1

Global System for Mobile Communications (GSM)

At the beginning of the 1990s, GSM, the Global System for Mobile Communications triggered an unprecedented change in the way people communicate with each other. While earlier analog wireless systems were used by only a few people, GSM was used by over 1.5 billion subscribers worldwide at the end of 2005. This has mostly been achieved by the steady improvements in all areas of telecommunication technology and due to the steady price reductions for both infrastructure equipment and mobile phones. The first chapter of this book discusses the architecture of this system, which also forms the basis for the packet-switched extension called GPRS, discussed in Chapter 2, and for the Universal Mobile Telecommunications System (UMTS), which is described in Chapter 3. While the first designs of GSM date back to the middle of the 1980s, GSM is still the most widely used wireless technology worldwide and it is not expected to change any time soon. Despite its age and the evolution towards UMTS, GSM itself continues to be developed. As will be shown in this Chapter, GSM has been enhanced with many new features in recent years. Therefore, many operators continue to invest in their GSM networks in addition to their UMTS activities to introduce new functionality and to lower their operational cost.

1.1 Circuit-Switched Data Transmission

The GSM mobile telecommunication network has been designed as a circuit-switched network in a similar way to fixed-line phone networks. At the beginning of a call, the network establishes a direct connection between two parties, which is then used exclusively for this conversation. As shown in Figure 1.1, the switching center uses a switching matrix to connect any originating party to any destination party. Once the connection has been established, the conversation is then transparently transmitted via the switching matrix between the two parties. The switching center only becomes active again to clear the connection in the switching matrix if one of the parties wants to end the call. This approach is identical in both mobile and fixed-line networks. Early fixed-line telecommunication networks were only

Communication Systems for the Mobile Information Society Martin Sauter

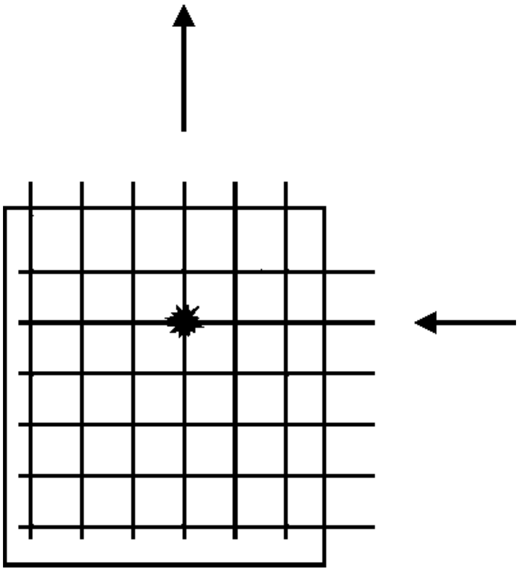


Figure 1.1 Switching matrix in a switching center

designed for voice communication for which an analog connection between the parties was established. In the mid-1980s, analog technology was superseded by digital technology in the switching center. This means that today, calls are no longer sent over an analog line from originator to terminator. Instead, the switching center digitizes the analog signal it receives from the subscribers, which are directly attached to it, and forwards the digitized signal to the terminating switching center. There, the digital signal is again converted back to an analog signal which is then sent over the copper cable to the terminating party. In some countries ISDN (Integrated Services Digital Network) lines are quite popular. With this system, the transmission is fully digital and the conversion back into an analog audio signal is done directly in the phone.

GSM reuses much of the fixed-line technology that was already available at the time the standards were created. Thus, existing technologies such as switching centers and long-distance communication equipment were used. The main development for GSM was the means to wirelessly connect the subscribers to the network. In fixed-line networks, subscriber connectivity is very simple as only two dedicated wires are necessary per user. In a GSM network, however, the subscribers are mobile and can change their location at any time. Thus, it is not always possible to use the same input and output in the switching matrix for a user as in fixed-line networks.

As a mobile network consists of many switching centers, with each covering a certain geographical area, it is not even possible to predict in advance which switching center a call should be forwarded to for a certain subscriber. This means that the software for subscriber management and routing of calls of fixed-line networks cannot be used for GSM. Instead of a static call-routing mechanism, a flexible mobility management architecture is necessary in the core network, which needs to be aware of the current location of the subscriber and is thus able to route calls to the subscribers at any time.

It is also necessary to be able to flexibly change the routing of an ongoing call as a subscriber can roam freely and thus might leave the coverage area of the radio transmitter

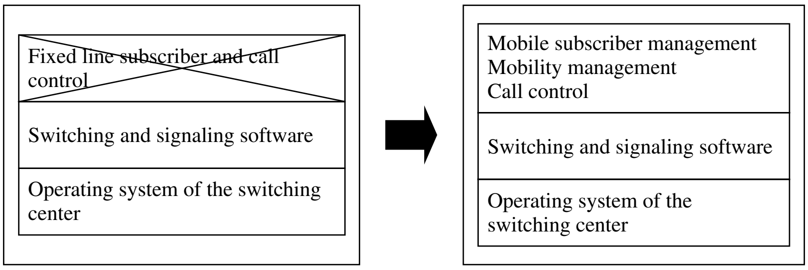

~~Fixed line subscriber and call control~~
Switching and signaling software
Operating system of the switching center
Mobile subscriber management
Mobility management
Call control
Switching and signaling software
Operating system of the switching center

Figure 1.2 Necessary software changes to adapt a fixed-line switching center for a wireless network

of the network over which the call was established. While there is a big difference in the software of a fixed and a mobile switching center, the hardware as well as the lower layers of the software which are responsible for example for the handling of the switching matrix are mostly identical. Therefore, most telecommunication equipment vendors like Siemens, Nortel, Ericsson, Nokia, or Alcatel offer their switching center hardware both for fixed-line as well as for mobile networks. Only the software in the switching center decides if the hardware is used in a fixed or mobile network (see Figure 1.2).

1.2 Standards

As many telecom companies compete globally for orders of telecommunication network operators, standardization of interfaces and procedures is necessary. Without standards, which are defined by the International Telecommunication Union (ITU), it would not be possible to make phone calls internationally and network operators would be bound to the supplier they initially select for the delivery of their network components. One of the most important ITU standards discussed in Section 1.4 is the signaling system number 7 (SS-7), which is used for call routing. Many ITU standards, however, only represent the smallest common denominator as most countries have specified their own national extensions. In practice, this incurs a high cost for software development for each country as a different set of extensions needs to be implemented in order for a vendor to be able sell its equipment. Furthermore, the interconnection of networks of different countries is complicated by this.

GSM, for the first time, set a common standard for Europe for wireless networks, which has also been adopted by many countries outside Europe. This is the main reason why subscribers can roam in GSM networks across the world that have roaming agreements with each other. The common standard also substantially reduces research and development costs as hardware and software can now be sold worldwide with only minor adaptations for the local market. The European Telecommunication Standards Institute (ETSI), which is also responsible for a number of other standards, was the main body responsible for the creation of the GSM standard. The ETSI GSM standards are composed of a substantial number of standards documents each called a technical specification (TS), which describe a particular part of the system. In the following chapters, many of those specifications will be referenced and can thus be used for further information about a specific topic. All standards are freely available on the Internet at http://www.etsi.org [1] or at http://www.3gpp.org [2], which is the organization that took over the standards maintenance and enhancement at the beginning of the UMTS standardization as described in Chapter 3.

1.3 Transmission Speeds

The smallest transmission speed unit in a telecommunication network is the digital signal level 0 (DS0) channel. It has a fixed transmission speed of 64 kbit/s. Such a channel can be used to transfer voice or data and thus it is usually not called a speech channel but simply referred to as a user data channel.

The reference unit of a telecommunication network is an E-1 connection in Europe and a T-1 connection in the United States, which use either a twisted pair or coaxial copper cable. The gross data rate of an E-1 connection is 2.048 Mbit/s and 1.544 Mbit/s for a T-1. An E-1 is divided into 32 timeslots of 64 kbit/s each while a T-1 is divided into 24 timeslots of 64 kbit/s each. One of the timeslots is used for synchronization which means that 31 timeslots for an E-1 or 23 timeslots for a T-1 respectively can be used to transfer data. In practice, only 29 or 30 timeslots are used for user data transmission while the rest (usually one or two) are used for SS-7 signaling data (see Figure 1.3). More about SS-7 can be found in Section 1.4.

Most of the time a single E-1 connection with 31 DS0s is not enough to connect two switching centers with each other. In this case E-3 connections can be used, which are also carried over twisted pair or coaxial cables. An E-3 connection is defined at a speed of 34.368 Mbit/s, which corresponds to 512 DS0s.

For higher transmission speeds and for long distances, optical systems are used which use the synchronous transfer mode (STM) standard. Table 1.1 shows some data rates and the number of 64 kbit/s DS0 channels which are transmitted per pair of fiber.

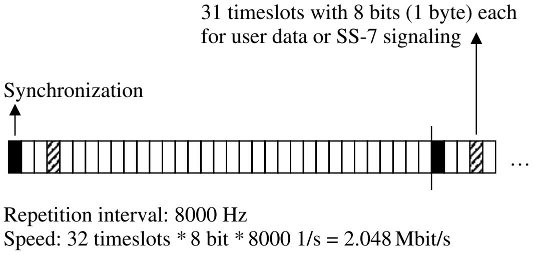

31 timeslots with 8 bits (1 byte) each
for user data or SS-7 signaling
Synchronization
…
Repetition interval: 8000 Hz
Speed: 32 timeslots * 8 bit * 8000 1/s = 2.048 Mbit/s

Figure 1.3 Timeslot architecture of an E-1 connection

Table 1.1 STM transmission speeds and number of DS0s

STM level	Speed	Approx. number of DS0 connections
STM-1	155.52 Mbit/s	2300
STM-4	622.08 Mbit/s	9500
STM-16	2488.32 Mbit/s	37,000
STM-64	9953.28 Mbit/s	148,279

1.4 The Signaling System Number 7

For establishing, maintaining, and clearing a connection, signaling information needs to be exchanged between the end user and network devices. In the fixed-line network, analog phones signal their connection request when the receiver is lifted off the hook and by dialing a phone number which is sent to the network either via pulses (pulse dialing) or via tone dialing which is called dual tone multi frequency (DTMF) dialing. With fixed-line ISDN phones and GSM mobile phones the signaling is done via a dedicated signaling channel, and information such as the destination phone number is sent via messages.

If several components in the network are involved in the call establishment, for example if originating and terminating parties are not connected to the same switching center, it is also necessary that the different nodes in the network exchange information with each other. This signaling is transparent for the user and a protocol called the signaling system number 7 (SS-7) is used for this purpose. SS-7 is also used in GSM networks and the standard has been enhanced by ETSI in order to be able to fulfill the special requirements of mobile networks, for example subscriber mobility management.

The SS-7 standard defines three basic types of network nodes:

- Service switching points (SSPs) are switching centers that are more generally referred to as network elements which are able to establish, transport, or forward voice and data connections.
- Service control points (SCPs) are databases and application software that can influence the establishment of a connection. In a GSM network, SCPs can be used for example for storing the current location of a subscriber. During call establishment to a mobile subscriber the switching centers query the database for the current location of the subscriber in order to be able to forward the call. More about this procedure can be found in Section 1.6.3 about the home location register.
- Signaling transfer points (STPs) are responsible for the forwarding of signaling messages between SSPs and SCPs as not all network nodes have a dedicated link to all other nodes of the network. The principal functionality of an STP can be compared to an IP router in the Internet, which also forwards packets to different branches of the network. Unlike IP routers however, STPs only forward signaling messages which are necessary for the establishing, maintaining, and clearing of a call. The calls themselves are directly carried on dedicated links between the SSPs.

Figure 1.4 shows the general structure of an SS-7 circuit-switched telecommunication network and how the nodes described above are interconnected with each other.

1.4.1 The SS-7 Protocol Stack

SS-7 comprises a number of protocols and layers. A well-known model for describing telecommunication protocols and different layers is the OSI 7 layer model which is used in Figure 1.5 to show the layers on which the different SS-7 protocols reside.

The message transfer part 1 (MTP-1) protocol describes the physical properties of the transmission medium on layer 1 of the OSI model. Thus, this layer is also called the physical layer. Properties that are standardized in MTP-1 are for example the definition of the different kinds of cables that can be used to carry the signal, signal levels, and transmission speeds.

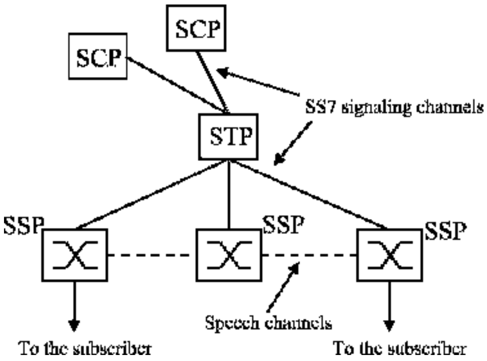
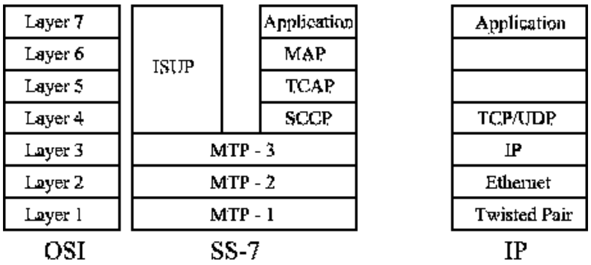


Figure 1.4 An SS-7 network with an STP, two SCP databases, and three switching centers



OSI	SS-7		IP
Layer 7	ISUP	Application	Application
Layer 6		MAP	
Layer 5		TCAP	
Layer 4		SCCP	TCP/UDP
Layer 3	MTP - 3		IP
Layer 2	MTP - 2		Ethernet
Layer 1	MTP - 1		Twisted Pair

Figure 1.5 Comparison of the SS-7, OSI, and TCP/IP protocol stacks

On layer 2, the data link layer, messages are framed into packets and a start and stop identification at the beginning and end of each packet is inserted into the data stream so the receiver is able to detect where a message ends and a new message begins.

Layer 3 of the OSI model, which is called the network layer, is responsible for packet routing. In order to enable network nodes to forward incoming packets to other nodes, each packet gets a source and destination address on this layer. This is done by the MTP-3 protocol of the SS-7 stack. For readers who are already familiar with the TCP/IP protocol stack it may be noted at this point that the MTP-3 protocol fulfills the same tasks as the IP protocol. Instead of IP addresses, however, the MTP-3 protocol uses so-called point codes to identify the source and the destination of a message.

A number of different protocols are used on layers 4 to 7 depending on the application. If a message needs to be sent for the establishment or clearing of a call the ISDN user part (ISUP) protocol is used. Figure 1.6 shows how a call is established between two parties by using ISUP messages. In the example, party A is a mobile subscriber while party B is a fixed-line subscriber. Thus, A is connected to the network via a mobile switching center (MSC) while B is connected via a fixed-line switching center.

In order to call B, the phone number of B is sent by A to the MSC. The MSC then analyzes the national destination code of the phone number, which usually comprises the first two to four digits of the number, and detects that the number belongs to a subscriber in the fixed-line network. In the example shown in Figure 1.6, the MSC and the fixed-line

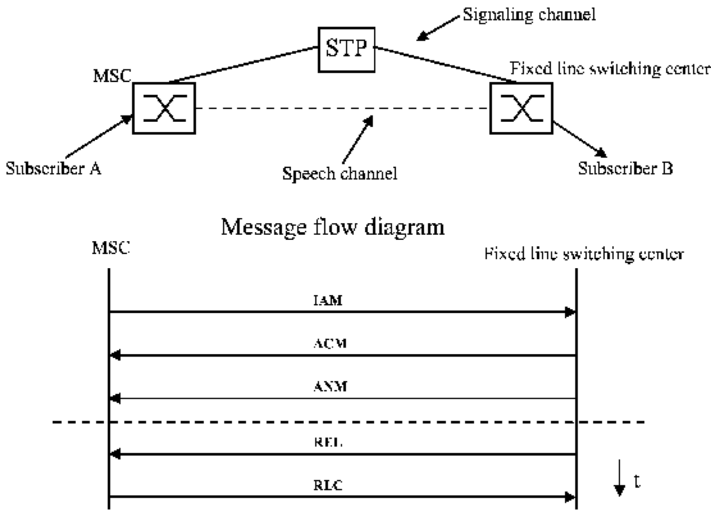


Figure 1.6 Establishment of a voice call between two switching centers

switching center are directly connected with each other. Therefore, the call can be directly forwarded to the terminating switching center. This is quite a realistic scenario as direct connections are often used if for example a mobile subscriber calls a fixed-line phone in the same city.

As B is a fixed-line subscriber, the next step for the MSC is to establish a voice channel to the fixed-line switching center. This is done by sending an ISUP initial address message (IAM). The message contains among other data the phone number of B and informs the fixed-line switching center and the channel which the MSC would like to use for the voice path. In the example, the IAM message is not sent directly to the fixed-line switching center. Instead, an STP is used to forward the message.

On the other end, the fixed-line switching center receives the message, analyzes the phone number, and establishes a connection via its switching matrix to subscriber B. Once the connection is established via the switching matrix, the switch applies a periodic current to the line of the fixed-line subscriber so the fixed-line phone can generate an alerting tone. To indicate to the originating subscriber that the phone number is complete and the destination party was found, the fixed-line switch sends back an address complete message (ACM). The MSC then knows that the number is complete and that the terminating party is being alerted of the incoming call.

If B answers the call, the fixed-line switching center sends an answer message (ANM) to the MSC and conversation can start.

When B ends the call, the fixed-line switching center resets the connection in the switching matrix and sends a release (REL) message to the MSC. The MSC confirms the termination of the connection by sending back a release complete (RLC) message. If A had terminated the call the messages would have been identical with only the direction of the REL and RLC reversed.

For the communication between the switching centers (SSPs) and the databases (SCPs), the signaling connection and control part (SCCP) is used on layer 4. SCCP is very similar to TCP and UDP in the IP world. Protocols on layer 4 of the protocol stack enable the distinction of different applications on a single system. TCP and UDP use ports to do this. If a PC for example is used as a web server and FTP server at the same time, both applications would be accessed over the network via the same IP address. However, while the web server can be reached via port 80, the FTP server waits for incoming data on port 21. Therefore, it is quite easy for the network protocol stack to decide which application to forward incoming data packets. In the SS-7 world, the task of forwarding incoming messages to the right application is done by SCCP. Instead of port numbers, SCCP uses subsystem numbers (SSNs).

For database access, the transaction capability application part (TCAP) protocol has been designed as part of the SS-7 family of protocols. TCAP defines a number of different modules and messages that can be used to query all kinds of different databases in a uniform way.

1.4.2 SS-7 Protocols for GSM

Apart from the fixed-line network SS-7 protocols, the following additional protocols were defined to address the special needs of a GSM network.

The mobile application part (MAP): this protocol has been standardized in 3GPP TS 29.002 [3] and is used for the communication between an MSC and the home location register (HLR) which maintains subscriber information. The HLR is queried for example if the MSC wants to establish a connection to a mobile subscriber. In this case, the HLR returns the information about the current location of the subscriber. The MSC is then able to forward the call to the responsible switching center for the mobile subscriber by establishing a voice channel between itself and the next hop by using the ISUP message flow that has been shown in Figure 1.6. MAP is also used between two MSCs if the subscriber moves into the coverage area of a different MSC while a call is ongoing. As shown in Figure 1.7, the MAP protocol uses the TCAP, SCCP, and MTP protocols on lower layers.

The base station subsystem mobile application part (BSSMAP): this protocol is used for the communication between the MSC and the radio network. Here, the additional protocol is necessary for example to establish a dedicated radio channel for a new connection to a mobile subscriber. As BSSMAP is not a database query language like the MAP protocol, BSSMAP is based on SCCP directly instead of using TCAP in between.

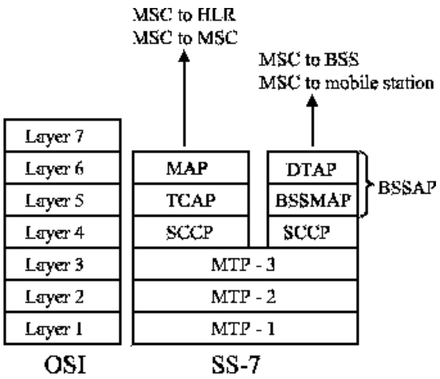


Figure 1.7 Enhancement of the SS-7 protocol stack for GSM

The direct transfer application part (DTAP): this protocol is used between the user's mobile phone, which is also called mobile station (MS), to communicate transparently with the MSC. In order to establish a voice call the MS sends a setup message to the MSC. As in the example in Section 1.4.1, this message contains among other things the phone number of the called subscriber. As it is only the MSC's task to forward calls, all network nodes between the MS and the MSC forward the message transparently and thus need not understand the DTAP protocol.

1.5 The GSM Subsystems

A GSM network is split into three subsystems which are described in more detail below:

- The base station subsystem (BSS), which is also called 'radio network', contains all nodes and functionalities that are necessary to wirelessly connect mobile subscribers over the radio interface to the network. The radio interface is usually also referred to as the 'air interface'.
- The network subsystem (NSS), which is also called 'core network', contains all nodes and functionalities that are necessary for switching of calls, for subscriber management and mobility management.
- The intelligent network subsystem (IN) comprises SCP databases which add optional functionality to the network. One of the most important optional IN functionality of a mobile network is the prepaid service, which allows subscribers to first fund an account with a certain amount of money which can then be used for network services like phone calls, SMS messages, and of course data services via GPRS and UMTS as described in Chapters 2 and 3. When a prepaid subscriber uses a service of the network, the responsible IN node is contacted and the amount the network operator charges for a service is deducted from the account in real time.

1.6 The Network Subsystem

The most important responsibilities of the NSS are call establishment, call control, and routing of calls between different fixed and mobile switching centers and other networks. Other networks are, for example, the national fixed-line network which is also called the public standard telephone network (PSTN), international fixed-line networks, other national and international mobile networks, and voice over IP (VoIP) networks. Furthermore, the NSS is responsible for subscriber management. The nodes necessary for these tasks are shown in Figure 1.8 and are further described in the next sections.

