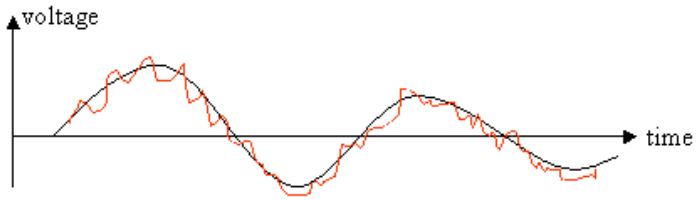
About the GSM-Dm-Channels

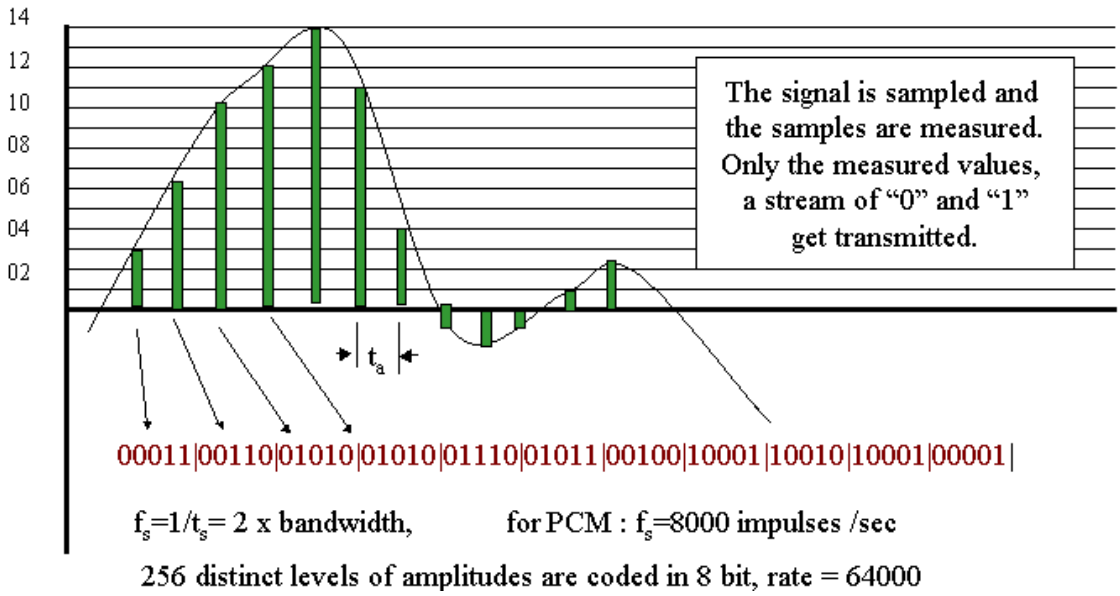
0. A little bit of History

In around 1986 a military Radio Transceiver was large (15 x 40 x 60cm) and heavy, weighing around 10kg. American devices were somewhat more sophisticated but only slightly smaller and lighter than the soviet equipment.
At the same time (1986) a “central co-ordination group”, called a nucleus, was set up to co-ordinate efforts for the development of a European Digital Mobile Radio System.
What has happened in the world of communication?
Since Phillip Reis and Graham Bell invented the telephone engineers have had problems transmitting the signal over long distances. Noise always interferes with the useful signal. Amplifying the useful signal also means amplifying the noise. Until 1938 there was no way to prevent this....



Picture 1: Noise interference during communication

In 1938 the French engineer Reves had a revolutionary idea: “The signal can be sampled and the samples measured. Only the measured values, i.e. a stream of “0s” and “1s”, are then transmitted.” i.e. the analog voice signal is changed into a digital signal



Picture 2: Reves’ innovation, digitalizing the analog information.

In 1938 it was impossible to utilise this idea because the electrical components available were not practical: the size of the tubes, coils, transformer, resistors, capacitors and so on, was in

the order of centimeters. An experimental breadboard circuit comprising of a twenty four-channel PCM device built in 1949 in East Berlin was as large as a sitting room.

For this reason an ISDN at that time was out of the question.
A lot of thought and time were necessary to bridge the gap.

You might ask 'Why are we considering the development of ISDN?'
The reason, as you shall see, is that the development of ISDN was prerequisite to the development of GSM, not only from a technological point of view, but also because of the amount of thought required to work out the signaling between a telephone station and a network. As you can read in the 'How To' section of this CBT, GSM Pioneers Michel MOULY and Marie-Bernadette PAUTET call ISDN 'the Godfather of GSM' because the work was inspired by the principles of ISDN and its access protocols.

Now let's move onto a short history of the technological development of electronics and have a look at the following picture:

1938	Invention of PCM by Reves
1943	The World's first digital Computer is built by Konrad Zuse
1948	Bardeen and Brattain invent the Transistor
1959	Noyce builds ICs in a planar process
1965	PCM in local telephone networks
1971	Ted Hoff invents the microprocessor
1972	**In a Japanese publication the concept ISDN appears for the first time**
1975	Local exchanges are controlled by microprocessors
1980-85	CCITT (today ITU) passes the main ISDN Standards
1982	Decision of DBP to introduce ISDN
1989	ISDN is introduced in Germany
1989	MoU introduces Euro-ISDN (DSS-1)
1993	Euro-ISDN is introduced in Germany

Picture 3: Timetable of main inventions leading to ISDN and therefore GSM

This is the background of events leading to the development of GSM:

1958	A-Network, first German Mobile Cellular Network starts
1979	The first Cellular System AMPS (Advanced Mobile Phone Service) is invented in Chicago, USA (**analog**)
1981	Sweden begins the **N**ordic **M**obile **T**elephone System (**analog**)
1982	"*Groupe Spècial Mobile"* is created within CEPT *(Conférence Européenne des Postes et Télécommunications)*
1985	C-Network (**analog**) is invented in Germany
1986	A Permanent Nucleus (a central co-ordinating group) is set up
1987	Memorandum of Understanding (MoU) GSM between 12 countries
1991	First Systems are running (Telecom 91... Exhibition) (***GSM*** *now stands for* ***Global System for Mobile Communication*** *)*
2000	357 GSM-Networks with 311 million subscribers in 133 countries

Picture 4: A Short History of GSM development

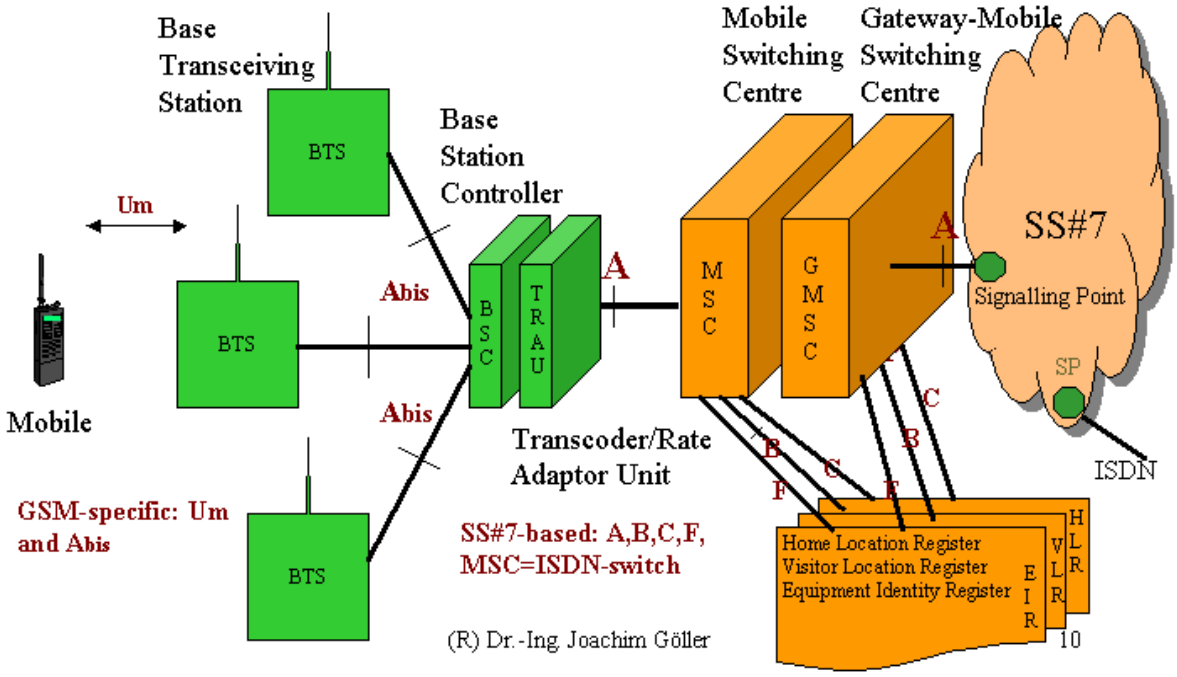
As you can see in picture 4, until the 1990s analog radio equipment was used in civil as well as military radio equipment.

However, during the introduction of analog devices into daily service, scientists in Europe worked to develop a very new technology made possible by the digital revolution.

We will now consider:
- what is the Global System of Mobile Communication?
- what are its components and how does it work?
- what are the basics of communication between the Mobile station and Network?

1. Structure and Components of a Mobile Network

Please consider the picture of components and interfaces in a Public Land Mobile Network.



Picture 5: Components and Interfaces in a Public Land Mobile Network PLMN

1.1 The Mobile Station

I shall begin with a description of the element on the far left, the Mobile Station.
You must bear in mind that a mobile station represents the latest developments not only in miniaturized electronics but also in:
- compression of speech to minimize bandwidth
- encoding to avoid eavesdropping of speech or data messages
- coding and decoding to detect and correct failures during transmission over the air interface.

There is an interesting difference between the Mobile Equipment and the Mobile Station. The former is the body, you only have the latter once you have added the Subscriber Identity Module (SIM) to the ME.
Let's have a look at the features of the body and brain.

1.1.1 The Mobile Equipment

The ME is a small transmitter–receiver station equipped with large-scale integrated circuits which allow:

- High-level digital filtering to enable a very short changeover time
- Fast signal processing and highly stable oscillators
- High performance signal processing for encoding and decoding of information
- Battery power supply allowing long standby time and a transmitting power of up to 8 watts
- Colour display with high resolution suited to viewing pictures taken by a 1.3 MB Pixel camera
- The body is characterized by an *International Mobile Equipment Identity* (IMEI). The IMEI consists of 15 digits (60 bits). There is a 6 digit type approval code TAC, a 2 digit Final Assembly Code FAC, 6 digit serial number SNR and a 4 bit space SP.

1.1.2 Subscriber Identity Module

The SIM consists of the mobile's data bank and free usable memory. The data bank consists of:

<u>Administrating data</u>

- The *Personal Identification Number* PIN
- The *Pin Unblocking Key* PUK
- The SIM-Service Table

<u>Authentication and Ciphering</u>

- The Encoding algorithms (A3, A8), identical to the ones held in the network, and the authentication computation
- Ciphering Key Sequence Number (CKSN) (3 bit) identical to the one held in the network
- The highly secret Kc and Ki

<u>Subscriber specific</u>

- International Mobile Subscriber Identity IMSI, consisting of 15 digits or less with a 3 digit mobile country code MCC, a 2 digit mobile network code MNC and an up to 10 digit mobile subscriber identification number MSIN
- Temporary Mobile Subscriber Identity TMSI, given to the mobile by the network during roaming (to hide the IMSI)

<u>Roaming data</u>

- Local Area Identity LAI
- Preferred PLMNs list
- Forbidden PLMNs list
- List of beacon frequencies (ARFCNs of the home PLMN)
- Storage of location information

<u>Personal data of the user</u>

- Directory number of a mobile radio subscriber MSISDN
- Storage of SMS, Telephone Numbers etc.

The most attractive feature of the separation of ME and SIM is that it makes it possible to put the SIM into another ME. In this way I have upgraded my mobile communication from GSM to GPRS to UMTS, in each case using newer Mobile Equipment but the same SIM-Card.

1.2. The Base Station Subsystem BSS

The Base Station Subsystem is coloured green in picture 5. Its main components are:

1.2.1 The *Base Transceiver Station* (BTS)

The Base Transceiver Station realises the Air-Interface between mobile and network.
It consists of:
- the **antennas**
- output and input **filte**rs, which are band-pass filters. While the input filter is broadband and not tuneable, the output filter is wideband and tuneable
- radio **transmitter** and radio **receiver**
- the Transmission/Reception-Module **TRX** which serves: Channel Coding and Decoding, Ciphering, Slow Frequency Hopping, Burst formatting, Gausian Minimum Shift Keying (GMSK) of all transmitted and received data, the generation and sending of the BCCH on Channel 0, the realisation of the protocol LAPD on the channel to the BSC
- Operation and Maintenance (**O&M) Module**.

1.2.2 The *Base Station Controller* (BSC)

The Base Station Controller is the BSS's centre of intelligence. It consists of :
- a **switching array** which connects several BTSs to the MSC
- a **data bank** in which the quality and availability of the radio resources are stored and the status of the BSS-Hardware is dynamically watched
- a central processing unit (**CPU**) which makes the handover decisions.

1.2.3 The *Transcoding Rate and Adaptation Unit* (TRAU)

The Transcoding Rate and Adaptation Unit is responsible for compressed data transmission on the air interface. The compression method used is called *Regular Pulse Excitation-Long Term Prediction* (**RPE-LPT**). The bit rate of an ISDN channel with 64 kbit/sec is reduced to a bit rate on the air interface of 16 kbit/sec (if the *Full Rate Transport Channel* is used*)*.

1.3. The Network Switching Subsystem (NSS)

The Network Switching Subsystem is dark yellow in picture 5. It is the central part of any Mobile Radio System and controls several BSSs. Its components are responsible for all the call processing, controlling and data bank functions which are necessary to examine the authentication, to make set-up the call, to encrypt the data and to control roaming. Its components are:

1.3.1 Mobile Services Switching Centre MSC

The MSC is a standard ISDN-switching system adapted to be used in Mobile Radio Networks. It takes over the exchange of channels inside a PLMN or between several PLMNs and controls handover between several MSC areas.
The MSC also adapts protocols between Call Control (ISDN-typical) and ISDN User Part ISUP as used in SS#7
The MSC receives the information necessary for switching a signal processing from the HLR and the VLR (see paragraphs 1.3.3 and 1.3.4).

1.3.2 Gateway Mobile Services Switching Centre GMSC

Only the GMSC is able to create a connection from a PLMN to another network.
e.g. There is a subscriber in the fixed network who wishes to call a subscriber of the mobile radio network. The calling information comes from ISDN using the D-Channel, passes the

trunk network using the SS#7 and arrives at the GMSC. The GMSC initiates a search for the called subscriber using their Home Location Register. It then switches to the responsible MSC which links the call to the BSC and a BTC where the subscriber is camping. The call is then sent with a PAGING REQUEST to the wanted subscriber.

1.3.3 Home Location Register HLR

Generally one PLMN consists of several HLRs. The first two digits of the mobile directory number (e.g. 0171 **26**20757) are the number of the HLR where the mobile subscriber is stored. Among other things, the following data from any subscriber is stored:

Subscriber specific:
- IMSI
- Ki
- Restriction of services
- Supplementary Services
- Directory Number (MS ISDN)

Authentication and Ciphering:
- Algorithm A3
- Algorithm A8
- RAND, SRES, KC

Seeking for Subscriber/Call Control
- Information related to the current location of the subscriber e.g. the actual VLR
- Number of the MSC

1.3.4 Visitor Location Register VLR

A VLR stores subscription data for those subscribers currently situated in the service area of the corresponding MSC. A subscriber who logs into an allowed PLMN is registered by the responsible VLR after the latter has asked for their user data from the responsible HLR. A VLR function is integrated with every MSC. The following information is stored in the VLR

Subscriber specific:
- International Mobile Subscriber Identity IMSI
- Temporary Mobile Subscriber Identity TMSI

1.3.5 Equipment Identity Register EIR

Every MS possesses an *International Mobile Equipment Identity* IMEI. It is possible to ask for this ID by typing the string *#06# on the Mobile. The IMEI is stored in the EIR in a so-called ‘white-list’. A ‘black-list’ contains a list of defective or stolen MS and this equipment is therefore blocked.

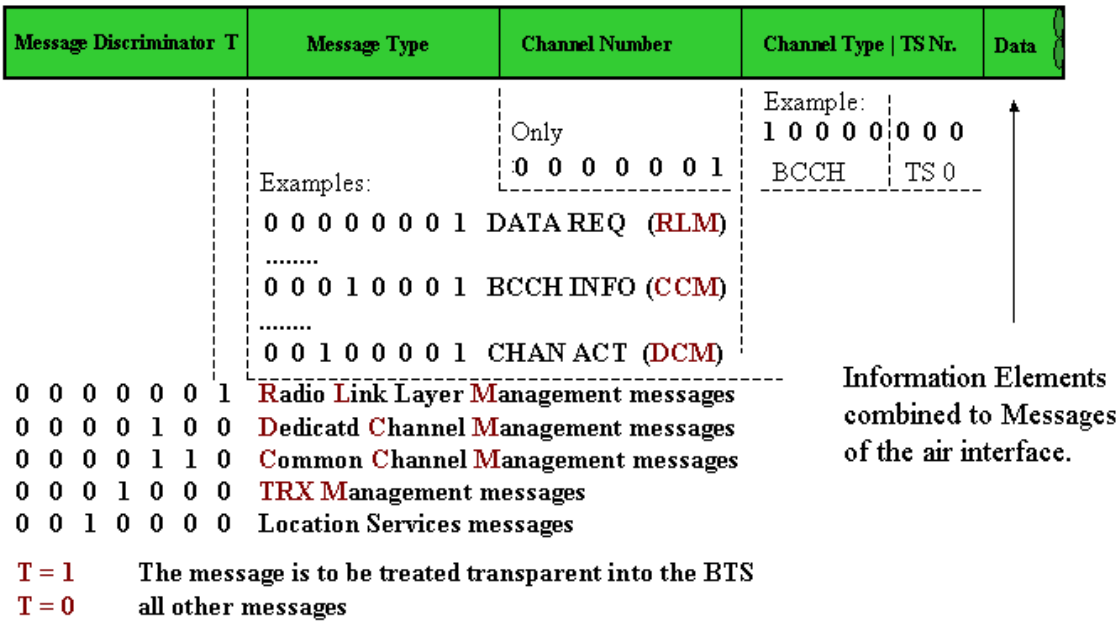
2. About Interfaces

Please have another look at picture 5 where you can see 3 main interfaces: the Air interface Um, the Abis interface and the A (BCF) interface. In this lecture we will deal mostly with the Air interface (Um) because we have equipment to trace the signal channels of this interface i.e. we are able to prove all statements with an experiment.

In lectures about ISDN we will deal mainly with the D-Channel, the signal channel of the final mile. However, in order to have an overview of the sophisticated system of signalling between a mobile and an ISDN telephone, in the following paragraph we will provide a description of the main features of signalling in a network.

2.1. The Abis Interface.

The Abis interface between BTS and BSC is typical ISDN. It is built by a PCM 30-interface, i.e. there are 30 channels with a speed of 64 kbit/sec. A full rate GSM data channel is compressed to16 kbit/sec. Thus 4 GSM channels fit into a 64 kbit/sec ISDN-channel. Layer 1 and Layer 2 are the same as in ISDN-channels.



Picture 6: Layer 3 in the Abis interface

In Layer 2 there exists a SAPI and a TEI (see § 5.1). The number of the TEI corresponds to the number of the BTS to which the message is sent. As you can see in Picture 6, the Protocol discriminator in ISDN is exchanged to a Message discriminator and a flag which decides whether or not the message is to be treat transparently into the BTS. The following three octets are instructions for controlling the the BTS and telling this component how to process the contents of the data field. For more information see [2].

