM
Coding:	Time interval for searching for the home network in minutes; coding: per GSM 02.11
Example:	'05' ⇒ search for home network every 5 minutes
$DF_{GSM}.EF_{IMSI}$	**International mobile subscriber identity (IMSI)**
Description:	This file holds the international subscriber identity number.
File:	FID = '6F07'; structure: transparent, file size: 9 bytes; accesses: READ: CHV 1; UPDATE: ADM
Coding:	byte 1: length of the IMSI in bytes byte 2, bits 1–3: °100° byte 2, bit 4: parity of the IMSI, coded per GSM 04.08 byte 2, bits 5 –8: digit 1 of the IMSI bytes 3–9: digits 2 –10 of the IMSI IMSI = MCC || MNC || serial number of the network operator, BCD-coded and right-padded with 'F' as necessary Coding: from MCC; for MNC see $EF_{PLMNsel}$
Example:	'08 92 62 01 71 00 10 92 67' '08' ⇒ length ⇒ 8 bytes '9' || '2 62' ⇒ MCC ⇒ Germany '01' ⇒ MNC ⇒ Germany D1 '71 00 10 92 67' ⇒ serial number of the network operator
$DF_{GSM}.EF_{KC}$	**Kc key**
Description:	This file holds the key Kc for encrypting data on the air interface.
File:	FID = '6F20'; structure: transparent, file size: 9 bytes; accesses: READ: CHV 1; UPDATE: CHV 1

Table 13.6 (*Cont.*)

	Coding:	bytes 1–8: key Kc byte 9, bits 1–3: serial number of the key
$DF_{GSM}.EF_{LOCI}$		**Location information (LOCI)**
	Description:	This file holds current location information for the mobile telephone.
	File:	FID = '6F7E'; structure: transparent, file size: 11 bytes; accesses: READ: CHV 1; UPDATE: CHV 1
	Coding:	bytes 1–4: TMSI (temporary mobile subscriber identity) bytes 5–9: LAI (location area information) byte 10: TMSI TIME (not used from Phase 2 onwards) byte 11: Location update status: b3–b1 = °000°: updated b3–b1 = °001°: not updated b3–b1 = °010°: forbidden PLMN b3–b1 = °011°: forbidden location area Coding: per GSM 04.08
	Example:	'5F 40 96 46 62 F2 10 80 04 FF 00' '5F 40 96 46' ⇒ TMSI '62 F2 10 80 04' ⇒ LAI 'FF' ⇒ TMSI TIME ⇒ not used '00' ⇒ location update status ⇒ updated
$DF_{GSM}.EF_{LP}$		**Language preference (LP)**
	Description:	This file holds a list of the preferred languages for the user interface.
	File:	FID = '6F05'; structure: transparent, file size: n bytes, $n \geq 1$; accesses: READ: always, UPDATE: CHV 1
	Coding:	per GSM 03.38 byte 1: highest-priority language ... byte n: lowest-priority language
	Sample languages:	Valid for the GSM alphabet according to GSM 03.38 '00': German '01': English '02': Italian '03': French '04': Spanish '05': Dutch '06': Swedish '07': Danish '08': Portuguese '09': Finnish '0A': Norwegian '0B': Greek '0C': Turkish '0D': Hungarian '0E': Polish '0F': Unspecified language

(*Cont.*)

Table 13.6 (*Cont.*)

Example:	'00 01 03 05' '00' ⇒ highest-priority language: German '01' ⇒ second highest-priority language: English '03' ⇒ third highest-priority language: French '05' ⇒ lowest-priority language: Dutch
$DF_{GSM}.EF_{PHASE}$	**Phase information**
Description:	This file holds information about the phase supported by the SIM.
File:	FID = '6FAE'; structure: transparent, file size: 1 byte; accesses: READ: always, UPDATE: ADM
Coding:	byte 1: 00 = Phase 1; 02 = Phase 2
Example:	'02' ⇒ Phase 2
$DF_{GSM}.EF_{PLMNsel}$	**Public land mobile network selector (PLMNsel)**
Description:	This file holds a list of the preferred network operators.
File:	FID = '6F30'; structure: transparent, $3n$ bytes ($n \geq 8$); accesses: READ: CHV 1; UPDATE: CHV 1
Coding:	bytes 1–3: PLMN for the highest selection priority bytes 4–6: PLMN for the second-highest selection priority Data structure: 2 bytes MCC (mobile country code) || 1 byte MNC (mobile network code), BCD-coded per GSM 04.08, high and low nibbles swapped; 'FFFFFF' ⇒ entry not used
Sample MCC codes:	262: Germany 208: France 234: Great Britain 222: Italy 232: Austria 310: USA
Sample MNC codes for Germany:	01: Germany D1 02: Germany D2 03: Germany E-plus 07: Germany Viag Intercom

Table 13.6 (*Cont.*)

Example:	'62 F2 20 72 F0 10 32 F4 01 32 F2 30 32 F0 10 62 F2 10 62 F0 20 42 F0 10 22 F8 10', remainder 'FF' '62 F2' ⇒ MCC ⇒ '262' ⇒ Germany '20' ⇒ MNC ⇒ '02' ⇒ Germany D2 etc.
$DF_{GSM}.EF_{PUCT}$	**Price per unit and currency table (PUCT)**
Description:	This file holds the price per call unit and the currency, for the current summary of call charges.
File:	FID = '6F41'; structure: transparent, file size: 5 bytes; accesses: READ: CHV 1; UPDATE: CHV 1 or CHV 2
Coding:	bytes 1 –3: currency code, character coded using the GSM alphabet bytes 4 & 5: price per unit = EPPU$\times 10^{\text{EX}}$ EPPU: elementary price per unit; EX: exponent EPPU component: B5.b1: 2^0 B5.b2: 2^1 B5.b3: 2^2 B5.b4: 2^3 B4.b1: 2^4 B4.b2: 2^5 B4.b3: 2^6 B4.b4: 2^7 B4.b5: 2^8 B4.b6: 2^9 B4.b7: 2^{10} B4.b8: 2^{11} Exponent component (EX): B5.b6: 2^0 B5.b7: 2^1 B5.b8: 2^2 B5.b5: sign of the exponent: 0: +, 1: –
Examples:	'44 45 4D 01 57' '44 45 52' ⇒ currency code ⇒ "EUR" '01 57' = °0000 0001° || °0101 0001° ⇒ price per unit ⇒ $17 \times 10^{-2} = 0.17$
$DF_{GSM}.EF_{SPN}$	**Service provider name (SPN)**
Description:	This file holds the name of the service provider.
File:	FID = '6F46'; structure: transparent, file size: 17 bytes; accesses: READ: always, UPDATE: ADM
Coding:	byte 1: conditions for display '00': display of PLMN name not required '01': display of PLMN name required bytes 2–17: service provider name, coded per GSM 03.38, left-justified and right-padded with 'F' as necessary
Example:	'01 50 72 6F 76 69 64 65 72 20 41' '01' ⇒ display of PLMN name required '50 72 6F 76 69 64 65 72 20 41' ⇒name of service provider ⇒ "Provider A"

(*Cont.*)

Table 13.6 (*Cont.*)

$DF_{GSM}.EF_{SST}$	**SIM service table (SST)**
Description:	This file holds a table of available and activated services supplementary to the voice service.
File:	FID = '6F38'; structure: transparent, file size: $\geq$ 2 bytes; accesses: READ: CHV 1; UPDATE: ADM
Coding:	byte 1, bits 1 & 2: service no. 1 byte 1, bits 3 & 4: service no. 2 byte 1, bits 5 & 6: service no. 3 byte 1, bits 7 & 8: service no. 4 byte 2, bits 1 & 2: service no. 5 etc. Bit coding: b1, b3, b5, b7 = 1 / 0: service available / not activated b2, b4, b6, b8 = 1 / 0: service enabled / not activated
Sample services:	Service no. 1: disable CHV testing Service no. 2: abbreviated dialing numbers (ADN) Service no. 3: fixed dialing numbers (FDN) Service no. 4: short message service (SMS) Service no. 18: service dialing numbers (SDN) Service no. 35: status report for short messages Service no. 38: GPRS Service no. 39: image (IMG)
Example:	'DF 3F DF FF 03' = °1101 1111° || °0011 1111° || °1101 1111° || °1111 1111° || °0000 0011° °11° $\Rightarrow$ disable PIN available and activated °11° $\Rightarrow$ abbreviated dialing numbers available and activated °01° $\Rightarrow$ fixed dialing numbers available and not activated °11° $\Rightarrow$ short message service available and activated etc.
$DF_{GSM}.DF_{GRAPHICS}.EF_{IMG}$	**Image (IMG)**
Description:	This file holds references to files containing graphics that can be shown on the display of the mobile telephone.
File:	FID = '4F20'; structure: linear fixed, $(9n + 2)$ bytes; accesses: READ: CHV 1; UPDATE: ADM

Table 13.6 (*Cont.*)

	Coding:	byte 1: number of references to image files bytes 2–10: description of the reference to image file 1 bytes 11 –19: description of the reference to image file 2 ... byte $9n + 2$: RFU
	Coding of the references:	byte 1: width of the image in pixels byte 2: height of the image in pixels byte 3: image coding scheme bytes 4 & 5: FID of $EF_{IMGData}$ bytes 6 & 7: offset to the image data in $EF_{IMGData}$ bytes 8 & 9: size to the image data in $EF_{IMGData}$ in bytes
$DF_{GSM}.DF_{GRAPHICS}.$ $EF_{IMGDattaX}$		**Image data (IMGData)**
	Description:	Each of these files holds a bitmapped graphic that can be shown on the display of the mobile telephone.
	File:	FID = '4Fxx'; structure: transparent, n bytes; accesses: READ: CHV 1; UPDATE: ADM
	Coding:	bytes 1 – n: image data
$DF_{TELECOM}.EF_{ADN}$		**Abbreviated dialing numbers (ADN)**
	Description:	This file holds the abbreviated dialing numbers. Each record contains a name and the associated dialing number.
	File:	FID = '6F3A'; structure: linear fixed, record size: $n + 14$ bytes; accesses: READ: CHV 1; UPDATE: CHV 1
	Coding:	bytes 1 – n: name coded in characters per GSM 03.38 byte $n + 1$: length of the BCD-coded dialing number in bytes byte $n + 2$: type of dialing number, coded per GSM 04.08 e.g.: '81' = unknown type of dialing number, ISDN dialing number scheme '91' = international type of dialing number, ISDN dialing number scheme bytes $(n + 3)$ – $(n + 12)$: BCD-coded dialing number with upper and lower nibbles swapped in byte bytes $(n + 13)$ – $(n + 14)$: pointer to supplementary data for this entry in EF_{CCP} and EF_{EXT1}, generally not used (i.e. 'FF') Unused bytes are set to 'FF'