1.6.1 The Mobile Switching Center (MSC)

The mobile switching center (MSC) is the central element of a mobile telecommunication network, which is also called a public land mobile network (PLMN) in the standards. All connections between subscribers are managed by the MSC and are always routed over the switching matrix even if two subscribers that have established a connection communicate over the same radio cell. The management activities to establish and maintain a connection are part of the call control (CC) protocol, which is generally responsible for the following tasks:

- Registration of mobile subscribers: when the mobile station (MS) is switched on, it registers to the network and is then reachable by all other subscribers of the network.
- Call establishment and call routing between two subscribers.
- Forwarding of SMS (short messaging service) messages.

As subscribers can roam freely in the network, the MSC is also responsible for the mobility management (MM) of subscribers. This activity is comprises the following tasks:

- Authentication of subscribers at connection establishment: this is necessary because a subscriber cannot be identified as in the fixed network by the pair of copper cables over which the signaling arrives. Authentication of subscribers and the authentication center are further discussed in Section 1.6.4.
- If no active connection exists between the network and the mobile station, the MSC has to report a change of location to the network in order to be reachable for incoming calls and SMS messages. This procedure is called location update and is further described in Section 1.8.1.
- If the subscriber changes its location while a connection is established with the network, the MSC is part of the process that ensures that the connection is not interrupted and is rerouted to the next cell. This procedure is called handover and is described in more detail in Section 1.8.3.

In order to enable the MSC to communicate with other nodes of the network, it is connected to them via standardized interfaces as shown in Figure 1.8. This allows network operators to buy different components for the network from different network vendors.

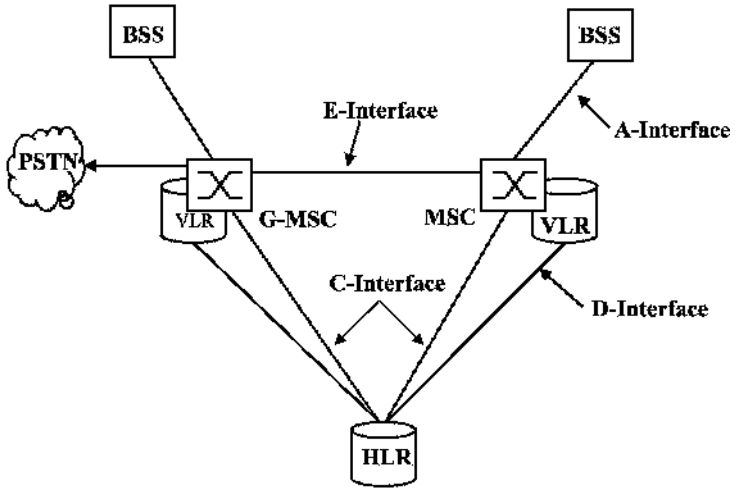


Figure 1.8 Interfaces and nodes in the NSS

The base station subsystem (BSS), which connects all subscribers to the core network, is connected to the MSCs via a number of 2 Mbit/s E-1 connections. This interface is called the A-interface. As has been shown in Section 1.4 the BSSMAP and DTAP protocols are used over the A-interface for communication between the MSC, the BSS, and the mobile stations. As an E-1 connection can only carry 31 channels, many E-1 connections are necessary to connect an MSC to the BSS. In practice, this means that many E-1s are bundled and sent over optical connections such as STM-1 to the BSS. Another reason to use an optical connection is that electrical signals can only be carried over long distances with great effort and it is not unusual that an MSC is over 100 kilometers away from the next BSS node.

As an MSC only has a limited switching capacity and processing power, a PLMN is usually composed of dozens or even hundreds of independent MSCs. Each MSC thus covers only a certain area of the network. In order to ensure connectivity beyond the immediate coverage area of an MSC, E-1s, which are again bundled into optical connections, are used to interconnect the different MSCs of a network. As a subscriber can roam into the area that is controlled by a different MSC while a connection is active, it is necessary to change the route of an active connection to the new MSC (handover). The necessary signaling connection is called the E-interface. ISUP is used for the establishment of the speech path between different MSCs and the MAP protocol is used for the handover signaling between the MSCs. Further information about the handover process can be found in Section 1.8.3.

The C-interface is used to connect the MSCs of a network with the home location register (HLR) of the mobile network. While the A-and E-interface, described previously, always consist of signaling and speech path links, the C-interface is a pure signaling link. Speech channels are not necessary for the C-interface as the HLR is a pure database which cannott accept or forward calls. Despite being only a signaling interface, E-1 connections are used for this interface. All timeslots are used for signaling purposes or are unused.

As has been shown in Section 1.3, a voice connection is carried on a 64 kbit/s E-1 timeslot in a circuit-switched fixed line or mobile network. Before the voice signal can be forwarded, it needs to be digitized. For an analog fixed-line connection this is done in the switching center, while an ISDN fixed-line phone or a GSM mobile phone digitizes the voice signal themselves.

An analog voice signal is digitized in three steps: in the first step, the bandwidth of the input signal is limited to 300–3400 Hz in order to be able to carry the signal with the limited bandwidth of a 64 kbit/s timeslot. Afterwards, the signal is sampled at a rate of 8000 times a second. The next processing step is the quantization of the samples, which means that the analog samples are converted into eight-bit digital values that can each have a value from 0 to 255. See Figure 1.9.

The higher the volume of the input signal, the higher the amplitude of the sampled value and its digital representation. In order to be able to also transmit low-volume conversations, the quantization is not linear over the whole input range but only in certain areas. For small amplitudes of the input signal a much higher range of digital values is used than for high amplitude values. The resulting digital data stream is called a pulse code modulated (PCM) signal. Which volume is represented by which digital eight-bit value is described in the A-law standard for European networks and in the μ-law standard in North America.

The use of different standards unfortunately complicates voice calls between networks that use different standards. Therefore, it is necessary for example to convert a voice signal for a connection between France and the United States.

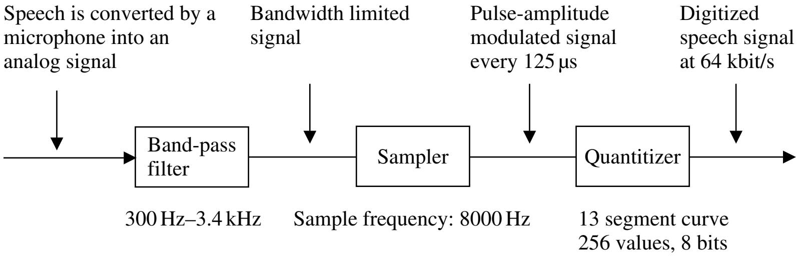

Speech is converted by a microphone into an analog signal
Bandwidth limited signal
Pulse-amplitude modulated signal every 125 µs
Digitized speech signal at 64 kbit/s
Band-pass filter
Sampler
Quantitizer
300 Hz–3.4 kHz
Sample frequency: 8000 Hz
13 segment curve
256 values, 8 bits

Figure 1.9 Digitization of an analog voice signal

As the MSC controls all connections, it is also responsible for billing. This is done by creating a billing record for each call which is later transferred to a billing server. The billing record contains information like the number of caller and calling party, cell ID of the cell from which the call was originated, time of call origination, the duration of the call, etc. Calls for prepaid subscribers are treated differently as the charging is already done while the call is running. The prepaid billing service is usually implemented on an IN system and not on the MSC as is further described in Section 1.11.

1.6.2 The Visitor Location Register (VLR)

Each MSC has an associated visitor location register (VLR), which holds a record of each subscriber that is currently served by the MSC (Figure 1.10). These records are only a copy of the original records, which are stored in the HLR (see Section 1.6.3). The VLR is mainly used to reduce the signaling between the MSC and the HLR. If a subscriber roams into the area of an MSC, the data is copied to the VLR of the MSC and is thus locally available for every connection establishment. The verification of the subscriber's record at every connection establishment is necessary, as the record contains information about which

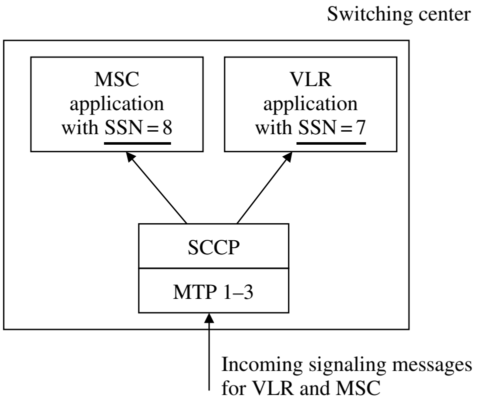

Switching center
MSC application with SSN = 8
VLR application with SSN = 7
SCCP
MTP 1–3
Incoming signaling messages for VLR and MSC

Figure 1.10 Mobile switching center (MSC) with integrated visitor location register (VLR)

services are active and from which services the subscriber is barred. Thus, it is possible, for example, to bar outgoing calls while allowing incoming calls to prevent abuse of the system. While the standards allow implementing the VLR as an independent hardware component, all vendors have implemented the VLR simply as a software component in the MSC. This is possible because MSC and VLR use different SCCP subsystem numbers (see Section 1.4.1) and can thus run on a single physical node.

When a subscriber leaves the coverage area of an MSC, the subscriber's record is copied from the HLR to the VLR of the new MSC, and is then removed from the VLR of the previous MSC. The communication with the HLR is standardized in the D-interface specification which is shown together with other MSC interfaces in Figure 1.8.

1.6.3 The Home Location Register (HLR)

The HLR is the subscriber database of a GSM network. It contains a record for each subscriber, which contains information about the individually available services.

The international mobile subscriber identity (IMSI) is an internationally unique number that identifies a subscriber and used for most subscriber-related signaling in the network (Figure 1.11). The IMSI is stored in the subscriber's SIM card and in the HLR and is thus the key to all information about the subscriber. The IMSI consists of the following parts:

- The mobile country code (MCC): the MCC identifies the subscriber's home country. Table 1.2 shows a number of MCC examples.
- The mobile network code (MNC): this part of the IMSI is the national part of a subscriber's home network identification. A national identification is necessary because there are usually several independent mobile networks in a single country. In the UK for example the following MNCs are used: 10 for O2, 15 for Vodafone, 30 for T-Mobile, 33 for Orange, 20 for Hutchison 3G, etc.
- The mobile subscriber identification number (MSIN): the remaining digits of the IMSI form the MSIN, which uniquely identifies a subscriber within the home network.

As an IMSI is internationally unique, it enables a subscriber to use his phone abroad if a GSM network is available that has a roaming agreement with his home operator. When the mobile phone is switched on, the IMSI is retrieved from the SIM card and sent to the MSC. There, the MCC and MNC of the IMSI are analyzed and the MSC is able to request the subscriber's record from the HLR of the subscriber's home network.

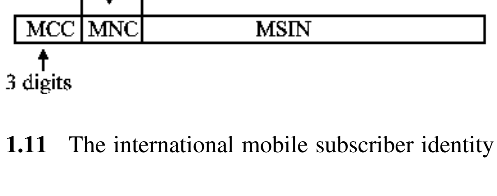
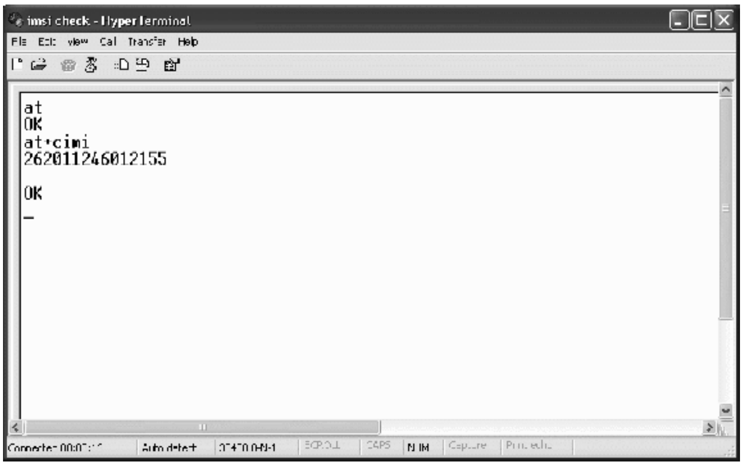


Figure 1.11 The international mobile subscriber identity (IMSI)

Table 1.2 Mobile country codes

MCC	Country
234	United Kingdom
310	United States
228	Switzerland
208	France
262	Germany
604	Morocco
505	Australia



```
at
OK
at+cimi
262011246012155

OK
_
```

Figure 1.12 A terminal program can be used to retrieve the IMSI from the SIM card

For information purposes, the IMSI can also be retrieved from the SIM card with a PC and a serial cable that connects to the mobile phone. By using a terminal program such as HyperTerminal, the mobile can be instructed to return the IMSI by using the ‘at+cimi’ command, which is standardized in 3GPP TS 27.007 [4]. Figure 1.12 shows how the IMSI is returned by the mobile phone.

The phone number of the user, which is called the mobile subscriber ISDN number (MSISDN) in the GSM standards, has a length of up to 15 digits and consists of the following parts:

- The country code is the international code of the subscriber’s home country. The country code has one to three digits such as +44 for the UK, +1 for the US, +353 for Ireland.
- The national destination code (NDC) usually represents the code with which the network operator can be reached. It is normally three digits in length. It should to be noted that mobile networks in the US use the same NDCs as fixed-line networks. Thus, it is not possible for a user to distinguish if he is calling a fixed line or a mobile phone. This

impacts both billing and routing, as the originating network cannot deduct which tariff to apply from the NDC.

- The remainder of the MSISDN is the subscriber number, which is unique in the network.

There is usually a 1:1 or 1:N relationship in the HLR between the IMSI and the MSISDN. Furthermore, a mobile subscriber is normally assigned only a single MSISDN. However, as the IMSI is the unique identifier of a subscriber in the mobile network, it is also possible to assign several numbers to a single subscriber.

Another advantage of using the IMSI as the key to all subscriber information instead of the MSISDN is that the phone number of the subscriber can be changed without replacing the user's SIM card or changing any information on it. In order to change the MSISDN, only the HLR record of the subscriber needs to be changed. In effect, this means that the mobile station is not aware of its own phone number. This is not necessary because the MSC automatically adds the user's MSISDN to the message flow for a mobile-originated call establishment so it can be presented to the called party.

Many countries have introduced a functionality called mobile number portability (MNP), which allows a subscriber to keep his MSISDN if he wants to change his mobile network operator. This is a great advantage for the subscribers and for competition between the mobile operators, but also implies that it is no longer possible to discern the mobile network to which the call will be routed from the NDC. Furthermore, the introduction of MNP also increased the complexity of call routing and billing in both fixed-line and mobile networks, because it is no longer possible to use the NDC to decide which tariff to apply to a call. Instead of a simple call-routing scheme based on the NDC, the networks now have to query a mobile number portability database for every call to a mobile subscriber to find out if the call can be routed inside the network or if it has to be forwarded to a different national mobile network.

Apart from the IMSI and MSISDN, the HLR contains a variety of information about each subscriber, such as which services he is allowed to use. Table 1.3 shows a number of 'basic services' that can be activated on a per subscriber basis:

In addition to the basic services described above, the GSM network offers a number of other services that can also be activated on a per subscriber basis. These services are called supplementary services and are shown in Table 1.4.

Table 1.3 Basic services of a GSM network

Basic service	Description
Telephony	If this basic service is activated, a subscriber can use the voice telephony services of the network. This can be partly restricted by other supplementary services which are described below
Short messaging service (SMS)	If activated, a subscriber is allowed to use the SMS
Data service	Different circuit-switched data services can be activated for a subscriber with speeds of 2.4, 4.8, 9.6, and 14.4 kbit/s data calls
FAX	Allows or denies a subscriber the use of the FAX service that can be used to exchange FAX messages with fixed-line or mobile terminals

Table 1.4 Supplementary services of a GSM network

Supplementary service	Description
Call forward unconditional (CFU)	If this service is configured, a number can be configured to which all incoming calls are forwarded immediately [5]. This means that the mobile phone will not even be notified of the incoming call even if it is switched on
Call forward busy (CFB)	This service allows a subscriber to define a number to which calls are forwarded if he is already engaged in a call when a second call comes in
Call forward no reply (CFNRY)	If this service is activated, it is possible to forward the call to a user-defined number if the subscriber does not answer the call within a certain time. The subscriber can change the number to which to forward the call to as well as the timeout value (e.g. 25 seconds)
Call forward not reachable (CFNR)	This service forwards the call if the mobile phone is attached to the network but is not reachable momentarily (e.g. temporary loss of network coverage)
Barring of all outgoing calls (BAOC)	This functionality can be activated by the network operator if, for example, the subscriber has not paid his monthly invoice in time. It is also possible for the network operator to allow the subscriber to change the state of this feature together with a PIN (personal identification number) so the subscriber can lend the phone to another person for incoming calls only [6]
Barring of all incoming calls (BAIC)	Same functionality as provided by BAOC for incoming calls [6]
Call waiting (CW)	This feature allows signaling an incoming call to a subscriber while he is already engaged on another call [7]. The first call can then be put on hold to accept the incoming call. The feature can be activated or barred by the operator and switched on or off by the subscriber
Call hold (HOLD)	This functionality is used to accept an incoming call during an already active call or to start a second call [7]
Calling line identification presentation (CLIP)	If activated by the operator for a subscriber, the functionality allows the switching center to forward the number of the caller
Calling line identification restriction (CLIR)	If allowed by the network, the caller can instruct the network not to show his phone number to the called party
Connected line presentation (COLP)	Shows the calling party the MSISDN to which a call is forwarded, if call forwarding is active at the called party side
Connected line presentation restriction (COLR)	If COLR is activated at the called party, the calling party will not be notified of the MSISDN the call is forwarded to
Multi party (MPTY)	Allows subscribes to establish conference bridges with up to six subscribers [8]

Most supplementary services can be activated by the network operator on a per subscriber basis and allow the operator to charge an additional monthly fee for some services if desired. Other services, like multi party, can be charged on a per use basis. Most services can be configured by the subscriber via a menu on the mobile phone. The menu, however, is just a graphical front end for the user and the mobile phone translates the user's commands into numerical strings which start with a '*' character. These strings are then sent to the network by using an unstructured supplementary service data (USSD) message. The codes are standardized in 3GPP TS 22.030 [9] and are thus identical in all networks. As the menu is only a front end for the USSD service, the user can also input the USSD strings himself via the keypad. After pressing the 'send' button, which is usually the button that is also used to start a phone call after typing in a phone number, the mobile phone sends the string to the HLR via the MSC, where the string is analyzed and the requested operation is performed. For example, call forwarding to another phone (e.g. 0782 192 8355), while a user is already engaged in another call (CFB), is activated with the following string: **67*07821928355# + call button.

1.6.4 The Authentication Center

Another important part of the HLR is the authentication center (AC). The AC contains an individual key per subscriber (Ki) which is a copy of the Ki in the SIM card of the subscriber. As the Ki is secret, it is stored in the AC and especially on the SIM card in a way that prevents it being read directly.

For many operations in the network, for instance during the establishment of a call, the subscriber is identified by using this key. Thus it can be ensured that the subscriber's identity is not misused by a third party. Figures 1.13 and 1.14 show how the authentication process is performed.

The authentication process is initiated when a subscriber establishes a signaling connection with the network before the actual request (e.g. call establishment request) is sent. In the first step of the process, the MSC requests an authentication triplet from the HLR/authentication center. The AC retrieves the Ki of the subscriber and the authentication algorithm (A3 algorithm) based on the IMSI of the subscriber that is part of the message from the MSC. The Ki is then used together with the A3 algorithm and a random number to generate the authentication triplet which contains the following values:

- RAND: a 128-bit random number.
- SRES: the signed response (SRES) is generated by using Ki, RAND, and the authentication A3 algorithm, and has a length of 32 bits.
- Kc: the ciphering key, Kc, is also generated by using Ki and RAND. It is used for the ciphering of the connection once the authentication has been performed successfully. Further information on this topic can be found in Section 1.7.5.

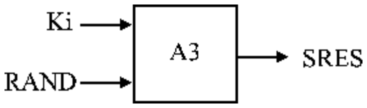


Figure 1.13 Creation of a signed response (SRES)

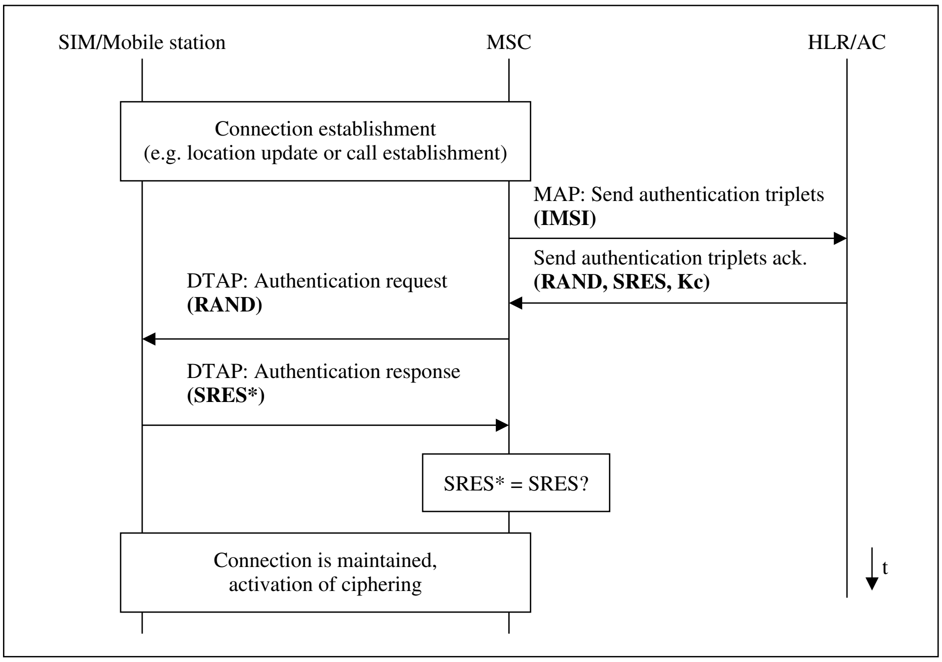

SIM/Mobile station
MSC
HLR/AC
Connection establishment
(e.g. location update or call establishment)
MAP: Send authentication triplets
(IMSI)
Send authentication triplets ack.
(RAND, SRES, Kc)
DTAP: Authentication request
(RAND)
DTAP: Authentication response
(SRES*)
SRES* = SRES?
Connection is maintained,
activation of ciphering
t

Figure 1.14 Message flow during the authentication of a subscriber

RAND, SRES, and Kc are then returned to the MSC, which then performs the authentication of the subscriber. It is important to note that the secret Ki key never leaves the authentication center.