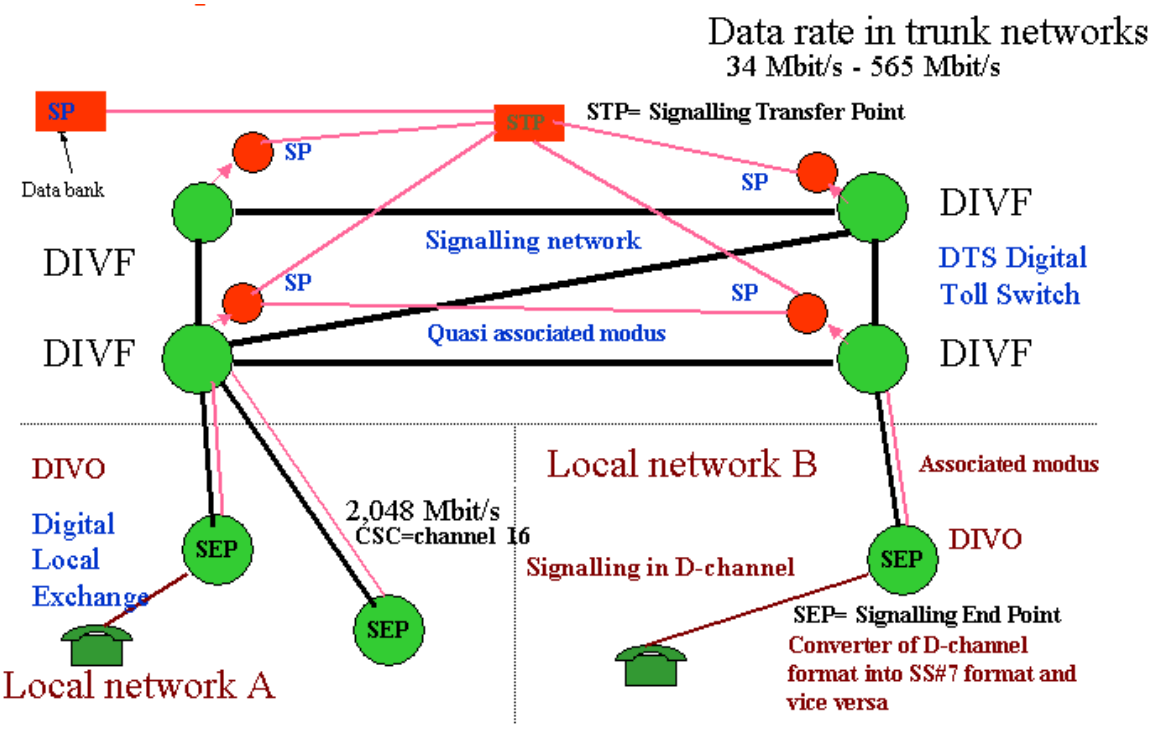
2.2 The A-Interface

The A-Interface is built by several PCM-primary groups (a primary group consists of 30 PCM channels). In a Primary group, channel 16 is the signal channel (this is known from ISDN and SS#7). The data rate of the message channels between TRAU and MSC is 64 kbit/sec. This is a sampling rate of 8000 where each sample consists of 8 bits. Between the Transcoder/Rate Adaptor Unit TRAU and BSC the message channels are compressed to 13 kbit/sec,
i.e. speech is transmitted using groups of 260 bits every 20m.
Signalling is made by the Signalling system Number 7 (SS#7) especially by
the *Signalling Connection Control Part* (SCCP),
the *Base Station Subsystem Application Part* (BSSAP) and
the *Transaction Capabilities* and *Mobile Application Part* (TCAP/MAP).

Don't worry, in the next paragraph we will briefly explain these terms by looking at some pictures.

3. Information about the Signalisation System Number 7 (SS#7)

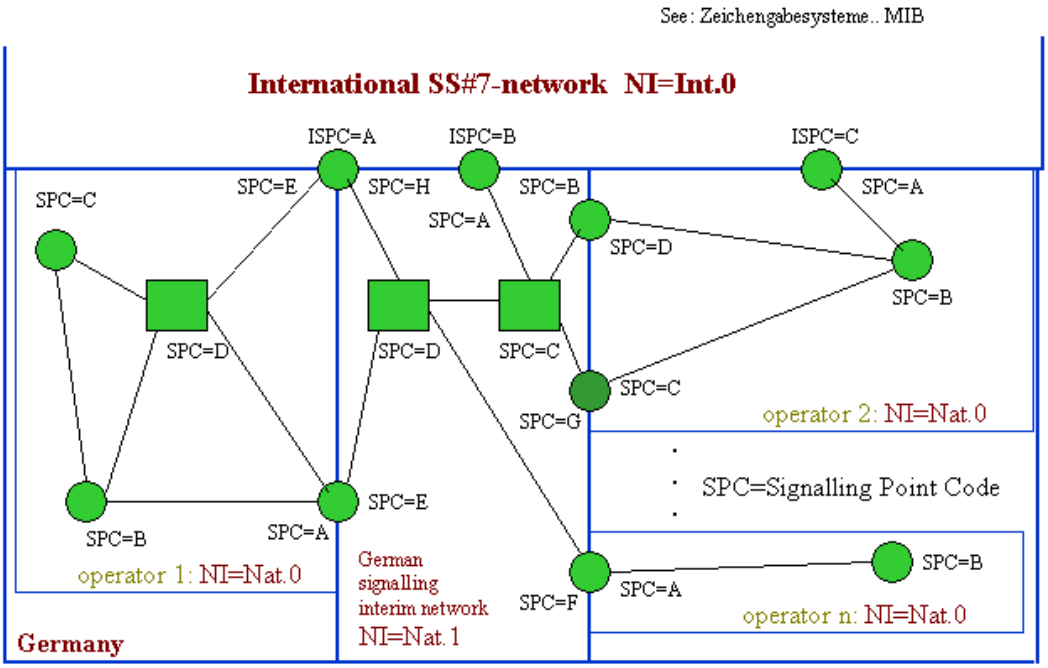
In the digital trunk network the signalling channels do not run in the same cable as the information channels. The signalling network is therefore a separate network beneath the network of information cables.



Picture 7: The digital trunk network

The information in this network runs between Signalling Points which route the signal streams. The signalling networks of different countries are connected worldwide as you can see in picture 8. This picture is tailored to the communication between operators of the different mobile networks, T-mobile, Vodafone, O2 and so on.

.



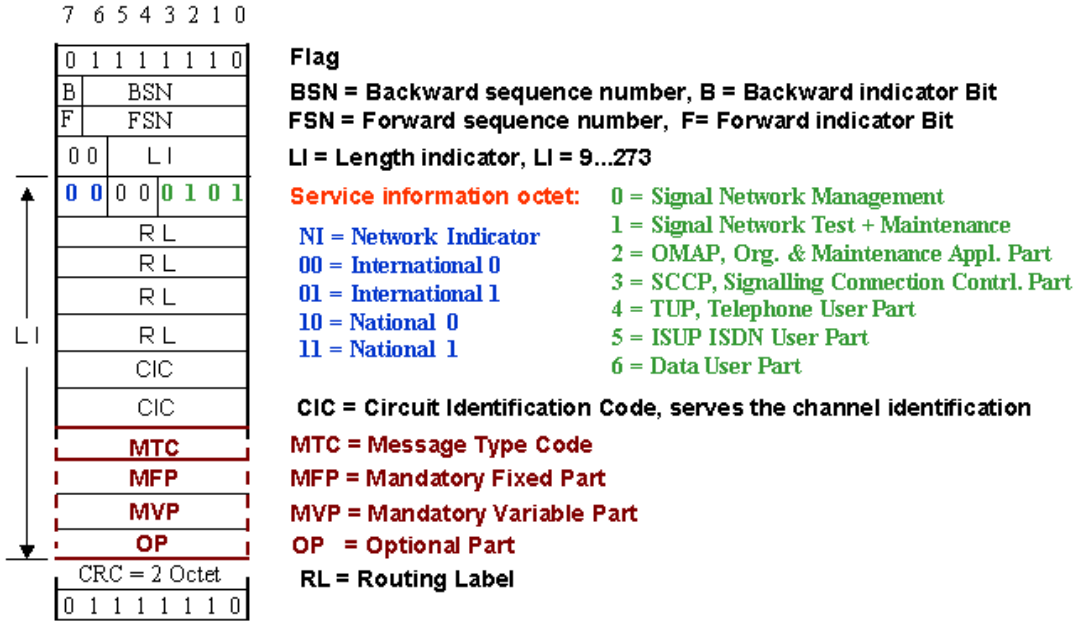
Picture 8: Structure of the German signalling network

The next picture shows how a message in SS#7 is structured. The signalling system in the trunk network is older than the signalling system in the ISDN. Therefore the construction of the layer 3 frame shown in picture 9 differs from the frames we know from the ISDN.

The part of the signalling system SS#7 which allows the transfer and maintenance of signalling messages in the national and international Trunk Network is called the Message Transfer Part MTP. The MTP may be divided into three layers known from the OSI model.
MTP1 is known as the Signalling Data Link (Bit Layer).
MTP2 defines the principle frame structure known from the Link Access Protocol used in the ISDN D-Channel (LAPD).
We will deal only with MTP3 which describes the signalling message handling dependent on the served user (e.g. ISDN =>ISDN Served User Part ISUP).
The control information is, for example, put into a frame called the Message Signal Unit MSU.

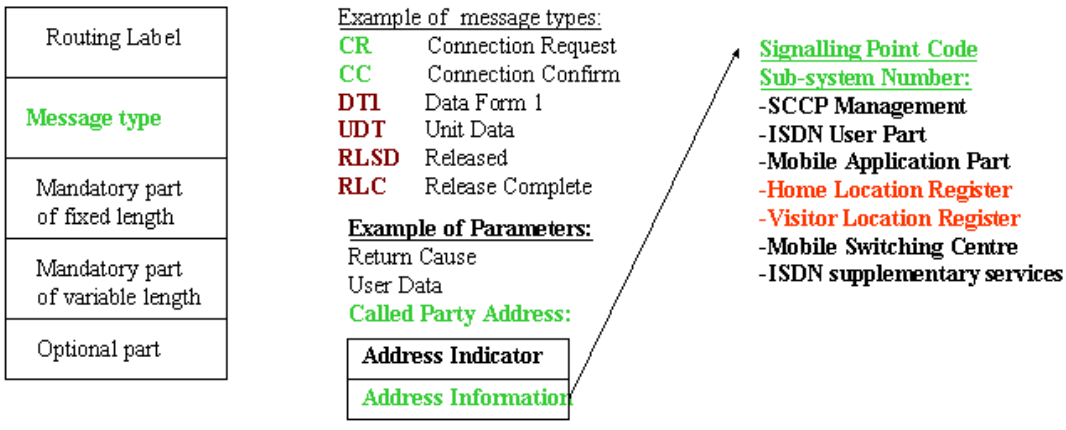
As you can see from the different *service information octets* the content of the Message Signal Unit MSU may serve several different uses.

.



Picture 9: The Message Signal Unit MSU

Let's have a look at the case where the MSU transports the Signalling Connection Control Part SCCP.
The SCCP is, like the ISDN User Part ISUP, an application of MTP. It grants network functions to other subsystems.
A subsystem using this network function is the *Transaction Capabilities Application Part.* The TCAP, for example, can convey user data from a HLR to a VLR in the international trunk network.



Picture 10: The Signalling Connection Control Part SCCP

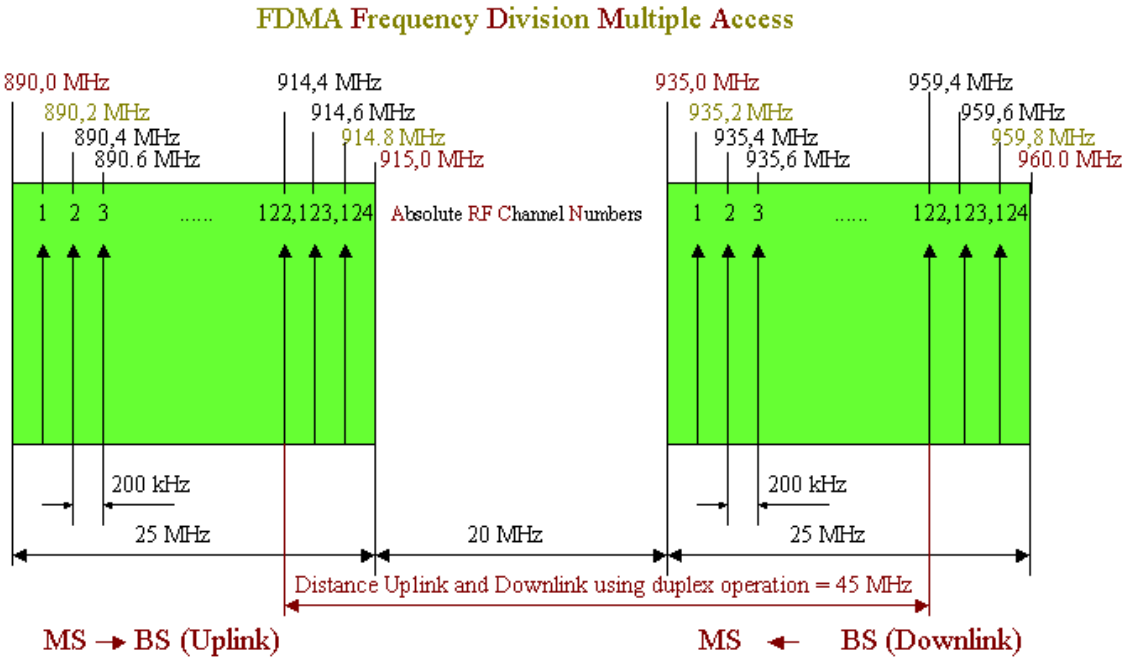
From all this complicated information you need only keep in mind that there is data which is put into frames which are then stacked into each other for transportation in the worldwide signalling network☺

4. Layer 1 on the air interface

4.1 Frequencies used in Mobile Communication

4.1.1 GSM 900

In GSM 900 there are two frequency bands, one for
Uplink (890.2-915 MHz) and the other for
Downlink (935.2-960 MHz).
Both are at a distance of 20 MHz from each other.
Frequencies are expressed by channel numbers 1 to 124 (the so-called 'ARFCN' = *Absolute Radio Frequency Number*).
Channel numbers are used in messages instead of explicit frequencies.
If the ARFCN = n is known the absolute frequency can be calculated by
for the downlink: F(DL) = (935.2 + 0.2*(n-1) MHz,
for the uplink: F(UL) = (890.2 + 0.2*(n-1) MHz,



Picture 11: Frequency plan GSM 900

4.1.2 Extended GSM

In order to create more frequencies after starting GSM an Extended Band was defined.
Uplink (880.4-890.0 MHz)
Downlink (925.4- 935.0 MHz)

In Extended GSM the channel numbers are n= ARFCN=975-1023. The absolute frequency can be calculated by
for the downlink: F(DL) = (935.2 + 0.2*(n-1024) MHz,
for the uplink: F(UL) = (890.2 + 0.2*(n-1024) MHz,
The high values are selected to avoid overlapping with ARFCNs used by DCS 1800.

4.1.3 Digital Communication System 1800

In the Digital Communication System 1800 there are the frequencies

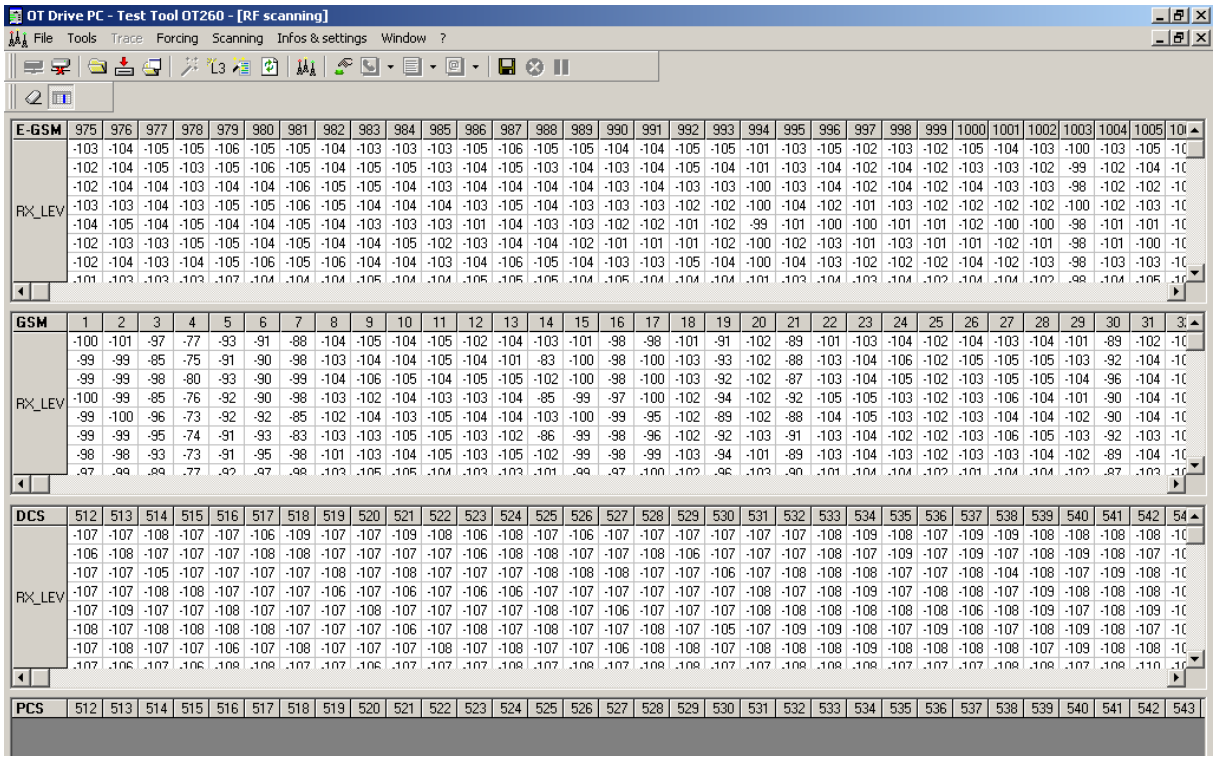
Uplink (1710-1785 MHz) and
Downlink (1805-1880 MHz).

If n = ARFCN=512-885 the absolute frequency can be calculated by

for the downlink: F(DL) = (1805.2 + 0.2*(n-512) MHz,
for the uplink: F(UL) = (1710.2 + 0.2*(n-512) MHz,

4.1.4 An Exercise with OT Drive PC and Mobile OT 260

Let's have a look at which frequencies with which field strengths can be measured at the author's residence.



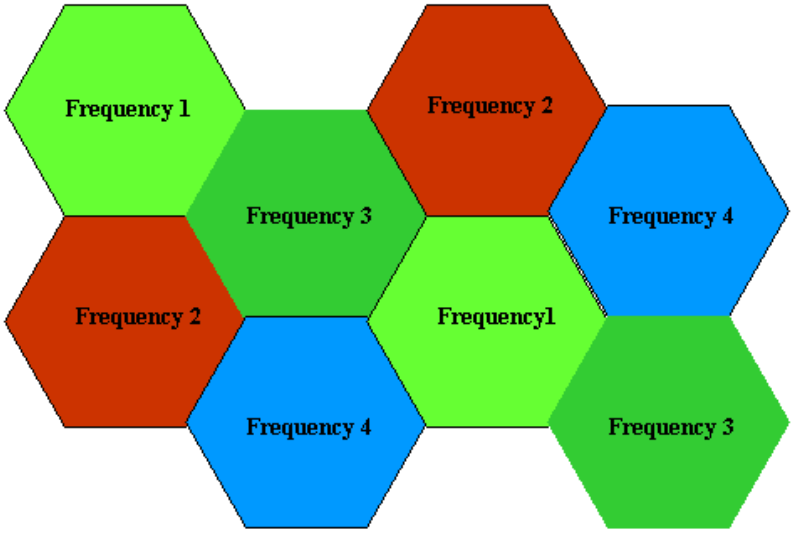
Picture 12: Scanning frequencies with OTDrivePC and OT260

You must bear in mind that a field strength of less than around -102 dB is unusable for a GSM-connection. Therefore the GSM-Channels 3,4,5,6,7, 16, 19, 21, 30 in picture 12 can be used to set up a call. We don't yet know to which operator the selected channels belong but we will deal with this problem later.

4.2 The Cellular coverage representation

Because of the restricted reach of the mobile transmitter on these frequencies it is possible to reuse all frequencies in a calculable distance.

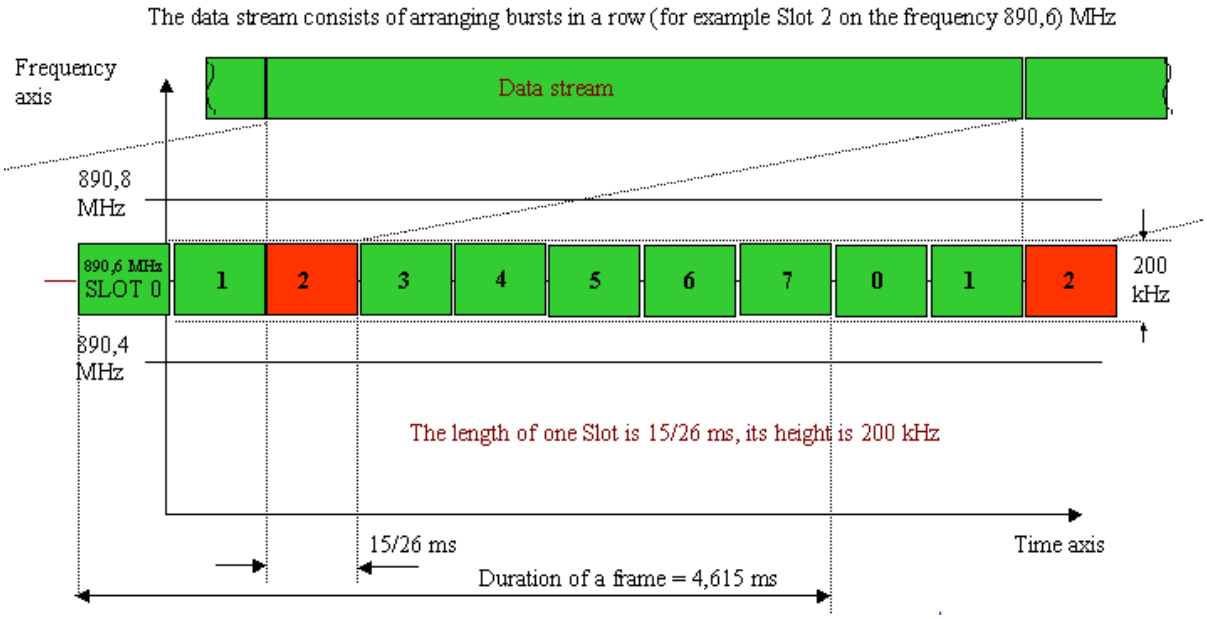
.