(*Cont.*)

Table 13.6 (*Cont.*)

Example 1:	Record content: '57 4F 4C 46 47 41 4E 47 FF FF FF FF FF FF FF FF 07 91 94 98 69 35 24 46 FF FF FF FF FF FF' '57 4F 4C 46 47 41 4E 47' ⇒ "Wolfgang" 'FF FF FF FF FF FF FF FF' ⇒ not used '07' ⇒ length of the dialing number (7 bytes) '91' ⇒ international dialing number, ISDN dialing number scheme '94 98 69 35 24 46' ⇒ dialing number 49 89 96 53 42 64 'FF FF FF FF' ⇒ not used 'FF FF' ⇒ EF_{CCP} and EF_{EXT1} not used
Example 2:	Record content: '57 4F 4C 46 47 41 4E 47 FF FF FF FF FF FF FF FF 07 91 94 98 69: '57 4F 4C 46 47 41 4E 47 FF FF FF FF FF FF FF FF 07 81 80 99 56 43 62 F4 FF FF FF FF FF FF' '57 4F 4C 46 47 41 4E 47' ⇒ "Wolfgang" 'FF FF FF FF FF FF FF FF' ⇒ not used '07' ⇒ length of the dialing number (7 bytes) '81' ⇒ unknown type of dialing number, ISDN dialing number scheme '80 99 56 43 62 F4' ⇒ dialing number 089 96 53 42 64 'FF FF FF FF' ⇒ not used 'FF FF' ⇒ EF_{CCP} and EF_{EXT1} not used
$DF_{TELECOM}.EF_{FDN}$	**Fixed dialing numbers (FDN)**
Description:	Fixed dialing numbers can be stored in this file as needed. These dialing numbers are used when the subscriber is only allowed to dial certain numbers.
File:	FID = '6F3B'; structure: linear fixed, record size: $(n + 14)$ bytes; accesses: READ: CHV 1; UPDATE: CHV 2
Coding:	same as EFADN
Example:	see EFADN
$DF_{TELECOM}.EF_{LND}$	**Last number dialed (LND)**
Description:	The most recently dialed numbers are stored in this file.
File:	(optional file) FID = '6F44'; structure: cyclic, record size: $(n + 14)$ bytes; accesses: READ: CHV 1; UPDATE: CHV 1
Coding:	same as EF_{ADN}

Table 13.6 (*Cont.*)

$DF_{TELECOM}.EF_{MSISDN}$		**Mobile station ISDN number (MSISDN)**
	Description:	This file holds the dialing number of the mobile station.
	File:	FID = '6F40'; structure: linear fixed, record size: $(n + 14)$ bytes; accesses: READ: CHV 1; UPDATE: CHV 1
	Coding:	same as EFADN
$DF_{TELECOM}.EF_{SDN}$		**Service dialling numbers (SDN)**
	Description:	This file holds the service dialing numbers, which may for example be dialing numbers for directory information or schedule information.
	File:	FID = '6F49'; structure: linear fixed, record size: $(n + 14)$ bytes; accesses: READ: CHV 1; UPDATE: ADM
	Coding:	same as EFADN
$DF_{TELECOM}.EF_{SMS}$		**Short message service (SMS)**
	Description:	This file belongs to the short message service. It holds the short messages sent to and received from the network.
	File:	FID = '6F3C'; structure: linear fixed, record size: 176 bytes; accesses: READ: CHV 1; UPDATE: CHV 1
	Coding:	byte 1: status of the record in question: '00' = free record '01' = message coming from the network and read '03' = message coming from the network and still to be read '05' = message sent to the network '07' = message to be sent to the network bytes 2–176: message coded per GSM 03.40; unused bytes at the end of the message are set to 'FF'

(*Cont.*)

Table 13.6 (*Cont.*)

Coding of a message from the network to the mobile telephone	byte 2:	number of bytes in the SMSC dialing number, including the dialing number type
	next 2–12 bytes:	SMSC dialing number: '81' = unknown type of dialing number (no "+"), '91' = international type of dialing number ("+"), data nibblewise swapped
	next byte:	control information (generally '04')
	next byte:	number of digits in the dialing number of the sender, excluding the dialing number type
	next 2–12 bytes:	dialing number of the sender, with data nibblewise swapped
	next byte:	protocol tag ('00' = text message)
	next byte:	data coding ('00' = GSM standard alphabet)
	next 7 bytes:	SMSC time stamp, data nibblewise swapped: year || month || day || hours || minutes || seconds || time zone ('00' = GMT)
	next byte:	number of characters in the message
	next 1 –140 bytes:	message (if the GSM standard alphabet is used, the text portion is compressed, which means the 7-bit codes are continuously packed into bytes)
Coding of a message from the mobile telephone to the network	byte 2:	number of bytes in the SMSC dialing number, including the dialing number type
	next 2–12 bytes:	SMSC dialing number: '81' = unknown type of dialing number, (no "+") '91' = international type of dialing number, ("+"), data nibblewise swapped
	next byte:	relative time of the mobile telephone (generally 'FF')
	next byte:	message reference
	next 2–12 bytes:	dialing number of the destination, with data nibblewise swapped
	next byte:	protocol tag ('00' = text message)
	next byte:	data coding ('00' = GSM standard alphabet)
	next X bytes:	term of validity of the message: 1–143: t = (X + 1) × 5 min 144–167: t = 12 h + (X – 143) × 30 min 168–196: t = (X – 166) × 1 day 197–255: t = (X – 192) × 1 week
	next byte:	number of characters in the message
Sample SMS message from the network to a mobile telephone	'01 07 91 94 71 01 67 05 00 04 0C 91 94 71 71 46 53 42 00 00 00 60 52 31 63 15 00 17 C8 A0 93 28 AC 0E 91 20 62 51 0A 1A 22 93 D0 65 50 4A 2D 3A 01' || remainder of record is 'FF' '01' ⇒ message coming from the network and read '07' ⇒ number of bytes in the SMSC dialing number, including the dialing number type	

Table 13.6 (*Cont.*)

	'91 94 71 01 67 05 00' ⇒ SMSC dialing number = +49 17 10 76 50 00 '04' ⇒ no further messages '0C' ⇒ 12 ⇒ number of digits in the dialing number of the sender, excluding the dialing number type, is 12 '91 94 71 71 46 53 42' ⇒ sender dialing number = +49 17 17 64 35 24 '00' ⇒ test message '00' ⇒ GSM standard alphabet '00 60 52 31 63 15 00' ⇒ SMSC time stamp = 00 06 25 13 36 51 00 ⇒ 25.06.0013 : 36 : 51,time zone 0 (GMT) '17' ⇒ 23 ⇒ number of characters in the message is 23 'C8 A0 93 28 AC 0E 91 20 62 51 0A 1A 22 93 D0 65 50 4A 2D 3A 01' ⇒ message: "Handbuch der Chipkarten"
Sample SMS message from a mobile telephone to the network	'07 02 81 F0 11 FF 00 81 00 00 00 08 D7 27 D3 78 0C 3A 8F FF' || remainder of record is 'FF' '07' ⇒ message to be sent to the network '02' ⇒ number of bytes in the dialing number, including this length specification ☎ '81' ⇒ unknown dialing number ☎ 'F0' ⇒ control information '11' ⇒ relative time of mobile telephone 'FF' ⇒ message reference ☎ '00' ⇒ length of the dialing number of the destination = 0 ☎ '81' ⇒ unknown dialing number ☎ '00' ⇒ test message '00' ⇒ GSM standard alphabet '00' ⇒ validity interval ☎ '08' ⇒ number of characters in the message is 8 'D7 27 D3 78 0C 3A 8F FF' ⇒ message: "WOLFGANG" Note 1: The record structure depends on the implementation in the actual mobile telephone and is not universally valid. Note 2: After this SMS record has been read from the SIM, the data elements above marked with ☎ are expanded before being sent from the mobile telephone. After the message has been sent to the network, the first byte of this data set is changed from '07' to '05'.
$DF_{TELECOM}$.EF_{SMSP}	**Short message service parameters (SMSP)**
Description:	This file belongs to the short message service. It holds the settings for sending short messages.
File:	FID = '6F42'; structure: linear fixed, record size: $(28 + n)$ bytes; accesses: READ: CHV 1; UPDATE: CHV 1

(*Cont.*)

Table 13.6 (*Cont.*)

$DF_{TELECOM}.EF_{SMSS}$	**Short message service status (SMSS)**
Description:	This file belongs to the short message service. It holds the status of the stored short messages.
File:	FID = '6F43'; structure: linear fixed, record size: $(2 + n)$ bytes; accesses: READ: CHV 1; UPDATE: CHV 1
Coding:	byte 1: last used SMS message reference number per GSM 03.40 byte 2: b1 = 0: no space for the message in the SIM memory b1 = 1: enough space for the message in the SIM memory b2 – b7: RFU; set to '1'
Example:	'70 FF' '70' ⇒ last used SMS message reference number 'FF' ⇒ memory space available in the SIM

current smart card operating systems do not treat files having this attribute any differently than files that do not have it.

It was originally planned to replace GSM smart cards every two years in order to avoid failures due to the limited number of EEPROM write/erase cycles. However, since practically no problems have arisen in this regard up to now, most network operators replace smart cards only in the event of actual failure. This yields considerable cost savings for the provider, since his logistics only have to deal with replacing defective cards. The number of cards that have to be replaced is also considerably reduced by the fact that the useful life of most cards is significantly longer than two years. This markedly decreases procurement costs, since it is only necessary to replace smart cards when they no longer work properly. Practical experience has shown that cards must be replaced every five to seven years.

Authenticating the SIM

Besides storing data, one of the primary functions of the SIM is performing authentication with respect to the GSM network. This involves a unilateral authentication of the SIM by the background system. The SIM thus does not test whether the background system is authentic; instead, the background system only tests whether the SIM is authentic. If the authenticity of the SIM is confirmed, the network operator knows that it can bill the call to the owner of the mobile telephone. However, this unilateral authentication has the disadvantage that the user of the mobile telephone cannot be certain that he is connected to an authentic network instead of a counterfeit network. As a consequence, it is possible to eavesdrop on calls using a suitable piece of equipment, called an IMSI catcher, without knowing the secret keys. The operating principle of the IMSI catcher is based on having the device establish its own radio cell by acting as a counterfeit base station, which allows it to interpose itself in the air interface between a genuine base station and the mobile telephones by representing itself as a base station to the mobile telephones and as a mobile telephone to the base station. Such an attack would not be

possible with mutual authentication followed by encryption of all call data between the SIM and the background system.