In order to speed up subsequent connection establishments the AC usually returns several authentication triplets per request. These are buffered by the MSC/VLR and are used during the next connection establishments.

In the next step, the MSC sends the RAND inside an authentication request message to the mobile station. The terminal forwards the RAND to the SIM card which then uses the Ki and the authentication A3 algorithm to generate a signed response (SRES*). The SRES* is returned to the mobile station and then sent back to the MSC inside an authentication response message. The MSC then compares SRES and SRES* and if they are equal the subscriber is authenticated and allowed to proceed with the communication.

As the secret key, Ki, is not transmitted over any interface that could be eavesdropped on, it is not possible for a third party to correctly calculate an SRES. As a fresh random number is used for the next authentication, it is also pointless to intercept the SRES* and use it for another authentication. A detailed description of the authentication procedure and many other procedures between the mobile station and the core network can be found in [10].

Figure 1.15 shows some parts of an authentication request and an authentication response message. Apart from the format of RAND and SRES, it is also interesting to note the different protocols which are used to encapsulate the message (see Section 1.4.2).

Extract of a decoded Authentication Request message

```
SCCP MSG: Data Form 1
DEST. REF ID: 0B 02 00
DTAP MSG   LENGTH: 19
PROTOCOL DISC.: Mobility Management
DTAP MM MSG: Auth. Request
Ciphering Key Seq.: 0
RAND in hex: 12 27 33 49 11 00 98 45
             87 49 12 51 22 89 18 81 (16 byte = 128 bit)
```

Extract of a decoded Authentication Response message

```
SCCP MSG: Data Form 1
DEST. REF ID: 00 25 FE
DTAP MSG   LENGTH: 6
PROTOCOL DISC.: Mobility Management
DTAP MM MSG: Auth. Response
SRES in hex: 37 21 77 61 (4 byte = 32 bit)
```

Figure 1.15 Authentication between network and mobile station

1.6.5 The Short Messaging Service Center (SMSC)

Another important network element is the short message service center (SMSC) which is used to store and forward short messages. The short messaging service was only introduced about four years after the first GSM networks went into operation as add on and has been specified in 3GPP TS 23.040 [11]. Most industry observers were quite skeptical at the time as the general opinion was that if it is needed to convey some information, it is done by calling someone rather than to cumbersomely type in a text message on the small keypad. However, they were proven wrong and today most GSM operators generate over 15% of their revenue from the short messaging service alone with a total number of over 25 billion SMS messages exchanged annually in the United Kingdom.

The short messaging service can be used for person-to-person messaging as well as for notification purposes of received email messages or a new call forwarded to the voice mail system. The transfer method for both cases is identical.

The sender of an SMS prepares the text for the message and then sends the SMS via a signaling channel to the MSC. As a signaling channel is used, an SMS is just an ordinary DTAP SS-7 message and thus, apart from the content, very similar to other DTAP messages, such as a location update message or a setup message to establish a voice call. Apart from the text, the SMS message also contains the MSISDN of the destination party and the address of the SMSC which the mobile station has retrieved from the SIM card. When the MSC receives an SMS from a subscriber it transparently forwards the SMS to the SMSC. As the message from the mobile station contains the address of the subscriber's SMSC, international roaming is possible and the foreign MSC can forward the SMS to the home SMSC without the need for an international SMSC database. See Figure 1.16.

In order to deliver a message, the SMSC analyses the MSISDN of the recipient and retrieves its current location (the responsible MSC) from the HLR. The SMS is then forwarded to the responsible MSC. If the subscriber is currently attached, the MSC tries to contact the mobile station and if an answer is received, the SMS is forwarded. Once the mobile station

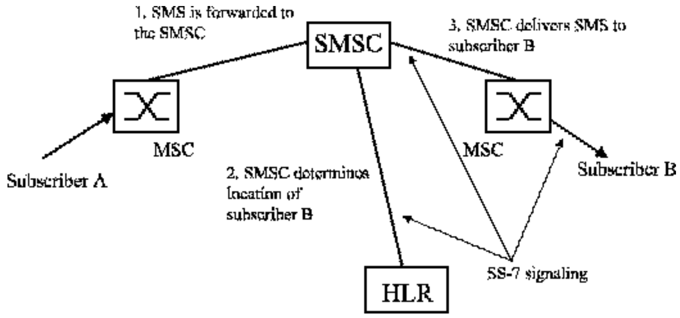

1. SMS is forwarded to the SMSC
SMSC
3. SMSC delivers SMS to subscriber B
MSC
MSC
Subscriber A
Subscriber B
2. SMSC determines location of subscriber B
HLR
SS-7 signaling

Figure 1.16 SMS delivery principle

has confirmed the proper reception of the SMS, the MSC notifies the SMSC as well and the SMS is deleted from the SMSC's data storage.

If the subscriber is not reachable because the battery of the mobile station is empty, the network coverage has been lost temporarily, or if the device is simply switched off, it is not possible to deliver the SMS. In this case, the message waiting flag is set in the VLR and the SMSC is stored in the SMSC. Once the subscriber communicates with the MSC, the MSC notifies the SMSC to reattempt delivery.

As the message waiting flag is also set in the HLR, the SMS also reaches a subscriber that has switched off the mobile station in London for example and switches it on again after a flight to Los Angeles. When the mobile station is switched on in Los Angeles, the visited MSC reports the location to the subscriber's home HLR (location update). The HLR then sends a copy of the user's subscription information to the MSC/VLR in Los Angeles including the message waiting flag and thus the SMSC can also be notified that the user is reachable again.

The SMS delivery mechanism does not unfortunately include a delivery reporting functionality for the sender of the SMS. The sender is only notified that the SMS has been correctly received by the SMSC. If and when the SMS is also correctly delivered to the recipient, however, is not signalled to the originator of the message. Most SMSC vendors have therefore implemented their own proprietary solutions. Some vendors use a code for this purpose that the user has to include in the text message. With some operators for example, '*N#' or '*T#' can be put into the text message at the beginning to indicate to the SMSC that the sender wishes a delivery notification. The SMSC then removes the three-character code and returns an SMS to the originator once the SMS was successfully delivered to the recipient.

1.7 The Base Station Subsystem (BSS)

While most functionality required in the NSS for GSM could be added via additional software, the BSS had to be developed from scratch. This was mainly necessary because earlier generation systems were based on analog transmission over the air interface and thus had not much in common with the GSM BSS.

1.7.1 Frequency Bands

In Europe, GSM was initially only specified for operation in the 900 MHz band between 890–915 MHz in the uplink direction and between 935–960 MHz in the downlink direction (Figure 1.17). 'Uplink' refers to the transmission from the mobile station to the network and 'downlink' to the transmission from the network to the mobile station. The bandwidth of 25 MHz is split into 125 channels with a bandwidth of 200 kHz each.

It soon became apparent that the number of available channels was not sufficient to cope with the growing demand in many European countries. Therefore, the regulating bodies assigned an additional frequency range for GSM which uses the frequency band from 1710–1785 MHz for the uplink and 1805–1880 for the downlink. Instead of a total bandwidth of 25 MHz as in the 900 MHz range, the 1800 MHz band offers 75 MHz of bandwidth which corresponds to 375 additional channels. The functionality of GSM is identical on both frequency bands, with the channel numbers, also referred to as the absolute radio frequency channel numbers (ARFCNs), being the only difference. See Table 1.5.

While GSM was originally intended only as a European standard, the system soon spread to countries in other parts of the globe. In countries outside Europe, GSM sometimes competes with other technologies, such as CDMA. Today, only a few countries, like Japan and South Korea, are not covered by GSM systems. However, some of the operators in these countries operate W-CDMA UMTS networks (see Chapter 3). Therefore, GSM/UMTS subscribers with dual-mode phones can also roam in these countries.

In North America, analog mobile networks continued to be used for some time before second-generation networks, with GSM being one of the technologies used, were introduced. Unfortunately, however, the 900 MHz as well as the 1800 MHz band were already in use by other systems and thus the North American regulating body chose to open frequency bands for the new systems in the 1900 MHz band and later on in the 850 MHz band. The disadvantage of this approach is that many US GSM mobile phones cannot be used in Europe

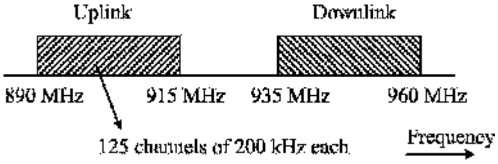


Figure 1.17 GSM uplink and downlink in the 900 MHz frequency band

Table 1.5 GSM frequency bands

Band	ARFCN	Uplink (MHz)	Downlink (MHz)
GSM 900 (Primary)	0–124	890–915	935–960
GSM 900 (Extended)	975–1023, 0–124	880–915	925–960
GSM 1800	512–885	1710–1785	1805–1880
GSM 1900 (North America)	512–810	1850–1910	1930–1990
GSM 850 (North America)	128–251	824–849	869–894
GSM-R	0–124, 955–1023	876–915	921–960

and vice versa. Fortunately, many new GSM and UMTS phones support the US frequency bands as well as the European frequency bands, which are also used in most countries in other parts of the world. These tri-band or quad-band phones thus enable a user to truly roam globally.

The GSM standard is also used by railway communication networks in Europe and other parts of the world. For this purpose, GSM was enhanced to support a number of private mobile radio and railway specific functionalities and is known as GSM-R. The additional functionalities include:

- The voice group call service (VGCS): this service offers a circuit-switched walkie-talkie functionality to allow subscribers that have registered to a VGCS group to communicate with all other subscribers in the area who have also subscribed to the group. In order to talk, the user has to press a push to talk button. If no other subscriber holds the uplink, the network grants the request and blocks the uplink for all other subscribers while the push to talk button is pressed. The VGCS service is very efficient especially if many subscribers participate in a group call, as all mobile stations that participate in the group call listen to the same timeslot in downlink direction. Further information about this service can be found in 3GPP TS 43.068 [12].
- The voice broadcast service (VBS): same as VGCS with the restriction that only the originator of the call is allowed to speak. Further information about this service can be found in 3GPP TS 43.069 [13].
- Enhanced multi level precedence and preemption (eMLPP): this functionality, which is specified in 3GPP TS 23.067 [14], is used to attach a priority to a point-to-point, VBS, or VGCS call. This enables the network and the mobile stations to automatically preempt ongoing calls for higher priority calls to ensure that emergency calls (e.g. a person has fallen on the track) is not blocked by lower priority calls and a lack of resources (e.g. because no timeslots are available).

As GSM-R networks are private networks, it has been decided to assign a private frequency band in Europe for this purpose which is just below the public 900 MHz GSM band. To use GSM-R, mobile phones need to be slightly modified to be able to send and receive in this frequency range. This requires only minor software and hardware modifications. In order to be also able to use the additional functionalities described above, further extensions of the mobile station software are necessary. More about GSM-R can be found at http://gsm-r.uic.asso.fr [15].

1.7.2 The Base Transceiver Station (BTS)

Base stations, which are also called base transceiver stations (BTSs), are the most visible network elements of a GSM system (Figure 1.18). Compared to fixed-line networks, the base stations replace the wired connection to the subscriber with a wireless connection which is also referred to as the air interface. The base stations are also the most numerous components of a mobile network as according to press reports each wireless operator in the UK for example has well over 10,000 base stations.

In theory, a base station can cover an area with a radius of up to 35 km. This area is also called a cell. As a base station can only serve a limited number of simultaneous users,

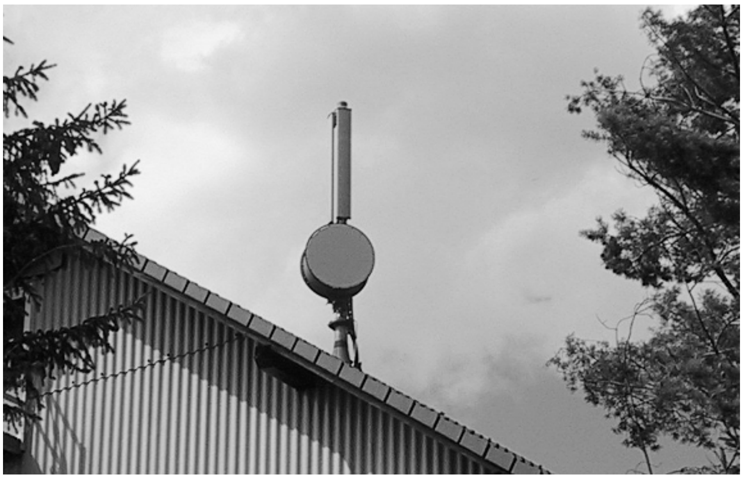


Figure 1.18 A typical antenna of a GSM base station. The optional microwave directional antenna (round antenna at the bottom of the mast) connects the base station with the GSM network

cells are much smaller in practice especially in dense urban environments. There, cells cover areas with a radius between 3 and 4 km in residential and business areas, and down to only several 100 m and minimal transmission power in heavily frequented areas like shopping centers and downtown streets. Even in rural areas, a cell's coverage area is usually less then 15 km as the transmission power of the mobile station of one or two watts is the limiting factor in this case.

As the emissions of different base stations of the network must not interfere with each other, all neighboring cells have to send on different frequencies. As can be seen in Figure 1.19, a singe base station usually has quite a number of neighboring sites. Therefore, only a limited number of different frequencies can be used per base station in order to increase capacity.

To increase the capacity of a base station, the coverage area is usually split into two or three sectors which are then covered on different frequencies by a dedicated transmitter.

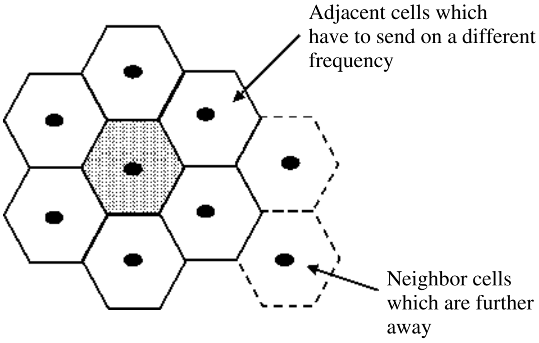

Adjacent cells which have to send on a different frequency
Neighbor cells which are further away

Figure 1.19 Cellular structure of a GSM network

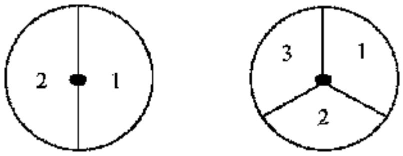


Figure 1.20 Sectorized cell configurations

This allows the reuse of frequencies in two-dimensional space better than if only a single frequency was used for the whole base station. Each sector of the base station therefore forms its own independent cell (Figure 1.20).

1.7.3 The GSM Air Interface

The transmission path between the BTS and the mobile terminal is referred to in the GSM specifications as the air interface or the Um interface. To allow the base station to communicate with several subscribers simultaneously, two methods are used. The first method is frequency division multiple access (FDMA) which means that users communicate with the base station on different frequencies. The second method used is time division multiple access (TDMA). See Figure 1.21. GSM uses carrier frequencies with a bandwidth of 200 kHz over which up to eight subscribers can communicate with the base station simultaneously.

Subscribers are time multiplexed by dividing the carrier into frames with durations of 4.615 ms. Each frame contains eight physically independent timeslots, each for communication with a different subscriber. The timeframe of a timeslot is called a burst and the burst duration is 577 microseconds. If a mobile station is allocated timeslot number two for a voice call for example, the mobile station will send and receive only during this burst. Afterwards, it has to wait until the next frame before it is allowed to send again.

By combining the two multiple access schemes it is possible to approximately calculate the total capacity of a base station. For the following example it is assumed that the base station is split into three sectors and each sector is covered by an independent cell. Each cell is equipped with two transmitters and receivers, a configuration that is used quite often. In each sector, $2 \times 8 = 16$ timeslots are thus available. Two timeslots are usually assigned for signaling purposes which leaves 14 timeslots per sector for user channels. Let us further assume that four timeslots or more are used for the packet-switched GPRS service (see Chapter 2). Therefore, 10 timeslots are left for voice calls per sector, which amounts to 30

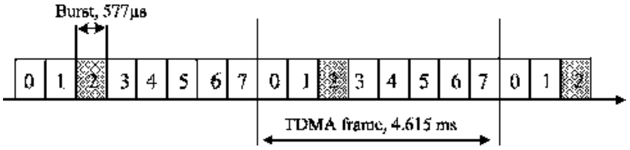


Figure 1.21 A GSM TDMA frame

channels for all sectors of the base station. In other words this means that 30 subscribers can communicate simultaneously per base station.

A single BTS, however, provides service for a much higher number of subscribers, as they do not all communicate at the same time. Mobile operators, therefore, base their network dimensioning on a theoretical call profile model in which the number of minutes a subscriber statistically uses the system per hour is one of the most important parameters. A commonly used value for the number of minutes a subscriber uses the system per hour is one minute. This means that a base station is able to provide service for 60 times the number of active subscribers. In this example a base station with 30 channels is therefore able to provide service for about 1800 subscribers.

This number is quite realistic as the following calculation shows: Vodafone Germany had a subscriber base of about 25 million in 2005. If this value is divided by the number of subscribers per cell, the total number of base stations required to serve such a large subscriber base can be determined. With our estimation above, the number of base stations required for the network would be about 14,000. This value is quite accurate and in line with numbers published by the operator.

Each burst of a TDMA frame is divided into a number of different sections as shown in Figure 1.22. Each burst is encapsulated by a guard time in which no data is sent. This is necessary because the distance of the different subscribers relative to the base station can change while they are active. As airwaves 'only' propagate through space at the speed of light, the signal of a far away subscriber takes a longer time to reach the base station compared to a subscriber that is closer to the base station. In order to prevent any overlap, guard times were introduced. These parts of the burst are very short, as the network actively controls the timing advance of the mobile station. More about this topic can be found below.

The training sequence in the middle of the burst always contains the same bit pattern. It is used to compensate for interference caused for example by reflection, absorption, and multi-path propagation. On the receiver side these effects are countered by comparing the received signal to the training sequence and thus adapting the analog filter parameters for the signal. The filter parameters calculated this way can then be used to modify the rest of the signal and thus to better recreate the original signal.

At the beginning and end of each burst, another well-known bit pattern is sent to enable the receiver to detect the beginning and end of a burst correctly. These fields are called 'tails'. The actual user data of the burst, i.e. the digitized voice signal, is sent in the two user data fields with a length of 57 bits each. This means, that a 577-microsecond burst transports 114 bits of user data. Finally, each frame contains two bits to the left and right of the training sequence which are called 'stealing bits'. These bits indicate if the data fields

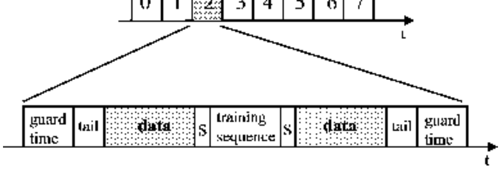


Figure 1.22 A GSM burst

contain user data or are used ('stolen') for urgent signaling information. User data of bursts which carry urgent signaling information, however, is lost. As shown below, the speech decoder is able to cope with short interruptions of the data stream quite well and thus are not normally audible to the user.

For the transmission of user or signaling data, the timeslots are arranged into logical channels. A user data channel for the transmission of digitized voice data for example is a logical channel. On the first carrier frequency of a cell the first two timeslots are usually used for common logical signaling channels while the remaining six independent timeslots are used for user data channels or GPRS. As there are more logical channels then physical channels (timeslots) for signaling, 3GPP TS 45.002 [16] describes how 51 frames are grouped into a multiframe to be able to carry a number of different signaling channels over the same timeslot. In such a multiframe, which is infinitely repeated, it is specified in which bursts on timeslots 0 and 1 which logical channels are transmitted. For user data timeslots (e.g. voice) the same principle is used. Instead of 51 frames, these timeslots are grouped into a 26-multiframe pattern. In order to visualize this principle, Figure 1.23 shows how the eight timeslots of a frame are grouped into a two-dimensional table. Figure 1.24 then uses this principle to show how the logical channels are assigned to physical timeslots in the multiframe.

Logical channels are arranged into two groups. If data on a logical channel is dedicated to a single user, the channel is called a dedicated channel. If the channel is used for data that needs to be distributed to several users, the channel is called a common channel.