Picture 13: A cellular array

4.3 The frequency time division principle

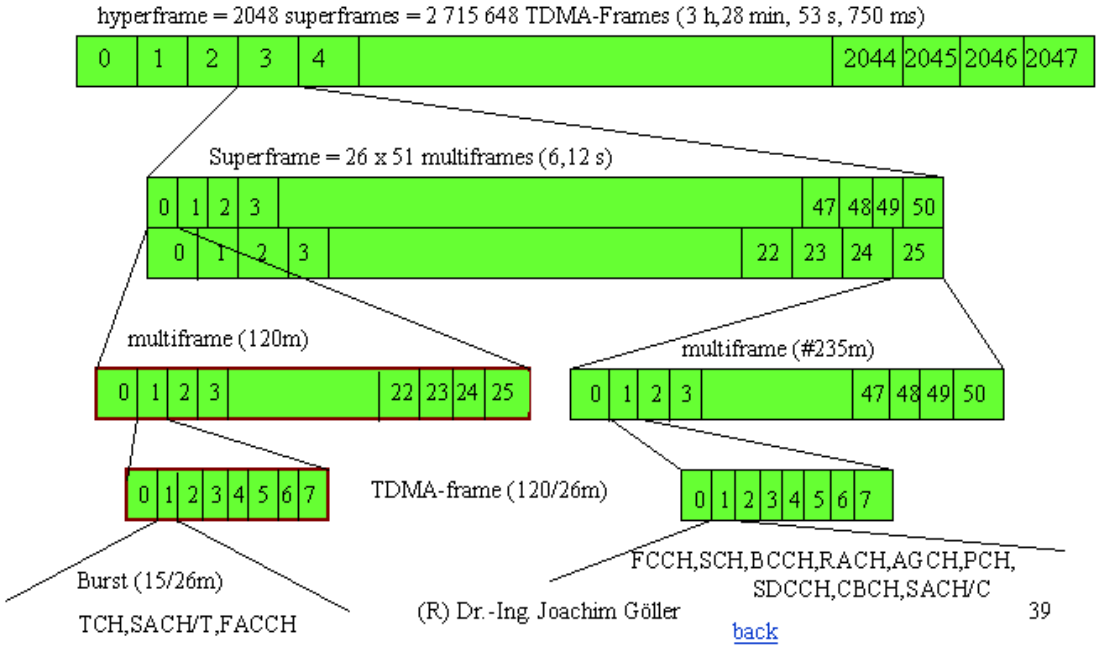
As mentioned in paragraph 4.1.4 the Operators (D1, D2, O2 etc) have to share the amount of existing frequencies. Thus the number of usable frequencies in one cell per operator is reduced still more. By using time-division the number of possible subscribers increases again.



Picture 14: Time Division Multiple Access TDMA

As you can see in picture 14, at every GSM frequency bursts of 576.9 /u sec are emitted. Eight consecutive bursts emitted are called a frame. The bursts in a frame are numbered from 0 to 7. If a mobile requests a channel it receives a dedicated frequency and a timeslot.
As you can also see in picture 14, the data stream between a mobile and the BTS consists of a stream of bursts. We shall deal with the construction of a burst later in this lecture.

Now we have to consider how the consecutive frames are numbered.
The Time Division Multiple Access frames are not simply repeated but are put into a hierarchy of frames. The frame number is not repeated until 3h, 28min, 53s, 750m (see picture 15).
The reason for this peculiar mode of counting is the use of the frame number during the encoding procedure.



Picture 15: Frame hierarchy (See Mouly, Pautet, "GSM ...")

Let's have a look at picture 15. To build a transport channel the frame in the lower left corner is first put into a multi-frame consisting of 26 TDMA frames.
To build a control channel the frame in the lower right corner is first put into a multi-frame consisting of 51 TDMA frames. The reason for this will be explained later.

4.4 About GSM channels

We are now able to make some statements about GSM channels.
The GSM channel consists of the arrangement of bursts in a row, possibly situated on different frequencies.
You must distinguish between fixed frequency channels, where the time slots always belong to the same frequency, and frequency-hopping channels, where the time slots may belong to different frequencies
Furthermore you must distinguish between Control Channels and Transport Channels.

Traffic channels are bi-directional. Their frequency separation (uplink and downlink) amounts to 45 MHz in the 900 MHz band and 75 MHz in the 1.8 GHz Band.
In addition there is a time shift of 3 Burst Periods (BP) between transmitting and receiving which allows the same Timeslot Number to be used for up and downward transmission.

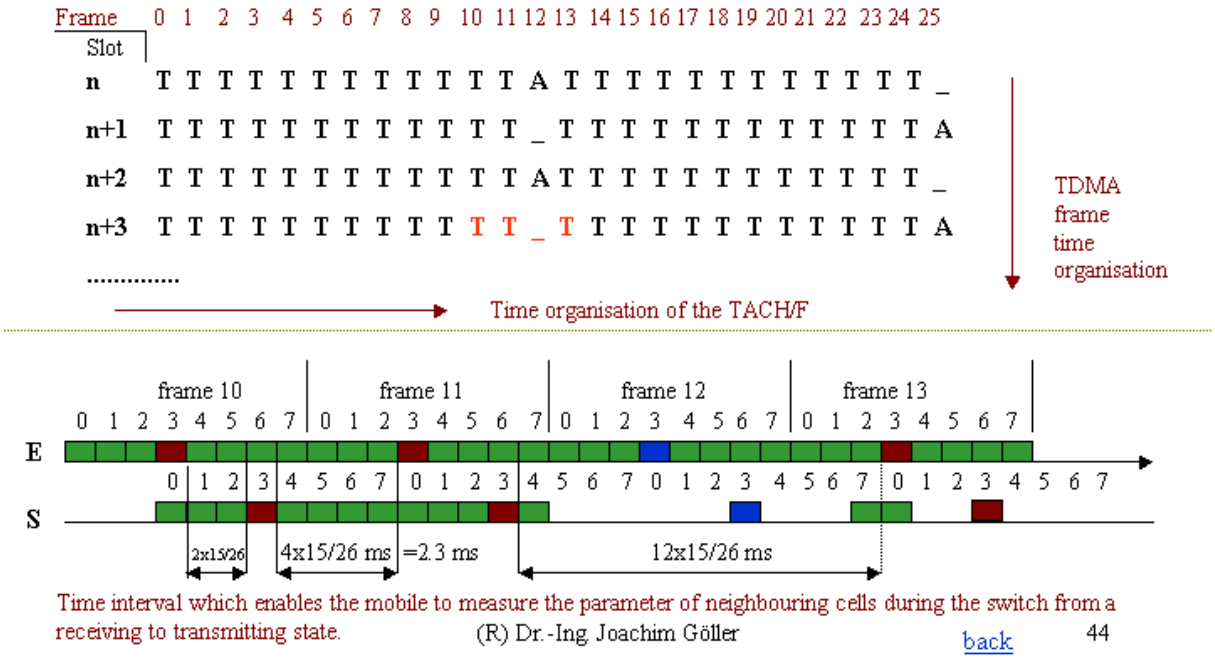
Traffic channels are built by grouping 26 TDMA frames into a multi-frame. Out of the 26 timeslots 24 BP are used to build TCH/F, one to build a Slow Associated Control Channel and one slot is kept free.
A Slow Associated Control Channel (SACCH) is always compounded with a full rate Traffic channel TCH/F.
The frame of a control message consists of 23 octets. 4 Bursts are necessary to transmit it over the air interface. In one multi-frame there is only one burst to build the SACCH. Hence it lasts 4 times 120m, i.e. 0.48 sec to generate a SACCH-frame.

The time of 120m for one multi-frame stems from the need of easy synchronisation with the ISDN. This is the reason for the duration of one Burst Period.

$$120/(26x8)m = 15/26m \sim 0.577m$$

As already mentioned, the burst reserved for SACCH in the TACH/F frame allows a control message to be sent every 480m.

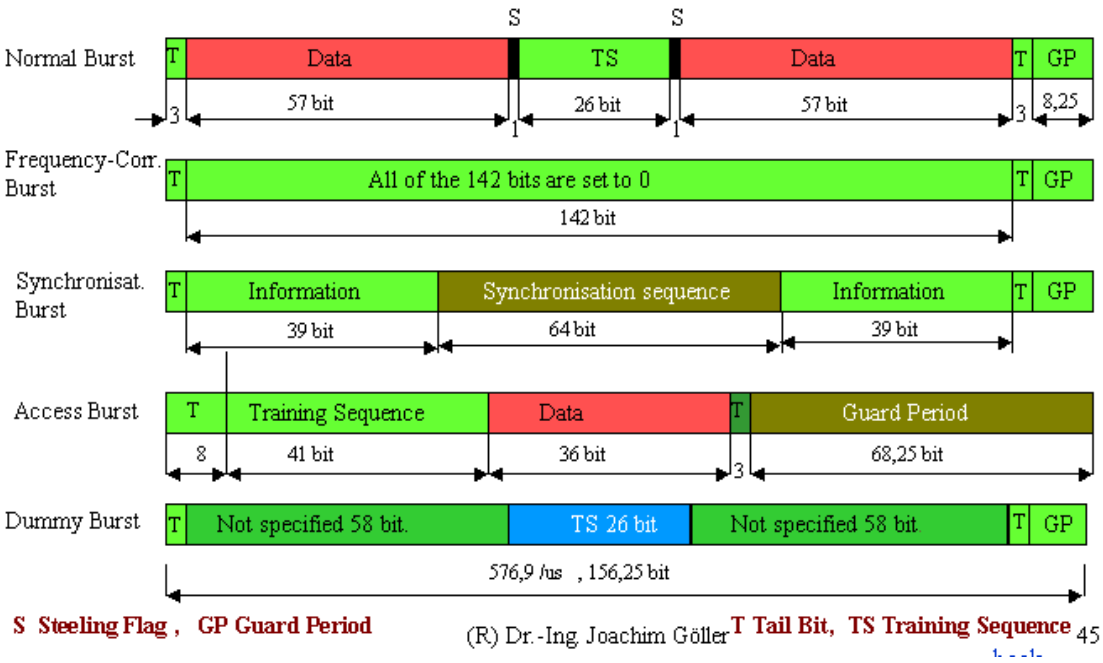
In contrast to this, the empty burst is necessary to make measurements on neighbouring channels. As you can see in Picture 16 the time gained is 12x15/26 = 6.92m.



Picture 16: Organisation of the TCH/F + SACH (TACH/F)

4.5 About Bursts

Please have a look at picture 17. In GSM there are five different Bursts.



Picture 17: The construction of bursts

The *Normal Burst* consists of two packages each of 58 bits grouped around the so-called 'Training Sequence'. The 58 bit packages consist of 57 bits of error-protected user data. One bit is called the Stealing-Flag. If the S-Flag is set, the Burst is stolen to build a Fast Associated Control Channel FACCH.
The *Training Sequence* is a sequence of Bits with a pattern known to the transmitter and receiver. It is used to adjust the parameters of the equalizer circuit and to guess the bit error rate. There are 8 different Training Sequences. Normal bursts are used to build the Transport Channel.
The *Frequency Correction Burst* consists of 142 zero bits. During the process of finding a beacon signal (this process will be discussed later) the mobile can adjust its frequency to that of the strongest signal found.
Following this the mobile can read the *Synchronisation Burst*. The Synchronisation Sequence allows the mobile to adjust to the bit stream and to read beneath other information to discover which operator the signal belongs to.

The *Access Burst* is used if the mobile has to ask the network for a channel. This process will also be discussed later.

The *Dummy Burst* looks similar to a Normal Burst. Bursts are to be sent continuously by the mobile and by the network. Sometimes it might occur that a burst is to be sent but no useful burst is available, in this case the dummy burst is taken.

4.6 Idle mode and dedicated mode

If an active connection exists between the Mobile (MS) and Base-station (BS) the MS is said to be in *dedicated mode*.
If the mobile is switched on but remains passive to the network the mobile is said to be in *idle mode*.
In idle mode the MS has to listen to the *Paging Channel* in order to detect a call to its address and to read the *System Information* sent by the *Broadcast Control Channel* (BCCH)

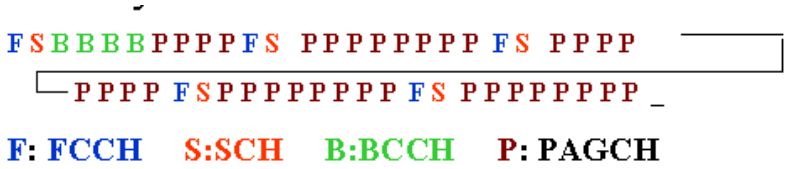
Direction	Channel	Name
MS ←BS	FCCH	Frequency Correction Channel
MS ← BS	SCH	Synchronisation Channel
MS ← BS	BCCH	Broadcast Control Channel
MS ← BS	PAGCH	Paging and Access Grant Channel
MS → BS	RACH	Random Access Channel
MS ↔ BS	SDCCH	Stand-Alone Dedicated Control Channel
MS ↔ BS	SACCH	Slow Associated Control Channel
MS ↔ BS	FACCH	Fast Associated Control Channel

Picture 18: Control Channels in GSM

Please try to find these channels in Picture 18. The following channels are used in idle mode:

Frequency Correction CHannel	in search of a new beacon frequency
Synchronisation CHannel	in search of a new beacon frequency
Broadcast Control CHannel	while monitoring the System Information
Paging CHannel	while monitoring whether there is a call
Access Grant Channel	waiting for the Immediate Assignment of a channel
Random Access Channel	sending a channel request to the network

Access to these channels is possible following the burst sequence shown in picture 19.



Picture 19: A burst sequence at the beacon frequency time slot 0

The illustrated sequence of Bursts is always sent on slot 0 of the *beacon frequency*. You can see that a SCH Burst follows a FCCH burst exactly 8 Bursts later. The following 4 Bursts set up a message from the Broadcast Control Channel (BCCH). The next 4 Bursts set up a message from the Paging Channel, and so on. As will be explained later, one message frame needs 4 Bursts to be conveyed over the air interface. The RANDOM ACCESS CHANNEL may **UPLINK** all Bursts on slot 0 of the *beacon frequency*.

Now have another look at picture 15. The absence of a common divisor in the cycles 26 and 51 in the left and right lower corners serves the following purpose:
a Mobile station being in dedicated Mode, i.e. sending and receiving Bursts in a “26 multi-frame”, is periodically able to measure the Synchronisation Channel and the Frequency Correction Channel in the “51 multi-frame” of the neighbouring BS (Pre-synchronisation).

If there was a common divisor in the two multi-frames it might happen that, during the gap shown in picture 19, the same bursts but not the SCH or FCCH are seen. If there is no common divisor another burst in the sequence (as shown in picture 19) is always seen.

4.7 How the Mobile finds the BCCH

As mentioned above, there is a *beacon frequency* **(BCCH)**, a distinguishing frequency in a cell. In timeslot 0 all the modulated channels shown in Picture 19 are downlinked. The Bursts associated with these channels are shown in Picture 17. After being switched on the mobile seeks the strongest transmitter, in most cases this is a BCCH. As is explained above, in timeslot 0 of this frequency a *Frequency correction Burst* is emitted and eight BP later a *Synchronization Burst*. The MS will therefore first seek the strongest transmitter and then the Frequency Correction Channel with which it can adjust to the BTS.

From the Synchronisation Burst (8 BP after the Frequency correction Burst) the Mobile learns the exact number of the timeslot in the cycle of the 8 x 26 x 51 x 2048 Burst Periods.
The MS furthermore learns the *Base Station Identity Code* (**BSIC**).
The *Base Station Identity Code* BSIC consists of 6 bits combined from **NCC** and **BCC** (each with a length of 3 bits). Allowed and disallowed NCC’s are stored on the SIM card.

Therefore a mobile equipped with a SIM-Card issued by operator D1 cannot camp on a BTS of operator D2 even if this BTS is emitting a stronger carrier.

Let’s have a little exercise to find out which frequencies have which signal strength and belong to which Operator (NCC) having which BCC.

GSM	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83
BSIC	***	***	***	***	***	6-5	***	5-2	***	***	***	4-5	***	***	***	***	***	3-6	***	***	***	3-4	***	***	***	***	***	***	3-2	***	***	***
RX_LEV	-108	-104	-109	-107	-107	-95	-104	-102	-108	-107	-108	-104	-107	-100	-107	-106	-107	-92	-104	-107	-109	-103	-109	-109	-108	-108	-109	-109	-97	-109	-108	-110
	-108	-103	-108	-108	-107	-96	-103	-104	-108	-107	-88	-105	-107	-99	-106	-105	-108	-91	-103	-108	-109	-105	-109	-107	-92	-106	-109	-109	-96	-109	-108	-110

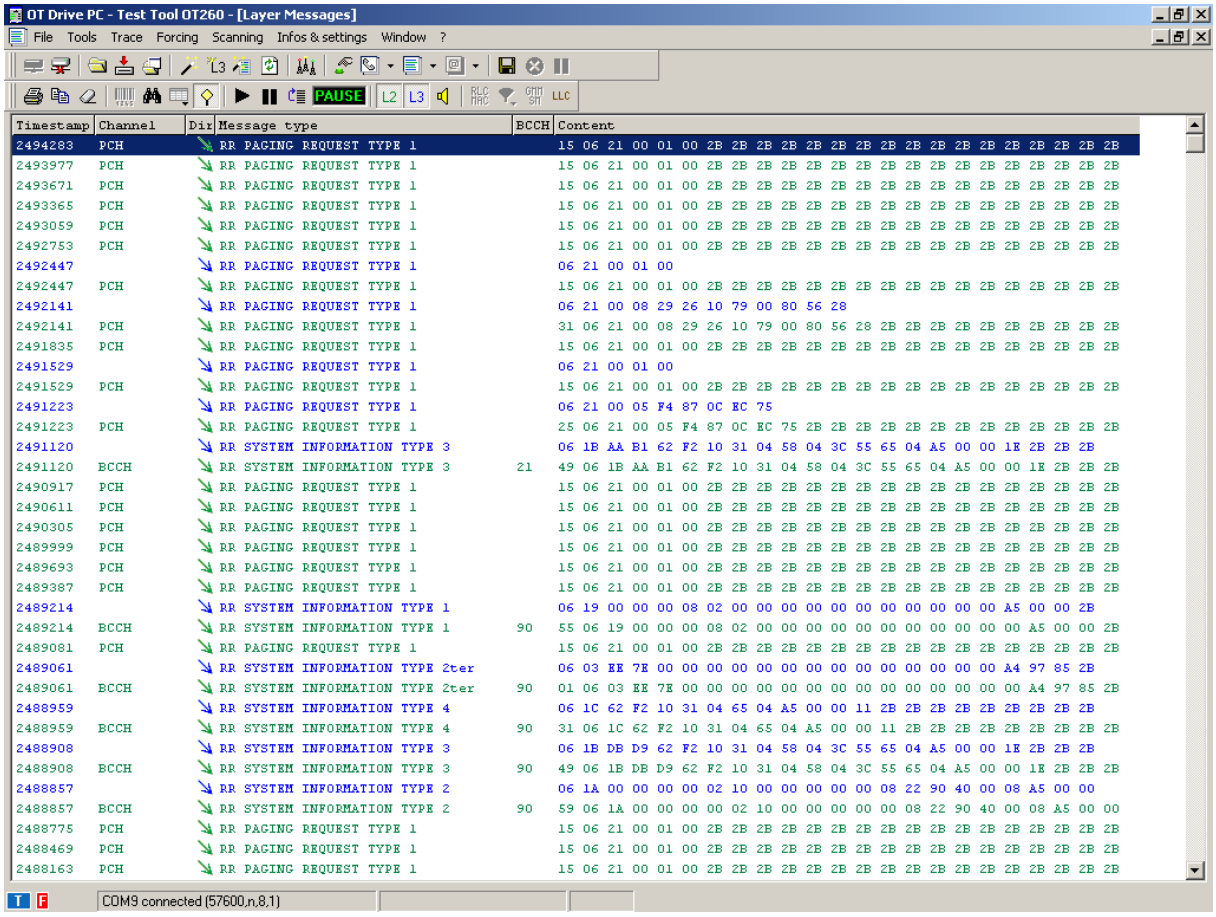
Picture 20: A look at OTDrivePC during BCCH scanning and BSIC detecting

If we start OTDrivePC and click *File->Connect* and *Scanning->BCH-Scanning->BSIC-detection* we will see a picture similar to the detail shown in picture 20. The mobile scans the whole (e.g. the 900 MHz) band. Beneath the line of ARFCNs you can see a line which shows whether or not the frequency is a beacon frequency. A beacon frequency is represented by two digits connected by a hyphen (NCC-BCC). The NCC of T-Mobile (D1) is “3”. Vodafone (D2), being an international player, possesses NCCs 4, 5, 6 and 7. *System Information Type 2* tells the mobile which NCCs are allowed.

Two transmitters not far from on another could be emitting the same BCCH frequency. It must be possible to distinguish between these carriers when they are both received by one mobile. Therefore, during the planning and building a network, neighbouring BCCH with the same frequency are assigned a different “colour”. This colour is represented by the terminus *Base Station Colour Code* (BCC).