The SIM is identified using a number that is unique within the entire GSM system. This number, which has a maximum length of eight bytes, is called the 'international mobile subscriber identity' (IMSI). The subscriber can be identified using the IMSI in all GSM networks throughout the world. In order to keep the identity of the subscriber as confidential as possible within the network, whenever possible a temporary mobile subscriber identity (TMSI) is used instead of the IMSI. The TMSI is generated from the visitor location register (VLR) and is thus valid only within a portion of the GSM network in question. Nevertheless, in combination with the location area information (LAI) the TMSI is unique within the entire GSM network. For all further identification transactions, only the TMSI is used once it has been assigned. The relationship between the IMSI and the TMSI is stored in the visitor location register (VLR) for the duration of its actual use. In the exceptional case that the TMSI is not known in the VLR, the IMSI must be transmitted in cleartext over the air interface in order to identify the subscriber.

The card-specific keys for authentication and encrypting data on the air interface can be derived from the IMSI. However, the SIM cannot encrypt data for the air interface, since the processing and data transmission capacity of a smart card are not adequate for real-time encryption of voice data. Instead, the SIM computes a derived temporary key for transmission encryption and passes it to the mobile equipment. The mobile equipment has a high-performance encryption unit in the form of a signal processor, which can encrypt and decrypt voice data on the air interface in real time. The encrypted data on the air interface are usually decrypted back into cleartext by the base station controller (BSC).

If a subscriber wishes to make a call, his mobile telephone establishes a connection to the base station with the best reception and gives it the TMSI from the SIM memory along with the LAI, or in exceptional cases the IMSI. If the subscriber is located in the region of his or her home network, a 'triple' of authentication and encryption data is generated by the authentication center (AuC). This data set includes the ciphering key (Kc) for encrypting data on the air interface, a random number (RAND) and the resulting signed response (SRES). The advantage of this procedure is that the secret individual key (Ki) and the authentication algorithm, which is partly confidential, never have to leave the authentication center. This triple is then passed to the home location register (HLR).

If the mobile telephone is logged in to its home network, the triple (Kc, RAND and SRES) is sent to the appropriate visitor location register (VLR). There the result of encrypting the random number (SRES) is requested from the SIM by the mobile switching center (MSC) and compared with the result received from the AuC (SRES'). If the two results match, the SIM has been authenticated and the system can start encrypting the data on the air interface using the A5 cryptographic algorithm and associated key (Kc).

On the other hand, if the mobile telephone is logged in to a foreign network the triple is passed to the foreign network, where it can be used in the same manner as in the home network. This situation clearly shows the cleverness of this authentication and encryption scheme, since the A3 and A5 cryptographic algorithms are specific to individual network operators and cannot be computed in a foreign network, even if the secret key is known. Only the A5 cryptographic algorithm, which is used for encrypting data on the air interface, is common throughout the GSM system, in order to allow these data to be given suitable cryptographic protection if the key Kc is known.

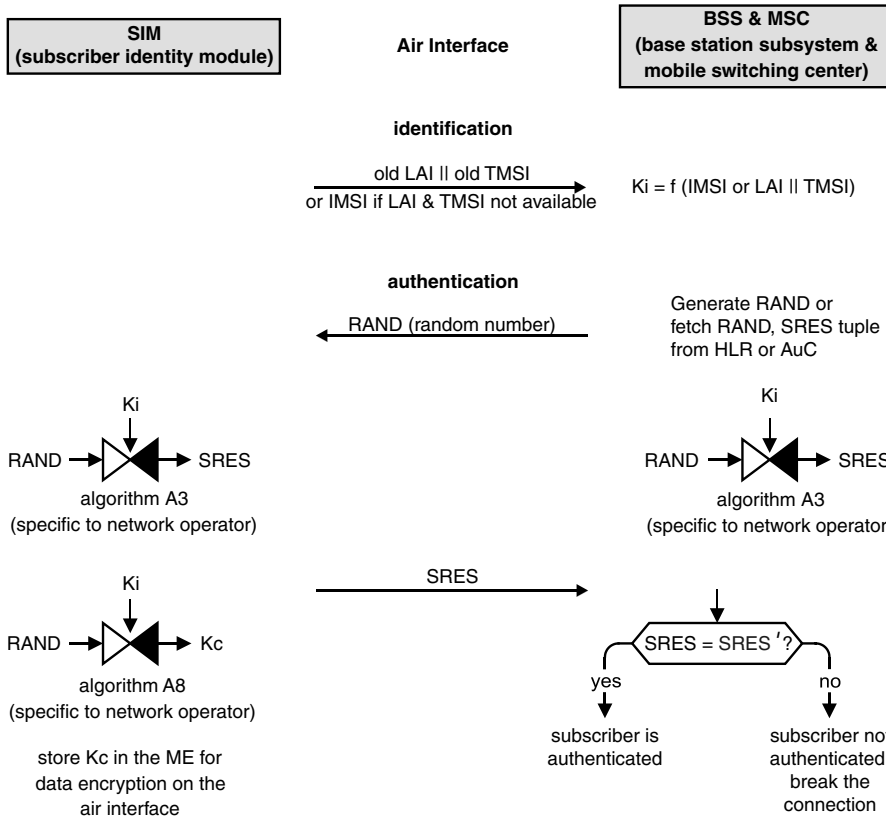

Figure 13.13 Procedure for the identification and subsequent authentication of the SIM by the GSM background system using the A3 and A8 cryptographic algorithms, which are specific to the individual network operator. Key Kc is later used for encrypting the data transmitted between the mobile station and the base station via the air interface

The cryptographic algorithms used in the GSM system are generally confidential, which is the only departure from Kerckhoff's principle[11] in this system. All other information about the system is publicly accessible. Originally, an algorithm called COPM 128 was often used for the A3 and A8 cryptographic algorithms, which are specific to individual network operators. However, this algorithm was cracked in 1998, since its key was too short. In retrospect, this shows the value of Kerckhoff's principle, since cryptologists would have probably recognized that the key was too short if the algorithm had been made public. The COMP 128 cryptographic algorithm is still presently used, but in an improved form called COMP 128-2. The A5 cryptographic algorithm, which is the same throughout the GSM system, is a stream cipher consisting of three linear feedback shift registers (LFSRs) with lengths of 19, 22 and 23 [Anderson 01], incremented by the TDMA frame number.

[11] See also Section 4.7, 'Cryptology'

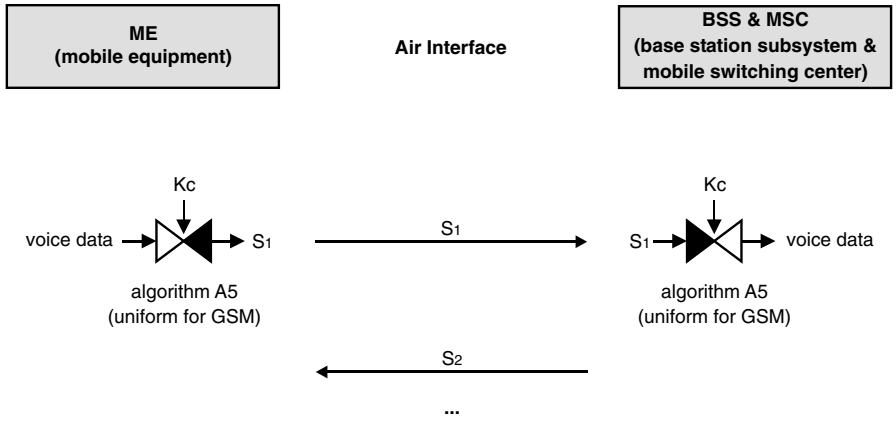

Figure 13.14 Data transmitted between the mobile station and the base station via the air interface are encrypted using the A5 cryptographic algorithm and the secret key Kc. This process must be preceded by authentication of the SIM by the GSM background system

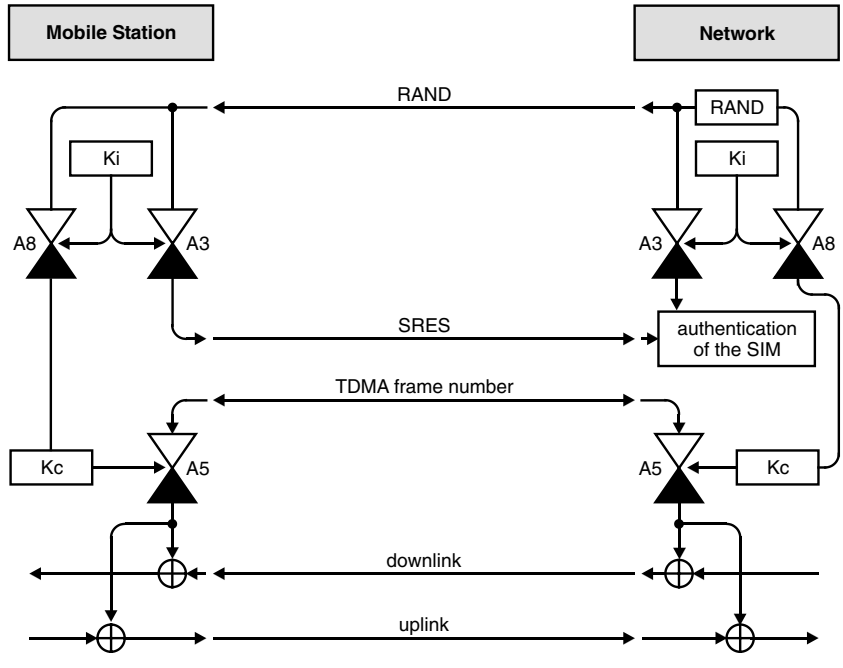

Figure 13.15 Functional overview of the cryptographic functions of the SIM, mobile equipment and background system in the GSM system

Switch-on and switch-off procedures for the mobile telephone

The procedures associated with switching a mobile telephone on and off are briefly described below, with a strong focus on the role of the SIM.

When the mobile telephone is switched on, hardware self-tests are first run and the operating system, which occupies several megabytes, is then started up. In order to distract the impatient user during the several seconds taken by this process, entertaining animations are often shown on the display. Once the operating system is fully active, one of the next steps is to initiate the activation sequence for the SIM. The activation sequence is followed by several measures for configuring the optimum transmission parameters, such as analyzing the ATR and executing a PPS procedure.[12] Following this, it is now common practice to create a virtual SIM in the memory of the mobile telephone. For this purpose, the mobile telephone reads a large amount of data from the files in the SIM, such as the abbreviated dialing numbers, and stores them in appropriate data fields in the mobile telephone. The objective of this is to ensure fast read and write access to the SIM data, which would otherwise not be possible due to the low data transmission rate between the mobile telephone and the SIM and the amount of time taken for EEPROM write accesses. Consequently, most mobile telephones primarily work with the copies of the SIM data that are located in their memories. Of course, this technique cannot be used with all of the data in the SIM. Activities such as PIN verification and authentication must always be performed in combination with the SIM, since the data needed for these activities are not allowed to leave the SIM.