Let us take a look at the dedicated channels first:

- The traffic channel (TCH) is a user data channel. It can be used to transmit a digitized voice signal or circuit-switched data services of up to 14.4 kbit/s.
- The fast associated control channel (FACCH) is transmitted on the same timeslot as a TCH. It is used to send urgent signaling messages like a handover command. As these messages do not have to be sent very often, no dedicated physical bursts are allocated to the FACCH. Instead, user data is removed from a TCH burst. In order to inform the

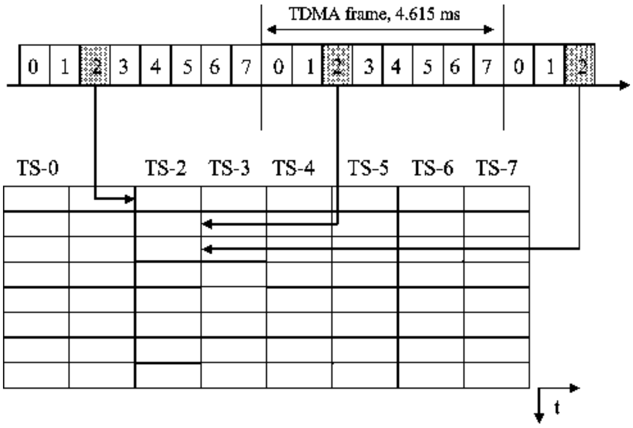
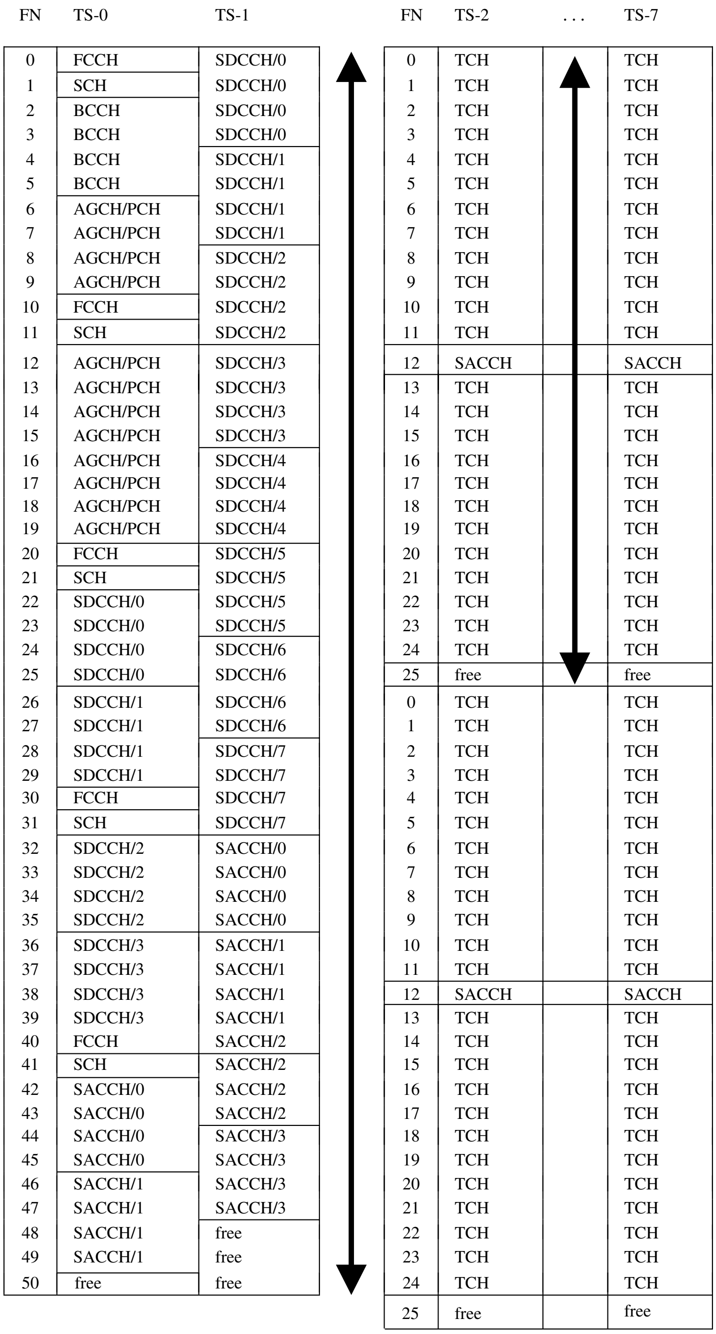


Figure 1.23 Arrangement of bursts of a frame for the visualization of logical channels in Figure 1.24



FN	TS-0	TS-1	FN	TS-2	. . .	TS-7
0	FCCH	SDCCH/0	0	TCH		TCH
1	SCH	SDCCH/0	1	TCH		TCH
2	BCCH	SDCCH/0	2	TCH		TCH
3	BCCH	SDCCH/0	3	TCH		TCH
4	BCCH	SDCCH/1	4	TCH		TCH
5	BCCH	SDCCH/1	5	TCH		TCH
6	AGCH/PCH	SDCCH/1	6	TCH		TCH
7	AGCH/PCH	SDCCH/1	7	TCH		TCH
8	AGCH/PCH	SDCCH/2	8	TCH		TCH
9	AGCH/PCH	SDCCH/2	9	TCH		TCH
10	FCCH	SDCCH/2	10	TCH		TCH
11	SCH	SDCCH/2	11	TCH		TCH
12	AGCH/PCH	SDCCH/3	12	SACCH		SACCH
13	AGCH/PCH	SDCCH/3	13	TCH		TCH
14	AGCH/PCH	SDCCH/3	14	TCH		TCH
15	AGCH/PCH	SDCCH/3	15	TCH		TCH
16	AGCH/PCH	SDCCH/4	16	TCH		TCH
17	AGCH/PCH	SDCCH/4	17	TCH		TCH
18	AGCH/PCH	SDCCH/4	18	TCH		TCH
19	AGCH/PCH	SDCCH/4	19	TCH		TCH
20	FCCH	SDCCH/5	20	TCH		TCH
21	SCH	SDCCH/5	21	TCH		TCH
22	SDCCH/0	SDCCH/5	22	TCH		TCH
23	SDCCH/0	SDCCH/5	23	TCH		TCH
24	SDCCH/0	SDCCH/6	24	TCH		TCH
25	SDCCH/0	SDCCH/6	25	free		free
26	SDCCH/1	SDCCH/6	0	TCH		TCH
27	SDCCH/1	SDCCH/6	1	TCH		TCH
28	SDCCH/1	SDCCH/7	2	TCH		TCH
29	SDCCH/1	SDCCH/7	3	TCH		TCH
30	FCCH	SDCCH/7	4	TCH		TCH
31	SCH	SDCCH/7	5	TCH		TCH
32	SDCCH/2	SACCH/0	6	TCH		TCH
33	SDCCH/2	SACCH/0	7	TCH		TCH
34	SDCCH/2	SACCH/0	8	TCH		TCH
35	SDCCH/2	SACCH/0	9	TCH		TCH
36	SDCCH/3	SACCH/1	10	TCH		TCH
37	SDCCH/3	SACCH/1	11	TCH		TCH
38	SDCCH/3	SACCH/1	12	SACCH		SACCH
39	SDCCH/3	SACCH/1	13	TCH		TCH
40	FCCH	SACCH/2	14	TCH		TCH
41	SCH	SACCH/2	15	TCH		TCH
42	SACCH/0	SACCH/2	16	TCH		TCH
43	SACCH/0	SACCH/2	17	TCH		TCH
44	SACCH/0	SACCH/3	18	TCH		TCH
45	SACCH/0	SACCH/3	19	TCH		TCH
46	SACCH/1	SACCH/3	20	TCH		TCH
47	SACCH/1	SACCH/3	21	TCH		TCH
48	SACCH/1	free	22	TCH		TCH
49	SACCH/1	free	23	TCH		TCH
50	free	free	24	TCH		TCH
			25	free		free

Figure 1.24 Use of timeslots in downlink direction as per 3GPP TS 45.002 [16]

mobile station, the stealing bits to the left and right of the training sequence, as shown in Figure 1.22, are used. This is the reason why the FACCH is not shown in Figure 1.24.

- The slow associated control channel (SACCH) is also assigned to a dedicated connection. It is used in the uplink direction to report signal quality measurements of the serving cell and neighboring cells to the network. The network then uses these values for handover decisions and power control. In the downlink direction, the SACCH is used to send power control commands to the mobile station. Furthermore, the SACCH is used for timing advance control which is described in Section 1.7.4 and Figure 1.29. As these messages are only of low priority and the necessary bandwidth is very small, only a few bursts are used on a 26 multiframe at fixed intervals.
- The standalone dedicated control channel (SDCCH) is a pure signaling channel which is used during call establishment when a subscriber has not yet been assigned a traffic channel. Furthermore, the channel is used for signaling which is not related to call establishment such as for the location update procedure or for sending or receiving a text message (SMS).

Besides the dedicated channels, which are always assigned to a single user, there are a number of common channels that are monitored by all subscribers in a cell:

- The synchronization channel (SCH) is used by mobile stations during network and cell searches.
- The frequency correction channel (FCCH) is used by the mobile stations to calibrate their transceiver units und is also used to detect the beginning of a multiframe.
- The broadcast common control channel (BCCH) is the main information channel of a cell and broadcasts SYS_INFO messages that contain a variety of information about the network. The channel is monitored by all mobile stations, which are switched on but currently not engaged in a call or signaling connection (idle mode), and broadcasts among many other things the following information:
  - the MCC and MNC of the cell;
  - the identification of the cell which consists of the location area code (LAC) and the cell ID;
  - to simplify the search for neighboring cells for a mobile station, the BCCH also contains information about the frequencies used by neighboring cells. Thus, the mobile station does not have to search the complete frequency band for neighboring cells.
- The paging channel (PCH) is used to inform idle subscribers of incoming calls or SMS messages. As the network is only aware of the location area the subscriber is roaming in, the paging message is broadcast in all cells belonging to the location area. The most important information element of the message is the IMSI of the subscriber or a temporary identification called the temporary mobile subscriber identity (TMSI). A TMSI is assigned to a mobile station during the network attach procedure and can be changed by the network every time the mobile station contacts the network once encryption has been activated. Thus, the subscriber has to be identified with the IMSI only once and is then addressed with a constantly changing temporary number when encryption is not yet activated for the communication. This increases anonymity in the network and prevents eavesdroppers from creating movement profiles of subscribers.

- The random access channel (RACH) is the only common channel in the uplink direction. If the mobile station receives a message via the PCH that the network is requesting a connection establishment or if the user wants to establish a call or send an SMS, the RACH is used for the initial communication with the network. This is done by sending a channel request message. Requesting a channel has to be done via a 'random' channel because subscribers in a cell are not synchronized with each other. Thus, it cannot be ensured that two devices do not try to establish a connection at the same time. Only once a dedicated channel (SDCCH) has been assigned to the mobile station by the network can there no longer be any collision between different subscribers of a cell. If a collision occurs during the first network access, the colliding messages are lost and the mobile stations do not receive an answer from the network. Thus, they have to repeat their channel request messages after expiry of a timer which is set to an initial random value. This way, it is not very likely that the mobile stations will interfere with each other again during their next connection establishment attempts because they are performed at different times.
- The access grant channel (AGCH): if a subscriber sends a channel request message on the RACH, the network allocates an SDCCH or in exceptional cases a TCH and notifies the subscriber on the AGCH via an immediate assignment message. The message contains information about which SDCCH or TCH the subscriber is allowed to use.

Figure 1.25 shows how PCH, AGCH, and SDCCH are used during the establishment of a signaling link between the mobile station and the network. The BSC, which is responsible for assigning SDCCH and TCH channels of a base station, is further described in Section 1.7.4.

As can also be seen in Figure 1.24, not all bursts on timeslots 2 to 7 are used for traffic channels. Every twelfth burst of a timeslot it used for the SACCH. Furthermore, the 25th

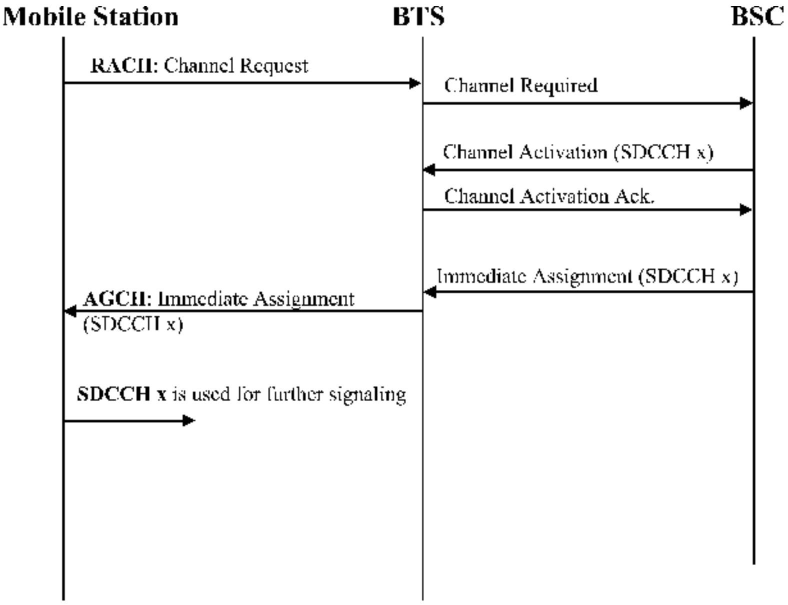

Mobile Station
BTS
BSC
RACH: Channel Request
Channel Required
Channel Activation (SDCCH x)
Channel Activation Ack.
Immediate Assignment (SDCCH x)
AGCH: Immediate Assignment (SDCCH x)
SDCCH x is used for further signaling

Figure 1.25 Establishment of a signaling connection

burst is also not used for carrying user data. This gap is used to enable the mobile station to perform signal strength measurements of neighboring cells on other frequencies. This is necessary so that the network can redirect the connection into a different cell (handover) to maintain the call while the user is moving.

The GSM standard offers two possibilities to use the available frequencies. The simplest case, which has been described so far, is the use of a constant carrier frequency (ARFCN) for each channel. In order to improve the transmission quality it is also possible to use alternating frequencies for a single channel of a cell. This concept is known as frequency hopping and changes the carrier frequency for every burst during a transmission. This increases the probability that only few bits are lost if one carrier frequency experiences a lot of interference from other sources like neighboring cells. In the worst case only a single burst is affected because the next burst is already sent on a different frequency. Up to 64 different frequencies can be used per base station for frequency hopping. In order to inform the mobile of the use of frequency hopping, the immediate assignment message used during the establishment of a signaling link contains all the information about which frequencies are used and which hopping pattern is applied to the connection.

For carriers that transport the SCH, FCCH, and BCCH channels, frequency hopping must not be used. This restriction is necessary because it would be very difficult for mobile stations to find neighboring cells.

In practice, network operators use static frequencies as well as frequency hopping in their networks.

The interface which connects the base station to the network and which is used to carry the information for all logical channels is called the A-bis interface. An E-1 connection is usually used for the A-bis interface and due to its 64 kbit/s timeslot architecture the logical channels are transmitted in a different way than on the air interface. All common channels as well as the information sent and received on the SDCCH and SACCH channels are sent over one or more common 64 kbit/s E-1 timeslots. This is possible because these channels are only used for signaling data which is not time critical. On the A-bis interface these signaling messages are sent by using the link access protocol (LAPD). This protocol was initially designed for the ISDN D-channel of fixed-line networks and has been reused for GSM with only minor modifications.

For traffic channels that use a bandwidth of 13 kbit/s on the A-bis interface, only one-quarter of an E-1 timeslot is used. This means that all eight timeslots of an air interface frame can be carried on only two timeslots of the E-1 interface. A base station composed of three sectors which uses two carriers each thus requires 12 timeslots on the A-bis interface plus an additional timeslot for the LAPD signaling. The remaining timeslots of the E-1 connection can be used for the communication between the network and other base stations. For this purpose, several cells are usually daisy chained via a single E-1 connection. See Figure 1.26.

1.7.4 The Base Station Controller (BSC)

While the base station is the interface element that connects the mobile stations with the network, the base station controller (BSC) is responsible for the establishment, release, and maintenance of all connections of cells which are connected to it.

If a subscriber wants to establish a voice call, send an SMS, etc., the mobile station sends a channel request message to the BSC as shown in Figure 1.25. The BSC then checks if

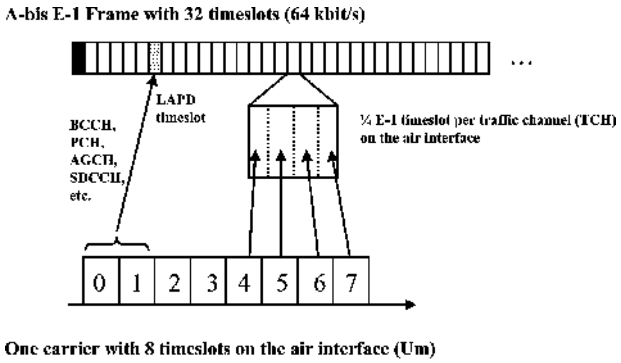

A-bis E-1 Frame with 32 timeslots (64 kbit/s)
...
LAPD timeslot
BCCH, PCH, AGCH, SDCCH, etc.
¼ E-1 timeslot per traffic channel (TCH) on the air interface
0
1
2
3
4
5
6
7
One carrier with 8 timeslots on the air interface (Um)

Figure 1.26 Mapping of E-1 timeslots to air interface timeslots

an SDCCH is available and activates the channel in the BTS. Afterwards, the BSC sends an immediate assignment message to the mobile station on the AGCH which includes the number of the assigned SDCCH. The mobile station then uses the SDCCH to send DTAP messages which the BSC forwards to the MSC.

The BSC is also responsible for establishing signaling channels for incoming calls or SMS messages. In this case, the BSC receives a paging message from the MSC which contains the IMSI and TMSI of the subscriber, as well as the location area ID in which the subscriber is currently located. The BSC in turn has a location area database which it uses to identify all cells in which the subscriber needs to be paged. When the mobile station receives the paging message, it responds to the network in the same way as in the example above by sending a channel request message.

The establishment of a traffic channel for voice calls is always requested by the MSC for both mobile-originated and mobile-terminated calls. Once the mobile station and the MSC have exchanged all necessary information for the establishment of a voice call via an SDCCH, the MSC sends an assignment request for a voice channel to the BSC as shown in Figure 1.27.

The BSC then verifies if a TCH is available in the requested cell and if so, activates the channel in the BTS. Afterwards, the mobile station is informed via the SDCCH that a TCH is now available for the call. The mobile station then changes to the TCH and FACCH. To inform the BTS that it has switched to the new channel, the mobile station sends a message to the BTS on the FACCH which is acknowledged by the BTS. In this way, the mobile also has a confirmation that its signal can be decoded correctly by the BTS. Finally, the mobile station sends an assignment complete message to the BSC which in turn informs the MSC of the successful establishment of the traffic channel.

Apart from the establishment and release of a connection, another important task of the BSC is the maintenance of the connection. As subscribers can roam freely through the network while a call is ongoing it can happen that the subscriber roams out of the coverage area of the cell in which the call was initially established. In this case, the BSC has to redirect the call to the appropriate cell. This procedure is called handover. In order to be able to perform a handover into another cell, the BSC requires signal quality measurements for the air interface. The results of the downlink signal quality measurements are reported to the

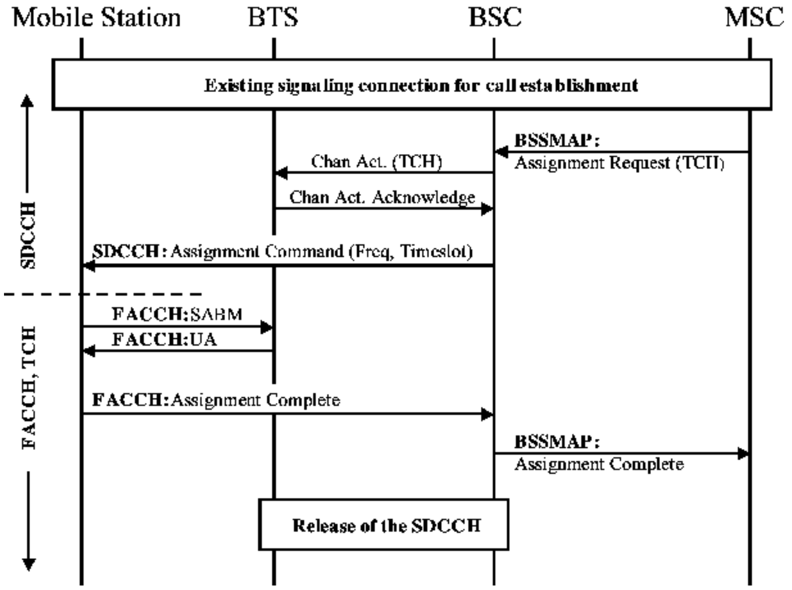


Figure 1.27 Establishment of a traffic channel (TCH)

BSC by the mobile station, which continuously performs signal quality measurements which it reports via the SACCH to the network. The uplink signal quality is constantly measured by the BTS and also reported to the BSC. Apart from the signal quality of the user's current cell, it is also important that the mobile station reports the quality of signals it receives from other cells. To enable the mobile station to perform these measurements, the network sends the frequencies of neighbouring cells via the SACCH during an ongoing call. The mobile station then uses this information to perform the neighbouring cell measurements while the network communicates with other subscribers and reports the result via measurement report messages in the uplink SACCH.

The network receives these measurement values and is thus able to periodically evaluate if a handover of an ongoing call to a different cell is necessary. Once the BSC decides to perform a handover, a TCH is activated in the new cell as shown in Figure 1.28. Afterwards, the BSC informs the mobile station via the old cell with a handover command message that is sent over the FACCH. Important information elements of the message are the new frequency and timeslot number of the new TCH. The mobile station then changes its transmit and receive frequency, synchronizes to the new cell if necessary, and sends a handover access message in four consecutive bursts. In the fifth burst, an SABM message is sent which is acknowledged by the BTS to signal to the mobile station that the signal can be received. At the same time, the BTS informs the BSC of the successful reception of the mobile station's signal with an establish indication message. The BSC then immediately redirects the speech path into the new cell.