4.8. About the idle mode

After the mobile has found an allowed BCCH it registers with the network. This process is called LOCATION UPDATE and we will discuss it in greater detail later. After this the mobile watches the PAGING REQUEST messages waiting for a call. This mode is called the 'idle mode'. Let's have a look at the messages the Mobile receives in idle mode.
To do so, start OTDrivePC, click File->Connect, Trace-> Define... -> Select all -> Send... In the window *Layer Messages* we can find **PAGING REQUEST TYPE 1 (2)**. Some of this will be passed to layer 3. On the other hand all of the **SYSTEM INFORMATION TYPE 1, 2, 3, 4, 13,** are passed to layer 3.



Picture 21:The "Layer Messages" window of the OTDrivePC tool.

When it was last connected to the network the mobile received a *Temporary Mobile Subscriber Identity* (TMSI), a number 4 octets in length assigned by the network. The mobile receives a new TMSI from the VLR when every new connection is made. The TMSI was introduced to make the tracking of a subscriber more complicated.

4.9 The Mobile is called

If the mobile is called it recognizes its address (TMSI) in a message from the Paging Channel. The mobile has to request a channel in response and uses the *Random Access Channel* to do so. As mentioned in paragraph 4.6, a *Random Access Burst* can be sent on every BP of slot 0 of the BCCH. The *Random Access Burst* possesses an effective length of only 88 bits (please have another look at picture 17). This is necessary because the mobile does not know the real

distance to the BTS and consequently does not know the delay with which the burst will arrive at the BTS.
The construction of the Access Burst allows it to fit into the receiving window of the BTS even if the Burst arrives with time delay. The BTS is now able to calculate the so-called 'Timing Advance' TA and inform the mobile about it.

4.9.1 Timing Advance

After the Access Burst has been decoded the signal delay is computed by the BTS and transmitted to the mobile by signalling.
The value of the *Timing Advance* TA can be between 0 and 232/us, expressed by 0 to 63 bits (that is 1 bit = 48/13/us). If the TA is known the distance between the mobile and BTS can be calculated.
TA = 0 means the mobile is not more than 300m away from the BTS. The distance increases by 550m per Bit of the TA. i.e.

Distance/m = 300m + (TA/bit x 550)m.

A mobile at a distance of more than 35 km from the BTS is unreachable.

4.9.2 Content of the ACCESS BURST

At the beginning of the ACCESS BURST there are 8 Tail bits in fixed code with the pattern "00111010" followed by a Synchronization Sequence of 41 bits. This pattern allows the BTS to distinguish the ACCESS BURST from random noise.
The following 36 data bits contain only 8 information bits (yyyxxxxx). At least 3 bits (y) contain the cause of the channel request (for instance "Emergency call", "Answer to paging ...", "Originating call ..."). The other bits (x) form a random digit which allows this ACCESS BURST to be distinguished from another one arriving at the BTS at the same time.

4.10 The message IMMEDIATE ASSIGNMENT

In response to the Channel Request the BTS sends the message IMMEDIATE ASSIGNMENT on the ACCESS GRANT CHANNEL (AGCH). The AGCH takes the timeslot normally used by the PCH (and is therefore named PACH).
The message IMMEDIATE ASSIGNMENT dedicates a working channel to the MS (a so-called 'Slow Dedicated Control Channel') and tells the mobile where to find this channel, i.e.
- the type of the logical channel,
- the frequency,
- the time slot,
- the frame number expressed by the three Parameters T1, T2, T3,
- the Timing Advance Value,

and so on.

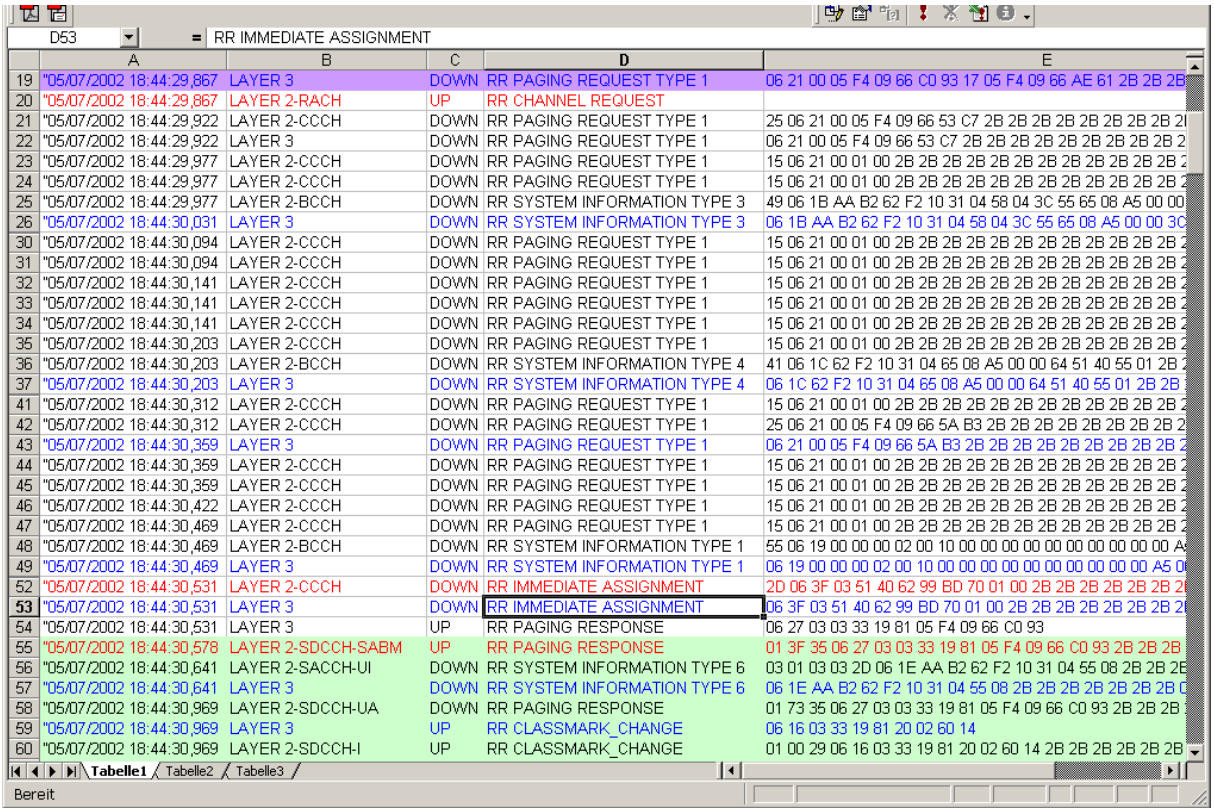
The message IMMEDIATE ASSIGNMENT enables the MS to exchange information with the BTS. A translated frame of this message is over the page:

```
_____[ 9 ]___[ 12:02:42,320 ]___[ DOWN ]____[ CCCH ]_____________________________

2d 06 3f 03 49 40 62 95 ee 57 01 00

2d  00101101  Pseudo length : 45
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
3f  0-------  1 spare bit         : 0
    -0------  Send sequence number: 0

    --111111  MESSAGE TYPE        : IMMEDIATE ASSIGNMENT

: Page Mode
03  ----00--  2 spare bits        : 0
    ------11  Page mode           : same as before
: Dedicated Mode or TBF
    0-------  1 spare bit         : 0
    -0------  Two messages assign.: No meaning
    --0-----  Downlink assig to MS: No meaning
    ---0----  This message assigns a dedicated mode resource

: Channel Description
49  01001---  Ch.type & TDMA offs.: SDCCH/8 + SACCH/C8|CBCH(SDCCH/8),SubChannel 1
    -----001  Timslot number      : 1

40  010-----  Training sequ. code : 2
    ---000--  Single channel      : RF single channel
    ------00  Singl.RF ch.high prt: 0
62  01100010  abs.RFch.num.low prt: 98

: Request Reference
95  100-----  Establishing Cause  : Answer to paging
    ---10101  Random Reference    : 21

ee  11101---  29      = (T1)     coded as bin. represent. of (Frame Number div 1326) mod 32.
    -----110  6       = (T3 high)is coded as the binary representation of Frame Number mod 51.
57  010-----  2       = (T3 low) is coded as the binary representation of Frame Number mod 51.
    ---10111  23      = (T2)     is coded as the binary representation of Frame Number mod 26.
: The frame number, FN modulo 42432 can be calculated as 51x((T3-T2)mod 26)+T3+51x26xT1'

01  00------  2 spare bits         : 0
    --000001  Timing advance value : 1 bit period

00  00000000  lgth of Mob.Alloc.IE : 0
```

Table 1: Immediate Assignment

We can see how this looks on the radio channel (the air interface) by starting the Exercise CD item ‘Raw traces’. Please click *"call from the ISDN to the D1 Mobile Network”*. As opposed to a live-trace the Excel sheet gives an overview of the whole transmission.
In Picture 22 you can see detail from the EXCEL sheet made from a trace captured by OTDrivePC. Let's have a closer look at this picture:
- On line 19 appears a (Layer 3) PAGING REQUEST message which consists of the TMSI of our Trace Mobile.
- The mobile immediately sends the CHANNEL REQUEST MESSAGE (there is no time difference detected)
- 664m later the network answers by sending the IMMEDIATE ASSIGNMENT MESSAGE (Line 52) which is copied to Layer 3 (Line 53)
- Only 47m later the mobile answers with a PAGING RESPONSE Message
- This Message is sent on Layer 2 together with a SABME

In response to the IMMEDIATE ASSIGNMENT Message, the message PAGING RESPONSE is sent to the BTS, together with SABM which allows error detection on layer 2.



D53 = RR IMMEDIATE ASSIGNMENT

	A	B	C	D	E
19	"05/07/2002 18:44:29,867	LAYER 3	DOWN	RR PAGING REQUEST TYPE 1	06 21 00 05 F4 09 66 C0 93 17 05 F4 09 66 AE 61 2B 2B 2B
20	"05/07/2002 18:44:29,867	LAYER 2-RACH	UP	RR CHANNEL REQUEST	
21	"05/07/2002 18:44:29,922	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	25 06 21 00 05 F4 09 66 53 C7 2B 2B 2B 2B 2B 2B 2B 2B 2B
22	"05/07/2002 18:44:29,922	LAYER 3	DOWN	RR PAGING REQUEST TYPE 1	06 21 00 05 F4 09 66 53 C7 2B 2B 2B 2B 2B 2B 2B 2B 2
23	"05/07/2002 18:44:29,977	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
24	"05/07/2002 18:44:29,977	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
25	"05/07/2002 18:44:29,977	LAYER 2-BCCH	DOWN	RR SYSTEM INFORMATION TYPE 3	49 06 1B AA B2 62 F2 10 31 04 58 04 3C 55 65 08 A5 00 00
26	"05/07/2002 18:44:30,031	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 3	06 1B AA B2 62 F2 10 31 04 58 04 3C 55 65 08 A5 00 00 3C
30	"05/07/2002 18:44:30,094	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
31	"05/07/2002 18:44:30,094	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
32	"05/07/2002 18:44:30,141	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
33	"05/07/2002 18:44:30,141	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
34	"05/07/2002 18:44:30,141	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
35	"05/07/2002 18:44:30,203	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
36	"05/07/2002 18:44:30,203	LAYER 2-BCCH	DOWN	RR SYSTEM INFORMATION TYPE 4	41 06 1C 62 F2 10 31 04 65 08 A5 00 00 64 51 40 55 01 2B
37	"05/07/2002 18:44:30,203	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 4	06 1C 62 F2 10 31 04 65 08 A5 00 00 64 51 40 55 01 2B 2B
41	"05/07/2002 18:44:30,312	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
42	"05/07/2002 18:44:30,312	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	25 06 21 00 05 F4 09 66 5A B3 2B 2B 2B 2B 2B 2B 2B 2B 2
43	"05/07/2002 18:44:30,359	LAYER 3	DOWN	RR PAGING REQUEST TYPE 1	06 21 00 05 F4 09 66 5A B3 2B 2B 2B 2B 2B 2B 2B 2B 2
44	"05/07/2002 18:44:30,359	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
45	"05/07/2002 18:44:30,359	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
46	"05/07/2002 18:44:30,422	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
47	"05/07/2002 18:44:30,469	LAYER 2-CCCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
48	"05/07/2002 18:44:30,469	LAYER 2-BCCH	DOWN	RR SYSTEM INFORMATION TYPE 1	55 06 19 00 00 00 02 00 10 00 00 00 00 00 00 00 00 00 A
49	"05/07/2002 18:44:30,469	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 1	06 19 00 00 00 02 00 10 00 00 00 00 00 00 00 00 00 A5 0
52	"05/07/2002 18:44:30,531	LAYER 2-CCCH	DOWN	RR IMMEDIATE ASSIGNMENT	2D 06 3F 03 51 40 62 99 BD 70 01 00 2B 2B 2B 2B 2B 2B 2
53	"05/07/2002 18:44:30,531	LAYER 3	DOWN	RR IMMEDIATE ASSIGNMENT	06 3F 03 51 40 62 99 BD 70 01 00 2B 2B 2B 2B 2B 2B 2B 2
54	"05/07/2002 18:44:30,531	LAYER 3	UP	RR PAGING RESPONSE	06 27 03 03 33 19 81 05 F4 09 66 C0 93
55	"05/07/2002 18:44:30,578	LAYER 2-SDCCH-SABM	UP	RR PAGING RESPONSE	01 3F 35 06 27 03 03 33 19 81 05 F4 09 66 C0 93 2B 2B 2B
56	"05/07/2002 18:44:30,641	LAYER 2-SACCH-UI	DOWN	RR SYSTEM INFORMATION TYPE 6	03 01 03 03 2D 06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B
57	"05/07/2002 18:44:30,641	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B 0
58	"05/07/2002 18:44:30,969	LAYER 2-SDCCH-UA	DOWN	RR PAGING RESPONSE	01 73 35 06 27 03 03 33 19 81 05 F4 09 66 C0 93 2B 2B 2B
59	"05/07/2002 18:44:30,969	LAYER 3	UP	RR CLASSMARK_CHANGE	06 16 03 33 19 81 20 02 60 14
60	"05/07/2002 18:44:30,969	LAYER 2-SDCCH-I	UP	RR CLASSMARK_CHANGE	01 00 29 06 16 03 33 19 81 20 02 60 14 2B 2B 2B 2B 2B 2B

Tabelle1 / Tabelle2 / Tabelle3

Bereit

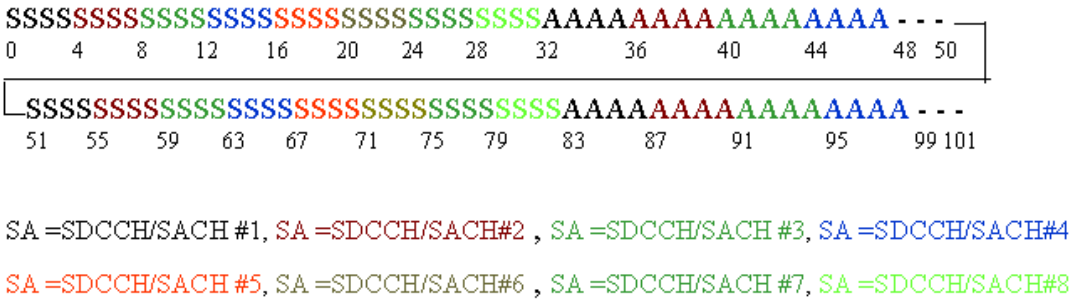
Picture 22: Excel representation of a MTC (detail)

4.11 Dedicated Channels

As shown in the paragraph above, the network dedicates a channel to the mobile. Now we have to deal with the questions: What are dedicated channels and how are they organized? The dedication of a Transport Channel is quite simple. The mobile receives a frequency, a timeslot and a frame number. However, if we only have to negotiate between the network and mobile conditions for the connection to be established, dedicating a full transport channel to this task is a waste of channel capacity.

The authors Mouly and Pautet say only an eighth of the valuable capacity of a Transport Channel (TCH/F) is necessary to transport this control information. They call this Signal channel TACH/8 (TACH stands for the combination TCH/SACH)

In GSM-Specifications this eighth TCH is called the SDCCH (Slow Dedicated Control CHannel). The SDCCHs are organized in a cycle of 102 consecutive bursts (as shown in picture 24). One possible configuration of the cycle consists of the following:
8 consecutive series of 4 bits, each belonging to one SDCCH (called Sub channel 1-8). Then 4 consecutive series of 4 bits, each belonging to one SACCH. Three slots are left unused.



Picture 23: Organisation of a TACH/8

In the illustrated time organization, eight SDCCH/SACH/8 sub-channels exist. A grouping of only four sub-channels is also possible.

4.12 How to transport a layer 2 frame to layer 1

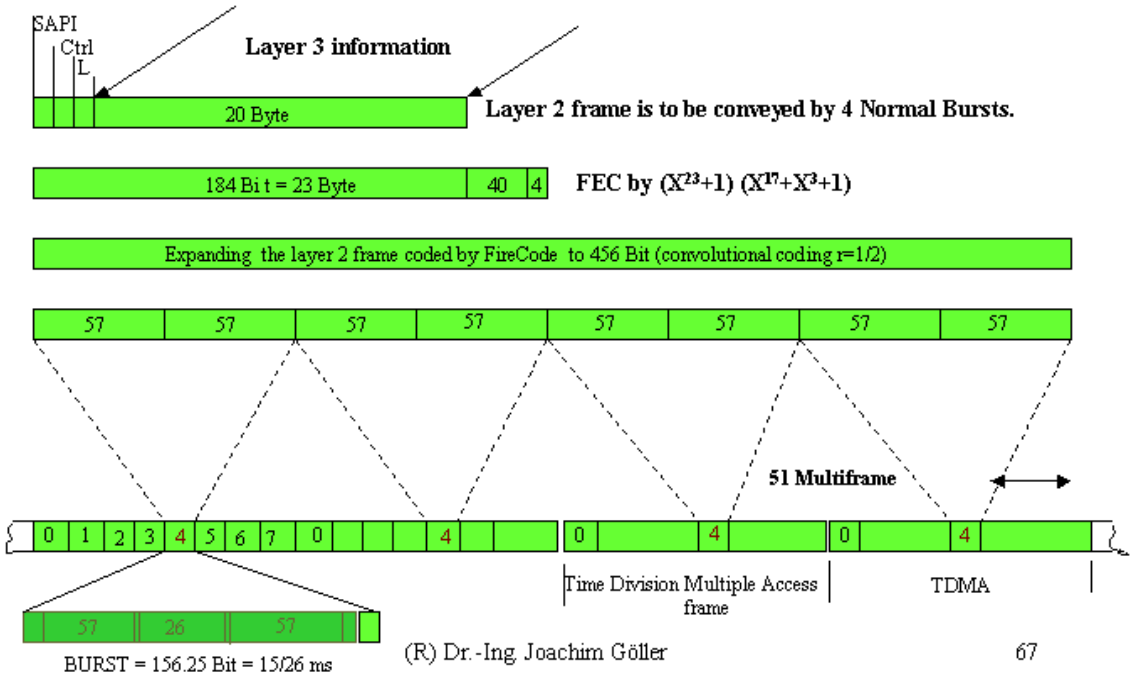
A layer 2 frame may convey a maximum of 23 octets of control information (i.e. a length of 184 bits). These 184 bits are encrypted by a Fire Code represented by the polynomial

$$(x^{23}+1)(x^{17}+x^3+1)$$

This Fire Code allows the correction of burst errors up to the weight of eleven.
By encryption the length of the frame is enlarged to 184 + 40 = 224 bits (4 bits are added, so the length of the frame is 228).

It is expected that the mobile channel will contain a high density of burst errors. This means the error correction capability of 11 consecutive wrong bits is not sufficient. There is a trick to overcome this:
We spread the sequence of 228 bits to 456 bits by a so-called ‘convolutional code’.
Imagine that the convolutional code inserts one dummy bit between two of the 228 information bits.
If there are large bursts of error bits half of them meet dummy bits. This increases the probability of the Fire Code correcting the 11 errors in the 228 bit sequence.

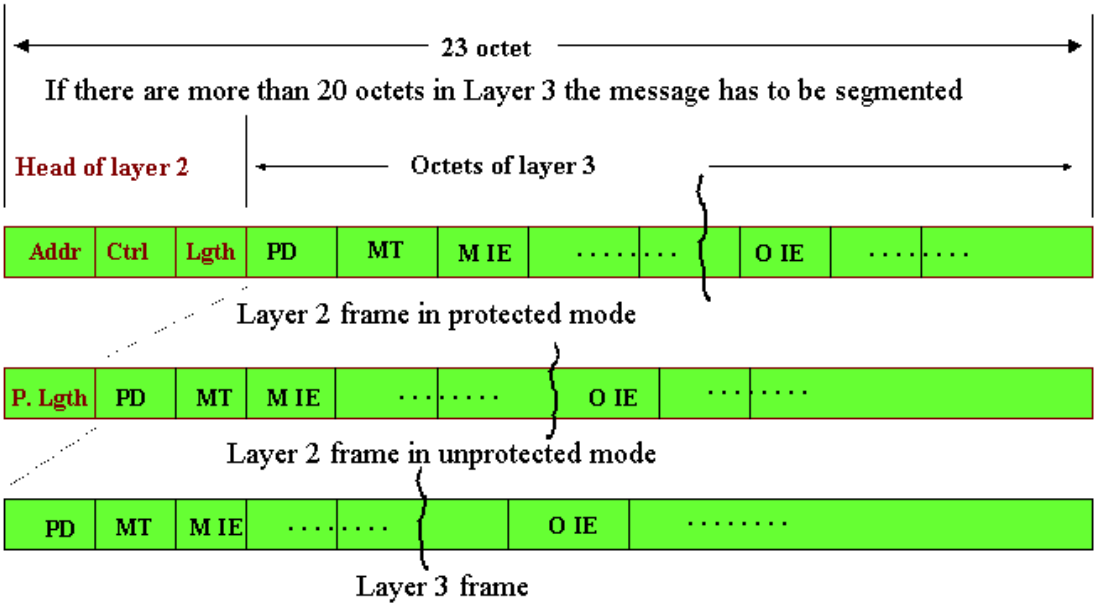
The final coding action is to put the 456 coded bits into 4 Normal Bursts (each consisting of 114 information bits), see picture 24.