One of the side effects of using a virtual SIM is that it considerably increases the life expectancy of the SIM, since a large number of EEPROM write accesses that would otherwise be necessary simply never occur. The stress on certain files within the SIM resulting from frequent write accesses is thereby considerably reduced. A typical example of this is the EF_{LOCI} file, which contains information about the current location of the mobile telephone. The EEPROM locations containing this file are especially heavily stressed in mobile telephones that frequently change GSM cells, for which reason this file has the attribute ‘high update activity’. If the data in this file are primarily updated in the RAM of the mobile telephone, the problem of an excessive number of write accesses to the EEPROM of the SIM is rendered insignificant.

The data in the virtual SIM in the memory of the mobile telephone are written back to the SIM following critical operations, so the data stored in the files in the SIM are again current data following the writeback operation. This is frequently performed asynchronously by the mobile station using a low-priority operating system task, so the user is not aware that it is happening. Updating the SIM at critical points in time is also important because the SIM should always hold essentially current data in its EEPROM in the event of a sudden loss of power, such as may happen when the batteries are removed. For instance, it would be extremely annoying if removing the batteries resulted in the loss of all of the dialing numbers painstakingly entered into the telephone since the last time the mobile telephone was switched on.

When the mobile telephone is switched off, the user usually sees only a brief sequence of animated characters on the display. However, all the files in the virtual SIM are written to the physical SIM while this is happening, in order to bring it up to date. After this, a SIM

[12] See also Section 6.2, ‘Answer to Reset (ATR)’, and Section 6.3, ‘Protocol Parameter Selection (PPS)’

Listing 13.1 Typical activities of a mobile telephone that are related to the SIM, shown in proper temporal sequence. The portrayed activities and command sequences correspond to a typical mobile telephone, although it must be borne in mind that the GSM specifications generally leave the relevant details to the manufacturer of the mobile telephone. In this example, the SIM used in the mobile telephone essentially has only the functionality necessary for making telephone calls, with the exception of the files for abbreviated dialing numbers and short messages. In the case of a SIM or mobile telephone with a greater range of functions, the activities of the two communicating parties would increase accordingly.

The user switches on the mobile telephone.	
Perform SIM activation sequence	Activate the SIM.
Receive ATR	Determine whether a SIM is present and ascertain the parameters of the transmission protocol.
Execute PPS	Modify the transmission protocol parameters as necessary.
The mobile telephone has now established a working communications link with the SIM.	
SELECT DF_{GSM} GET RESPONSE	Select the GSM directory and retrieve information about the directory.
SELECT EF_{PHASE} READ BINARY	Select and read the EF containing the phase data.
SELECT EF_{LP} GET RESPONSE READ BINARY	Select the language preference EF, retrieve information about the file structure and read the file.
The user enters a PIN. VERIFY CHV STATUS	Test the PIN, and then query the state of the retry counter.
SELECT EF_{SST} GET RESPONSE READ BINARY	Select the SIM service table EF, retrieve information about the file structure and read the file.
TERMINAL PROFILE	Transfer information about the properties of the mobile telephone to the SIM. (important for SIM Toolkit applications)
SELECT MF	Select the root directory.
SELECT EF_{ICCID} GET RESPONSE READ BINARY	Select the ICC identification number EF, retrieve information about the file structure and read the file.
SELECT DF_{GSM}	Select the GSM directory.

SELECT EF_{IMSI} GET RESPONSE READ BINARY	Select the international mobile subscriber identity EF, retrieve information about the file structure and read the file.
SELECT EF_{AD} GET RESPONSE READ BINARY	Select the administrative data EF (which contains the administrative data for the mobile station), retrieve information about the file structure and read the file.
SELECT EF_{LOCI} READ BINARY	Select and read the location information EF.
SELECT EF_{KC} READ BINARY	Select and read the cipher key EF.
SELECT EF_{BCCH} READ BINARY	Select and read the broadcast control channels EF, which contains network-specific information.
SELECT EF_{FPLMN} READ BINARY	Select and read the forbidden PLMN EF.
SELECT EF_{HPLMN} READ BINARY	Select and read the HPLMN search period EF.
SELECT $DF_{TELECOM}$	Select the telecom directory.
SELECT EF_{SMSS} GET RESPONSE READ BINARY	Select the SMS status EF (which contains information about stored messages), retrieve information about the file structure and read the file.
SELECT EF_{SMSP} GET RESPONSE READ BINARY	Select the SMS parameters EF, retrieve information about the file structure and read the file.
SELECT EF_{SMS} GET RESPONSE n × READ RECORD	Select the SMS EF, retrieve information about the file structure and read all *n* records of the file.
SELECT EF_{ADN} GET RESPONSE n × READ RECORD	Select the abbreviated dialing numbers EF, retrieve information about the file structure and read all *n* records of the file.
The mobile telephone is now ready to make a call or transmit data.	
The user makes a call. SELECT DF_{GSM}	Select the GSM directory.
RUN GSM ALGORITHM GET RESPONSE	Authenticate the SIM with respect to the background system.

SELECT EF_{KC} UPDATE BINARY	Select the cipher key (Kc) EF and write the updated cipher key to the EF.
SELECT EF_{LOCI} UPDATE BINARY	Select the location information EF and write the updated location information to the EF.
SELECT EF_{BCCH} UPDATE BINARY	Select the broadcast control channels EF and write network-specific data to the EF.
The user switches off the mobile telephone.	
SELECT EF_{LOCI} UPDATE BINARY	Select the location information EF and write the updated location information to the EF.
SELECT EF_{BCCH} UPDATE BINARY	Select the broadcast control channels EF and write network-specific data to the EF.

deactivation sequence is executed and the operating system of the mobile telephone is then shut down.

The procedures and mechanisms just described are not part of the GSM specification. Consequently, they are generally implemented in completely different manners in different types of mobile telephones. What has been described here should be regarded as only a possible and technically effective implementation. With the GSM system in particular, it should also be borne in mind that it is quite common for mobile telephones that are already 10 years old to still be in use. It can confidently be assumed that such telephones do not have virtual SIMs, but instead perform all read and write operations directly in the SIM.

Example of a typical command sequence

Reading dialing numbers from an EF with a record-oriented structure, such as EF_{ADN}, is a practical example of a typical command sequence. The first step is to select the appropriate file in the proper directory. Since the number of records in the file is left up to the network operator, the first thing that must be done is to determine the size of the file. The number of entries is then calculated from the file size and the record length. After this, each record containing a dialing number can be read using READ RECORD with the number of the record in question. This process is shown in detail in Figure 13.16.

SIM Application Toolkit

In the original specifications for the GSM system, the GSM card was simply seen as a means to identify the user using PIN and an authentication token, in the interest of billing security, that was independent of the mobile telephone. However, in the course of time the desire to utilize the GSM card for additional functions, particularly supplementary services, became increasingly pronounced. For instance, a mobile telephone is also a competent medium for checking the balance of a bank account or receiving vital news, such as football scores and

Terminal		SIM
SELECT FILE	→	
Command [$DF_{TELECOM}$]		return code := file selection result
IF (return code = OK)	←	*Response* [return code]
THEN file successfully selected		
ELSE abort		
SELECT FILE	→	
Command [EF_{ADN}]		return code := file selection result
IF (return code = OK)	←	*Response* [return code]
THEN file successfully selected		
ELSE abort		
GET RESPONSE	→	Ascertained file size s
		Ascertained record length m
IF (return code = OK)	←	*Response* [s || m || return code]
THEN command successfully executed		
ELSE abort		
Computer number of records n		
n := s ÷ m		
VERIFY CHV	→	Test CHV
Command [CHV 1]		return code: = result of CHV testing
IF (return code = OK)	←	*Response* [return code]
THEN CHV testing successful		
ELSE abort		
FOR x := 1 TO n {		
READ RECORD	→	
Command [record number n]		
IF (return code = OK)	←	*Response* [record data || return code]
THEN record successfully read		
ELSE abort }		

Figure 13.16 Basic command sequence for reading the abbreviated dialing numbers from the EF_{ADN} file. The illustrated sequence shows only the essential aspects of the process and assumes that all commands are successfully executed

daily horoscopes. However, the modest capabilities of the GSM were not sufficient to permit the technical implementation of these value-added services (VAS). The response to this was the development of the GSM 11.14 specification, entitled 'SIM Application Toolkit' (SAT). The first version of this specification was published in 1996 by ESTI.

The SIM Application Toolkit enables the SIM to directly access functions of the mobile station, such as driving the display, polling the keypad, sending short messages and other functions needed in connection with a value-added service. Ultimately, the SIM Application Toolkit is a construction kit that allows almost any desired application to be implemented in a SIM.

A number of new commands had to be defined for the SIM Application Toolkit. A noteworthy feature of these commands is that they are sent to the mobile equipment by the SIM, which requires a certain change in mental attitude. The data part of these 'proactive' commands is

BER-TLV coded.[13] This makes it possible to easily achieve expansion capability while ensuring downward compatibility. However, the greatest advantage of this is the enormous flexibility obtained by using TLV-coded data.

With the SIM Application Toolkit, it was necessary to devise a way to circumvent the usual master–slave arrangement between the terminal and the smart card for the SIM, but for reasons of compatibility, modifying the transmission protocol was not allowed. The solution to this problem was relatively simple. In a process called 'polling', the mobile equipment sends the query command STATUS to the SIM at a definable regular interval (such as every 20 seconds), and if necessary the SIM can indicate in its response that a command for the mobile equipment is ready to be sent and should be fetched from the SIM. In practice, the polling interval is not maintained all that exactly by the mobile equipment, but this is not critical. This circumvention of the master–slave principle is designated 'proactivity of the SIM', and the associated commands are called 'proactive commands'.

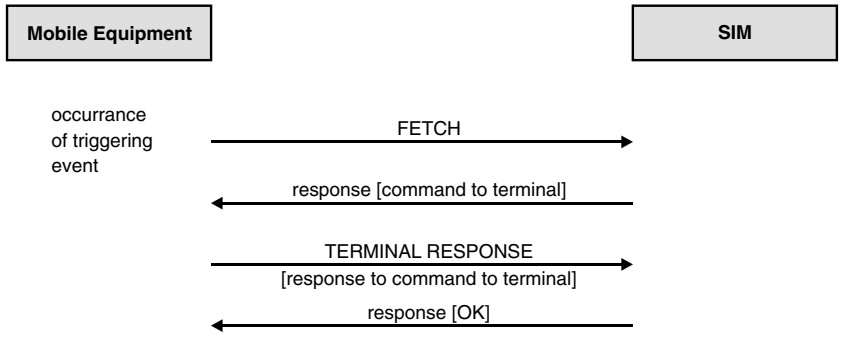

Figure 13.17 The extended protocol process between the mobile equipment and the SIM for the proactive commands of the SIM Application Toolkit, as specified in GSM 11.14. The response of the smart card to a command contains a command to the terminal in the data part. The terminal executes this command and returns the associated response to the smart card in the data part of a command. The sequence shown here is based on the transmitted APDUs and shows only successful results

This technique effectively reverses the master–slave relationship between the mobile equipment and the SIM. This makes it possible for the card, acting on its own initiative, to poll the keypad, show its own data and menu structures on the display of the mobile telephone and emit a beep sound. The SMS mechanism can also be used to exchange data between the SIM and the GMS background system via the air interface. For instance, a news server can be regularly polled in this manner, with the result being presented on the display of the mobile telephone as an e-mail or short message.