From the mobile's point of view the handover is now finished. The BSC, however, has to release the TCH in the old cell and has to inform the MSC of the performed handover

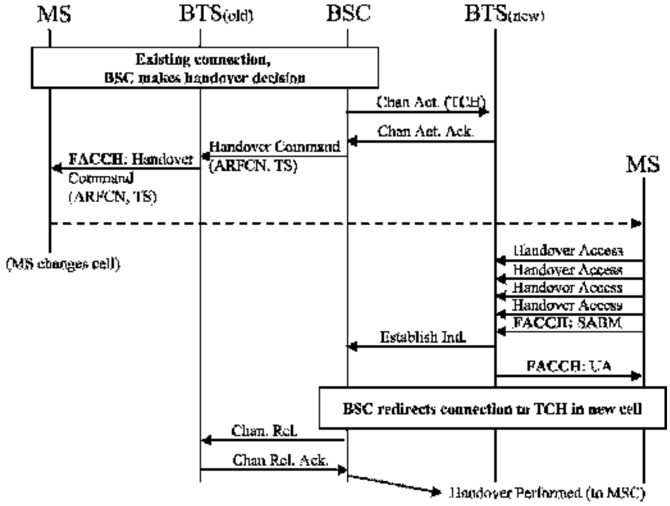


Figure 1.28 Message flow during a handover procedure

before the handover is finished from the network's point of view. The message to the MSC is only informative and has no impact on the continuation of the call.

In order to reduce interference, the BSC is also in charge of controlling the transmission power for every air interface connection. For the mobile station an active power control has the advantage that the transmission power can be reduced under favorable reception conditions. The control of the mobile station's transmission power is done using the signal quality measurements of the BTS for the connection. If the mobile station's transmission power has to be increased or decreased, the BSC sends a power control message to the BTS. The BTS in turn forwards the message to the mobile station and repeats the message on the SACCH in every frame. In practice, it can be observed that power control and adaptation is performed every one to two seconds. During call establishment, the mobile station always uses the highest allowed power output level which is then reduced or increased again by the network step by step. Table 1.6 gives an overview of the mobile station power classes. A distinction is made for the 900 MHz versus the 1800 MHz band. While mobile stations operating on the 900 MHz band are allowed to use up to 2 watts, connections on the 1800 MHz band are limited to 1 watt. For stationary devices or car phones with external antennas, power values for up to 8 watts are allowed. The power values in the table represent the power output when the transmitter is active in the assigned timeslot. As the mobile station only sends on one of the eight timeslots of a frame, the average power output of the mobile station is only one-eighth of this value. The average power output of a mobile station which sends with a power output of 2 watts is thus only 250 milliwatts.

The BSC is also able to control the power output of the base station. This is done by evaluating the signal measurements of the mobile stations in the current cell. It is important to note that power control can only be performed for downlink carriers which do not broadcast the common channels like FCH, SCH, and BCCH of a cell. On such carriers the power output has to be constant in order to allow mobile stations, which are currently located in other cells of the network, to perform their neighbouring cell measurements. This would not

Table 1.6 GSM power levels and corresponding power output

GSM 900 Power level	GSM 900 Power output	GSM 1800 Power level	GSM 1800 Power output
(0–2)	(8 W)		
5	2 W	0	1 W
6	1.26 W	1	631 mW
7	794 mW	2	398 mW
8	501 mW	3	251 mW
9	316 mW	4	158 mW
10	200 mW	5	100 mW
11	126 mW	6	63 mW
12	79 mW	7	40 mW
13	50 mW	8	25 mW
14	32 mW	9	16 mW
15	20 mW	10	10 mW
16	13 mW	11	6.3 mW
17	8 mW	12	4 mW
18	5 mW	13	2.5 mW
19	3.2 mW	14	1.6 mW
		15	1.0 mW

be possible if the signal amplitude would varies over time as the mobile stations can only listen to the carrier signal of neighbouring cells for a short time.

Due to the limited speed of radio waves, a time shift of the arrival of the signal can be observed when a subscriber moves away from a base station during an ongoing call. If no countermeasures are taken, this would mean that at some point the signal of a subscriber would overlap with the next timeslot despite the guard time of each burst which is shown in Figure 1.22. Thus, the signal of each subscriber has to be carefully monitored and the timing of the transmission of the subscriber has to be adapted. This procedure is called timing advance control (Figure 1.29).

The timing advance can be controlled in 64 steps (0 to 63) of 550 m. The maximum distance between a base station and a mobile subscriber is in theory 64 × 550 m = 35.2 km. In practice, such a distance is not reached very often as base stations usually cover a much smaller area due to capacity reasons. Furthermore, the transmission power of the terminal is also not sufficient to bridge such a distance under non-line-of-sight conditions to the base

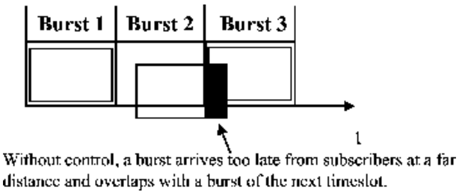

Burst 1
Burst 2
Burst 3
t
Without control, a burst arrives too late from subscribers at a far distance and overlaps with a burst of the next timeslot.

Figure 1.29 Time shift of bursts of distant subscribers without timing advance control

station. Therefore, one of the few scenarios where such a distance has to be overcome is in costal areas from ships at sea.

The control of the timing advance already starts with the first network access on the RACH with a channel request message. This message is encoded into a very short burst that can only transport a few bits in exchange for large guard periods at the beginning and end of the burst. This is necessary because the mobile phone is unaware of the distance between itself and the base station when it attempts to contact the network. Thus, the mobile station is unable to select an appropriate timing advance value. When the base station receives the burst it measures the delay and forwards the request including a timing advance value required for this mobile station to the BSC. As has been shown in Figure 1.25, the BSC reacts to the connection request by returning an immediate assignment message to the mobile station on the AGCH. Apart from the number of the assigned SDCCH, the message also contains a first timing advance value to be used for the subsequent communication on the SDCCH. Once the connection has been successfully established, the BTS continually monitors the delay experienced for this channel and reports any changes to the BSC. The BSC in turn instructs the mobile station to change its timing advance by sending a message on the SACCH.

For special applications, like coastal communication, the GSM standard offers an additional timeslot configuration in order to increase the maximum distance to the base station to up to 120 km. This is achieved by only using every second timeslot per carrier which allows a burst to overlap into the following (empty) timeslot. While this dramatically increases the range of a cell, the number of available communication channels is cut in half. Another issue is that mobile phones that are limited to a transmission power of 1 watt (1800 MHz band) or 2 watts (900 MHz band) may be able to receive the BCCH of such a cell at a great distance but are unable to communicate with the cell in the uplink. Thus, such an extended range configuration mostly makes sense with permanently installed mobile phones with external antennas that can transmit with a power level of up to 8 watts.

1.7.5 The TRAU for Voice Data Transmission

For the transmission of voice data, a TCH is used in GSM as described in Section 1.7.3. A TCH uses all but two bursts of a 26-burst multiframe with one being reserved for the SACCH as shown in Figure 1.24, and one which remains empty to allow the mobile station to perform neighbouring cell measurements. As has been shown in the preceding section, a burst which is sent to or from the mobile every 4.615 ms can carry exactly 114 bits of user data. When taking the two bursts into account, which are not used for user data of a 26-burst multiframe, this results in a raw data rate of 22.8 kbit/s. As will be shown in the remainder of this section, a substantial part of the bandwidth of a burst is required for error detection and correction bits. The resulting data rate for the actual user data is thus around 13 kbit/s.

The narrow bandwidth of a TCH stands in contrast to how a voice signal is transported in the core network. Here, the PCM algorithm is used (see Section 1.6.1) to digitize the voice signal, which makes full use of the available 64 kbit/s bandwidth of an E-1 timeslot to encode the voice signal. See Figure 1.30

A simple solution for the air interface would have been to define air interface channels that can also carry 64 kbit/s PCM-coded voice channels. This has not been done because the scarce resources on the air interface have to be used as efficiently as possible. The decision to compress the speech signal was taken during the first standardization phase in the 1980s

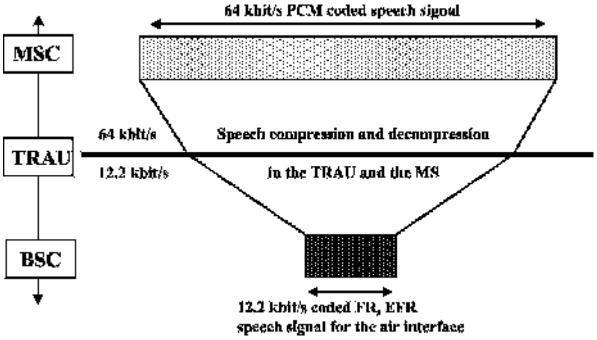

64 kbit/s PCM coded speech sigoal
MSC
64 kbit/s
Speech compression and decompression
TRAU
12,2 kbit/s
in the TRAU and the MS
BSC
12.2 kbit/s coded FR, EFR
speech signal for the air interface

Figure 1.30 GSM speech compression

because it was foreseeable that advances in hardware and software processing capabilities would allow compression of a voice data stream in real time.

In the mobile network, the compression and decompression of the voice data stream is performed in the transcoding and rate adaptation unit (TRAU) which is located between the MSC and a BSC and controlled by the BSC. During an ongoing call, the MSC sends the 64 kbit/s PCM-encoded voice signal towards the radio network and the TRAU converts the voice stream in real time into a 13 kbit/s compressed data stream which is transmitted over the air interface. In the other direction, the BSC sends a continuous stream of compressed voice data towards the core network and the TRAU converts the stream into a 64 kbit/s coded PCM signal. In the mobile station, the same algorithms are implemented as in the TRAU to compress and decompress the speech signal. See Figure 1.31.

While the TRAU is a logical component of the BSS, it is most often installed next to an MSC in practice. This has the advantage that four compressed voice channels can be transmitted in a single E-1 timeslot. After compression, each voice channel uses a 16 kbit/s sub-timeslot. Thus, only one-quarter of the transmission capacity between an MSC and BSC is needed in comparison to an uncompressed transmission. As the BSCs of a network are usually located in the field and not close to an MSC, this helps to reduce transmission costs for the network operator substantially.

The TRAU offers a number of different algorithms for speech compression. These algorithms are called speech codecs or simply codecs. The first codec that was standardized for GSM is the full-rate (FR) codec which reduces the 64 kbit/s voice stream to about 13 kbit/s.

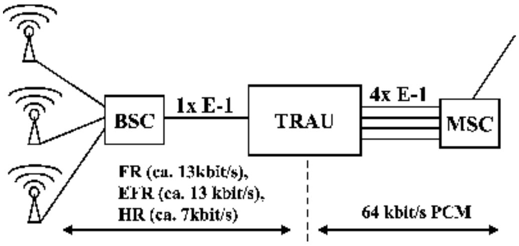


Figure 1.31 Speech compression with a 4:1 compression ratio in the TRAU

At the end of the 1990s, the enhanced full-rate (EFR) codec was introduced and is still the most widely used codec in operational GSM networks today. The EFR codec not only compresses the speech signal to about 13 kbit/s but also offers a superior voice quality compared to the FR codec. The disadvantage of the EFR codec is the higher complexity of the compression algorithm which requires more processing power. However, the processing power available in mobile phones has increased substantially in recent years and thus modern GSM phones easily cope with the additional complexity.

Besides those two codecs, a half-rate (HR) codec has been defined for GSM which only requires a bandwidth of 7 kbit/s. While there is almost no audible difference between the EFR codec compared to a PCM-coded speech signal, the voice quality of the HR codec is noticeably inferior. The advantage for the network operator of the HR codec is that the number of simultaneous voice connections per carrier can be doubled. With HR codec, a single timeslot, which is used for a single EFR voice channel, can carry two TCH (HR). In practice, however, operators do not use the HR codec very often. Even during big events like fairs, operators still assign a TCH (FR) or TCH (EFR) to the subscriber for a voice call.

The latest speech codec development is the adaptive multi rate (AMR) algorithm [17]. Instead of using a single codec, which is selected at the beginning of the call, AMR allows a change to the codec during a call. The considerable advantage of this approach is the ability to switch to a speech codec with a higher compression rate during bad radio signal conditions in order to increase the number of error detection and correction bits. If signal conditions permit, a lower rate codec can be used which only uses every second burst of a frame for the call. This in effect doubles the capacity of the cell as a single timeslot can be shared by two calls similarly to the HR codec. Unlike the HR codec, however, the AMR codecs, which only use every second burst and which are thus called HR AMR codecs, still have a voice quality which is comparable to the EFR codec. While AMR is optional for GSM, it has been chosen for the UMTS system as a mandatory feature. In the United States, AMR is used by some network operators to increase the capacity of their network, especially in very dense traffic areas like New York, where it has become very difficult to increase the capacity of the network any further with over half a dozen carrier frequencies per sector already used. In Europe, however, it is not certain that AMR will be widely deployed as most operators invested heavily in the deployments of their UMTS networks which offer ample capacity for both voice and data communication, even in high density traffic areas. Further information about AMR can also be found in Chapter 3.

While the PCM algorithm digitizes analog volume levels by statically mapping them to digital values, the GSM speech digitization is much more complex to reach the desired compression rate. In the case of the FR codec, which is specified in 3GPP TS 46.010 [18], the compression is achieved by emulating the human vocal system. This is done by using a source-filter model (Figure 1.32). In the human vocal system, the speech is created in the larynx and by the vocal cords. This is emulated in the mathematical model in the signal creation part while the filters represent the signal forming which is done in the human throat and mouth.

On a mathematical level, the speech forming is simulated by using two time-invariant filters. The period filter creates the periodic vibrations of the human voice while the vocal tract filter simulates the envelope. The filter parameters are generated from the human voice, which is the input signal into the system. In order to digitize and compress the human voice, the model is used in reverse direction as shown in Figure 1.32. As time variant filters are

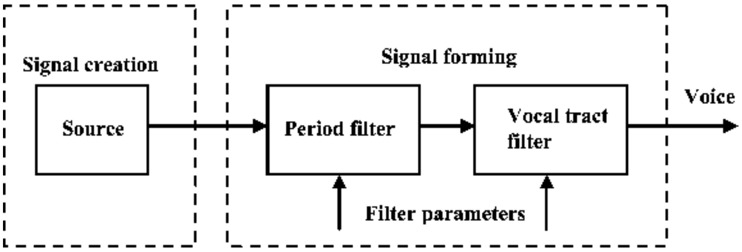


Figure 1.32 Source-filter model of the GSM FR codec

hard to model, the system is simplified by generating a pair of filter parameters for an interval of 20 milliseconds. As an input to the algorithm, a speech signal is used that has previously been converted into an 8- or 13-bit PCM codec. As the PCM algorithm delivers 8000 values per second, the FR codec requires 160 values for a 20 ms interval to calculate the filter parameters. As eight bits are used per value, 8 bits × 160 values = 1280 input bits are used per 20 ms interval. For the period filter, the input bits are used to generate a filter parameter with a length of 36 bits. Afterwards, the filter is applied to the original input signal. The resulting signal is then used to calculate another filter parameter with a length of 36 bits for the vocal tract filter. Afterwards, the signal is again sent through the vocal tract filter with the filter parameter applied. The signal, which is thus created, is called the 'rest signal' and coded into 188 bits. See Figure 1.33.

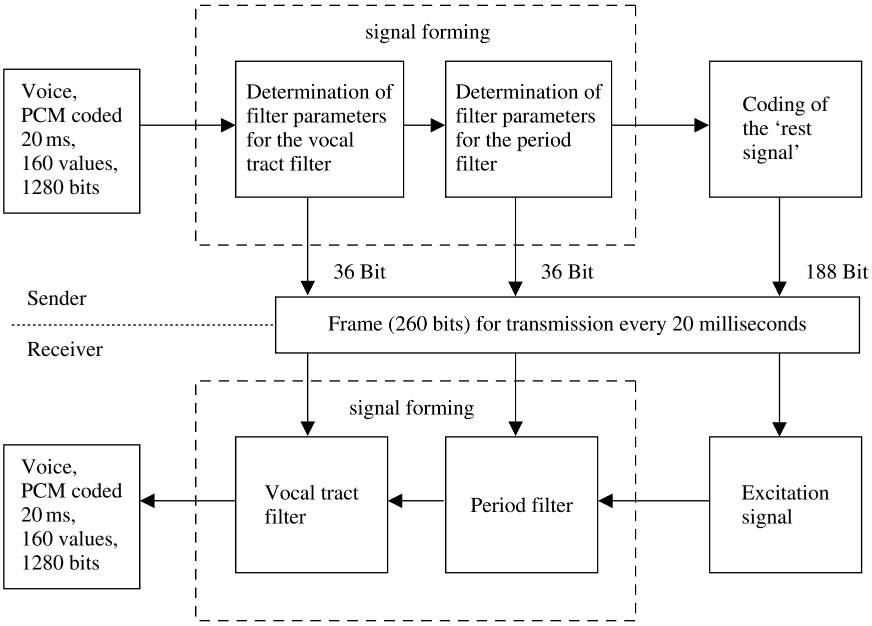

signal forming
Voice, PCM coded 20 ms, 160 values, 1280 bits
Determination of filter parameters for the vocal tract filter
Determination of filter parameters for the period filter
Coding of the 'rest signal'
36 Bit
36 Bit
188 Bit
Sender
Receiver
Frame (260 bits) for transmission every 20 milliseconds
signal forming
Voice, PCM coded 20 ms, 160 values, 1280 bits
Vocal tract filter
Period filter
Excitation signal

Figure 1.33 Complete transmission chain with transmitter and receiver of the GSM FR codec

Once all parameters have been calculated, the two 36-bit filter parameters and the rest signal, which is coded into 188 bits, are sent to the receiver. Thus, the original information, which was coded in 1280 bits, has been reduced to 260 bits. In the receiver, the filter procedure is applied in reverse order on the rest signal and thus the original signal is recreated. As the procedure uses a lossy compression algorithm, the original signal and the recreated signal at the other end are no longer exactly identical. For the human ear, however, the differences are almost inaudible.

Before a 260-bit data frame is transmitted over the air interface every 20 ms, it traverses a number of additional functional blocks which are not implemented in the TRAU but in the base station. These additional functional blocks are shown in Figure 1.34.

In a first step, the voice frames are processed in the channel coder unit, which adds error detection and correction information to the data stream. This step is very important as the transmission over the air interface is prone to frequent transmission errors due to the constantly changing radio environment. Furthermore, the compressed voice information is very sensitive and even a few bits that might be changed while the frame is transmitted over the air interface create an audible distortion. In order to prevent this, the channel coder separates the 260 bits of a voice data frame into three different classes as shown in Figure 1.35.

Fifty of the 260 bits of a speech frame are class Ia bits and extremely important for the overall reproduction of the voice signal at the receiver side. Such bits are for example the higher order bits of the filter parameters. In order to enable the receiver to verify the correct transmission of those bits, a three-bit CRC checksum is calculated and added to the data stream. If the receiver later on cannot recreate the checksum with the received bits, the frame is discarded.

Another 132 bits of the frame are also quite important and are thus put into class Ib. However, no checksum is calculated for them. In order to generate the exact amount of bits that are necessary to fill a GSM burst, four filler bits are inserted. Afterwards, the class Ia

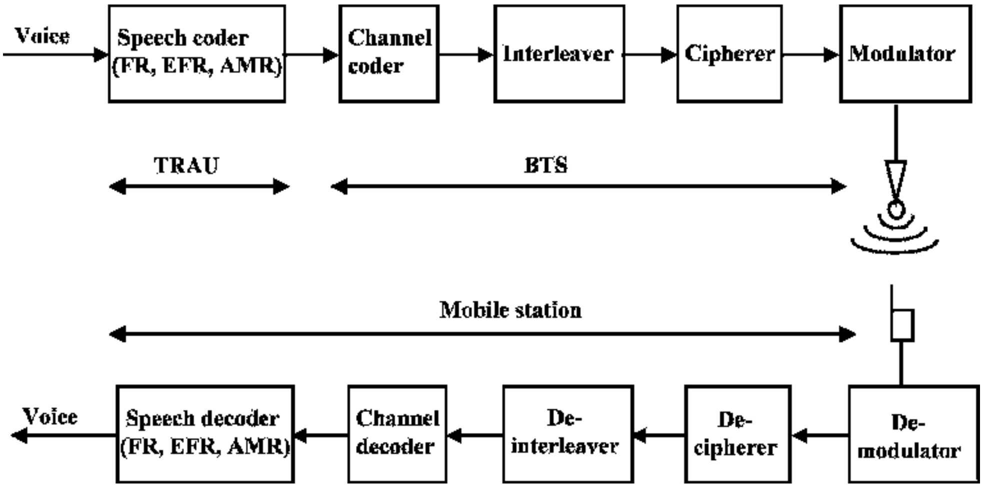


Figure 1.34 Transmission path in the downlink direction between network and mobile station

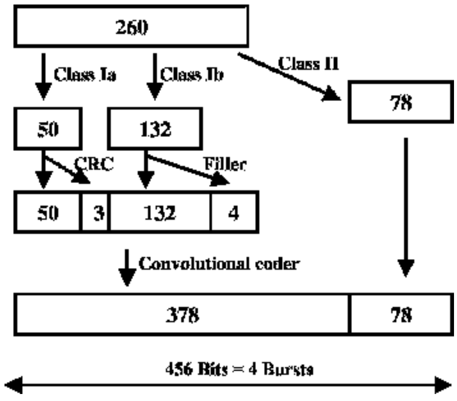


Figure 1.35 GSM channel coder for full-rate speech frames

bits, checksum, class Ib bits, and the four filler bits are treated by a convolutional coder which adds redundancy to the data stream. For each input bit, the convolutional decoder calculates two output bits. For the computation of the output bits the coder uses not only the current bit but also uses information about the values of the previous bits. For each input bit, two output bits are calculated. This mathematical algorithm is also called a half-rate convolutional coder.

The remaining 78 bits of the original 260-bit data frame belong to the third class which is called class II. These are not protected by a checksum and no redundancy is added for them. Errors which occur during the transmission of these bits can neither be detected nor corrected.