Picture 24: Copying a Layer 2 frame onto Layer 1

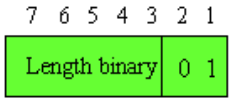
5. Construction of Layer 2 and Layer 3 in GSM

The information about the length of a layer 2 frame given in the last paragraph is illustrated in picture 25.



Picture 25: The construction of frames on the air interface

You must distinguish between layer 2 frames in protected mode and layer 2 frames in unprotected mode.
While the first construction is known from the ISDN, the latter is new. Please see picture 26 for the coding of the eight bits of the Pseudolength.



The pseudo-length octet declares the number of layer 3 octets in the frame (apart from rest octets)

Components of an Information Element (IE)
- **"Information Element Identifier" (IEI);**
- **"Length Indicator" (LI);**
- **"Value part".**

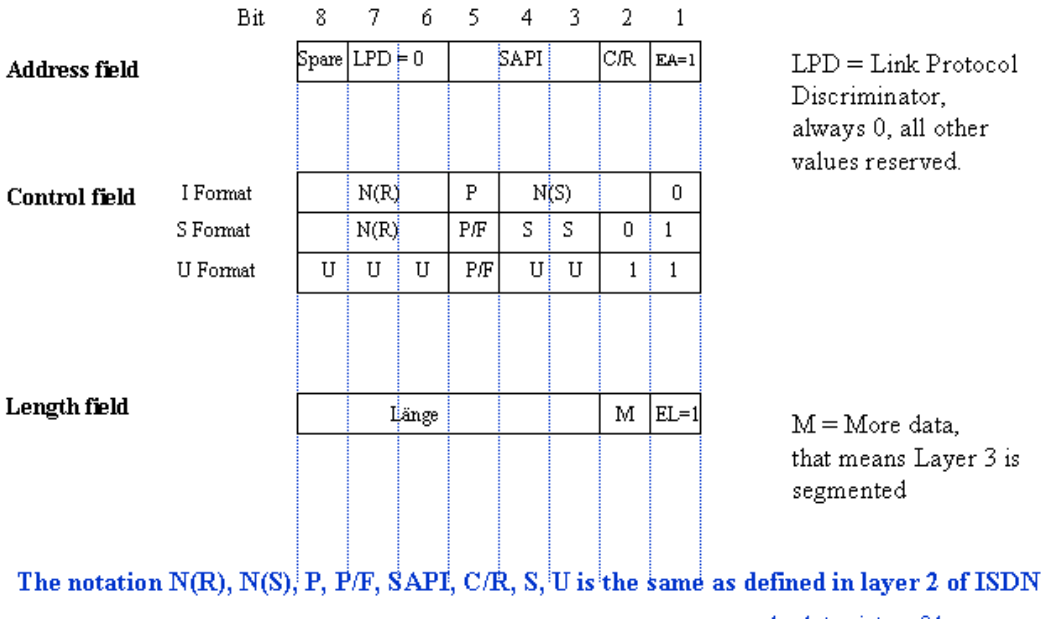
Format	meaning	IEI exists	length exists	value exists
T	Type only	yes	no	no
V	Value only	no	no	yes
TV	Type and Value	yes	no	yes
LV	Length and Value	no	yes	yes
TLV	Type, Length and Value	yes	yes	yes

Picture 26: Pseudolength and types of Information Elements.

A message is dividet into IE. In some messages it is necessary to transfer information in a compressed form, codet in CSN.1 (see later). These octets are called Rest octets. Not used octets in the message string are coded "2B".
From the ISDN it is known that an Information Element always possesses a type, a length and a value. In GSM space frames are limited to 23 bytes and therefore it is necessary to save bits.
For Example, there is an Information Element which is mandatory for a message,
i.e. its Type is known by the Recommendation.
In this case only the length and the value are specified (the type is LV).
If the length is always the same only the Value is specified (the type is V).

5.1 Construction of a Layer 2 Header

The coding of the Address, the Length and the Control octet in the Layer 2 header is of interest. Have a look at picture 27.



Picture 27: Construction of a layer 2 header

In contrast to ISDN:
- the value of the SAPI runs from 0 to 7
- the number of the sent and received bits can only be in the range from 0 to 7
- the length field contains a bit to announce segmentation

As shown in Picture 28, the coding of the S-Format and the U-Format octets are also very similar to those of the ISDN.

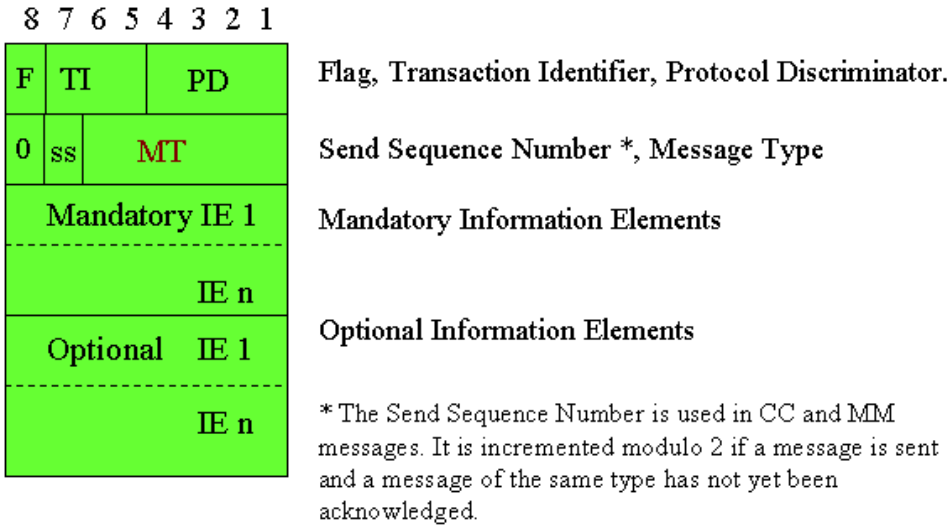
Format	command	answer	8 7 6	5	4 3 2	1
Information	I		N(R)	P	N(S)	0
Supervisory	RR	RR	N(R)	P/F	0 0 0	1
	RNR	RNR	N(R)	P/F	0 1 0	1
	REJ	REJ	N(R)	P/F	1 0 0	1
Unnumbered	SABM		0 0 1	P	1 1 1	1
		DM	0 0 0	F	1 1 1	1
	UI		0 0 0	P	0 0 1	1
	DISC		0 1 0	P	0 0 1	1
		UA	0 1 1	F	0 0 1	1

Picture 28: Commands on Layer 2 controlling the protected Mode

.

5.2 Construction of a Layer 3 Header

The Construction of a Layer 3 header is shown in picture 29.



Picture 29: Construction of a layer 3 header

In order to save bits the Protocol Discriminator uses only 4 bits rather than a whole octet. The other 4 bits belong to the Call reference which here, as in the German ISDN, is called the Transaction Identifier.
Flag = 0 is sent by the site which defines the TI
Flag = 1 is sent to the site which defines the TI

The values of the Protocol Discriminator are as follows:

0011 Call Control and call dependant SS messages
0101 Mobility Management Messages (non-GPRS)
0110 Radio Resource Management Messages
1000 GPRS Mobility Management Messages
1001 Short Message Service Messages
1010 Session Management Messages
1011 Call independent Supplementary Service Messages

Information Elements are sorted as illustrated in Picture 29. The mandatory IE are of types V or LV. The optional IE must always have a Title which shows whether or not the IE exists in the message.

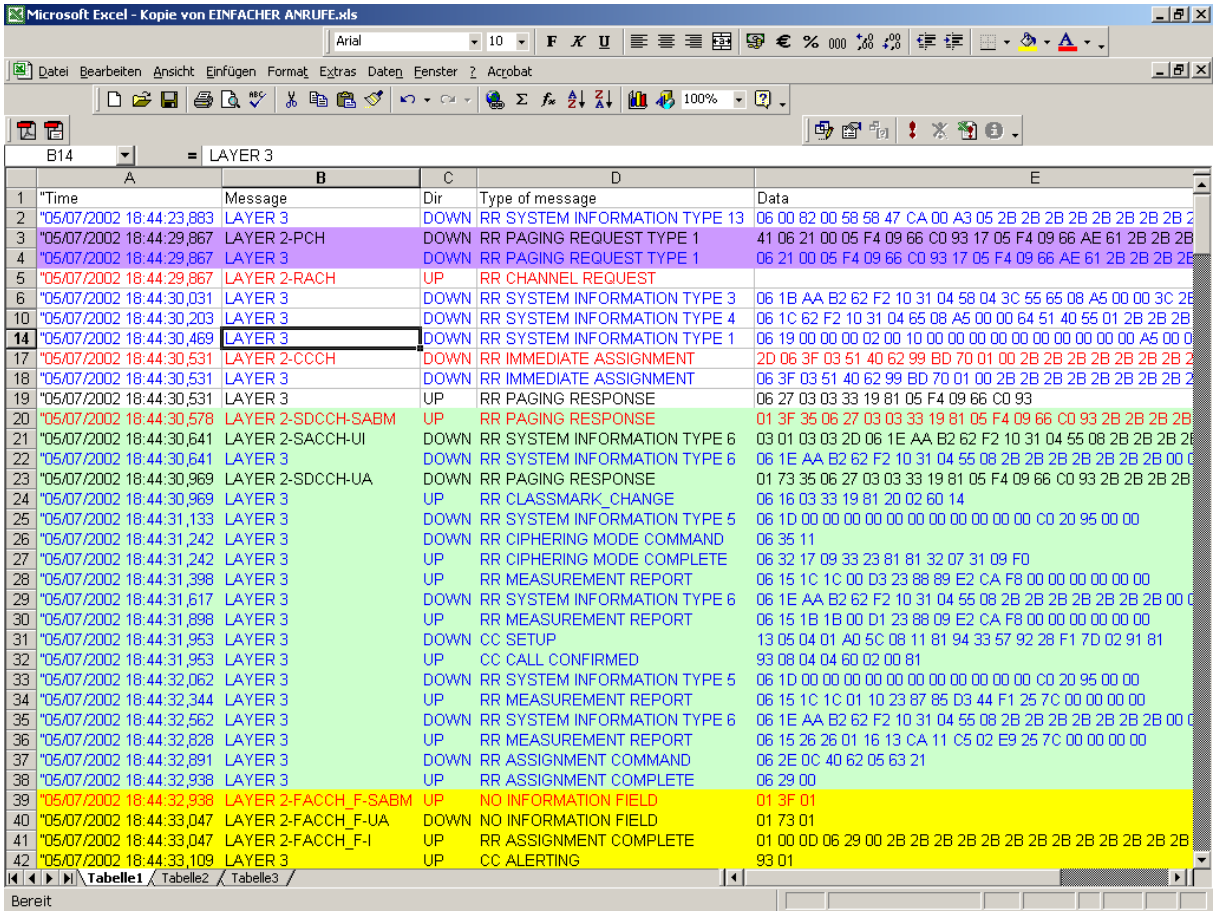
6. Radio Resource Management Messages

6.1 While reading the text please have a look at the Exercise CD

The Author has endeavoured to keep this text readable without any external sources of help. However, it is impossible to do an exercise only by reading a paper. Therefore you will find a CD with this text containing exercises, raw traces, translated messages and script files with the algorithm of how to translate a trace corresponding to the ETS Recommendations in [4].

6.2 Which RR-messages appear in a MTC?

Radio Resource Management Messages serve the organization of the radio connection between Mobile and BTS. Please look at the EXCEL sheet in picture 30 and find the RR-Messages which appear there. To fit as many RR-Messages as possible into the picture all Layer 2 messages have been deleted. If you would like to see the full Excel sheet click Raw traces on the Exercise CD followed by Call from the ISDN to the GSM.



Microsoft Excel - Kopie von EINFACHER ANRUFE.xls

B14 = LAYER 3

	A	B	C	D	E
1	"Time	Message	Dir	Type of message	Data
2	"05/07/2002 18:44:23,883	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 13	06 00 82 00 58 58 47 CA 00 A3 05 2B 2B 2B 2B 2B 2B 2B 2B 2
3	"05/07/2002 18:44:29,867	LAYER 2-PCH	DOWN	RR PAGING REQUEST TYPE 1	41 06 21 00 05 F4 09 66 C0 93 17 05 F4 09 66 AE 61 2B 2B 2B
4	"05/07/2002 18:44:29,867	LAYER 3	DOWN	RR PAGING REQUEST TYPE 1	06 21 00 05 F4 09 66 C0 93 17 05 F4 09 66 AE 61 2B 2B 2B 2B
5	"05/07/2002 18:44:29,867	LAYER 2-RACH	UP	RR CHANNEL REQUEST	
6	"05/07/2002 18:44:30,031	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 3	06 1B AA B2 62 F2 10 31 04 58 04 3C 55 65 08 A5 00 00 3C 2B
10	"05/07/2002 18:44:30,203	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 4	06 1C 62 F2 10 31 04 65 08 A5 00 00 64 51 40 55 01 2B 2B 2B
14	"05/07/2002 18:44:30,469	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 1	06 19 00 00 00 02 00 10 00 00 00 00 00 00 00 00 00 00 A5 00 0
17	"05/07/2002 18:44:30,531	LAYER 2-CCCH	DOWN	RR IMMEDIATE ASSIGNMENT	2D 06 3F 03 51 40 62 99 BD 70 01 00 2B 2B 2B 2B 2B 2B 2B 2
18	"05/07/2002 18:44:30,531	LAYER 3	DOWN	RR IMMEDIATE ASSIGNMENT	06 3F 03 51 40 62 99 BD 70 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2
19	"05/07/2002 18:44:30,531	LAYER 3	UP	RR PAGING RESPONSE	06 27 03 03 33 19 81 05 F4 09 66 C0 93
20	"05/07/2002 18:44:30,578	LAYER 2-SDCCH-SABM	UP	RR PAGING RESPONSE	01 3F 35 06 27 03 03 33 19 81 05 F4 09 66 C0 93 2B 2B 2B 2B
21	"05/07/2002 18:44:30,641	LAYER 2-SACCH-UI	DOWN	RR SYSTEM INFORMATION TYPE 6	03 01 03 03 2D 06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B
22	"05/07/2002 18:44:30,641	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B 00 0
23	"05/07/2002 18:44:30,969	LAYER 2-SDCCH-UA	DOWN	RR PAGING RESPONSE	01 73 35 06 27 03 03 33 19 81 05 F4 09 66 C0 93 2B 2B 2B 2B
24	"05/07/2002 18:44:30,969	LAYER 3	UP	RR CLASSMARK_CHANGE	06 16 03 33 19 81 20 02 60 14
25	"05/07/2002 18:44:31,133	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 5	06 1D 00 00 00 00 00 00 00 00 00 00 00 C0 20 95 00 00
26	"05/07/2002 18:44:31,242	LAYER 3	DOWN	RR CIPHERING MODE COMMAND	06 35 11
27	"05/07/2002 18:44:31,242	LAYER 3	UP	RR CIPHERING MODE COMPLETE	06 32 17 09 33 23 81 81 32 07 31 09 F0
28	"05/07/2002 18:44:31,398	LAYER 3	UP	RR MEASUREMENT REPORT	06 15 1C 1C 00 D3 23 88 89 E2 CA F8 00 00 00 00 00 00
29	"05/07/2002 18:44:31,617	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B 00 0
30	"05/07/2002 18:44:31,898	LAYER 3	UP	RR MEASUREMENT REPORT	06 15 1B 1B 00 D1 23 88 09 E2 CA F8 00 00 00 00 00 00
31	"05/07/2002 18:44:31,953	LAYER 3	DOWN	CC SETUP	13 05 04 01 A0 5C 08 11 81 94 33 57 92 28 F1 7D 02 91 81
32	"05/07/2002 18:44:31,953	LAYER 3	UP	CC CALL CONFIRMED	93 08 04 04 60 02 00 81
33	"05/07/2002 18:44:32,062	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 5	06 1D 00 00 00 00 00 00 00 00 00 00 00 C0 20 95 00 00
34	"05/07/2002 18:44:32,344	LAYER 3	UP	RR MEASUREMENT REPORT	06 15 1C 1C 01 10 23 87 85 D3 44 F1 25 7C 00 00 00 00
35	"05/07/2002 18:44:32,562	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B 00 0
36	"05/07/2002 18:44:32,828	LAYER 3	UP	RR MEASUREMENT REPORT	06 15 26 26 01 16 13 CA 11 C5 02 E9 25 7C 00 00 00 00
37	"05/07/2002 18:44:32,891	LAYER 3	DOWN	RR ASSIGNMENT COMMAND	06 2E 0C 40 62 05 63 21
38	"05/07/2002 18:44:32,938	LAYER 3	UP	RR ASSIGNMENT COMPLETE	06 29 00
39	"05/07/2002 18:44:32,938	LAYER 2-FACCH_F-SABM	UP	NO INFORMATION FIELD	01 3F 01
40	"05/07/2002 18:44:33,047	LAYER 2-FACCH_F-UA	DOWN	NO INFORMATION FIELD	01 73 01
41	"05/07/2002 18:44:33,047	LAYER 2-FACCH_F-I	UP	RR ASSIGNMENT COMPLETE	01 00 0D 06 29 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
42	"05/07/2002 18:44:33,109	LAYER 3	UP	CC ALERTING	93 01

Tabelle1 / Tabelle2 / Tabelle3

Bereit

Picture 30: RR-Messages in a MTC (first part)

You will recognize the following *Radio Resource Management* messages:

6.3 The message PAGING REQUEST 1

PAGING REQUEST TYPE 1 (2, 3) in lines 3 and 4 in picture 30 is a call from the network to the MS. The Mobile is generally called by its TMSI in this way.
In special cases the mobile is called by the IMSI, for example if the Mobile initiates a Location Update with another LAC registered in the VLR.
The message consists of Types 1, 2, 3, two, three or four TIMSI.

6.4 The message SYSTEM INFORMATION TYPE 1

SYSTEM INFORMATION TYPE 1 (line 14 in picture 30) is decoded in table 2. It is shown in the pre-information relating to the channel numbers of
- the transport channel and
- the BCCH .
If the cell serves frequency-hopping, all used frequencies are shown.

In the section RACH Control Parameters Rules for random access are given.
- Max. of retransmission means: if the first channel request from the mobile is not answered by the BTS the mobile may repeat the channel request the number of times given.
- Slots to spread TX means: if the access bursts are repeated there must be a gap of the given number of bursts between them.
- Cell re-establishment in cell means: if the connection is lost, perhaps due to the sudden appearance of an obstacle, the Mobile will try to re-establish the connection. The designated bit shows whether or not this is allowed in the same cell. In the example cell re-establishment is not allowed.
- In the Access control class parameter the users are divided into 16 classes. If there is a traffic overload some types of user may be barred.

```
_____[ 97 ]___[ 20:27:44,454 ]___[ DOWN ]____[ BCCH ]_____________________________

06 19 00 00 00 02 00 10 00 00 00 00 00 00 00 00 00 00 a5 00 00

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

19  00011001  MESSAGE TYPE         : SYSTEM INFORMATION TYPE 1

: Cell Channel Description
00  00------  Format Type          : Bit Map 0 format
    --00----  2 spare bits         : 0

02  ------1-  Cell Allocation      : ARFCN 98
10  ---1----  Cell Allocation      : ARFCN 85

: RACH Control Parameters
a5  10------  Max. of retransmiss  : 4
    --1001--  slots  to spread TX  : 12
    ------0-  The cell is barred   : no
    -------1  Call reestabl.i.cell : not allowed

00  00000---  Acc. contr. cl. 11-15: 0 Access allowed.,1 Access not allowed.
    -----0--  Emergency Call EC 10 : allowed
    ------00  Acc. contr. cl.  8-9 : 0 Access allowed.,1 Access not allowed.

00  00000000  Acc. contr. cl. 0-7  : 0 Access allowed.,1 Access not allowed.
```

Table 2: Message SYSTEM INFORMATION TYPE 1, single channel mode

6.5 The message SYSTEM INFORMATION TYPE 2

The message SYSTEM INFORMATION TYPE 2 (table 3) consists of the neighbouring cells to be monitored, the permitted NCC and the declared rules for random access (see paragraph 6.4).

```
_____[ 8 ]___[ 12:02:42,309 ]___[ DOWN ]____[ BCCH ]_____________________________

06 1a 10 00 00 00 00 10 00 00 00 00 00 c0 20 95 00 00 08 a5 00 00

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

1a  00011010  MESSAGHE TYPE       : SYSTEM INFORMATION TYPE 2

10  --0-----  Extension Indicator : The IE carries the complete BA
    ---1----  BCCH alloc. sequ.num: 1

10  ---1----  BCCH alloc. RF chan.: 85
c0  1-------  BCCH alloc. RF chan.: 40
    -1------  BCCH alloc. RF chan.: 39
20  --1-----  BCCH alloc. RF chan.: 30
95  1-------  BCCH alloc. RF chan.: 24
    ---1----  BCCH alloc. RF chan.: 21
    -----1--  BCCH alloc. RF chan.: 19
    -------1  BCCH alloc. RF chan.: 17

08  ----1---  BCCH carrier with NCC = 3 is permitted for monitoring;

a5  10------  Max. of retransmiss.: 4
    --1001--  12 slots used to spread TX
    ------0-  The cell is barred  : no
    -------1  Call reestablishment in cell is not allowed

00  -----0--  Emergency Call EC 10: allowed
    00000---  acc ctrl class 11-15: 0/1 access permitted/forbidden
    ------00  acc ctrl class  8-9 : 0/1 access permitted/forbidden

00  00000000  acc ctrl class  0-7 : 0/1 access permitted/forbidden
```

Table 3: Message SYSTEM INFORMATION TYPE 2

The message System Information Type 2 does not appear in Picture 30.