The commands that make this mechanism possible are FETCH, TERMINAL RESPONSE and ENVELOPE. The mobile equipment uses FETCH to retrieve a command from the SIM. After processing this command, the mobile equipment returns the associated result to the SIM using TERMINAL RESPONSE. The ENVELOPE command allows data to be transferred to the SAT application of the mobile equipment.

In addition to this proactivity, the SIM can also inform the mobile equipment of certain events for which the SIM must be immediately notified if they occur.

[13] See also Section 4.1, 'Structuring Data'

Table 13.7 The proactive SIM smart card commands specified for the SIM Application Toolkit in GSM 11.14. Note that the commands listed here are sent to the terminal by the smart card, rather than from the terminal to the smart card as usual. Certain commands can only be used if they are supported by the hardware configuration of the mobile equipment

Command	Brief description
User interface	
DISPLAY TEXT	Show a text or icon passed with the command on the display of the mobile station.
GET INKEY	Show a text or icon passed with the command on the display of the mobile station, followed by requesting a character from the keypad.
GET INPUT	Show a text or icon passed with the command on the display of the mobile station, followed by requesting one or more characters from the keypad.
LANGUAGE NOTIFICATION	Advise the mobile equipment of the language used by the SIM Application Toolkit in the text fields.
PLAY TONE	Instruct the mobile equipment to issue a tone.
SELECT ITEM	Transfer a selection list to the mobile equipment with the instruction that the user is to select an item.
SET UP IDLE MODE TEXT	Show a text or icon passed with the command on the display of the mobile station while the mobile station is switched on but not in use.
SET UP MENU	Transfer a menu list to the mobile equipment with the instruction to integrate it into the menu structure of the mobile equipment.
Second card terminal	
GET READER STATUS	Request the status of a supplementary card terminal in the mobile station.
PERFORM CARD APDU	Send an APDU to the smart card located in a supplementary card terminal in the mobile station.
POWER OFF CARD	Deactivate the smart card located in a supplementary card terminal in the mobile station.
POWER ON CARD	Activate the smart card located in a supplementary card terminal in the mobile station.
Network interface	
CLOSE CHANNEL	Instruct the mobile equipment to close a data channel.
GET CHANNEL STATUS	Instruct the mobile equipment to return the status of a data channel.
OPEN CHANNEL	Instruct the mobile equipment to open a data channel.
RECEIVE DATA	Instruct the mobile equipment to receive data via an open data channel.
RUN AT COMMAND	Transfer an AT command to the mobile equipment and execute the command in the mobile equipment, followed by passing the result back to the SIM.
SEND DATA	Instruct the mobile equipment to transmit data via an open data channel.
SEND DTMF	Transmit a DTMF during a current voice connection.
SEND SHORT MESSAGE	Transmit a short message.

Table 13.7 (*Cont.*)

Command	Brief description
SEND SS	Transmit a supplementary service (SS) message, which is a control sequence, to the network.
SEND USSD	Transmit an unstructured supplementary services data (USSD) message, which can be used to send any desired type of data.
SET UP CALL	Establish a connection.
Miscellaneous	
MORE TIME	Request the mobile equipment to give the SAT application more time for processing.
POLL INTERVAL	Start cyclic polling of the SIM and specify the interval.
POLLING OFF	Stop cyclic polling of the SIM.
PROVIDE LOCAL INFORMATION	Request the mobile equipment to provide current location information to the SIM.
REFRESH	Advise the mobile equipment that the data content of the SIM has changed, so it should read this data anew.
SET UP EVENT LIST	Transfer an event list to the mobile equipment with the request to inform the SIM if one of these events occurs.
TIMER MANAGEMENT	Start, end or configure the eight possible timers in the mobile equipment that can generate an event.
LAUNCH BROWSER	Start a microbrowser supported by the smart card operating system.

There are several different ways to launch SAT-based supplementary services in the SIM. The simplest manner involves an action on the part of the user. For example, if the user selects a certain function from the menu of the mobile telephone and this function is based on a supplementary SIM application, a corresponding command is sent to the SIM by the mobile equipment. The further course of events is then determined by the value-added service in the SIM. However, certain events in the mobile telephone, such as call setup, call termination or changing network cells, can be used to invoke a SAT-based application in the SIM. The simplest method for invoking a SAT application in the SIM is cyclic polling of the SIM by the mobile equipment. In practice, it is possible to implement SIM-based value-added services at a relatively moderate cost using these three basic invocation methods.

The actual capability for controlling supplementary services in the SIM Application Toolkit is achieved using executable program code, which can be generated using any desired programming language, such as assembler, C or Java.

The typical sequence of events with a SIM Application Toolkit application is as follows: first, following the activation sequence of the SIM, various types of data are read by the mobile equipment, including the EF_{Phase} file, which indicates which GSM phase the SIM supports. If the code for Phase 2+ is stored in the EF_{Phase} file, the terminal concludes that the SIM Application Toolkit is fully supported. Following this, the terminal uses the TERMINAL PROFILE command to inform the SIM of its properties that are relevant to the SIM Application Toolkit. This completes the initialization, and any other commands related to the GSM application that do not belong to the SIM Application Toolkit can then be sent as necessary.

Typically, the next process is installing a selection menu in the mobile equipment. This is done by placing BER-TLV coded data for the menu in the response to a FETCH command requested by the SIM and sent by the mobile equipment. The mobile equipment then integrates the new selection menu into its menu structure and acknowledges having done so with a confirmation in the subsequent TERMINAL RESPONSE command. The selection menu is thus installed in the mobile equipment and activated. After this, the usual GSM commands can be exchanged and processed. As soon as the user of the mobile telephone selects a menu entry, the ENVELOPE command is sent to the SIM with information about the selected menu entry. The SIM confirms receipt of the command and can then start a wide variety of processes belonging to the application and user selection.

For example, a share price on the stock exchange could be requested as the result of selecting a SIM application. This function can be implemented in a wide variety of manners. One simple method would be to send an SMS message to a server of the network operator with a request for the current share price for a particular company. If this request is successfully processed, the server could then send a SMS reply message to inform the application in SIM of the share price, and the application could then advise the mobile telephone user of the current share price using a DISPLAY TEXT command.

This is only a very simple example of what can be done using the SIM Application Toolkit, but clearly shows that the SIM Application Toolkit is a very powerful tool for producing value-added services in the SIM, and that it is relatively easy to implement such services. Things can start to become difficult when a value-added service must be implemented using functions of the mobile equipment that are not supported by the SIM Application Toolkit. Other well-known hindrances to SAT-based applications are the large variety of methods for presenting data on the display and fundamental incompatibilities or implementation errors in the mobile equipment. However, all of these hurdles can be overcome with a certain amount of effort and experience. In summary, it can thus be said that the SIM Application Toolkit is still the most technically mature and secure means to implement value-added services in mobile telephones. The SIM Application Toolkit forms a very powerful interface for value-added services in the SIM, and it can be integrated into the existing system without any modifications.

The ETSI Project Smart Card Platform (EP SCP) expert group is in the process of defining a generic foundation for all application toolkits for smart cards in mobile telecommunications, based on the SIM Application Toolkit. This toolkit will be called the Card Application Toolkit (CAT), and it will form the basis for the SIM Application Toolkit (SAT), the USIM Application Toolkit (USAT) and the UIM Application Toolkit (UATK).

Over-the-air (OTA) communication

After a SIM has been issued, it is sometimes necessary to establish a direct connection from the background system to the SIM. This type of communication is particularly essential for managing existing applications and generating new value-added services in the SIM. Consequently, mechanisms have been created in the GSM 03.48 specification to allow secure end-to-end communications to be established between the background system and the SIM via the air interface.

Since this requirement was not dealt with by the original GSM specifications and it is nearly impossible to make changes in a system of this magnitude, a trick is used for end-to-end

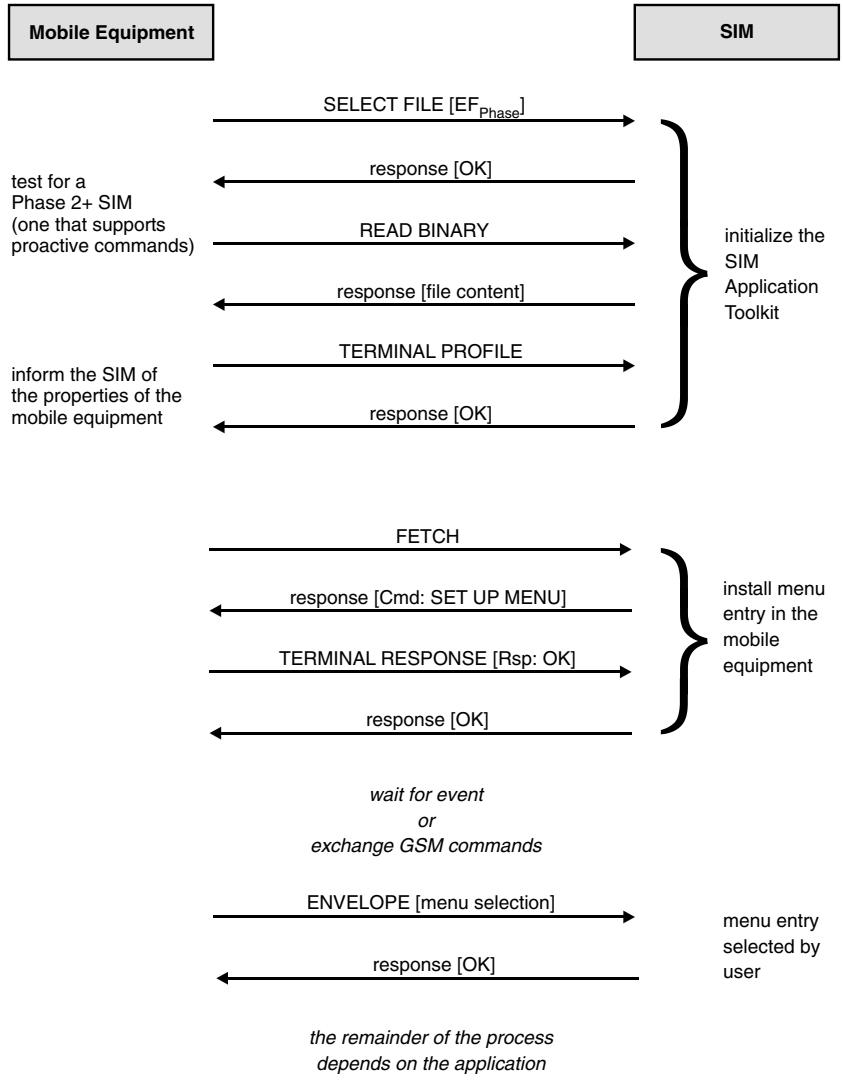

Figure 13.18 Typical example of using the SIM Application Toolkit to install a supplementary menu entry in the mobile equipment. The procedure illustrated here is based on the transmitted APDUs and shows only successful command execution

communication with the GSM card. The short messages available in the system are used as containers for messages to and from the SIM. All that this requires is modifications to the background system and issuing new smart cards, with all intermediate systems remaining unchanged. Nevertheless, short messages are presently only one of several possible bearers for OTA, although they are the most widely used type.