As has been shown, the channel coder uses the 260-bit input frame to generate 456 bits on the output side. As a burst on the air interface can carry exactly 114 bits, four bursts are necessary to carry the frame. As the bursts of a traffic channel are transmitted every 4.6152 ms, the time it takes to transmit the frame over the air interface is about 20 ms. In order to get to exactly 20 ms, the empty burst and the burst used for the SACCH per 26-burst multiframe has to be included in the calculation.

Due to the redundancy added by the channel coder, it is possible to correct a high number of faulty bits per frame. The convolutional decoder, however, has one weak point: if several consecutive bits are changed during the transmission over the air interface, the convolutional decoder on the receiver side is not able to correctly reconstruct the original frame. This effect is often observed as air interface disturbances usually affect several bits in a row.

In order to decrease this effect, the interleaver changes the bit order of a 456-bit data frame in a specified pattern over eight bursts (Figure 1.36). Consecutive frames are thus interlocked with each other. On the receiver side, the frames are put through the de-interleaver, which puts the bits again into the correct order. If several consecutive bits are changed due to air interface signal distortion, this operation disperses the faulty bits in the frame and the convolutional decoder can thus correctly restore the original bits. A disadvantage of the interleaver, however, is an increased delay of the voice signal. In addition to the delay of 20 ms generated by the full-rate coder, the interleaver adds another 40 ms as a speech frame is spread over eight bursts instead of being transmitted consecutively in four bursts. Compared

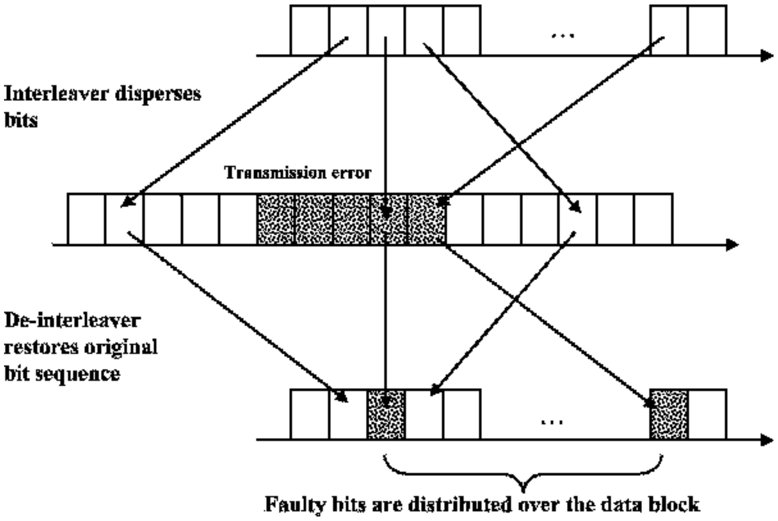

Interleaver disperses bits
Transmission error
De-interleaver restores original bit sequence
...
...
Faulty bits are distributed over the data block

Figure 1.36 Frame interleaving

to a voice call in a fixed-line network, a mobile network thus introduces a delay of at least 60 ms. If the call is established between two mobile phones, the delay is at least 120 ms as the transmission chain is traversed twice.

The next module of the transmission chain is the cipherer (Figure 1.37), which encrypts the data frames it receives from the interleaver. GSM uses, like most communication systems,

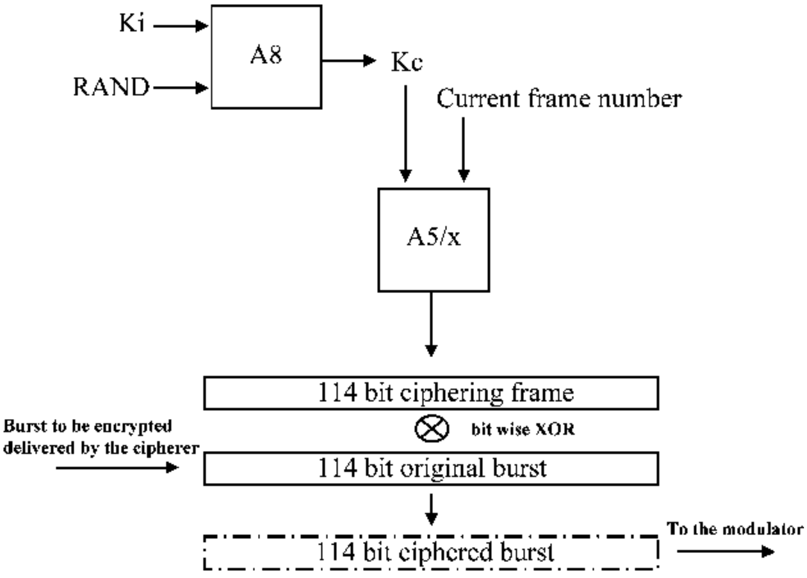


Figure 1.37 Ciphering of an air interface burst

a stream cipher algorithm. In order to encrypt the data stream, a ciphering key (Kc) is calculated in the authentication center and on the SIM card by using a random number (RAND) and the secret key (Ki) as input parameters for the A8 algorithm. Together with the GSM frame number, which is increased for every air interface frame, Kc is used as input parameter for the A5 ciphering algorithm. The A5 algorithm computes a 114-bit sequence which is XOR combined with the bits of the original data stream. As the frame number is different for every burst, it is ensured that the 114-bit ciphering sequence also changes for every burst which further enhances security.

In order to be as flexible as possible, a number of different ciphering algorithms have been specified for GSM. These are called A5/1, A5/2, A5/3, and so on. Thus, it is possible to export GSM network equipment to countries where export restrictions prevent the sale of some ciphering algorithms and technologies. Furthermore, it is possible to introduce new ciphering algorithms into already existing networks in order to react to security issues if a flaw is detected in one of the currently used algorithms. The selection of the ciphering algorithm also depends on the capabilities of the mobile station. During the establishment of a connection, the mobile station informs the network which ciphering algorithms it supports. The network can then choose an algorithm which is supported by the network and the terminal.

When the mobile station establishes a new connection to the network, its identity is verified before the mobile station is allowed to proceed with the call setup. This procedure has already been described in Section 1.6.4. Once the terminal and subscriber have been authenticated, it is also possible for the MSC to start encryption by sending a ciphering command to the mobile station. The ciphering command message contains, among other information elements, the ciphering key, Kc, which is used by the base station for the ciphering of the connection on the air interface. Before the BSC forwards the message to the mobile station, however, the ciphering key is removed from the message because this information must not be sent over the air interface. The mobile station, however, does not need to receive the ciphering key from the network as the SIM card calculates the Kc on its own and forwards the key to the mobile station together with the SRES during the authentication procedure. Figure 1.40 shows how ciphering is activated during a location update procedure.

Unfortunately, there are a number of weak spots in the overall GSM encryption architecture. One serious problem is that encryption has only been specified as an optional feature. Thus, encryption can be easily switched on or off by the network operator. Some mobile phones like the Siemens S series for example show a '*!*' symbol on the display if ciphering is disabled. So far, however, the author of this book has only seen this symbol in a laboratory environment where encryption was deactivated on purpose. Thus, it can be assumed that public networks, in the majority of cases, only very rarely deactivate this feature. Another weakness in the overall security architecture is the fact that a connection is only ciphered between the BTS and the mobile station. All other interfaces between components of the network like the connection between the base station and the BSC or the connection between the TRAU and the MSC are not protected. As many network operators use microwave links between base stations and BSCs, it is possible to intercept calls with suitable microwave equipment without having physical access to any component of the network.

At the end of the transmission chain, the modulator maps the digital data onto an analog carrier, which uses a bandwidth of 200 kHz. This mapping is done by encoding the bits into changes of the carrier frequency. As the frequency change takes a finite amount of time, a method called Gaussian minimum shift keying (GMSK) is used, which smoothes the flanks created by the frequency changes. GMSK has been selected for GSM as its modulation and demodulation properties are easy to handle and implement into hardware and due to the fact that it interferes only slightly with neighboring channels.

In order to reduce the interference on the air interface and to increase the operating time of the mobile station, data bursts are only sent if a speech signal is detected. This method is called discontinuous transmission (DTX) and can be activated independently in the uplink and downlink directions (Figure 1.38). Since only one person is speaking at a time during a conversation, one of the two speech channels can usually be deactivated. In the downlink direction, this is managed by the voice activity detection (VAD) algorithm in the TRAU while in the uplink direction the VAD is implemented in the mobile station.

Simply deactivating a speech channel, however, creates a very undesirable side effect. As no speech signal is transmitted anymore, the receiver no longer hears the background noise of the other side. This can be very irritating especially for high-volume background noise levels such as if a person is driving in a car or sitting in a train. Therefore, it is necessary to generate artificial noise, called comfort noise, which simulates the background noise of the other party to the listener. As the background noise can change over time, the mobile phone or the network respectively analyze the background noise of the channel and calculate an approximation for the current situation. This approximation is then exchanged between the mobile phone and the TRAU every 480 ms. Additional benefits for the network and mobile phone are the ability to perform periodic signal quality measurements of the channel and the ability to use these frames to get an estimation on the current signal timing in order to adapt the timing advance for the call if necessary. How well this method performs is clearly audible as this procedure is used in all mobile phone calls today and the simulation of the background noise in most cases cannot be differentiated from the original signal.

Despite using sophisticated methods for error correction, it is still possible that parts of a frame are destroyed beyond repair during the transmission on the air interface. In these cases, the complete 20 ms voice frame is discarded by the receiver and the previous data block is used instead to generate an output signal. Most errors that are repaired this way remain undetected by the listener. This trick, however, cannot be used indefinitely. If after 320 ms still no valid data block has been received, the channel is muted and the decoder keeps trying to decode the subsequent frames. If, during the following seconds, no valid data frame is received, the connection is terminated and the call drops.

Many of the previously mentioned procedures have specifically been developed for the transmission of voice frames. For circuit-switched data connections, however, a number of modifications are necessary. While it is possible to tolerate a number of faulty bits for voice frames or discarding frames if a CRC error is detected, this is not possible for data calls. If even a single bit is faulty, a retransmission of at least a single frame has to be performed as

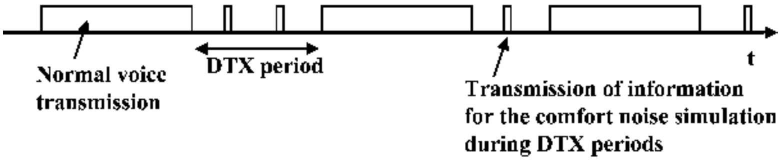

TCH
Normal voice transmission
DTX period
t
Transmission of information for the comfort noise simulation during DTX periods

Figure 1.38 Discontinuous transmission (DTX)

most applications cannot tolerate a faulty data stream. In order to increase the likelihood to correctly reconstruct the initial data stream, the interleaver spreads the bits of a frame over a much larger number of bursts than the eight bursts used for voice frames. Furthermore, the channel coder, which separates the bits of a frame into different classes based on their importance, had to be adapted for data calls as well, as all bits are equally important. Thus, the convolutional decoder has to be used for all bits of a frame. Finally, it is also not possible to use a lossy data compression scheme for data calls. Therefore, the TRAU operates in a transparent mode for data calls. If the data stream can be compressed this has to be performed by higher layers or by the data application itself.

With a radio receiver or an amplifier of a stereo set, the different states of a GSM connection can be made audible. This is possible due to the fact that the activation and deactivation of the transmitter of the mobile station induce an audible sound in the amplifier part of audio devices. If the GSM mobile station is held close enough to an activated radio or an amplifier during the establishment of a call, the typical noise pattern can be heard, which is generated by the exchange of messages on the signaling channel (SDCCH). At some point during the signaling phase, a TCH is assigned to the mobile station at which point the noise pattern changes. As a TCH burst is transmitted every 4.615 ms, the transmitter of the mobile station is switched on and off with a frequency of 217 Hertz. If the background noise is low enough or the mute button of the telephone is pressed, the mobile station changes into the discontinuous transmission mode for the uplink part of the channel. This can be heard as well, as the constant 217 Hz hum is replaced by single short bursts every 0.5 s.

For incoming calls, this method can also be used to detect that a mobile phone starts communicating with the network on the SDDCH already one to two seconds before it starts ringing. This delay is due to the fact that the mobile station first needs to go through the authentication phase and the activation of the ciphering for the channel. Only afterwards can the network forward further information to the mobile station as to why the channel was established. This is also the reason why it takes a much longer time for the alerting tone to be heard when calling a mobile phone compared to calling a fixed-line phone.

Some mobile phones possess a number of interesting network monitoring functionalities which are hidden in the mobile phone software and are usually not directly accessible via the phone's menu. These network monitors allow the visualization of many procedures and parameters that have been discussed in this chapter such as the timing advance, channel allocation, power control, the cell-id, neighboring cell information, handover, cell reselection, etc. On the Internet, various web pages can be found that explain how these monitors can be activated, depending on the type and model of the phone. As the activation procedures are different for every phone, it is not possible to give a general recommendation. However, by using the manufacturer and model of the phone in combination with terms like 'GSM network monitor', 'GSM netmonitor' or 'GSM monitoring mode', it is relatively easy to discover if and how the monitoring mode can be activated for a specific phone.

1.8 Mobility Management and Call Control

As all components of a GSM mobile network have now been introduced, the following section gives an overview of the three processes that allow a subscriber to roam throughout the network.

1.8.1 Location Area and Location Area Update

As the network needs to be able to forward an incoming call, the subscriber's location must be known. After the mobile phone is switched on, its first action is to register with the network. Therefore the network becomes aware of the current location of the user, which can change at any time due to the mobility of the user. If the user roams into the area of a new cell it may need to inform the network of this change. In order to reduce the signaling load in the radio network, several cells are grouped into a location area. The network informs the mobile station via the BCCH of a cell not only of the cell-ID but also of the location area that the new cell belongs to. The mobile station thus only has to report its new location if the new cell belongs to a new location area. Grouping several cells into location areas not only reduces the signaling load in the network but also reduces the power consumption of the mobile. A disadvantage of this method is that the network operator is only aware of the current location area of the subscriber but not of the exact cell. Therefore, the network has to search for the mobile station in all cells of a location area for an incoming call or SMS. This procedure is called paging. The size of a location area can be set by the operator depending on his particular needs. In operational networks, usually 20 to 30 cells are grouped into a location area (Figure 1.39).

Figure 1.40 shows how a location area update procedure is performed. After a signaling connection has been established, the mobile station sends a location update request message to the MSC, which is transparently forwarded by the radio network. Before the message can be sent, however, the mobile station needs to authenticate itself first and ciphering is usually activated before as well.

Once the connection is secured against eavesdropping, the mobile station is usually assigned a new TMSI by the network, which it will use for the next connection establishment

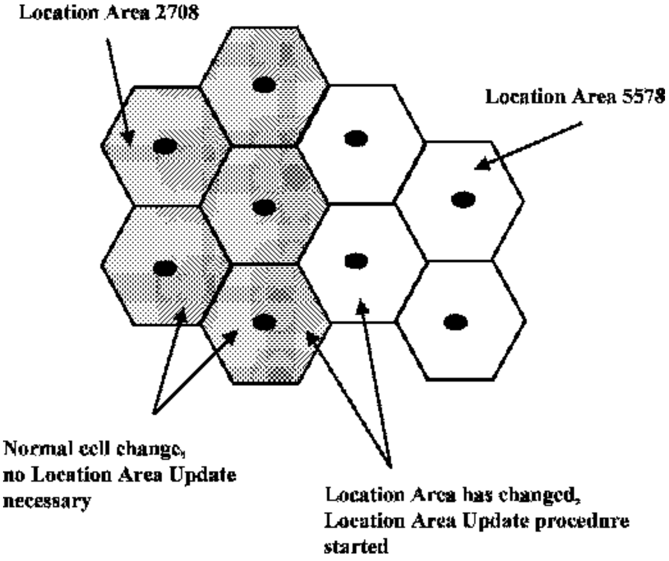

Location Area 2708
Location Area 5578
Normal cell change, no Location Area Update necessary
Location Area has changed, Location Area Update procedure started

Figure 1.39 Cells in different location areas

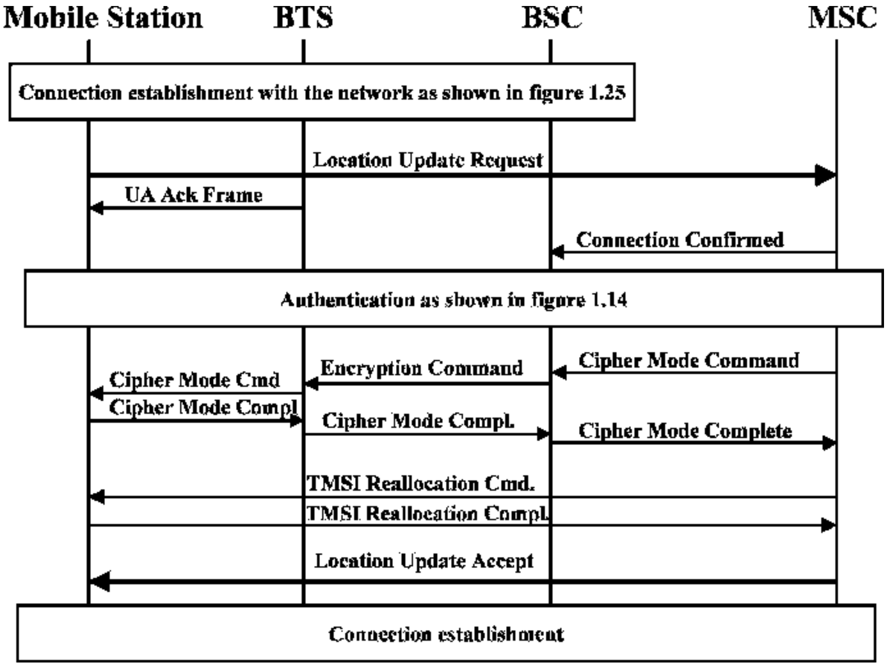


Figure 1.40 Message flow for a location update procedure

to identify itself instead of the IMSI. By using a constantly changing temporary ID, the identity of a subscriber is not revealed to listeners during the first phase of the call which is not ciphered. Once TMSI reallocation has been performed, the location area update message is sent to the network which acknowledges the correct reception. After receiving the acknowledgment, the connection is terminated and the mobile station returns to idle state.

If the old and new location areas are under the administration of two different MSC/VLRs, a number of additional steps are necessary. In this case, the new MSC/VLR has to inform the HLR that the subscriber has roamed into its area of responsibility. The HLR then deletes the record of the subscriber in the old MSC/VLR. This procedure is called an Inter-MSC location update. From the mobile point of view, however, there is no difference to a standard location update as the additional messages are only exchanged in the core network.

1.8.2 The Mobile Terminated Call

An incoming call for a mobile subscriber is called a mobile terminated call by the GSM standards. The main difference between a mobile network and a fixed-line PSTN network is the fact that the telephone number of the subscriber does not hold any information about where the subscriber is located. In the mobile network it is thus necessary to query the HLR for the current location of the subscriber before the call can be forwarded to the correct switching center.

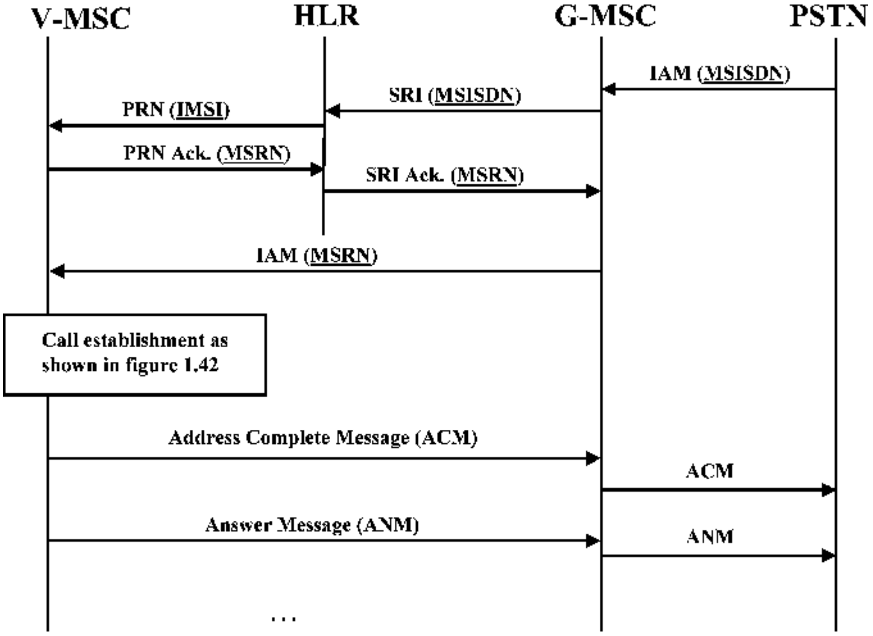


Figure 1.41 Mobile terminated call establishment, part 1

Figure 1.41 shows the first part of the message flow for a mobile terminated call initiated from a fixed-line subscriber. From the fixed-line network, the gateway-MSC (G-MSC) receives the telephone number (MSISDN) of the called party via an ISUP IAM message. The subsequent message flow on this interface is as shown in Figure 1.6 and the fixed-line network does not have to be aware that the called party is a mobile subscriber. The G-MSC in this example is simply a normal MSC with additional connections to other networks. When the G-MSC receives the IAM message, it sends a send routing information message (SRI) to the HLR in order to locate the subscriber in the network. The MSC currently responsible for the subscriber is also called the subscriber's visited MSC (V-MSC).

The HLR then determines the subscriber's IMSI by using the MSISDN to search through its database and thus is able to locate the subscriber's current V-MSC. The HLR then sends a provide roaming number (PRN) message to the V-MSC/VLR to inform the switching center of the incoming call. In the V-MSC/VLR, the IMSI of the subscriber, which is part of the PRN message, is associated with a temporary mobile station roaming number (MSRN) which is returned to the HLR. The HLR then transparently returns the MSRN to the Gateway-MSC.