6.6 The message SYSTEM INFORMATION TYPE 3

6.6.1 The Information elements of SYS INFO 3

The first Information Element in the message SYSTEM INFORMATION TYPE 3 describes the *Cell Identity* (the number of the BTS) consisting of two bytes.

The second IE, the *Local Area Identification* consists of the *Country Code* (in our case 262 for Germany; the Network Code 01 is the Operator t-Mobile (D1)) and the IDs of the MSC and the BSC.

The third IE represents the *Control Channel Description*.
- *IMSI Attach* (a somewhat strange term) means the Mobile registers to the VLR whilst logging into the network and deregisters from the VLR when releasing its channel. A user calling for that mobile therefore knows at once whether or not the mobile is logged in.
- The *Number of blocks reserved for access grant* specifies how many of the Paging Channels can be used for network access.
- The CCCH is constructed as shown in picture 19 and consists of no SDCCHs.

```
_____[ 4 ]___[ 12:02:41,629 ]___[ DOWN ]____[ BCCH ]_____________________________

06 1b aa b2 62 f2 10 31 04 58 04 3c 55 65 08 a5 00 00 3c 2b 2b 2b

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

1b  00011011  MESSAGE TYPE        : SYSTEM INFORMATION TYPE 3

: Cell Identity
aa  10101010  Cell identity value1: take hex-value
b2  10110010  Cell identity value2: take hex-value

: Location Area Identification
62  ----0010  Mobile CC digit 1   : 2
    0110----  Mobile CC digit 2   : 6
f2  ----0010  Mobile CC digit 3   : 2

    1111----  Mobile NC digit 3   : 15
10  ----0000  Mobile NC digit 1   : 0
    0001----  Mobile NC digit 2   : 1

31  00110001  Loc. area code (LAC) = ID of MSC (hex)
04  00000100  Loc. area code (LAC) = ID of BSC (hex)

: Control Channel Description
58  0-------  1 spare bit         : 0
    -1------  MSs in the cell shall apply IMSI attach and detach procedure
    --011---  Number of blocks    : 3 reserved for access grant
    -----000  1 basic physical channel used for CCCH not combined with SDCCHs

04  00000---  spare bits          : 5
    -----100  6 multi frames period for transmission PAGING REQUEST messages to the same
paging subgroup

3c  00111100  T3212 TimeOut value : 60 deci hours

: Cell Options BCCH,
55  0-------  1 spare bit         : 0
    -1------  PWRC Power control indicator is set
    --01----  MSs shall use uplink discontinous transmission
    ----0101  Radio Link Timeout  : 24

: Cell Selection Parameters;
65  011-----  Cell Resel. Hyster. : 6 dB RXLEV hysteresis for level average (LA) re-selection
    ---00101  Max Tx power level  : Mobile may use 5
08  0-------  Addition. Reselect Param ind: in SI4 rest octets,
    -0------  New establishment cause is not supported
    --001000  RXLEV ACCESS MIN    : -110 +8 db permitted

: RACH  Control Parameters
a5  10------  Max. of retransm.   : 4
    --1001--  used to spread TX   : 12 slots
    ------0-  The cell is barred  : no
    -------1  Call reestablishment in cell is not allowed
00  -----0--  Emergency Call EC10 : allowed
    00000---  Acc.contr.cl. 11-15 : 0/1 access permitted/forbidden
    ------00  Acc.contr.cl.   8-9 : 0/1 access permitted/forbidden
00  00000000  Acc.contr.cl.   0-7 : 0/1 access permitted/forbidden

: SI 3 Rest octet
           0 Selection Parameters not present
           0 Power Offset  not present
           1 System Information 2ter Indicator not present
           1 Early Classmark Sending Control  present
           1 Scheduling if and where not present
           1 High: GPRS indicator = present
: RA COLOUR
         000  Routing Area colour = 0
: SI13 Position
           0  SYSTEM INFORMATION TYPE 13 message is sent on BCCH Norm;
: End SI 3 Rest octet
```

Table 4: Message SYSTEM INFORMATION TYPE 3

- The *Discontinuous Reception* feature is designed to save energy.
Discontinuous Reception means the Mobile does not have to listen continuously when it is logged into the Paging Requests because the latter belong to Paging Groups. Therefore the Mobile only has to listen to Multi-frames belonging to its Paging Group.
A Mobile's Paging Group is calculated from its IMSI. In the frame shown in Table 4 there are 6 multi-frame periods between the appearance of a Paging Group and the next time it has to be observed by the Mobile.
- The Timer 3212 is responsible for the *Periodic Location Updating*. In Table 4 this value is 6 hours.

The fourth IE is called *Cell Options BCCH:*
- If the *Power Control Indicator* (PWRC) is set, the Power of the mobile can be controlled by the BTS.
- *Discontinuous Transmission* is another method of saving energy.
Pauses often appear in conversation and it is favourable to switch off the transmitter during them. However, a hard switch-off appears to the subscriber at the other end of the line as an acoustic shock. To avoid this shock a so-called 'comfort noise' is transmitted during pauses in speech. In this case energy conservation comes from the transmission of a comfort noise frame every 480m instead of transmitting an (empty) speech frame every 20m.
- *Radio link timeout* appears when an active connection suddenly breaks down e.g. if the caller drives their car into an underground car-park. In this case it must be possible to define the end of the connection. This is done by counting the un-decodeable SACH-Frames. In the message shown this number is defined as 24.

The fifth IE is called *Cell Selection Parameter:*
- Let's first have a look at the Parameter *RXLEV ACCESS MIN.* This defines the lowest RX level at which the Mobile's receiver can decode signals without error. In this trace it is given as 102dB.
- A *Cell Reselect Hysteresis* is necessary when the mobile is transported along the border of two cells. If the mobile dips into the area of a neighbouring cell and finds a stronger signal there it initiates a handover. If it is transported a short time later back into its original cell, a second handover occurs and so on. To avoid such continuous switching between two frequencies a *Cell Reselect Hysteresis* is defined, i.e. the network initiates a handover only if the field strengths in the new cell are greater than the measured field strengths in the old cell plus the *Cell Reselect Hysteresis*.
- The *Max TX Power level* is defined in the ETS 05.05 for GSM 900, see table 5.

Power class :	1	2	3	4	5
Nominal max. output power:	(20 W)	8 W (39 dBm)	5 W (37dBm)	2 W (33 dBm)	0,8 W (29 dBm)

Table 5: Power class in GSM 900

6.6.2 The Rest Octet of SYS INFO 3
As shown in the headline of table 4 the octet string to be decoded is

`06 1b aa b2 62 f2 10 31 04 58 04 3c 55 65 08 a5 00 00` **`3c 2b 2b 2b`**

As you can see in table 4, the decoding of all the octets is completed except for the boldly written digits in the string shown.
In GSM 4.08 Table 9.32 the SI 3 Rest Octet is defined to be mandatory (M) type of Value (V) and length 4. The decoding is contained in paragraph 10.5.2.34.
Let's have a look at how this works:

Decoding is done bit by bit in the language *Compact String Notation 1* CSN.1. There are no octet borders to be considered. Normally the octets which bear information are different from the 2b elements but it is possible that a part of the 2b octet may be included in the decoding of the Rest Octet.
Let's have an example. The octets **`3c 2b 2b 2b`** build the string (**00111100 00101011 00101011 00101011**) which is decoded as follows:

: SI 3 Rest Octet
0 Low: Selection Parameters not present
0 Power Offset not present
1 System Information 2nd Indicator present
1 Early Classmark Sending Control present
1 Scheduling if and where not present
1 High: GPRS indicator = present
: RA COLOUR
000 Routing Area colour = 0
: SI13 Position
0 SYSTEM INFORMATION TYPE 13 message is sent on BCCH Norm;
: End SI 3 Rest Octet

In the decoding scheme above there is the expression "High: GPRS indicator = present". This derives from the rule { L | H <GPRS Indicator> } in paragraph 10.5.2.34 SI 3 Rest Octets (GSM 04.08 version 7.8.0 Release 1998).

The rule is as follows: if in the decoding algorithm the expression "L|H" appears, the octet to be decoded must be superimposed bit by bit by 2b = 00101011 with the operation X-OR. If in the position in which L | H is required the result is 1, the value H is true. In our example we have to calculate

3c = **0**0111**1**00
2b = **0**0101**0**11

As we can see at position 6 "1 x-or 0 = 1 = High", while at position 1 "0 x-or 0 = 0 = Low".

6.7 The message SYSTEM INFORMATION TYPE 4

The message SYSTEM INFORMATION TYPE 4 repeats the main Information Elements sent in the SYSTEM INFORMATIONS 1-3. These are:
- Location Area Identification,
- Cell Selection Parameters,
- RACH Control Parameters.

The optional Information Element *Channel Description* is new. It describes where to find the *CELL BROADCAST CHANNEL.* This is a downlink channel which broadcasts information of common interest by SMS.

```
_____[ 2 ]___[ 14:12:01,238 ]___[ DOWN ]____[ BCCH ]_____________________________

06 1c 62 f2 10 31 04 65 08 a5 00 00 64 51 a0 13 01 2b 2b 2b 2b 2b

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

1c  00011100  MESSAGE TYPE        : SYSTEM INFORMATION TYPE 4

: Location Area Identification
62  ----0010  Mobile CC digit 1   : 2
    0110----  Mobile CC digit 2   : 6
f2  ----0010  Mobile CC digit 3   : 2

    1111----  Mobile NC digit 3   : 15
10  ----0000  Mobile NC digit 1   : 0
    0001----  Mobile NC digit 2   : 1

31  00110001  Loc. area code (LAI), ID of MSC (hex)
04  00000100  Loc. area code (LAI), ID of BSC (hex)

: Cell Selection Parameters
65  011-----  Cell Reselect Hyst. : 6 dB RXLEV hyst. For LA re-select
    ---00101  Max Tx power level  : MS may use 5

08  0-------  No Additional cells in SysInfo 7-8
    -0------  New establishm.cause: not supported
    --001000  RXLEV ACCESS MIN permitted = -110+8dB

: RACH Control Parameters
a5  10------  Max. of retransmissions
    --1001--  12 slots used to spread TX
    ------0-  The cell is barred  : no
    -------1  Call reestab.in cell: not allowed

00  -----0--  Emergency Call EC 10: allowed
    00000---  Acc. ctrl class11-15: bit pattern,0 = access permitted, 1 = access forbidden
    ------00  Acc. ctrl class 8-9 : bit pattern,0 = access permitted, 1 = access forbidden
00  00000000  Acc. ctrl class 0-7 : bit pattern,0 = access permitted, 1 = access forbidden

64  01100100  INFORMATION ELEMENT : CHANNEL DESCRIPTION

51  01010---  Channel type and TDMA offset = SDCCH/8 + SACCH/C8|CBCH(SDCCH/8),SC2
    -----001  Timslot number      : 1

          101  Training sequ. code : 5
            0  Single Channel = present
           00  spare

           00  Radio frequency high part
    00010011  Radio frequency low part= 19

: SI4 Rest Octets
: SI4 Rest Octets_O
: Optional  selection parameters
            0  Selection Parameters = not present
: End Optional  selection parameters
: Optional Power offset
            0  Power Offset = not present
: End Optional Power offset
: GPRS Indicator
            0  High: GPRS indicator = present
: RA COLOUR
          000  Routing Area colour = 0
: SI13 Position
            0  SYSTEM INFORMATION TYPE 13 message is sent on BCCH Norm;
: End GPRS Indicator
: End SI4 Rest Octets_O
: Break Indicator
            1  High Additional parameters, "SI4 Rest Octets_S" are sent in SYSTEM INFORMATION
            TYPE 7 and 8
: End SI4 Restoctet
```

Table 6: SYSTEM INFORMATION TYPE 4

6.8 The message SYSTEM INFORMATION TYPE 5

The message SYSTEM INFORMATION TYPE 5 is sent by the BTS if the Mobile is in dedicated mode. The mobile receives in this message information about frequencies of neighbouring cells which are suitable for a handover and are therefore to be monitored. The term BA means **B**CCH **A**RFCN.

```
_____[ 13 ]___[ 18:44:31,133 ]___[ DOWN ]____[ SACCH ]_____________________________

06 1d 00 00 00 00 00 00 00 00 00 00 c0 20 95 00 00

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

1d  00011101  MESSAGE TYPE        : SYSTEM INFORMATION TYPE 5

00  00------  Format Type         : Bit Map 0 format
    --0-----  Extension Indicator : The IE carries the complete BA
    ---0----  BCCH allocation sequence number indication 0

c0  1-------  BCCH alloc. RF chan.: 40
    -1------  BCCH alloc. RF chan.: 39
20  --1-----  BCCH alloc. RF chan.: 30
95  1-------  BCCH alloc. RF chan.: 24
    ---1----  BCCH alloc. RF chan.: 21
    -----1--  BCCH alloc. RF chan.: 19
    -------1  BCCH alloc. RF chan.: 17
```

Table 7: SYSTEM INFORMATION TYPE 5

6.9 The message SYSTEM INFORMATION TYPE 6

The message SYSTEM INFORMATION TYPE 6 is received by the Mobile in dedicated mode. This information is necessary for a possible handover.

```
_____[ 16 ]___[ 12:02:43,199 ]___[ DOWN ]____[ SACCH ]_____________________________

06 1e aa b2 62 f2 10 31 04 55 08 2b 2b 2b 2b 2b 2b 2b 00 00 08 1a

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

1e  00011110  MESSAGE TYPE        : SYSTEM INFORMATION TYPE 6

: Cell Identity
aa  10101010  Cell identity value1, Hex Wert
b2  10110010  Cell identity value2, Hex Wert

: Location Area Identification
62  ----0010  MCC digit 1         : 2
    0110----  MCC digit 2         : 6
f2  ----0010  MCC digit 3         : 2
    1111----  MNC digit 3         : 15
10  ----0000  MNC digit 1         : 0
    0001----  MNC digit 2         : 1
31  00110001  Location area code (LAI), Number of MSC
04  00000100  Location area code (LAI), Number of BSC

: Cell Options (SACH)
55  0-------  1 spare bit         : 0
    -1------  Power control indic.: is set
    --01----  MSs shall use uplink discont.transmission
    ----0101  Radio Link Timeout  : 24
08  ----1---  BCCH carrier with NCC = 3 is permitted for monitoring;
```

Table 8: SYSTEM INFORMATION TYPE 6

6.10 The message SYSTEM INFORMATION TYPE 13

This message only appears if GPRS is possible in the cell. The mobile does not need to wait until the SYSTEM INFORMATION TYPE 13 appears: the Rest Octets in SYSTEM INFORMATION TYPES 3 or 4 also say whether GPRS is available.

6.11 The message CHANNEL REQUEST

Please have another look at picture 30. In line 5, immediately after the message PAGING REQUEST has appeared, the Mobile sends a CHANNEL REQUEST.
The length of this message is only 8 bits. Three bits are used to express the cause of the Channel Request, five bits are left for a random number which serves as a distinguishing mark of the sender.
Possible causes for Channel Request are:

Emergency call	101
Answer to paging	100
Originating call…	111
Call re-establishing…	110
Location Updating	000

and so on.
To assign more than 5 causes, the number of random bits can be decreased to no less than 2.

6.12 The message IMMEDIATE ASSIGNMENT

With the message Immediate Assignment, negotiation about Radio Resources is initiated.

6.12.1 Assigning a single Channel

This message dedicates the mobile a Stand Alone Dedicated Control Channel SDCCH, a channel number, a timeslot number and a precise frame number.
Please have another look at Table 1 which shows a trace and a more detailed description of this message in paragraph 4.10.

6.12.2 Assigning frequency hopping

In GSM slow frequency hopping (SFH) is used, i.e. the transmission frequency remains the same during the transmission of a full burst. One of the reasons for the introduction of frequency hopping is *frequency diversity*.
As shown in picture 25, a message frame is encoded with a Fire Code which allows correction of 11 bit errors in the frame of 184 bits. The problem is the appearance of burst errors of more than eleven bits in the frame.
One solution to this problem is the additional coding with a convolutional code.
SFH offers another possibility of reducing errors: improved transmission is achieved by changing the frequency with every burst. I do not intend to have a closer look at this behaviour because it requires knowledge about the theory of the propagation of radio waves.

The Channel Description of frequency hopping consists of the following parameter:
- *Mobile Allocation* MA: the number of the frequency used during SFH.
- *Hopping Sequence number* HSN: a value between 0 and 63 which controls the *Hopping Generator*
- *Mobile Allocation Index Offset* MAIO: a number which can accept all values of the MA

MAIO and HSN together and determine the sequence of the frequencies and timeslots used after one another in the channel.
Two channels with the same HSN but different MAIO never use the same frequency on the same burst.

```
_____[ 30 ]___[ 11:36:27,504 ]___[ DOWN ]____[ CCCH ]_____________________________

31 06 3f 00 41 70 92 20 7b aa 01 01 07

31  00110001  Pseudo length : 49
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

3f  0-------  1 spare bit         : 0
    -0------  Send sequence number: 0

    --111111  MESSAGE TYPE        : IMMEDIATE ASSIGNMENT

: Page Mode
00  ----00--  2 spare bits        : 0
    ------00  Page mode           : Normal paging
: Dedicated Mode or TBF
    0-------  1 spare bit         : 0
    -0------  Two messages assign.: No meaning
    --0-----  Downlink assig to MS: No meaning
    ---0----  This message assigns a dedicated mode resource

: Channel Description
41  01000---  Ch.type & TDMA offs.: SDCCH/8 + SACCH/C8|CBCH(SDCCH/8),SubChannel 0
    -----001  Timslot number      : 1


70  011-----  Training seq. code  : 3
    ---1----  Hopping Channel     : RF hopping channel
    ----0000  MAIO  (high)        : 0
92  10------  MAIO  (low)         : 2
    --010010  Hopping Seq. Number : 18

20  0010----  Establishing Cause  : Answer to paging
    ----0000  Random Reference    : 0

       01111  15      = (T1)     is coded as the bin.repr.of (Frame. Number div 1326) mod 32.
      011101  29      = (T3)     is coded as the bin. repr. of Frame Number mod 51.
       01010  10      = (T2)     is coded as the binary representation of FrameNumber mod 26.
: The frame number, FN modulo 42432 can be calculated as 51x((T3-T2)mod 26)+T3+51x26xT1'


01  00------  2 spare bits         : 0
    --000001  Timing advance value : 1 bit period

01  00000001  lgth of Mob.Alloc.IE : 1

07  -----1--  Mobile allocation RF chann.: Nr. 03 in the cell all.frequency list
    ------1-  Mobile allocation RF chann.: Nr. 02 in the cell all.frequency list
    -------1  Mobile allocation RF chann.: Nr. 01 in the cell all.frequency
```

Table 9: IMMEDIATE ASSIGNMENT dedicates a frequency hopping channel

6.13 The message PAGING RESPONSE

With the message PAGING RESPONSE the mobile sends a receipt of the information and orders given by the message IMMEDIATE ASSIGNMENT. It also describes its ciphering possibilities, hardware features and identity to the network (see table 10). Because there now begins the negotiation of the conditions with which the communication is to established, the connection on the air interface is switched into the protected mode.
Therefore PAGING RESPONSE is sent on the SDCCH with a SABM on layer 2.
The network gives a receipt by sending back the same message with an UA on layer 2 (see picture 30 line 23).