OTA communication offers a relatively wide range of protective mechanisms for the transmitted data. For instance, the simplest security level consists of using a CRC checksum to protect the data against transmission errors. In the realm of cryptographic protection, it is also

possible to provide the data with a send sequence counter and encrypt them using DES or triple DES (with two or three keys). If necessary, a MAC or digital signature can also be computed for the data to be transmitted.

The operating principle of using the SMS as a bearer service is as follows. If the background system wishes to send a command (for example) to a particular SIM, it generates a short message to the card in question and embeds the command in the message, using the necessary cryptographic protective mechanisms. As soon as a mobile station containing the SIM in question logs in to the system, the short message is transmitted via the signaling channel. This does not require establishing a voice connection via a traffic channel. Based on the coding of the message as specified in GSM 03.40, the mobile equipment recognizes that the message contains SIM-specific data and uses the SIM Application Toolkit ENVELOPE command to send it to the SIM. The message is thus not automatically stored in the EF_{SMS} file by the mobile equipment using the UPDATE RECORD command, as is otherwise usual. The SIM stores the message received via the ENVELOPE command in a separate buffer. If the message is part of a set of chained messages, the next task of the SIM is to restore the correct sequence of the messages, since as is well known, SMS does not ensure that messages are received in the proper order.

The SIM then interprets the received message, extracts the command or commands from it and processes it or them. A SMS message may optionally be generated by the SIM as a response. This message is transferred to the mobile equipment in the response to a FETCH command requested by the SIM, and the mobile equipment forwards it to the background system in the usual manner via the service channel.

With this trick, it is possible to establish a bidirectional end-to-end link between the background system and the SIM that is fully transparent to all of the intermediate system components. This allows the SIM to be addressed just as though it were located in a terminal connected to a PC. This communications channel can be used for tasks such as modifying existing data in files as part of remote file management. A common use for OTA communication is updating the service dialing numbers stored in the SIM. It can also be used to carry out significantly more complex tasks. For instance, it can be used to download executable program code in the form of applets for supplementary applications in SIMs based on Java Card. The possibilities that OTA communication offers to the network operator are immense. Unfortunately, many parts of GSM 03.48 do not represent a specification, which is precisely defined at the bit level, but instead a standard, which offers a wide range of options, not all of which are specified in detail, that can be used by individual card manufacturers for their SIMs in the manner that best suits their purposes. This naturally has detrimental consequences for the mutual compatibility of SIMs from different manufacturers, which must be compensated in normal network operation by libraries in the background system of the network operator that are specific to the various smart card manufacturers.

Remote file management (RFM)

The mechanisms provided by OTA allow direct end-to-end communication between the background system and the SIM. This forms the basis (with regard to data transmission technology) for the remote management of the files in the SIM, which is called remote file management (RFM) in GSM terminology. This bearer-independent basic

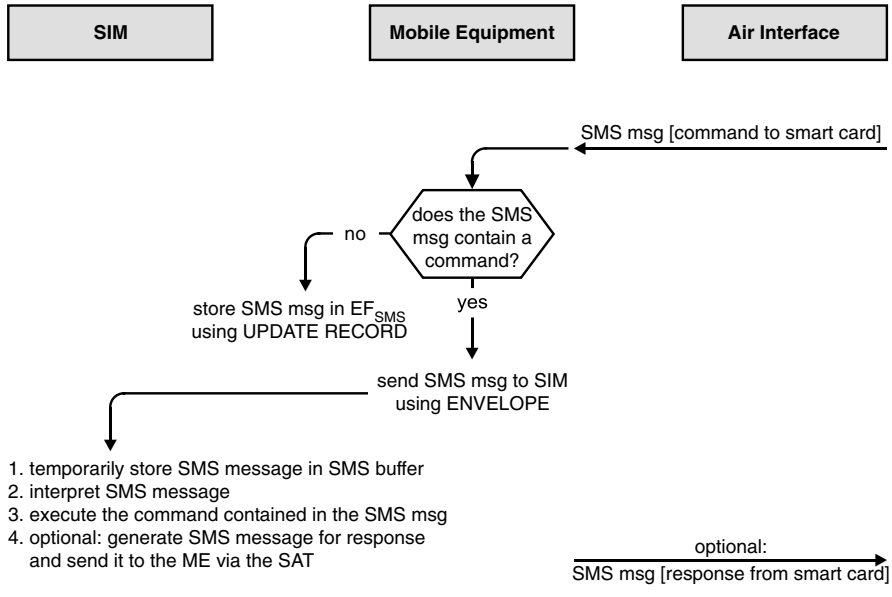

Figure 13.19 Procedure for exchanging data using SMS messages passed between the background system and the GSM card. This procedure is commonly called 'over the air' (OTA) communication

functionality is specified in GSM 03.48, which is in turn based on the requirements of GSM 02.48.

Only certain SIM commands are allowed to be used for remote file management, but it is possible to achieve a broad scope of functionality using these commands. They are divided into input commands, which send data to the SIM, and output commands, which request data from the SIM. The background system is allowed to send not only individual commands to the SIM within an OTA message, but also lists containing several commands. However, such lists are subject to the restriction that only the final command in the list is allowed to request data from the SIM. The reason for this restriction, which does not cause any difficulties in practice, is primarily that it significantly simplifies the remote file management software in the SIM. Due to this restriction, several OTA messages must be sent to the SIM if several files or records have to be read.

Table 13.8 Smart card commands allowed to be sent to the SIM for remote file management, as specified by GSM 03.48

Input commands		Output commands
SELECT	VERIFY CHV	READ BINARY
UPDATE BINARY	CHANGE CHV	READ RECORD
UPDATE RECORD	DISABLE CHV	GET RESPONSE
SEEK	ENABLE CHV	
INCREASE	UNBLOCK CHV	
	INVALIDATE	
	REHABILITATE	

The operating principle of remote file management using SMS as a bearer service can briefly be explained using a typical practical example. If a background system wants to modify an abbreviated dialing number stored in the EF_{ADN} file, it can proceed as follows. In the first OTA message, which may consists of a series of SMS messages, it selects the EF_{ADN} file by means of a SELECT command specifying the path within the $DF_{Telecom}$ directory. The final command in this OTA message is a READ RECORD command with a record number known to the background system, which causes the service number to be read from the file and returned via OTA. If this service number is not current, an UPDATE RECORD command is sent to the SIM using another OTA message, and the appropriate record is overwritten with the new number.

Naturally, caution must be exercised in using remote file management to modify files that are significant for an open session. A typical example of such files is EF_{SST}, which contains the SIM service table. This table lists all the available and potentially activated services of the SIM. Under certain conditions, modifying the content of this file can cause the mobile telephone to behave unpredictably, and in the worst case it can render the SIM unusable.

The SIM also contains two EFs for which modification is simply forbidden. These are the EF_{ICCID} file, which holds the identification number of the smart card (ICCID), and the EF_{Kc} file, which holds the key for encrypting data transmitted between the mobile station and the base station via the air interface. From a logical perspective, it makes no sense to modify either of these files, since the ICCID is a unique identification number for the smart card and plays no role in normal operation. The key (Kc) is always computed by the SIM for each session, so it would be pointless to modify it via RFM. If it is nevertheless modified during an open session, the connection to the network might be broken, since the mobile equipment would use an incorrect key for encrypting data on the air interface.

Remote applet management

The GSM 03.48 specification also contains a section related to remote applet management, which is similar to remote file management. Remote applet management makes it possible to manage applications based on Java Card via a direct end-to-end link between the background system and the SIM.

A general prerequisite is that the smart card in question must be a SIM that is compliant with GSM 03.19, which is essentially based on the Java Card 2.1 specifications.[14] All management commands for applets and packages are based on the Open Platform specification, which is effectively the industry standard for these mechanisms.[15]

The application management functions include loading, installing, deleting, locking and unlocking Java applets in the SIM and retrieving parameters from these Java applets. Similar mechanisms are defined for loading packages into the SIM and deleting packages from the SIM.

All of the procedures and mechanisms are basically independent of any particular bearer service, but the SMS is presently the most commonly used means for managing applets and packages in SIMs via OTA. If SMS is used as the bearer, data transmission to and from the SIM takes place in exactly the same manner as described above for remote file management using OTA.

[14] See also Section 5.14.1, 'Java Card'
[15] See also Section 5.11, 'Open Platform'

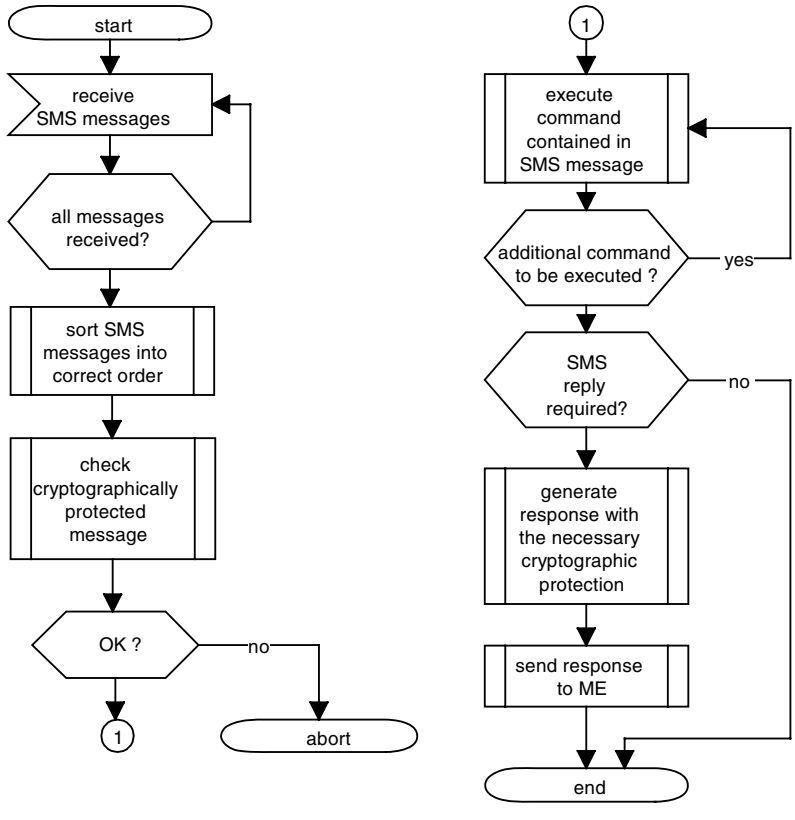

Figure 13.20 Flow chart of the basic program sequence for remote file management (RFM) via the air interface using OTA, as specified in GSM 03.48. Remote file management is essentially performed by the processes shown in the upper right branch of the flow chart, with the remainder of the processes serving to establish secure communications in accordance with GSM 03.48