The G-MSC uses the MSRN to forward the call to the V-MSC. This is possible as the MSRN not only temporarily identifies the subscriber in the V-MSC/VLR but also uniquely identifies the V-MSC to external switches. To forward the call from the G-MSC to the V-MSC, an IAM message is used again, which instead of the MSISDN contains the MSRN to identify the subscriber. This has been done as it is possible, and even likely, that there are transit switching centers between the G-MSC and V-MSC, which are thus able to forward the call without querying the HLR themselves.

As the MSRN is internationally unique instead of only in the subscriber's home network, this procedure can still be used if the subscriber is roaming in a foreign network. The presented procedure therefore works for both national and international roaming. As the MSRN is saved in the billing record for the connection, it is also possible to invoice the terminating subscriber for forwarding the call to a foreign network and to transfer a certain amount of the revenue to the foreign network operator.

In the V-MSC/VLR, the MSRN is used to find the subscriber's IMSI and thus the complete subscriber record in the VLR. This is possible because the relationship between the IMSI and MSRN was saved when the HLR first requested the MSRN. After the subscriber's record has been found in the VLR database, the V-MSC continues the process and searches the subscriber in the last reported location area, which was saved in the VLR record of the subscriber. The MSC then sends a paging message to the responsible BSC. The BSC in turn sends a paging message via each cell of the location area on the PCH. If no answer is received the message is repeated after a number of seconds.

After the mobile station has answered the paging message, an authentication and ciphering procedure has to be executed to secure the connection in a similar way as previously presented for a location update. Only afterwards is the mobile station informed about the details of the incoming call with a setup message. The setup message contains, for example, the telephone number of the caller if the CLIP supplementary service is active for this subscriber and not suppressed by the CLIR option which can be set by the caller (see Table 1.4).

If the mobile station confirms the incoming call with a call confirmed message, the MSC requests the establishment of a TCH for the voice path from the BSC. See Figure 1.42.

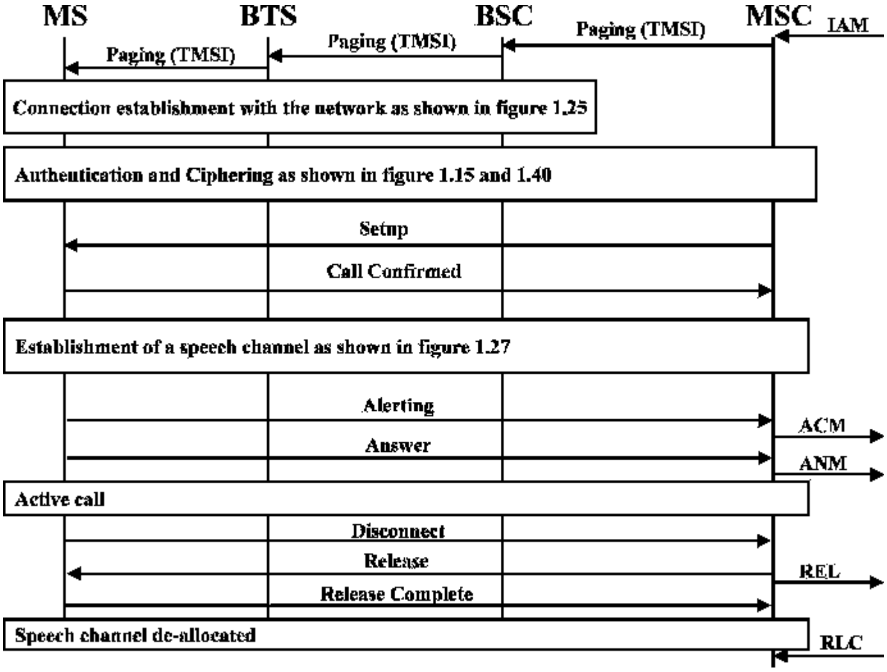

MS
BTS
BSC
MSC
IAM
Paging (TMSI)
Paging (TMSI)
Paging (TMSI)
Connection establishment with the network as shown in figure 1.25
Authentication and Ciphering as shown in figure 1.15 and 1.40
Setup
Call Confirmed
Establishment of a speech channel as shown in figure 1.27
Alerting
ACM
Answer
ANM
Active call
Disconnect
Release
REL
Release Complete
Speech channel de-allocated
RLC

Figure 1.42 Mobile terminated call establishment, part 2

After successful establishment of the speech path, the mobile station returns an alerting message and thus informs the MSC that the subscriber is informed of the incoming call (the phone starts ringing). The V-MSC then forwards this information via the address complete message (ACM) to the G-MSC. The G-MSC then also forwards the alerting indication to the fixed-line switch via its own ACM message.

Once the mobile subscriber accepts the call by pressing the answer button, the mobile station returns an answer message to the V-MSC. Here, an ISUP answer (ANM) message is generated and returned to the G-MSC. The G-MSC forwards this information again via an ANM message back to the fixed-line switching center.

While the conversation is ongoing, the network continues to exchange messages between different components in order to ensure that the connection is maintained. Most of the messages are measurement report messages, which are exchanged between the mobile station, the base station, and the BSC. If necessary, the BSC can thus trigger a handover to a different cell. More about the handover process can be found in Section 1.8.3.

If the mobile subscriber wants to end the call, the mobile station sends a disconnect message to the network. After releasing the traffic channel with the mobile station and after sending an ISUP release (REL) message to the other party, all resources in the network are freed and the call ends.

In this example, it has been assumed that the mobile subscriber is not in the area that is covered by the G-MSC. Such a scenario, however, is quite likely if a call is initiated by a fixed-line subscriber to a mobile subscriber which currently roams in the same region. As the fixed-line network usually forwards the call to the closest MSC to save costs, the G-MSC will in many cases also be the V-MSC for the connection. The G-MSC recognizes such a scenario if the MSRN returned by the HLR in the SRI acknowledge message contains a number, which is from the MSRN pool of the G-MSC. In this case, the call is treated in the G-MSC right away and the ISUP signaling inside the mobile network (IAM, ACM, ANM) is left out. More details about call establishment procedures in GSM networks can be found in [19].

1.8.3 Handover Scenarios

If reception conditions deteriorate during a call due to a change in the location of the subscriber, the BSC has to initiate a handover procedure. The basic procedure and the necessary messages have already been shown in Figure 1.28. Depending on which parts of the network are involved in the handover, one of the following handover scenarios is used to ensure that the connection remains established:

- Intra-BSC handover: in this scenario, the current cell and new cell are connected to the same BSC. This scenario is shown in Figure 1.28.
- Inter-BSC handover: if a handover has to be performed into a cell which is connected to a second BSC, the current BSC is not able to control the handover itself as no direct signaling connection exists between the BSCs of a network. Thus, the current BSC requests that the MSC initiates a handover to the other cell by sending a handover request message. Important parameters of the message are the cell-ID and the location area code (LAC) of the new cell. As the MSC administers a list of all LACs and cells under its control, it can find the correct BSC and request the establishment of a traffic channel for the handover

in a next step. Once the new BSC has prepared the speech channel (TCH) in the new cell, the MSC returns a handover command to the mobile station via the still existing connection over the current BSC. The mobile station then performs the handover to the new cell. Once the new cell and BSC have detected the successful handover, the MSC can switch over the speech path and inform the old BSC that the traffic channel for this connection can be released.

- Inter-MSC handover: if the current and new cells for a handover procedure are not connected to the same MSC, the handover procedure is even more complicated. As in the example before, the BSC detects that the new cell is not in its area of responsibility and thus forwards the handover request to the MSC. The MSC also detects that the LAC of the new cell is not part of its coverage area. Therefore, the MSC looks into another table which lists all LACs of the neighboring MSCs. As the MSC in the next step contacts a second MSC, the following terminology is introduced to unambiguously identify the two MSCs: the MSC which has assigned a MSRN at the beginning of the call is called the anchor-MSC (A-MSC) of the connection. The MSC that receives the call during a handover is called the relay-MSC (R-MSC). See Figure 1.43.

In order to perform the handover, the A-MSC sends a MAP (mobile application part, see Section 1.4.2) handover message to the R-MSC. The R-MSC then asks the responsible BSC to establish a traffic channel in the requested cell and reports back to the A-MSC. The A-MSC then instructs the mobile station via the still existing connection over the current cell to perform the handover. Once the handover has been performed successfully, the R-MSC reports the successful handover to the A-MSC. The A-MSC can then switch the voice path towards the R-MSC. Afterwards, the resources in the old BSC and cell are released.

If the subscriber yet again changes to another cell during the call, which is controlled by yet another MSC, a subsequent inter-MSC handover has to be performed (Figure 1.44).

For this scenario, the current relay-MSC (R-MSC 1) reports to the A-MSC that a subsequent inter-MSC handover to R-MSC 2 is required in order to maintain the call. The A-MSC then instructs R-MSC 2 to establish a channel in the requested cell. Once the speech channel is ready in the new cell, the A-MSC sends the handover command message via R-MSC 1.

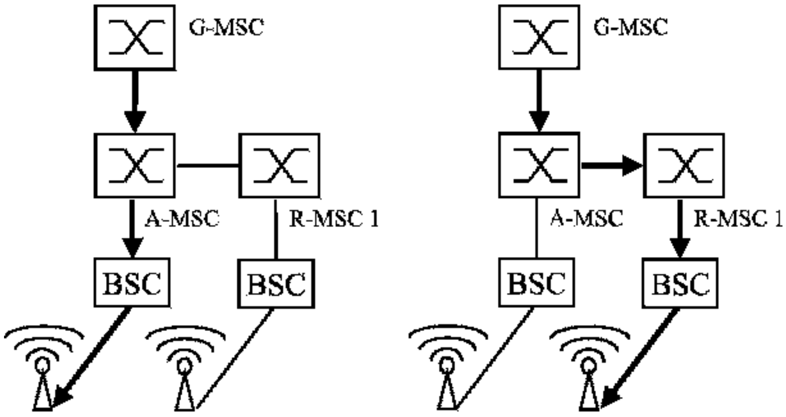


Figure 1.43 Inter-MSC handover

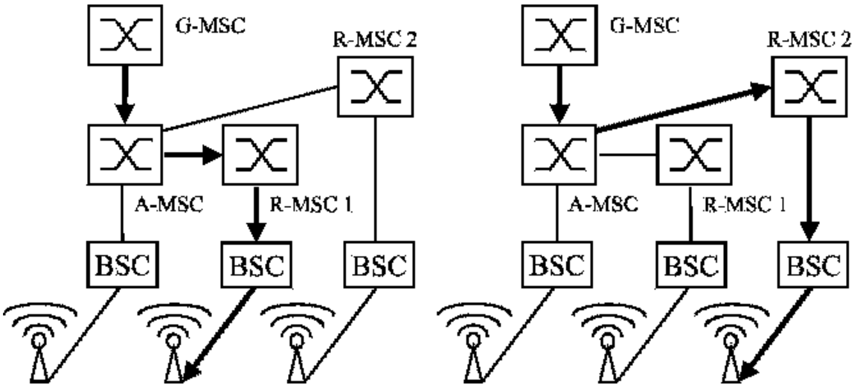


Figure 1.44 Subsequent inter-MSC handover

The mobile station then performs the handover to R-MSC 2 and reports the successful execution to the A-MSC. The A-MSC can then redirect the speech path to R-MSC 2 and instruct R-MSC 1 to release the resources. By having the A-MSC in command in all the different scenarios, it is assured that during the lifetime of a call only the G-MSC, the A-MSC, and at most one R-MSC are part of a call. Additionally, tandem switches might be necessary to route the call through the network or to a roaming network. However, these switches purely forward the call and are thus transparent in this procedure.

Finally, there is also a handover case in which the subscriber, who is served by an R-MSC, returns to a cell which is connected to the A-MSC. Once this handover is performed, no R-MSC is part of the call. Therefore, this scenario is called a subsequent handback.

From the mobile station point of view, all handover variants are performed in the same way, as the handover messages are identical for all scenarios. In order to perform a handover as quickly as possible, however, GSM can send synchronization information for the new cell inside the handover message. This allows the mobile station to immediately switch to the allocated timeslot instead of having to synchronize first. This can only be done, however, if current and new cell are synchronized with each other which is not possible for example if they are controlled by different BSCs. As two cells which are controlled by the same BSC may not necessarily be synchronized, synchronization information is by no means an indication of what kind of handover is being performed in the radio and core network.

1.9 The Mobile Station

Due to the progress of miniaturization of electronic components during the mid-1980s, it was possible to integrate all components of a mobile phone into a single portable device. Only a few years later, mobile phones have shrunk to such a small size that the limiting factor in future miniaturization is no longer the size of the electronic components. Instead, the space required for user interface components like display and keypad limit a further reduction. Due to the continuous improvement and miniaturization of electronic components, it is possible to integrate more and more functionalities into a mobile phone and to improve the ease of use. While mobile phones were at first only used for voice calls, the trend today is a move towards devices ‘with an integrated mobile phone’ for different user groups:

- PDA with mobile phone for voice and data communication.
- Game consoles with integrated mobile phone for voice and data communication (e.g. multi-user games with a real-time interconnection of the players via the wireless Internet).
- Mobile phones for voice communication with integrated Bluetooth interface that lets devices such as PDAs or notebooks use the phone as a connection to the Internet.

Independent of the size and variety of different functionalities, the basic architecture of all mobile phones, which is shown in Figure 1.45, is very similar. The core of the mobile phone is the base band processor which contains a RISC (reduced instruction set) CPU and a digital signal processor (DSP). The RISC processor is responsible for the following tasks:

- Handling of information that is received via the different signaling channels (BCCH, PCH, AGCH, PCH, etc.).
- Call establishment (DTAP).
- GPRS management and GPRS data flow.
- Parts of the transmission chain: channel coder, interleaver, cipherer (dedicated hardware component in some designs).
- Mobility management (network search, cell reselection, location update, handover, timing advance, etc.).
- Connections via external interfaces like Bluetooth, RS-232, IrDA, USB.
- User interface (keypad, display, graphical user interface).

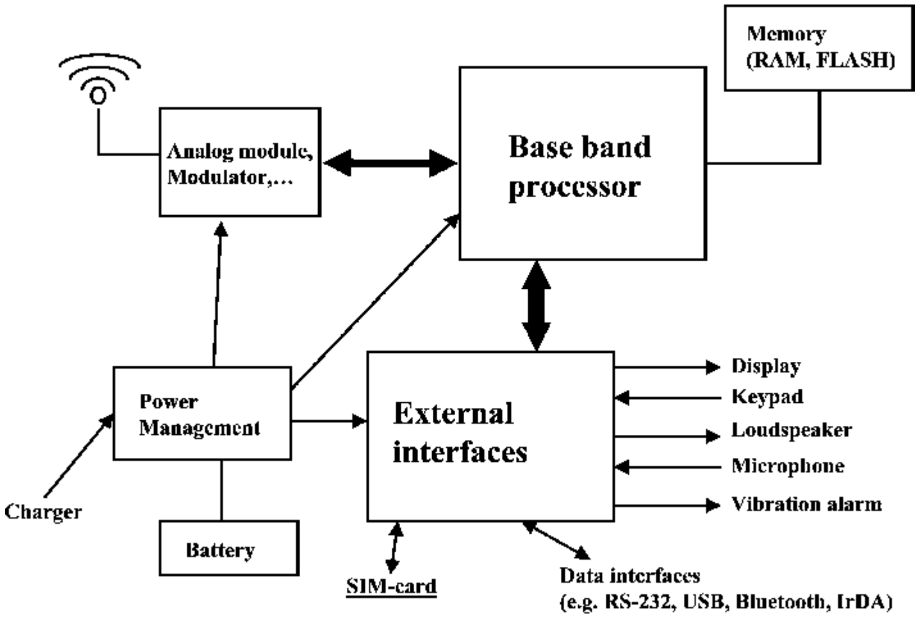


Figure 1.45 Basic architecture of a mobile phone

As many of these tasks have to be performed in parallel, a multitasking embedded real-time operating system is used on the RISC processor. The real-time component of the operating system is especially important as the processor has to be able to provide data for transmission over the air interface according to the GSM frame structure and timing. All other tasks like keypad handling, display update and the graphical user interface, in general, have a lower priority. This can be observed with many mobile phones during a GPRS data session. Here, the RISC CPU is not only used for signaling, but also for treating incoming and outgoing data and forwarding the data stream between the network and an external device like a notebook or PDA. Especially during times of high volume data transfers, it can be observed that the mobile phone reacts slowly to user input, because treating the incoming and outgoing data flow has a higher priority.

The processor capacity of the RISC processor is the main factor when deciding which applications and features to implement in a mobile phone. For applications like recording and displaying digital pictures or videos for example, fast processing capabilities are required. One of the RISC architectures that is used for high-end GSM and UMTS mobile phones is the ARM-9 architecture. This processor architecture allows CPU speeds of over 200 MHz and provides sufficient computing power for calculation intensive applications like those mentioned before. The downside of fast processors, however, is higher power consumption, which forces designers to increase battery capacity while trying at the same time to maintain the physical dimensions of a small mobile phone. Therefore, intelligent power-saving mechanisms are required in order be able to reduce power consumption during times of inactivity.

The DSP is another important component of a GSM and UMTS chipset. Its main task is FR, EFR, HR, or AMR speech compression. Furthermore, the DSP is used in the receiver chain to help decode the incoming signal. This is done by the DSP analyzing the training sequence of a burst (see Section 1.7.3). As the DSP is aware of the composition of the training sequence of a frame, the DSP can calculate a filter which is then used to decode the data part of the burst. This increases the probability that the data can be correctly reconstructed. The DSP 56600 architecture with a processor speed of 104 MHz is often used for these tasks.

Figure 1.46 shows which tasks are performed by the RISC processor and the DSP processor, respectively. If the transmission chain for a voice signal is compared between

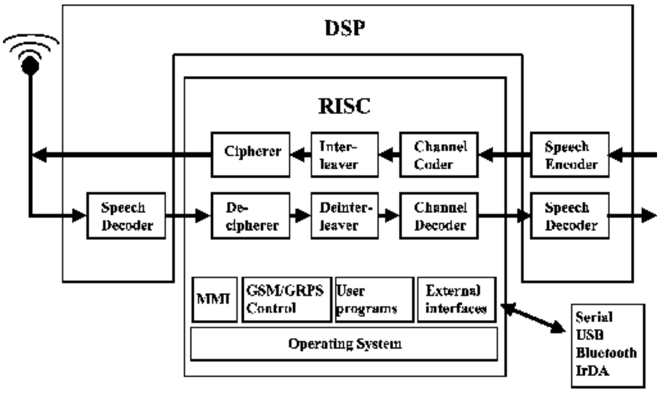


Figure 1.46 Overview of RISC and DSP functionalities

the mobile phone and the network, it can be seen that the TRAU mostly performs the task the DSP unit is responsible for in the mobile phone. All other tasks such as channel coding are performed by the BTS which is thus the counterpart of the RISC CPU of the mobile phone.

As millions of mobile phones are sold every year, there is a great variety of chipsets available on the market. The chipset is in many cases not designed by the manufacturer of the mobile phone. While Motorola design its own chipsets, Nokia relies on chipsets of STMicroelectronics and Texas Instruments. Other GSM chipset developers include Infineon, Analog Devices, and Philips, as well as many Asian companies.

Furthermore, mobile phone manufacturers are also outsourcing parts of the mobile phone software development. BenQ/Siemens for example uses the WAP browser of OpenWave, which the company has also sold to other mobile phone manufacturers. This demonstrates that many companies are involved in the development and production of a mobile phone. It can also be observed that most GSM and UMTS phones today are shipped with a device-independent Java runtime environment, which is called the Java 2 Micro Edition (J2ME) [20]. This allows third-party companies and individuals to develop programs which can be ported with no or only minor effort to other mobile phones as well. Most games for example, which are available for GSM and UMTS mobile phones today, are based on J2ME and many other applications like email and other office software is available via the mobile network operator or directly via the Internet.

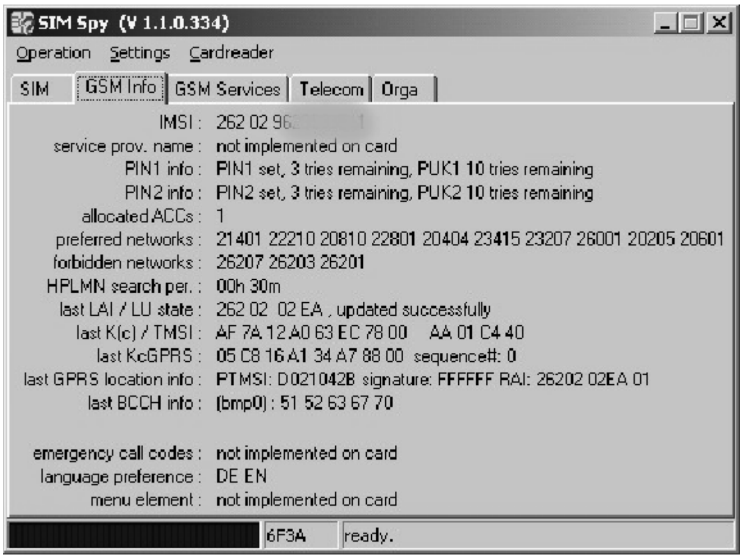
1.10 The SIM Card

Despite its small size, the SIM card is one of the most important parts of a GSM network because it contains all the subscription information of a subscriber. Since it is standardized, a subscriber can use any GSM or UMTS phone by simply inserting the SIM card. Exceptions are phones that contain a ‘SIM lock’ and thus only work with a single SIM card or only with the SIM card of a certain operator. However, this is not a GSM restriction. It was introduced by mobile phone operators to ensure that a subsidized phone is only used with SIM cards of their network.

The most important parameters on the SIM card are the IMSI and the secret key (Ki), which is used for authentication and the generation of ciphering keys (Kc). With a number of tools, which are generally available on the Internet free of charge, it is possible to read out most parameters from the SIM card, except for sensitive parameters that are read protected. Figure 1.47 shows such a tool. Protected parameters can only be accessed with a special unlock code that is not available to the end user.