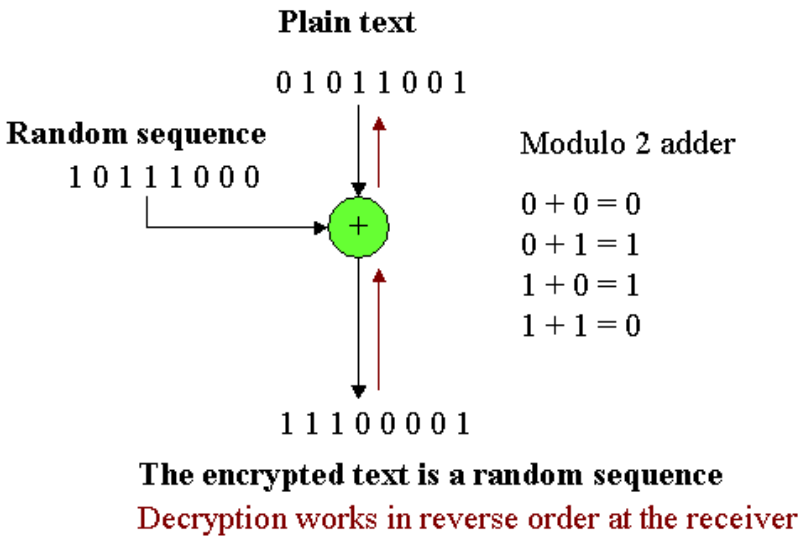
```
_____[ 11 ]___[ 12:02:42,328 ]___[ UP ]_____________________________________________

06 27 04 03 23 19 01 05 f4 65 32 7d 20

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

27  0-------  1 spare bit         : 0
    -0------  Send sequence number: value
    --100111  MESSAGE TYPE        : PAGING RESPONSE

: Ciphering Key Sequence  Number
04  ----0---  1 spare bit         : 0
    -----100  Ciph. key sequ. num.: 4 (7=no key available)
    0000----  4 spare bits        : 0

: Mobile Station Classmark 2
03  00000011  lgth of MS Cl.Mark2 : 3

23  0-------  1 spare             : 0
    -01-----  Revision Level      : Used by phase 2 mobile stations
    ---0----  "Controlled Early Classmark Sending" option is not implemented in the
MS
    ----0---  Encryp.Algor. A5_1  : available
    -----011  RF power capability : Class 4, handheld

19  0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------1  The MS does support the E-GSM or R-GSM

01  0-------  The MS does not support any options that are indicated in CM3
    -0------  1 spare bit         : 0
    --0-----  LocationServiceValueAdded Capability  not supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available

: Mobile Identity

05  00000101  length of Mob. ident: 5
f4  1111----  Identity Digit 1    : 15
    ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
65  01100101  Identity Digit 2,3  : take hex value
32  00110010  Identity Digit 4,5  : take hex value
7d  01111101  Identity Digit 6,7  : take hex value
20  00100000  Identity Digit 8,9  : take hex value
```

Table 10: The message PAGING RESPONSE

6.13.1 About the encryption of the Transport Channel

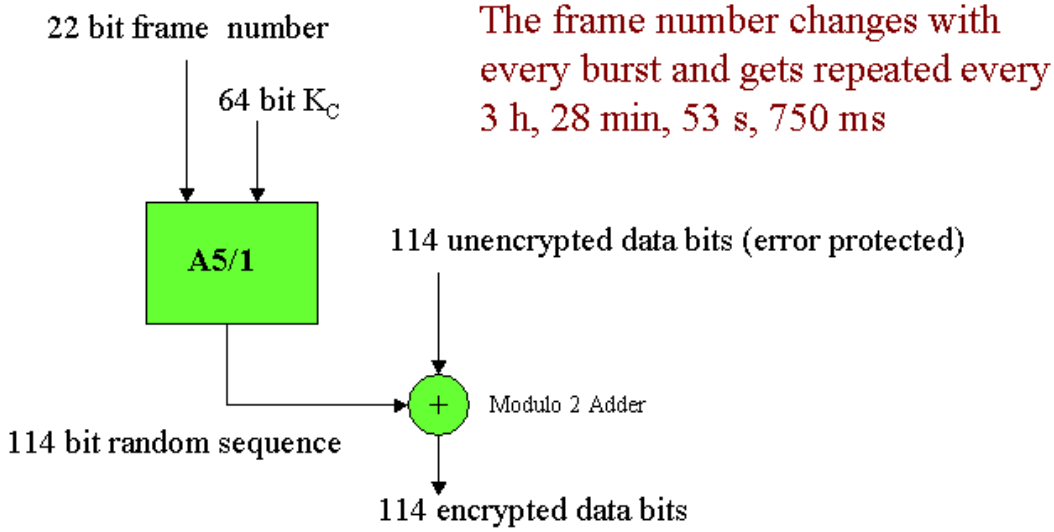
The first IE in the message PAGING RESPONSE is *Ciphering Key Sequence Number*. In order to understand this term we will have to deal with some ideas concerning the theory of ciphering. Picture 32 shows how a plain text can be ciphered. A modulo 2 random text is added to the plain text and the result is a random text.
The random text must be pure, i.e. it must stem for example from the noise of a radioactive source.

Because it is impossible for the sender and receiver simultaneously to have the same radioactive source, we must seek to install a quasi-random source with a very large repetition time.



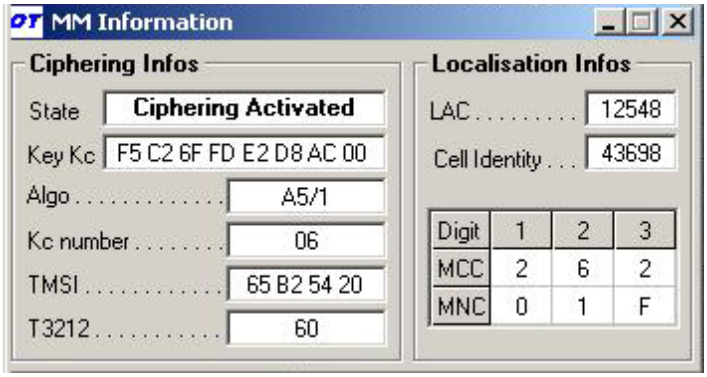
Picture 31: The principle of encryption.

Please bear in mind that the same frame number only appears every 3h, 28min, 53s, 750m. With this fact a quasi-random generator is built.



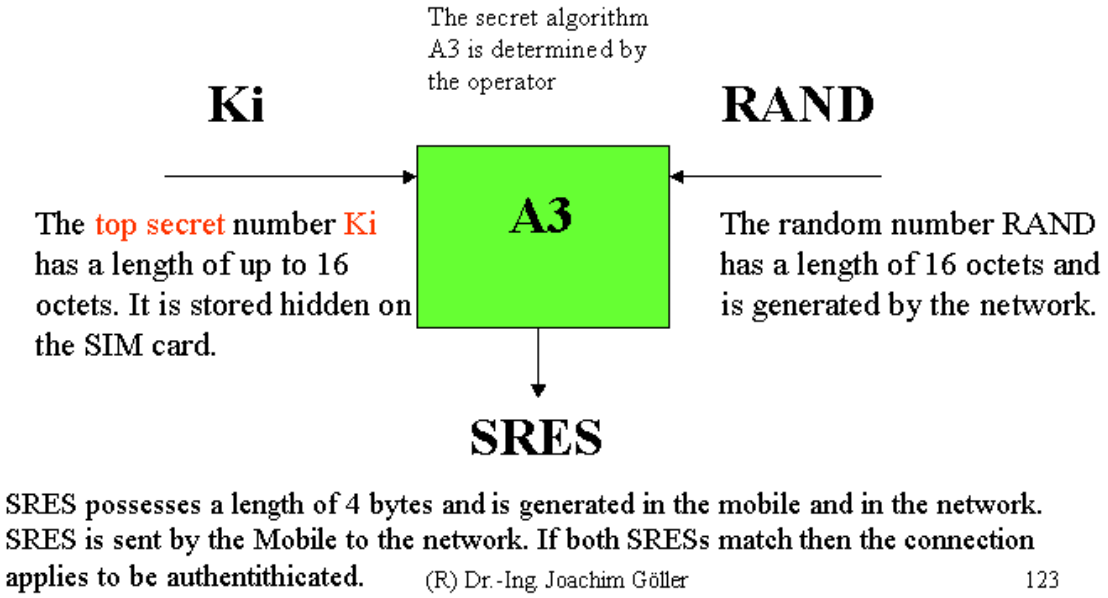
Picture 32: The principle of encryption with a quasi-random sequence.

As picture 32 shows, the random 114 bit sequence changes with every new frame number, therefore every burst is encrypted with a different random sequence.
The random sequence is calculated from the 22 bit frame number and the 64 bit Ciphering Key (K_C) by the algorithm A5/X (X=1…5).
The algorithm A5 is known by the manufacturers of mobiles and by the operators. From the called series of algorithms only A5/1 and A5/2 are used, A5/1 being the strongest .



Picture 33: The MM Information window of the OTDrivePC software

We will now consider how the Ciphering Key K_C is calculated and how it is ensured that the mobile and network use the same key.



Picture 34: The generation of a "password" (SRES)

First there is a highly secret number Ki which is stored hidden on the SIM card along with the algorithm A3. It is possible that every operator is using their own A3 but this does not matter because a user with a SIM card from operator D1 cannot have connections with users of the network of D2.
The network now sends the message AUTHENTICATION REQUEST and the Random number RAND which has a length of 16 octets.
This is like calling "Password" to a guard. In the same message the network sends the *Ciphering Key Sequence Number* CKSN to the mobile in order to assign the K_c to be used.

```
_____[ 19 ]___[ 11:22:03,895 ]___[ DOWN ]____[ SDCCH ]_____________________________

05 12 06 c2 fc da 27 44 9f 92 b4 ab 7a b5 72 8f ff c4 71

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
12  00------  SendSequenceNumber  : 0

    --010010  MESSAGE TYPE        : AUTHENTICATION REQUEST

06  0000----  Spare
    ----0---  Spare
    -----110  Ciph.Key Seq. Numb. : 6

: Authentication parameter RAND
c2  11000010  Parameter 1         : 194
fc  11111100  Parameter 2         : 252
da  11011010  Parameter 3         : 218
27  00100111  Parameter 4         : 39
44  01000100  Parameter 5         : 68
9f  10011111  Parameter 6         : 159
92  10010010  Parameter 7         : 146
b4  10110100  Parameter 8         : 180
ab  10101011  Parameter 9         : 171
7a  01111010  Parameter 10        : 122
b5  10110101  Parameter 11        : 181
72  01110010  Parameter 12        : 114
8f  10001111  Parameter 13        : 143
ff  11111111  Parameter 14        : 255
c4  11000100  Parameter 15        : 196
71  01110001  Parameter 16        : 113
```

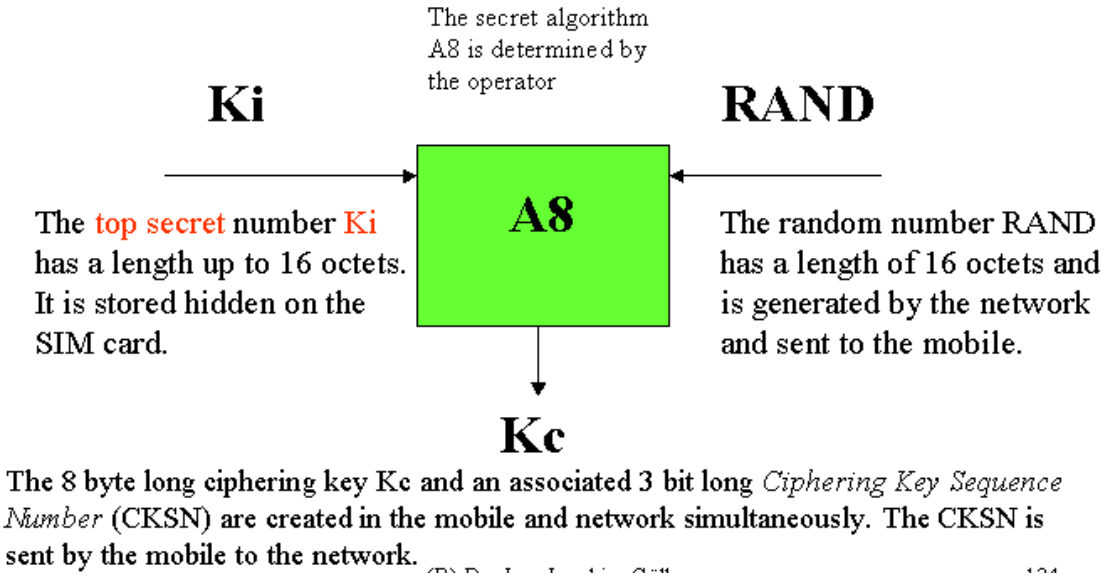
Table 11: The message AUTHENTICATION REQUEST

As shown in picture 35 the mobile immediately calculates the “password” SRES and sends it back to the network in the message AUTHENTICATION RESPONSE in response to the call of “Password” (see Table 12).

```
_____[ 22 ]___[ 11:22:04,074 ]___[ UP ]_____________________________________________

05 14 d3 47 dc 3b

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
14  00------  SendSequenceNumber  : 0

    --010100  MESSAGE TYPE        : AUTHENTICATION RESPONSE

: Authentication Parameter SRES
d3  11010011  Parameter 1         : 211
47  01000111  Parameter 2         : 71
dc  11011100  Parameter 3         : 220
3b  00111011  Parameter 4         : 59
```

Table 12: The message AUTHENTICATION RESPONSE

The network now knows that the subscriber is allowed to set up a communication link. Using Ki and RAND the Mobile now calculates K_c and a 3 bit *Ciphering Key Sequence Number* CKSN. Please bear in mind that the network has calculated K_c and CKSN before sending the message AUTHENTICATION REQUEST.



Picture 35: Calculating K_c

Network and mobile now dispose of the same ciphering key.
The network sends the message CIPHERING MODE COMMAND (Table 12) and orders the mobile to cipher with algorithm A5/1 or A5/2. In special situations some Operators (e.g. O2) might send “no ciphering”.
The operator orders the mobile to receipt the message by sending the IMEISV of the Mobile

```
_____[ 13 ]___[ 12:02:42,809 ]___[ DOWN ]____[ SDCCH ]_____________________________

06 35 11

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

35  00110101  MESSAGE TYPE        : CIPHERING MODE COMMAND

11  ----000-  cipher with algorithm A5/1
    -------1  Start ciphering
    000-----  spare                : 0
    ---1----  Cipher Response      : IMEISV shall be included
```

Table 13: The message CIPHERING MODE COMMAND

Let us recall the construction of the IMEI:

- 3 octets TAC (Type Approval Code) given after testing the mobile
- 1 octet FAC (Final Assembly Code) Factory
- 3 octets Serial Number
- 4 bits reserved

The IMEISV is like the IMEI but the reserved 4 bits are replaced by a 1 Octet Software Version Number SVR.

```
_____[ 14 ]___[ 12:02:42,809 ]___[ UP ]_____________________________________________

06 32 17 09 33 23 81 81 22 99 78 06 f0

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
32  00110010  MESSAGE TYPE        : CIPHERING MODE COMPLETE

17  00010111  INFORMATIONS ELEMENT: Mobile Identity

09  00001001  length of Mob.ident.3: 9

33  ----0---  No. of ID digits     : even
    -----011  Type of identity     : IMEISV
    0011----  Identity Digit 1     : 3
23  ----0011  Identity Digit 2     : 3
    0010----  Identity Digit 3     : 2
81  ----0001  Identity Digit 4     : 1
    1000----  Identity Digit 5     : 8
81  ----0001  Identity Digit 6     : 1
    1000----  Identity Digit 7     : 8
22  ----0010  Identity Digit 8     : 2
    0010----  Identity Digit 9     : 2
99  ----1001  Identity Digit 10    : 9
    1001----  Identity Digit 11    : 9
78  ----1000  Identity Digit 12    : 8
    0111----  Identity Digit 13    : 7
06  ----0110  Identity Digit 14    : 6
    0000----  Identity Digit 15    : 0
f0  ----0000  Identity Digit 16    : 0
    1111----  Identity Digit 17    : 15
```

Table 14: The message CIPHERING MODE COMPLETE with SVR = 0

6.13.2 The Mobile Station Classmark

Following this information on ciphering, we can now return to the content of the PAGING RESPONSE message (see table 10).

The second Information Element in the message is Mobile Station Classmark 2. This consists of the following properties of the Mobile:

- The Revision Level of the software. This is important because the Recommendations are permanently updated.
- Early Classmark Sending. This means the Mobile sends its technical features to the network as soon as is possible (this is not used in our example).
- The encryption algorithm indicates which ciphering algorithm is implemented in the mobile station.
- As seen in table 5, the power class 4 (handheld) is 2 W.
- Pseudo-synchronisation capability means the Mobile is not able to guess the timing advance value during handover.
- The purpose of the supplementary service screening indicator is to allow the network to asses the capabilities of the MS in advance of network initiated SS activity.
- The Mobile is able to send and receive SMS
- As you can see in picture 12, the Mobile supports E-GSM (see 4.1.2). Railway GSM, uplink 876-915 MHz, downlink 921- 960 MHz is not supported.
- The encryption algorithm is available.

The third Information Element in the message is Mobile Station Classmark 3

- Associated Radio Capability 1 is due to E and R-GSM (where class 4 means 2 W)
- Associated Radio Capability 2 is due to DCS 1800 (where class 1 means 1 W)

6.14 The message CLASSMARK CHANGE

Although we have seen that the Mobile sends its hardware capabilities within the PAGING RESPONSE message, it is possible to use the message CLASSMARK CHANGE (picture 31, line 24) either to send the same values again, or to correct these values.
For example, you send: Encryp.Algor. A5/1 not available. The network will either refuse the connection (operator D1, D2) or will take encryption Algorithm A5/2 (operator O2).
The Information Elements are as explained in paragraph 6.11.2.

```
_____[ 12 ]___[ 18:44:30,969 ]___[ UP ]____[ SDCCH ]_____________________________

06 16 03 33 19 81 20 02 60 14

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

16  00010110  MESSAGE TYPE        : CLASSMARK CHANGE

: Mobile Station Classmark 2
03  00000011  length              : 3

33  0-------  1 spare             : 0
    -01-----  Revision Level      : Used by phase 2 mobile stations
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  Encryp.Algor. A5_1  : available
    -----011  RF power capability : Class 4, handheld

19  0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------1  The MS does support the E-GSM or R-GSM

81  1-------  The MS does support any options that are indicated in CM3
    -0------  1 spare bit         : 0
    --0-----  LocationServiceValueAdded Capability  not supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available


20  00100000  INFORMATION ELEMENT : CLASSMARK 3

02  00000010  length              : 2

60  0110----  P-GSM, E-GSM or R-GSM supported, DCS 1800 not supported
    ----0---  encryption algorithm A5/7 not available
    -----0--  encryption algorithm A5/6 not available
    ------0-  encryption algorithm A5/5 not available
    -------0  encryption algorithm A5/4 not available

14  ----0100  Associated Radio capability 1 = power class 4
    0001----  Associated Radio capability 2 = power class 1
```

Table 15: The message CLASSMARK CHANGE

Now let's have a look at the message which appears in line 28 of picture 22.

6.15 The message MEASUREMENT REPORT

While in dedicated mode the mobile measures the field strength of its neighbouring cells given by SYSTEM INFORMATION TYPE 5 and transmits the results to the BTS .

```
_____[ 16 ]___[ 18:44:31,398 ]___[ UP ]_____________________________________________

06 15 1c 1c 00 d3 23 88 89 e2 ca f8 00 00 00 00 00 00

06  0-------  direction from      : originating site
    -000----  Transaction ID      : 0
    ----0110  Protocol Discrim.   : radio resource management messages

15  00010101  MESSAGE TYPE        : MEASUREMENT REPORT

1c  0-------  BA used             : no
    -0------  Discontinuous Transmission was not used
    --011100  RXLEV-FULL-SERVING-CELL= (-110 + 28) dB

1c  0-------  spare               : 0
    -0------  MEAS-VALID          : yes
    --011100  RXLEV-SUB-SERVING-CELL = (-110 + 28) dB
     0------  spare               : 0
     -000---  RX-QUAL-FULL-SERVING-CELL = ~0,14% error bit
     ----000  RX-QUAL-SUB -SERVING-CELL = ~0,14% error bit
         011  Number of neighbouring cell measurements  = 3

      010011  RXLEV-Neighbour-CELL 1 = (-110 + 19) dB
       00100  BCCH-FREQ-NCELL 1   : 4
      011100  Base station identity code of the 1'th neighbouring cell = 28

      010001  RXLEV-Neighbour-CELL 2 = (-110 + 17) dB
       00010  BCCH-FREQ-NCELL 2   : 2
      011110  Base station identity code of the 2'th neighbouring cell= 30

      001011  RXLEV-Neighbour-CELL 3 = (-110 + 11) dB
       00101  BCCH-FREQ-NCELL 3   : 5
      011111  Base station identity code of the 3'th neighbouring cell = 31

      000000  RXLEV-Neighbour-CELL 4 = (-110 + 0) dB
       00000  BCCH-FREQ-NCELL 4   : 0
      000000  Base station identity code of the 4'th neighbouring cell = 0

      000000  RXLEV-Neighbour-CELL 5 = (-110 + 0) dB
       00000  BCCH-FREQ-NCELL 5   : 0
      000000  Base station identity code of the 5'th neighbouring cell = 0

      000000  RXLEV-Neighbour-CELL 6 = (-110 + 0) dB
       00000  BCCH-FREQ-NCELL 6   : 0
      000000  Base station identity code of the 6'th neighbouring cell = 0
```

Table 16: Measurement Report

By looking at the measurement results the network is able to decide when the mobile has to perform a *Hand Over* to a cell with a stronger field strength than the one the mobile is currently camping on.
It must be mentioned that the Mobile is able to calculate the probability of the appearance of errors (RX-QUAL-FULL-SERVING-CELL) by watching the *Training Sequence* issued with every *Normal Burst*.
Mouly & Poutet tell us: “The mobile station is to report two sets of measurements concerning the connection:
- *Full* measurements, performed on all slots which may be used for transmission in the reporting period, and
- *sub* measurements, performed only on the mandatory sent bursts and blocks.”
The latter is performed in the case of DTX.