Table 13.9 Smart card commands allowed to be sent to the SIM for remote applet management via the air interface, as specified by GSM 03.48. These commands correspond to the Open Platform specification with regard to functionality and coding

Input commands	Output commands
DELETE	READ BINARY
SET STATUS	READ RECORD
INSTALL	GET RESPONSE
LOAD	
PUT KEY	

Dual IMSI

In the commercial realm, accrued call charges for a mobile telephone belonging to a company are usually paid by the company in question. However, if a person having such a mobile telephone also uses it for private calls, he or she must later settle the charges for such calls with the company, which is only possible with an itemized telephone bill. In practice, such a person will probably make private calls at the expense of the company, otherwise he or she must carry two telephones in order to make both business and private calls. Needless to say, this is too much to expect. This scenario is the reason why there are 'dual-IMSI' mobile telephones, which contain SIMs having an additional file holding two IMSIs and possibly also two Ki keys, depending on the implementation. This file is actually not part of any standard. A supplementary SAT-based application in the SIM generates a new menu entry in the mobile equipment that allows the user to select whether he or she wishes to make a business call or a private call. Depending on the user's selection, a particular IMSI is copied to the EF_{IMSI} file, and if necessary a different, related Ki key is used. This means that the mobile telephone has two different identities in terms of the IMSI, and the network operator can generate two separate bills. This makes it possible to charge separately for business calls and private calls.

This capability can be further extended, for example by activating the fixed dialing numbers for the IMSI used for business calls, thus limiting the possible dialing numbers to a particular set of numbers. This means that the user of such a mobile telephone cannot charge private calls to the company, since only the numbers related to the company can be dialed. If the second IMSI is activated using the value-added service in the SIM, the fixed dialing numbers are deactivated and the company is not billed for the calls. In this way, a single mobile telephone can be used to make both business and private calls without creating problems in settling the calling charges.

There is yet another use for multiple IMSIs, which it is not very elegant from a technical perspective. If IMSIs for several different network operators are stored in a SIM such that they can be individually selected by the user via a menu, the mobile telephone can be used for manual roaming. The user selects the IMSI belonging to the network in whose territory he or she happen to be located, and can then log into this network using the selected IMSI. The user will then receive a telephone bill from each network operator as appropriate. This sort of roaming using multiple IMSIs is practiced in large parts of India, for example, since regular roaming agreements between some of the network operators do not exist.

Implementing a home zone

Some network operators offer person-specific special rates for restricted local regions. Such a region is usually an approximately circular zone defined around the place of residence of the subscriber, within which calls are charged at the rate for the fixed network instead of the more expensive rate for the mobile network. For the user, the primary benefits of this type of location-specific service are that he or she no longer needs a connection to the fixed telephone network, and that it eliminates the need to coordinate two sets of abbreviated dialing numbers (one for the regular telephone and another one for the mobile telephone).

The most suitable way to implement such a service is to use a value-added service in the SIM and the functions of the SIM Application Toolkit. This also ensures that all information

about the home zone is stored in the person-specific SIM, rather than somewhere else such as in the mobile telephone.

In the GSM system, each base station continuously transmits a unique identifier via the air interface. This identifier consists of the location area information (LAI) and a cell identity (CI). One approach to implementing home zone capability would be to have the mobile telephone pass this information to the SIM, where it could be compared with one or more stored values. These values would preferably be stored in a file, so that they could be modified or updated at any desired time using remote file management. The drawback of this approach is the relatively large amount of memory needed in the SIM, since it is fundamentally necessary to accommodate regions with a high density of base stations, which would lead to large LAI and CI lists.

A similar approach would be to use the advance timing information of the air interface. With this approach, the current location of a mobile station could be determined to within significantly less than 10 meters by using cross-polling. This is more than adequate for implementing a home zone.

However, in practice a different solution is often preferred, in which all of the base stations belonging to a network operator periodically transmit their location coordinates on the signaling channel using the cell broadcast service.[16] The SIM has an EF containing reference values, which are read by the mobile equipment and compared with the received location coordinates. If the mobile equipment determines that the mobile telephone is located within the home zone, a suitable symbol (such as a small house icon) is shown on the display. Since the background system knows the location of the mobile telephone, it can switch incoming and outgoing calls over to a more favorable rate. The data for the coordinates of the home zone are stored in an EF in the SIM, so they can be easily modified using remote file management. This also allows home zones to be conveniently established or changed to a different location using remote maintenance. The drawback of this solution is that it requires special software in the mobile equipment, instead of being implemented as a value-added service in the SIM using the SIM Application Toolkit.

Operating principle of SIM Lock

SIM Lock is the name given to a technique for binding the mobile equipment to a particular SIM or group of SIMs. The SIM Lock function is used by network operators to bind mobile telephones subsidized by a network operator to a particular SIM and its payment mode for a certain length of time. It is based on the GSM 02.22 specification. The operating principle of the SIM Lock is always based on data that are stored in both the SIM and the mobile equipment and are compared by one of the two components each time the mobile telephone is switched on, with the telephone only being enabled for use if the two sets of data match.

There are two practical implementations of the SIM Lock function. With the more commonly used option, the mobile telephone reads certain data from the SIM and compares them with data stored in the mobile telephone. This usually consists of the group identifiers, which are stored in the EF_{GID1} (group identifier level 1) and EF_{GID2} (group identifier level 2) files. These

[16] Harald Bögeholz and Dusan Zivadinovic, 'Telefon-Zellen', c't 1999, Volume 18

group identifiers can be used to specify classes of SIMs, which can then be used to specify class-based pairings of particular SIMs to particular (subsidized) items of mobile equipment. The advantage of this variant is that the SIM and the mobile equipment do not have to be individually 'married'. The IMSI from the EF_{IMSI} file, or other static SIM-specific data stored in EFs, is sometimes used instead of the group identifiers as a reference value for forming pairs.

The second option, which is rarely used in practice, involves having the SIM use the SIM Application Toolkit to read unique data from the mobile equipment and compare it with stored data. If these data match, the mobile telephone can be used to make the desired call after being enabled by the SIM.

It is usually possible to disable the SIM Lock function, either via the air interface or by entering a secret key into the mobile telephone, in order to allow other SIMs to be used in mobile equipment previously protected by a SIM Lock. The reference value for this is usually the individual mobile equipment identity (IMEI) of the mobile equipment in question.

Operating principle of prepaid systems

The proportion of prepaid SIMs ranges from around 30 % to as much as 80 %, depending on the country. The principal reasons why people use prepaid SIM are that they provide better control of costs and avoid the need to pay subscription charges.

The operating principle of a system designed to work with prepaid SIMs is generally as follows. A card-shaped voucher, which often has the dimensions of an ID-1 card but is not as thick, has a 13-digit number printed underneath a rub-off coating, which acts as a seal. If a user wishes to 'reload' his mobile telephone, he or she purchases a voucher, whose integrity can be verified by the fact that the rub-off coating is still intact. After rubbing off the coating covering the number, the user must enter the now-visible number into her mobile telephone using a special menu. This reference value is immediately passed to the background system, where it is compared with the reference value for the issued voucher, which is stored in a database. If the result of the comparison is positive and if the voucher has not already been used, the load amount associated with the reference value is credited to the SIM in question.

At this point, the possible implementations diverge. The solution originally envisaged in the GSM specifications was a units counter in a file (the accumulated call meter file EF_{ACM}), whose value would be continuously updated by advice of charge data from the mobile equipment and compared with the value stored in the 'accumulated call meter maximum value' file (EF_{ACMmax}) by the SIM. If the actual value reached the maximum value, the mobile telephone would prohibit further calls until the actual value was again reset, which could be done via remote file management or some other means. Although this solution is certainly technically feasible, it is not used in practice, since communications between the mobile equipment and the SIM are not secure and thus could be manipulated relatively easily.

In practice, prepaid SIMs are managed by a centralized system, with two different approaches being used. The first approach entirely dispenses with using supplementary data in the SIM and runs entirely in the background system. The drawback of this approach is that the background system computer must have real-time capability, which increases its cost. With the second approach, a suitable value-added service must be present in the SIM, but there is

no need for general real-time capability in the background system. The disadvantage of this approach is that when the prepaid amount has been used up, there may be a delay before the connection is broken.

A typical background system for prepaid SIMs, which does not necessarily have to have real-time capability, can be described using the components shown in Figures 13.21 and 13.22. A number of supplementary components must be integrated into an existing GSM system in order to support prepaid SIMs. In this example, one of these components is the call management subsystem, which is a supplementary component of the mobile switching center (MSC) that can route or prohibit calls in real time, and which maintains an interface to the prepaid system. The prepaid system is the central component of the system, whose task is to coordinate the call management subsystem and the billing system. In the billing system, the credit balances in the individual SIM accounts are managed using a database. With this arrangement, the SIM contains only a few special commands along with corresponding data.

When a call to a mobile telephone arrives in the background system, the first thing that happens is that the call management subsystem advises the prepaid system that a call to particular mobile telephone having a particular SIM is pending. The prepaid system then has the billing system calculate the maximum allowable length of the call, based on the outstanding credit balance for the SIM, and passes this information to the call management subsystem. If the credit balance is sufficient, the call management subsystem routes the call. It will also interrupt the call if the maximum call duration is reached. On completion of the call, the call management subsystem informs the prepaid system of the duration of the call, and the prepaid system uses this information to update the credit balance of the account via the billing system. The updated balance can then be shown on the display of the mobile telephone.