Astonishingly, a SIM card is much more than just a simple memory card as it contains a complete microcontroller system that can be used for a number of additional purposes. The typical properties of a SIM card are shown in Table 1.7.

As shown in Figure 1.48, the mobile phone cannot access the information on the EEPROM directly, but has to request the information from the SIM’s CPU. Therefore, direct access to sensitive information is prohibited. The CPU is also used to generate the SRES during the network authentication procedure based on the RAND which is supplied by the authentication center (see Section 1.6.4). It is imperative that the calculation of the SRES is done on the SIM card itself and not in the mobile phone in order to protect the secret Ki key. If the



```
                   IMSI :  262 02 96[redacted]
      service prov. name :  not implemented on card
               PIN1 info :  PIN1 set, 3 tries remaining, PUK1 10 tries remaining
               PIN2 info :  PIN2 set, 3 tries remaining, PUK2 10 tries remaining
          allocated ACCs :  1
      preferred networks :  21401 22210 20810 22801 20404 23415 23207 26001 20205 20601
      forbidden networks :  26207 26203 26201
      HPLMN search per. :  00h 30m
       last LAI / LU state :  262 02  02 EA , updated successfully
        last K(c) / TMSI :  AF 7A 12 A0 63 EC 78 00    AA 01 C4 40
            last KcGPRS :  05 C8 16 A1 34 A7 88 00  sequence#: 0
 last GPRS location info :  PTMSI: D021042B signature: FFFFFF RAI: 26202 02EA 01
          last BCCH info :  (bmp0) : 51 52 63 67 70

    emergency call codes :  not implemented on card
     language preference :  DE EN
            menu element :  not implemented on card
```

Figure 1.47 Example of a tool to visualize the data contained on a SIM card

Table 1.7 SIM card properties

CPU	8- or 16-bit CPU
ROM	40–100 kbyte
RAM	1–3 kbyte
EEPROM	16–64 kbyte
Clock rate	10 MHz, generated from clock supplied by mobile phone
Operating voltage	3 V or 5 V

calculation was done in the mobile phone itself, this would mean that the SIM card would have to hand over the Ki to the mobile phone or any other device upon request. This would seriously undermine security as tools like the one shown in Figure 1.47 would be able to read the Ki which then could be used to make a copy of the SIM card.

Furthermore, the microcontroller system on the SIM can also execute programs which the network operator may have installed on the SIM card. This is done via the SIM application toolkit (SAT) interface, which is specified in 3GPP TS 31.111 [21]. With the SAT interface, programs on the SIM card can access functionalities of the mobile phone such as waiting for user input, or can be used to show text messages and menu entries on the display. Many mobile network operators use this functionality to put an operator-specific menu item into the overall menu structure of the mobile phone's graphical user interface. In the menu created by the SIM card program, the subscriber can, for example, request a current news overview. When the subscriber enters the menu, all user input via the keypad is forwarded by the mobile phone to the SIM card. The program on the SIM card in this example would

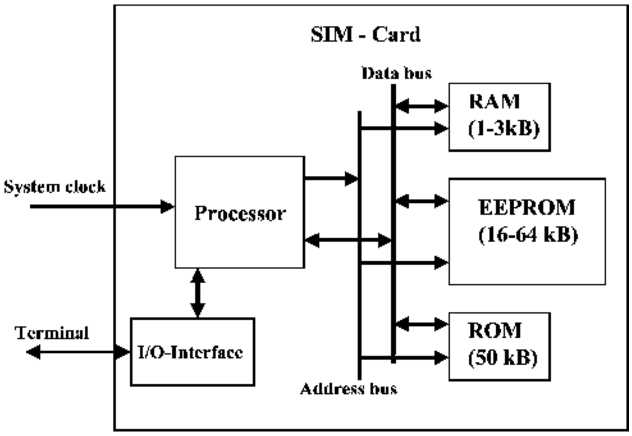


Figure 1.48 Block diagram of SIM card components

react to the news request by generating an SMS, which it then instructs the mobile phone to send to the network. The network replies with one or more SMS messages which contain a news overview. The SIM card can then extract the information from the SMS messages and present the content to the subscriber.

A much more complex application of the SIM application toolkit is in use by O2 Germany for a service called ‘Genion’. If a user has subscribed to ‘Genion’, he can make cheaper calls to fixed-line phones if the subscriber is currently located in his so-called ‘homezone’. To define the homezone, the SIM card contains information about its size and geographical location. In order to inform the user if he is currently located in his homezone, the SIM card receives information about the geographical position of the current serving cell. This information is broadcast to the mobile phone via the short message service broadcast channel (SMSCB) of the cell. When the program on the SIM card receives this information, it compares the geographical location contained on the SIM card with the coordinates received from the network. If the user is inside his homezone, the SIM card then instructs the mobile phone to present a text string (‘home’ or ‘city’) in the display for the user.

From a logical point of view, data is stored on a GSM SIM card in directories and files in a similar way as on a PC’s hard drive. The file and folder structure is specified in 3GPP TS 31.102 [22]. In the specification, the root directory is called the main file (MF) which is somewhat confusing at first. Subsequent directories are called dedicated files (DF) and normal files are called elementary files (EF). As there is only a very limited amount of memory on the SIM card, files are not identified via file and directory names. Instead, hexadecimal numbers with a length of four digits are used which require only two bytes of memory. The standard nevertheless assigns names to these numbers which are, however, not stored on the SIM card. The root directory for example is identified via ID 0x3F00, the GSM directory is identified by ID 0x7F20, and the file containing the IMSI for example is identified via ID 0x6F07. In order to read the IMSI from the SIM card, the mobile station thus has to open the following path and file: 0x3F00 0x7F20 0x6F07.

To simplify access to the data contained on the SIM card for the mobile phone, a file can have one of the following three file formats:

- Transparent: the file is seen as a sequence of bytes. The file for the IMSI for example is of this format. How the mobile station has to interpret the content of the files is again specified in 3GPP TS 31.002 [22].
- Linear fixed: this file type contains records of a fixed length and is used for example for the file that contains the telephone book records. Each phone record uses one record of the linear fixed file.
- Cyclic: this file type is similar to the linear fixed file type but contains an additional pointer which points to the last modified record. Once the pointer reaches the last record of the file, it wraps over again to the first record of the file. This format is used for example for the file in which the phone numbers are stored which have previously been called.

A number of different access right attributes are used to protect the files on the SIM card. By using these attributes, the card manufacturer can control if a file is read or write only when accessed by the mobile phone. A layered security concept also permits network operators to change files which are read only for the mobile phone over the air by sending special provisioning SMS messages.

The mobile phone can only access the SIM card if the user has typed in the PIN when the phone is started. The mobile phone then uses the PIN to unlock the SIM card. SIM cards of some network operators, however, allow deactivating the password protection and thus the user does not have to type in a PIN code when the mobile phone is switched on. Despite unlocking the SIM card with the PIN, the mobile phone is still restricted to only being able to read or write certain files. Thus, it is not possible for example to read or write the file which contains the secret key Ki even after unlocking the SIM card with the PIN.

Details on how the mobile station and the SIM card communicate with each other has been specified in ETSI TS 102 221 [23]. For this interface, layer 2 command and response messages have been defined which are called application protocol data units (APDU). When a mobile station wants to exchange data with the SIM card, a command APDU is sent to the SIM card. The SIM card analyzes the command APDU, performs the requested operation, and returns the result in a response APDU. The SIM card only has a passive role in this communication as it can only send response APDUs back to the mobile phone.

If a file is to be read from the SIM card, the command APDU contains among other information the file ID and the number of bytes to read from the file. If the file is of type cyclic or linear fixed, the command also contains the record number. If access to the file is allowed, the SIM card then returns the requested information in one or more response APDUs.

If the mobile phone wants to write some data into a file on the SIM card, the command APDUs contain the file ID and the data to be written into the file. In the response APDU, the SIM card then returns a response as to whether the data was successfully written to the file.

Figure 1.49 shows the format of a command APDU. The first field contains the class of instruction, which is always 0xA0 for GSM. The instruction (INS) field contains the ID of the command that has to be executed by the SIM card.

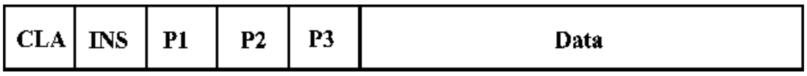


Figure 1.49 Structure of a command APDU

Table 1.8 shows some commands and their IDs. The fields P1 and P2 are used for additional parameters for the command. P3 contains the length of the following data field which contains the data that the mobile phone would like to write to the SIM card.

The format of a response APDU is shown in Figure 1.50. Apart from the data field, the response also contains two fields called SW1 and SW2. These are used by the SIM card to inform the mobile station if the command was executed correctly.

An example: to open a file for reading or writing, the mobile station sends a SELECT command to the SIM card. The SELECT APDU is structured as shown in Figure 1.51.

As a response, the SIM card replies with a response APDU which contains a number of fields. Some of them are shown in Table 1.9.

For a complete list of information returned for the example, see [23]. In a next step, the READ BINARY or WRITE BINARY APDU can be used to read or modify the file.

In order to physically communicate with the SIM card, there are six contact areas on the top side of the SIM card. Only four of those contacts are required:

- C1: power supply;
- C2: reset;
- C3: clock;
- C7: input/output.

Table 1.8 Examples for APDU commands

Command	ID	P1	P2	Length
Select (open file)	A4	00	00	02
Read Binary (read file)	B0	Offset High	Offset Low	Length
Update Binary (write file)	D6	Offset High	Offset Low	Length
Verify CHV (check PIN)	20	00	ID	08
Change CHV (change PIN)	24	00	ID	10
Run GSM algorithm (RAND, SRES, Kc,…)	88	00	00	10

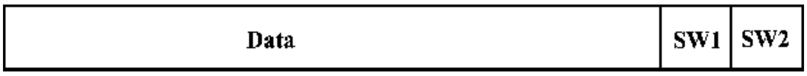


Figure 1.50 Response APDU

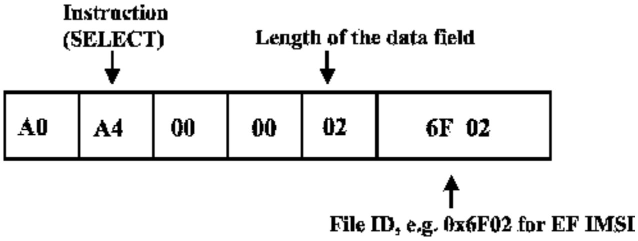


Figure 1.51 Structure of the SELECT command APDU

Table 1.9 Some fields of the response APDU for a SELECT command

Byte	Description	Length
3–4	File size	2
5–6	File ID	2
7	Type of file (transparent, linear fixed, cyclic)	1
9–11	Access rights	3
12	File status	1

As only a single line is used for input and output of command and status APDUs, the data is transferred in half-duplex mode only. The clock speed for the transmission has been defined as C3/327. At a clock speed of 5 MHz on C3, the transmission speed is thus 13,440 bit/s.

1.11 The Intelligent Network Subsystem and CAMEL

All components that have been described in this chapter are mandatory elements for the operation of a mobile network. Mobile operators, however, usually offer additional services beyond simple post-paid voice services for which additional logic and databases are necessary in the network. Here are a number of examples:

- Location based services (LBS) are offered by most network operators in Germany in different variations. One LBS example is to offer cheaper phone calls to fixed-lines phones in the area in which the mobile subscriber is currently located. In order to be able to apply the correct tariff for the call, the LBS service in the network checks if the current location of the subscriber and the dialed number are in the same geographical area. If so, additional information is attached to the billing record so the billing system can later calculate the correct price for the call.
- Prepaid services have become very popular in many countries since their introduction in the mid-1990s. Instead of receiving a bill once a month, a prepaid subscriber has an account with the network operator which is funded in advance with a certain amount of money determined by the subscriber. The amount on the account can then be used for phone calls and other services. During every call, the account is continually charged. If the account runs out of credit, the connection is interrupted. Furthermore, prepaid systems are also connected to the SMSC, the multimedia messaging server (MMS-Server, see

Chapter 2), and the GPRS network (see Chapter 2). Therefore, prepaid subscribers can also be charged in real time for the use of these services.

These and many other services can be realized with the help of the intelligent network (IN) subsystem. The logic and the necessary databases are located on a service control point (SCP), which has already been introduced in Section 1.4.

In the early years of GSM, the development of these services had been highly proprietary due to the lack of a common standard. The big disadvantage of such solutions was that they were customized to work only with very specific components of a single manufacturer. This meant that these services did not work abroad as foreign network operators used components of other network vendors. This was especially a problem for the prepaid service as prepaid subscribers were excluded from international roaming when the first services were launched.

In order to ensure the interoperability of intelligent network components between different vendors and in networks of different mobile operators, industry and operators standardized an IN network protocol in 3GPP TS 22.078 [24] which is called customized applications for mobile enhanced logic, or CAMEL for short. While CAMEL also offers functionality for SMS and GPRS charging, the following paragraph only describes the basic functionality necessary for circuit-switched connections.

CAMEL is not an application or a service, but forms the basis to create services (customized applications) on an SCP, which is compatible with network elements of other vendors and between networks. Thus, CAMEL can be compared with the HTTP protocol for example. HTTP is used for transferring web pages between a web server and a browser. HTTP ensures that any web server can communicate with any browser. If the content of the data transfer is a web page or a picture is of no concern to HTTP because this is managed on a higher layer directly by the web server and the web client. Transporting the analogy back to the GSM world, the CAMEL specification defines the protocol for the communication between the different network elements such as the MSC and the SCP, as well as a state model for call control.

The state model is called the basic call state model (BCSM) in CAMEL. A circuit-switched call for example is divided into a number of different states. For the originator (O-BCSM) the following states, which are also shown in Figure 1.52, have been defined:

- call establishment;
- analysis of the called party number;
- routing of the connection;
- notification of the called party (alerting);
- call is ongoing (active);
- disconnection of the call;
- no answer of the called party;
- called party busy.

For a called subscriber, CAMEL also defines a state model which is called the terminating BCSM (T-BCSM). T-BCSM can be used for prepaid subscribers who are currently roaming in a foreign network in order to control the call to the foreign network and to apply real-time charging.

For every state change in the state model, CAMEL defines a detection point (DP). If a DP is activated for a subscriber, the SCP is informed of the particular state change. Information

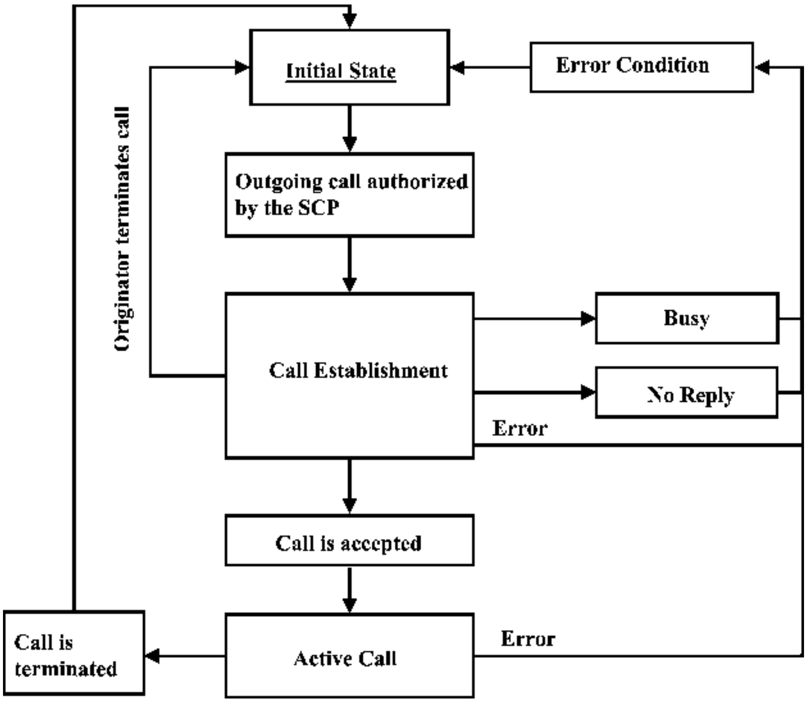


Figure 1.52 Simplified state model for an originator (O-BCSM) according to 3GPP TS 23.078 [25]

contained in this message is for example the IMSI of the subscriber, the current position (MCC, MNC, LAC, and cell-ID), and the number that was called. Whether a detection point is activated is part of the subscriber's HLR entry. This allows creating specific services on a per subscriber basis. When the SCP is notified that the state model has triggered a detection point, the SCP is able to influence how the call should proceed. The SCP can take the call down, change the number that was called, or return information to the MSC, which is put into the billing record of the call for later analysis on the billing system.

For the prepaid service for example the CAMEL protocol can be used between the MSC and the SCP as follows.

If a subscriber wants to establish a call, the MSC detects during the setup of the call, that the 'authorize origination' detection point is activated in the subscriber's HLR entry. Therefore, the MSC sends a message to the SCP and waits for a reply. As the message contains the IMSI of the subscriber as well as the CAMEL service number, the SCP recognizes that the request is for a prepaid subscriber. By using the destination number, the current time and other information, the SCP calculates the price per minute for the connection. If the subscriber's balance is sufficient, the SCP then allows the call to proceed and informs the MSC for how many minutes the authorization is valid. The MSC then continues and connects the call. At the end of the call, the MSC sends another message to the SCP to inform it of the total duration of the call. The SCP then modifies the subscriber's balance. If the time which the SCP initially granted for the call expires, the MSC has to contact the SCP again. The SCP then has the possibility to send an additional authorization to the MSC which is again limited to a certain duration. Other options for the SCP to react are to send a reply in which the MSC is asked to terminate the call or to return a message in which the MSC is asked to play a tone as an indication to the user that the balance on the account is almost depleted.

Location based services (LBS) are another application for CAMEL. Again the HLR entry of a subscriber contains information at which detection points the CAMEL service is to be invoked. For LBS, the 'authorize origination' DP is activated. In this case, the SCP determines, by analyzing the IMSI and the CAMEL service ID, that the call has been initiated by a user that has subscribed to an LBS service. The service on the SCP then deduces from the current location of the subscriber and the national destination code of the dialed number which tariff to apply for the connection. The SCP then informs the MSC of the correct tariff by returning a 'furnish charging information' (FCI) message. At the end of the call, the MSC includes the FCI information in the billing record and thus enables the billing system to apply the correct tariff for the call.

1.12 Questions

1. Which algorithm is used to digitize a voice signal for transmission in a digital circuit-switched network and at which data rate is the voice signal transmitted?
2. Name the most important components of the GSM network subsystem (NSS) and their tasks.
3. Name the most important components of the GSM radio network (BSS) and their tasks.
4. How is a BTS able to communicate with several subscribers at the same time?
5. Which steps are necessary in order to digitize a speech signal in a mobile phone before it can be sent over the GSM air interface?
6. What is a handover and which network components are involved?
7. How is the current location of a subscriber determined for a mobile terminated call and how is the call forwarded through the network?
8. How is a subscriber authenticated in the GSM network? Why is an authentication necessary?
9. How is an SMS message exchanged between two subscribers?
10. Which tasks are performed by the RISC processor and which tasks are performed by the DSP in a mobile phone?
11. How is data stored on the SIM card?
12. What is CAMEL and for which services can it be used?

Answers to these questions can be found on the companion website for this book at http://www.wirelessmoves.com.

References

[1] European Technical Standards Institute (ETSI), website, http://www.etsi.org.
[2] The 3rd Generation Partnership Project, website, http://www.3gpp.org.
[3] 3GPP, 'Mobile Application Part (MAP) Specification', TS 29.002.
[4] 3GPP, 'AT Command Set for 3G User Equipment', TS 27.007.
[5] 3GPP, 'Call Forwarding (CF) Supplementary Services – Stage 1', TS 22.082.

[6] 3GPP, ‘Call Barring (CB) Supplementary Services – Stage 1’, TS 22.088.

[7] 3GPP, ‘Call Waiting (CW) and Call Hold (HOLD) Supplementary Services – Stage 1’, TS 22.083.

[8] 3GPP, ‘Multi Party (MPTY) Supplementary Services – Stage 1’, TS 22.084.

[9] 3GPP, ‘Man–Machine Interface (MMI) of the User Equipment (UE)’, TS 22.030.

[10] 3GPP, ‘Mobile Radio Interface Layer 3 Specification; Core Network Protocols – Stage 3’, TS 24.008.

[11] 3GPP, ‘Technical Realisation of Short Message Service (SMS)’, TS 23.040.

[12] 3GPP, ‘Voice Group Call Service (VGCS) – Stage 2’, TS 43.068.

[13] 3GPP, ‘Voice Broadcast Service (VGS) – Stage 2’, TS 43.069.

[14] 3GPP, ‘Enhanced Multi-Level Precedence and Preemption Service (eMLPP) – Stage 2’, TS 23.067.

[15] Union Internationale des Chemins de Fer, GSM-R website, http://gsm-r.uic.asso.fr.

[16] 3GPP, ‘Multiplexing and Multiple Access on the Radio Path’, TS 45.002.

[17] 3GPP, ‘AMR Speech CODEC: General Description’, TS 26.071.

[18] 3GPP, ‘Full Speech Transcoding’, TS 46.010.

[19] 3GPP, ‘Basic Call Handling: Technical Realization’, TS 23.018.

[20] Sun Microsystems, The Java 2 Micro Edition, http://java.sun.com/j2me/.

[21] 3GPP, ‘USIM Application Toolkit’, TS 31.111.

[22] 3GPP, ‘Characteristics of the USIM Application’, TS 31.102.

[23] ETSI, ‘Smart Cards; UICC-Terminal Interface; Physical and Logical Characteristics’, TS 102 221.

[24] 3GPP, ‘Customised Applications for Mobile Network Enhanced Logic (CAMEL): Service Description – Stage 1’, TS 22.078.

[25] 3GPP, ‘Customised Applications for Mobile Network Enhanced Logic (CAMEL): Service Description – Stage 2’, TS 23.078.