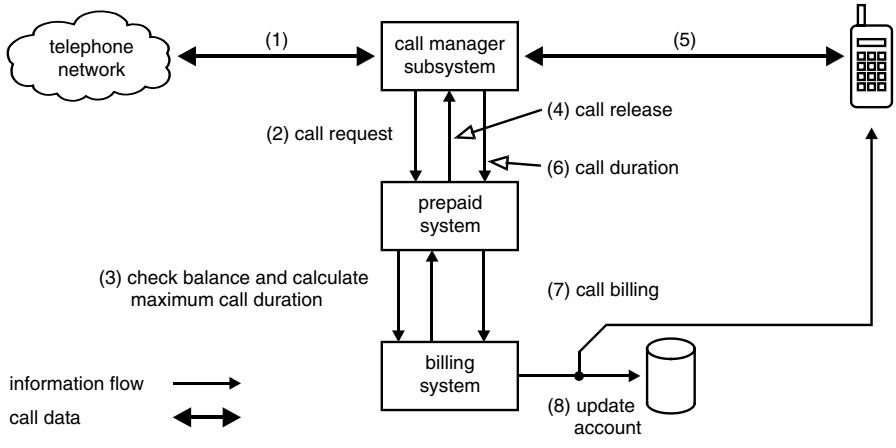

Figure 13.21 Basic architecture of a system for prepaid SIMs using the SICAP Prepaid Roaming solution as an example. This diagram shows the progress of a call made to a mobile telephone, with the numbers in parentheses indicating the sequence of events. The call management subsystem is part of the GSM background system, and may for example be a component of the mobile switching center (MSC)

When a call is made from a mobile telephone, a similar process occurs. First, the maximum allowable call duration is computed via a USSD query to the prepaid system and the billing

system and then passed to the call management subsystem. If the maximum duration is reached during the call, the call is interrupted. Otherwise, the balance of the call account is updated on completion of the call and the corresponding amount is stored in the database. Naturally, the remaining credit can also optionally be displayed on the mobile telephone.

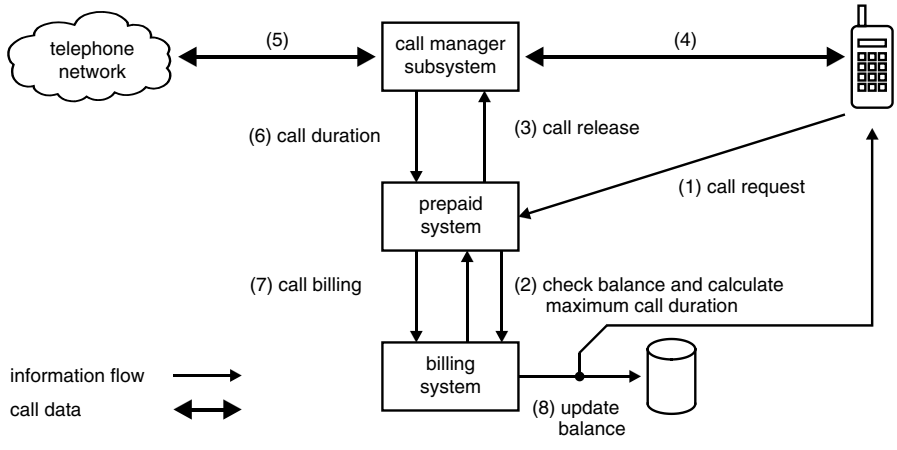

Figure 13.22 Basic architecture of a system for prepaid SIMs using the SICAP Prepaid Roaming solution as an example. The diagram shows the progress of a call originating from the mobile telephone, with the numbers in parentheses indicating the sequence of events. The call management subsystem is part of the GSM background system, and may for example be a component of the mobile switching center (MSC)

13.2.5 General Packet Radio System (GPRS)

The General Packet Radio System (GPRS) is an extension of the original GMS system. It has been defined as an ETSI standard, and its purpose is to provide a packet-switched data service with a high data transmission rate, as specified in GSM 01.60 ('Requirements specification of GPRS') and GSM 02.60 ('Service description; Stage 1'). GPRS can be dynamically adapted to actual capacity demand, so only the actually necessary capacity is used. A maximum data transmission rate of 115.2 kbit/s can be achieved by bundling the eight available time slots, each of which has a capacity of 14,400 kbit/s. A mobile telephone with GPRS technology is constantly logged in to the network with respect to data transport, and thus always available for data transmission without requiring a connection to first be established for this purpose. Consequently, GPRS is highly suitable for discontinuous data transmission. GPRS also forms the basis for mobile telecommunications services based on the Internet protocol (IP).

With regard to system architecture, GPRS is based on a GSM system augmented by several new components. The serving GPRS support node (SGSN), which coordinates the exchange of data packets with the mobile equipment at the MSC level, is analogous to the MSC. The SGSN is subordinate to a gateway GPRS support node (GGSN), whose primary function is to provide an interface to other packet-switched data services, such as X.25 and IP. The GGSN transforms GPRS-specific data packets into packets corresponding to the other packet-switched services

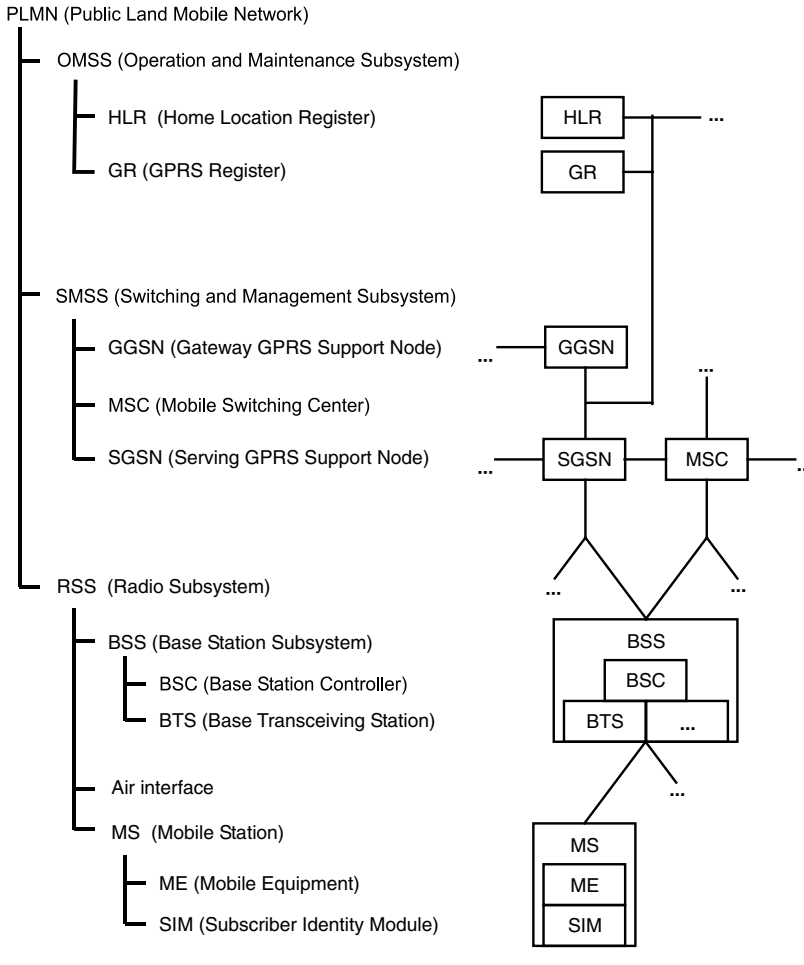

Figure 13.23 Architecture of a portion of a GSM network belonging to a single network operator, with a superimposed GPRS network as specified by GSM 01.60 and GSM 02.60

and vice versa. The central component of the system is the GPRS register (GR), which is analogous to the HLR and manages all of the data related to specific GPRS subscribers.

13.2.6 Future developments

The GMS application represented the international breakthrough for smart cards, and it is still *the* standard for smart cards and smart card operating systems. Compared with the latest developments in the smart card world, some of the commands and mechanisms in the GSM realm may appear outdated, but GSM was and still is the pioneer for large international smart card applications. Ultimately, all subsequent applications can only learn and benefit from the experience gained and problems encountered using this application. In many respects, GSM in

the form of the GSM 11.11 and 11.14 specifications forms the foundation for all more recent and more sophisticated smart card applications.

Recent models of mobile telephones are incorporating an increasing number of the functions of personal digital assistants (PDAs), in addition to pure telephone functions. Since it is relatively difficult to externally manipulate the software of a mobile telephone, it can be considered to be a trusted device. The consequences of this can be seen in many service functions and telephones with hardware extensions. For example, there are mobile telephones with IrDA-compliant infrared interfaces or Bluetooth interfaces, as well as mobile telephones with larger and more powerful displays.

This makes it technically possible to use mobile telephone to make payments from an electronic purse at a suitably equipped POS station. If the user has to enter a PIN, in the future he can do so using his relatively tamper-proof telephone keypad instead of an unfamiliar terminal. The corresponding data can be exchanged using an infrared or Bluetooth interface, with no need to establish (and pay for) a telephone connection. The potential uses of such capabilities are extremely varied, so they can only be outlined in broad terms at present.

For a variety of reasons, dual-slot mobile telephones have failed to achieve widespread use. This is probably more due to the business strategies of network operators than technical reasons, such as the size of the mobile telephone. Up to now, network operators have shown little interest in encouraging the use of third-party applications in the smart cards of their highly subsidized mobile equipment. Presently, the development trend is focused on value-added services in SIMs. The wide-scale introduction of digital signature applications as part of WIM, which despite its name cannot be used for WAP, at least creates the necessary technical conditions for the entire spectrum of mobile business applications.

A microbrowser implemented in the SIM will doubtless continue to form the basis for secure data-based applications in the coming years, which could inevitably lead to a market shakeout between this technology and GSM-capable Java cards. However, in the first instance the primary uses for the latter types of cards will be in the area of value-added services based on program code.

MExE (Mobile Station Execution Environment) is a framework for integrating procedures defined by the network operator and executable program code into the mobile station. Stage 1 of MExE specifies the integration of WAP browsers for the WML markup language in the mobile equipment. The subsequent step, Stage 2, adds a Java virtual machine (JVM) to these functions. This allows Java programs to be loaded into mobile telephones and run there, and it allows value-added services to be implemented directly in the mobile telephone, rather than in the SIM (as is presently common).

CAMEL (Customized Applications for Mobile Enhanced Logic) provides the GSM network with a new option that extends functionality in the direction of intelligent networks (IN). With CAMEL, it is for example possible for the network to modify dialing numbers during call setup. This would permit services such as international roaming with prepaid cards or standardized international service numbers to be implemented significantly more simply than at present.

Even an established system such as GSM must be further developed in order to meet new requirements and satisfy additional customer desires. This is presently taking place in small steps, and it has led to modifications and extensions such as proactive SIM commands, OTA, WIM, microbrowsers and RFM, as well as extended capabilities such as HSCSCD, GPRS and EDGE. Nevertheless, at some point in time it will be necessary to make a major evolutionary step in order to convert all of these extensions, modifications and special cases

into a new system that is once again self-contained. This new system will be the Universal Mobile Telecommunication System (UMTS), which provisionally can be expected to exist alongside the GSM system for many years, and which may at some time supplant the GMS system.