6.16 The message ASSIGNMENT COMMAND

With the message ASSIGNMENT COMMAND the mobile is assigned: a transport channel, a channel number, a timeslot number, the channel mode and the power level.

```
_____[ 23 ]___[ 12:02:44,453 ]___[ DOWN ]____[ SDCCH ]_____________________________

06 2e 0a 40 62 05 63 21

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

2e  00101110  MESSAGE TYPE        : ASSIGNMENT COMMAND

: Channel Description 2
0a  00001---  Channel type and TDMA offset = TCH/F + ACCHs
    -----010  Timslot number      : 2

40  010-----  Training sequ. code : 2
    ---000--  Single channel      : RF single channel
    ------00  Sgl RF chan.high prt: 0
62  01100010  abs.RFchan. low part: 98

: POWER LEVEL
05  000-----  spare
    ---00101  Power level         : 5

: Channel Mode

63  01100011  INFORMATION ELEMENT : CHANNEL MODE
21  00100001  channel mode        : speech full rate or half rate version 2
```

Table 17: The message ASSIGNMENT COMMAND

6.17 Setting up the protected mode again and the message ASSIGNMENT COMPLETE

With ASSIGNMENT COMPLETE the mobile reports the successful assignment of the channel.

```
_____[ 24 ]___[ 12:02:44,492 ]___[ UP ]_____________________________________________

06 29 00

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

29  00101001  MESSAGE TYPE        : ASSIGNMENT COMPLETE

00  00000000  RR-Cause (reason of event) = Normal event
```

Table 18: The message ASSIGNMENT COMPLETE

Before sending ASSIGNMENT COMPLETE to the BTS on layer 2 the Mobile requests a change to the protected mode. The Mobile sends SABM on a FACH and the BTS responds with UA, also on a FACH.
Now the Call Control messages are exchanged between the Mobile and network. We shall discuss this later in paragraph 9.

6.18 The message CHANNEL RELEASE

After the Call is finished and the communication channel has been disconnected and released, the transport channel is also released.

```
_____[ 79 ]___[ 14:12:23,910 ]___[ DOWN ]____[ FACCH_F ]_____________________________

06 0d 00

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages

0d  00001101  MESSAGE TYPE        : CHANNEL RELEASE

00  00000000  RR-Cause (reason of event) = Normal event
```

Table 19: The message CHANNEL RELEASE

It is of interest to see a list of causes which can be used in the messages CHANNEL RELEASE and ASSIGNMENT COMPLETE (see table 20)

```
00000000  RR-Cause (reason of event) = Normal event
00000001  RR-Cause (reason of event) = Abnormal release, unspecified
00000010  RR-Cause (reason of event) = Abnormal release, channel unacceptable
00000011  RR-Cause (reason of event) = Abnormal release, timer expired
00000100  RR-Cause (reason of event) = Abnormal release, no activity on the radio path
00000101  RR-Cause (reason of event) = Pre-emptive release
00001000  RR-Cause (reason of event) = Handover impossible, timing advance out of range
00001001  RR-Cause (reason of event) = Channel mode unacceptable
00001010  RR-Cause (reason of event) = Frequency not implemented
01000001  RR-Cause (reason of event) = Call already cleared
01011111  RR-Cause (reason of event) = Semantically incorrect message
01100000  RR-Cause (reason of event) = Invalid mandatory information
01100001  RR-Cause (reason of event) = Message type non-existent or not implemented
01100010  RR-Cause (reason of event) = Message type not compatible with protocol state
01100100  RR-Cause (reason of event) = Conditional IE error
01100101  RR-Cause (reason of event) = No cell allocation available
01101111  RR-Cause (reason of event) = Protocol error unspecified
```

Table 20: The causes which may be used in CHANNEL RELEASE and ASSIGNMENT COMPLETE

6.19 The message CLASSMARK ENQUIRY

The message CLASSMARK ENQUIRY is sent by the BTS in order to request the technical properties of the mobile. It does not consist of any Information Element.

```
_____[ 17 ]___[ 11:22:03,684 ]___[ DOWN ]____[ SDCCH ]_____________________________

06 13

06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
13  00010011  MESSAGE TYPE        : CLASSMARK ENQUIRY
```

Table 21: The message CLASSMARK ENQUIRY

7. The Handover Procedure

7.1 Determination of the strongest transmitter

Before we deal with the Handover procedure we must first consider how to determine the strongest transmitter. Up to this point we have only looked at the largest field strength during the Measurement Report. The method which is actually applied is somewhat more sophisticated.

IDLE	BCCH	BSIC		Cell ID	Level(dBm)		Tx Max	C1	C2
		NCC	BCC		Rx	RM			
Serving cell	90	3	2	56281	-82	-106	5	25	25
Neighbour 1	85	3	2	43698	-81	-106	5	25	25
Neighbour 2	21	3	6	43697	-93	-106	5	13	13
Neighbour 3	30	3	4	52538	-87	-106	5	19	19
Neighbour 4	15	***	***	***	-98	***	***	***	***
Neighbour 5	36	3	3	56283	-97	-106	5	9	9
Neighbour 6	***	***	***	***	***	***	***	***	***

Picture 36: Layer 1 Report on OTDrivePC

In picture 36 you can see the two columns, the *path loss criterion parameter* C1, and the *reselection criterion* C2.

The ETS recommendations define the path loss criterion parameter C1 as follows

$$C1 = (A - Max(B,0))$$

where

A = Rx - RM
B = MS_TXPWR_MAX_CCH - Maximum RF output power of the MS.

Rx = Received Level Average, as shown in picture 36
RM = Minimum received level at the MS required for access to the system, as shown in picture 36
MS_TXPWR_MAX_CCH = Maximum TX power level a MS may use when accessing the system

The path loss criterion is satisfied if $C1 > 0$.

The reselection criterion C2 is defined as

$$C2 = C1 - F$$

where F, in our case zero, will not be discussed here.
Concerning the above, we know that the field strength reported in the Measurement Report is part of the calculation of C1. If the C1 value of the neighbouring cell, taking into account the cell Hysteresis, is greater than the C1 of the cell which the mobile is camping on, the Message HANDOVER COMMAND is issued by the BTS.

7.2 The Message HANDOVER COMMAND

From the message HANDOVER COMMAND the mobile receives a new BCCH, the number of the Transport Channel, the timeslot and the Handover Reference (a random number).

```
_____[ 193 ]___[ 20:26:11,430 ]___[ DOWN ]____[ FACCH_F ]_____________________________

03 62 25 06 2b 1e 15 0f c0 20 05 05

03  0-------  Spare               : 0
    -00-----  Link Prot. Disc.    : 1
    ---000--  SAPI                : 0
    ------1-  C/R Flag            : 1, BS side to MS side
    -------1  EA                  : 1
62  01100010  Information Transf. : INFORMATION         N(R)=3, N(S)=1, P=0
25  001001--  length              : 9
    ------0-  M                   : 0
    -------1  EL                  : 1
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
2b  00101011  MESSAGE TYPE        : HANDOVER COMMAND

: Celldescription
1e  --011---  PLMN Colour Code NCC: 3
    -----110  BS Colour code  BCC : 6
    00------  BCCH ARFCN high part
15  00010101  BCCH ARFCN low part : 21

: Channel Description 2
0f  00001---  Channel type and TDMA offset = TCH/F + ACCHs
    -----111  Timslot number      : 7

c0  110-----  Training sequ. code : 6
    ---000--  Single channel      : RF single channel
    ------00  Sgl RF chan.high prt: 0
20  00100000  abs.RFchan. low part: 32

: Handover Reference
05  00000101  Handover refer. val.: 5

: Power Command and Access Type
05  0-------  Sending of Handover access is mandatory
    -00-----  spare
    ---00101  Power Level         : 5
```

Table 22: The message HANDOVER COMMAND

7.3 The Message HANDOVER COMPLETE

With the Message HANDOVER COMPLETE the Mobile reports the successful change to a new cell to the BTS.

```
_____[ 198 ]___[ 20:26:11,758 ]___[ UP ]____[ FACCH_F ]_____________________________
01 00 0d 06 2c 00

01  0-------  Spare               : 0
    -00-----  Link Prot. Disc.    : 0
    ---000--  SAPI                : 0
    ------0-  C/R Flag            : 0, MS side to BS side
    -------1  EA                  : 1
00  00000000  Information Transf. : INFORMATION         N(R)=0, N(S)=0, P=0
0d  000011--  length              : 3
    ------0-  M                   : 0
    -------1  EL                  : 1
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
2c  00101100  MESSAGE TYPE        : HANDOVER COMPLETE

: RR Cause
00  00000000  Normal event
```

Table 23: The message HANDOVER COMPLETE

7.4 The Message PHYSICAL INFORMATION

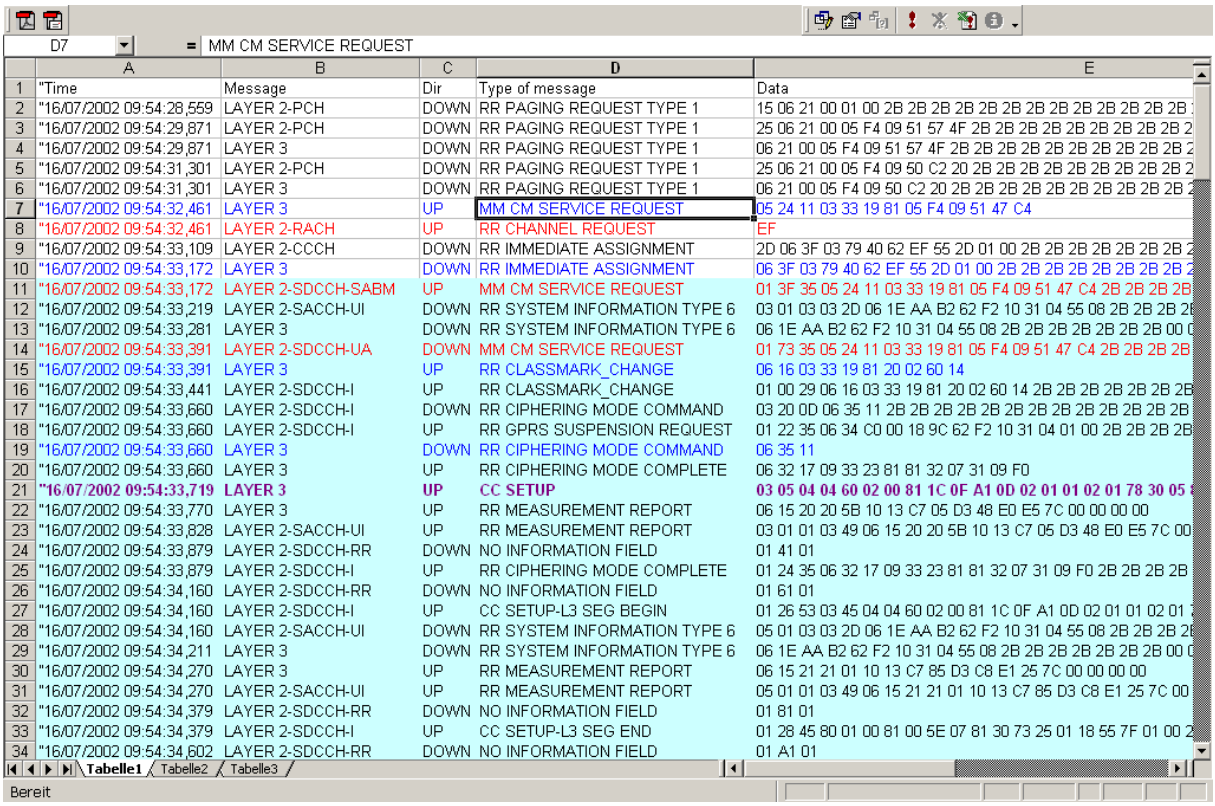
With this message the Mobile receives the new *Timing Advance* value (see table 24).

```
_____[ 195 ]___[ 20:26:11,539 ]___[ DOWN ]____[ FACCH_F ]_____________________________
03 03 0d 06 2d 01

03  0-------  Spare               : 0
    -00-----  Link Prot. Disc.    : 1
    ---000--  SAPI                : 0
    ------1-  C/R Flag            : 1, BS side to MS side
    -------1  EA                  : 1
03  00000011  Unnumbered          : UNNUMBERED INFORMATION    P=0
0d  000011--  length              : 3
    ------0-  M                   : 0
    -------1  EL                  : 1
06  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0110  Protocol Discrim.   : radio resource management messages
2d  00101101  MESSAGE TYPE        : PHYSICAL INFORMATION

: Timing Advance
01  00------  spare
    --000001  Timing advance value: 1 x 48/13 /usec
```

Table 24: The message PHYSICAL INFORMATION

8. Mobility Management messages

Now we will deal with messages responsible for Mobility Management in Mobile Originated Calls (MOC) and in Location Updating Procedures. Let's first have a look at the EXCEL sheet of a MOC.



D7 = MM CM SERVICE REQUEST

	A	B	C	D	E
1	"Time	Message	Dir	Type of message	Data
2	"16/07/2002 09:54:28,559	LAYER 2-PCH	DOWN	RR PAGING REQUEST TYPE 1	15 06 21 00 01 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
3	"16/07/2002 09:54:29,871	LAYER 2-PCH	DOWN	RR PAGING REQUEST TYPE 1	25 06 21 00 05 F4 09 51 57 4F 2B 2B 2B 2B 2B 2B 2B 2B 2
4	"16/07/2002 09:54:29,871	LAYER 3	DOWN	RR PAGING REQUEST TYPE 1	06 21 00 05 F4 09 51 57 4F 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
5	"16/07/2002 09:54:31,301	LAYER 2-PCH	DOWN	RR PAGING REQUEST TYPE 1	25 06 21 00 05 F4 09 50 C2 20 2B 2B 2B 2B 2B 2B 2B 2B 2
6	"16/07/2002 09:54:31,301	LAYER 3	DOWN	RR PAGING REQUEST TYPE 1	06 21 00 05 F4 09 50 C2 20 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
7	"16/07/2002 09:54:32,461	LAYER 3	UP	MM CM SERVICE REQUEST	05 24 11 03 33 19 81 05 F4 09 51 47 C4
8	"16/07/2002 09:54:32,461	LAYER 2-RACH	UP	RR CHANNEL REQUEST	EF
9	"16/07/2002 09:54:33,109	LAYER 2-CCCH	DOWN	RR IMMEDIATE ASSIGNMENT	2D 06 3F 03 79 40 62 EF 55 2D 01 00 2B 2B 2B 2B 2B 2B 2
10	"16/07/2002 09:54:33,172	LAYER 3	DOWN	RR IMMEDIATE ASSIGNMENT	06 3F 03 79 40 62 EF 55 2D 01 00 2B 2B 2B 2B 2B 2B 2B 2
11	"16/07/2002 09:54:33,172	LAYER 2-SDCCH-SABM	UP	MM CM SERVICE REQUEST	01 3F 35 05 24 11 03 33 19 81 05 F4 09 51 47 C4 2B 2B 2B 2B
12	"16/07/2002 09:54:33,219	LAYER 2-SACCH-UI	DOWN	RR SYSTEM INFORMATION TYPE 6	03 01 03 03 2D 06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2
13	"16/07/2002 09:54:33,281	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B 00
14	"16/07/2002 09:54:33,391	LAYER 2-SDCCH-UA	DOWN	MM CM SERVICE REQUEST	01 73 35 05 24 11 03 33 19 81 05 F4 09 51 47 C4 2B 2B 2B 2B
15	"16/07/2002 09:54:33,391	LAYER 3	UP	RR CLASSMARK_CHANGE	06 16 03 33 19 81 20 02 60 14
16	"16/07/2002 09:54:33,441	LAYER 2-SDCCH-I	UP	RR CLASSMARK_CHANGE	01 00 29 06 16 03 33 19 81 20 02 60 14 2B 2B 2B 2B 2B 2B 2B
17	"16/07/2002 09:54:33,660	LAYER 2-SDCCH-I	DOWN	RR CIPHERING MODE COMMAND	03 20 0D 06 35 11 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
18	"16/07/2002 09:54:33,660	LAYER 2-SDCCH-I	UP	RR GPRS SUSPENSION REQUEST	01 22 35 06 34 C0 00 18 9C 62 F2 10 31 04 01 00 2B 2B 2B 2B
19	"16/07/2002 09:54:33,660	LAYER 3	DOWN	RR CIPHERING MODE COMMAND	06 35 11
20	"16/07/2002 09:54:33,660	LAYER 3	UP	RR CIPHERING MODE COMPLETE	06 32 17 09 33 23 81 81 32 07 31 09 F0
21	"16/07/2002 09:54:33,719	LAYER 3	UP	CC SETUP	03 05 04 04 60 02 00 81 1C 0F A1 0D 02 01 01 02 01 78 30 05
22	"16/07/2002 09:54:33,770	LAYER 3	UP	RR MEASUREMENT REPORT	06 15 20 20 5B 10 13 C7 05 D3 48 E0 E5 7C 00 00 00 00
23	"16/07/2002 09:54:33,828	LAYER 2-SACCH-UI	UP	RR MEASUREMENT REPORT	03 01 01 03 49 06 15 20 20 5B 10 13 C7 05 D3 48 E0 E5 7C 00
24	"16/07/2002 09:54:33,879	LAYER 2-SDCCH-RR	DOWN	NO INFORMATION FIELD	01 41 01
25	"16/07/2002 09:54:33,879	LAYER 2-SDCCH-I	UP	RR CIPHERING MODE COMPLETE	01 24 35 06 32 17 09 33 23 81 81 32 07 31 09 F0 2B 2B 2B 2B
26	"16/07/2002 09:54:34,160	LAYER 2-SDCCH-RR	DOWN	NO INFORMATION FIELD	01 61 01
27	"16/07/2002 09:54:34,160	LAYER 2-SDCCH-I	UP	CC SETUP-L3 SEG BEGIN	01 26 53 03 45 04 04 60 02 00 81 1C 0F A1 0D 02 01 01 02 01
28	"16/07/2002 09:54:34,160	LAYER 2-SACCH-UI	DOWN	RR SYSTEM INFORMATION TYPE 6	05 01 03 03 2D 06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2
29	"16/07/2002 09:54:34,211	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B 00
30	"16/07/2002 09:54:34,270	LAYER 3	UP	RR MEASUREMENT REPORT	06 15 21 21 01 10 13 C7 85 D3 C8 E1 25 7C 00 00 00 00
31	"16/07/2002 09:54:34,270	LAYER 2-SACCH-UI	UP	RR MEASUREMENT REPORT	05 01 01 03 49 06 15 21 21 01 10 13 C7 85 D3 C8 E1 25 7C 00
32	"16/07/2002 09:54:34,379	LAYER 2-SDCCH-RR	DOWN	NO INFORMATION FIELD	01 81 01
33	"16/07/2002 09:54:34,379	LAYER 2-SDCCH-I	UP	CC SETUP-L3 SEG END	01 28 45 80 01 00 81 00 5E 07 81 30 73 25 01 18 55 7F 01 00 2
34	"16/07/2002 09:54:34,602	LAYER 2-SDCCH-RR	DOWN	NO INFORMATION FIELD	01 A1 01

Tabelle1 / Tabelle2 / Tabelle3

Bereit

Picture 37: Messages in a MOC reported by OTDrivePC

In picture 37 we can see many of the messages already dealt with in paragraph 6. One of the messages is new: the Connection Management SERVICE REQUEST.

8.1 The message CM SERVICE REQUEST

This is the new Information Element in the messages shown in table 26. Its length is half an octet and its type is Mandatory. Its name is CM Service Request. The types of message which can be invoked with CM SERVICE REQUEST are shown in table 25

0 0 0 1	Mobile originating call establishment or packet mode connection establishment
0 0 1 0	Emergency call establishment
0 1 0 0	Short message service
1 0 0 0	Supplementary service activation
1 0 0 1	Voice group call establishment
1 0 1 0	Voice broadcast call establishment
1 0 1 1	Location Services

Table 25: The IE CM Service Type

The Information Elements Ciphering Key Sequence Number, Mobile Station Classmark 2 and Mobile Identity are known from the messages discussed above.

_____[3]___[09:54:32,461]___[UP]_____

```
05 24 11 03 33 19 81 05 f4 09 51 47 c4

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
24  00------  SendSequenceNumber  : 0

    --100100  MESSAGE TYPE        : CM SERVICE REQUEST

11  0-------  spare               : 0
    -001----  value for the ciphering key sequence number = 1
    ----0001  Requ.service type   : Mobile originating call establishment, or packet mode
                                    connection establishment

: Mobile Station Classmark 2
03  00000011  length              : 3

33  0-------  1 spare             : 0
    -01-----  Revision Level      : Used by phase 2 mobile stations
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  Encryp.Algor. A5_1  : available
    -----011  RF power capability : Class 4, handheld

19  0-------  1 spare bit         : 0
    -0------  pseudo-synch.capab. : not present
    --01----  SS Screening Indic. : phase 2 error handling
    ----1---  Mobile station supports mobile terminated point to point SMS
    -----0--  no VoiceBroadcastService (VBS) capability or no notifications wanted
    ------0-  no VoiceGroupCallService (VGCS) capability or no notifications wanted
    -------1  The MS does support the E-GSM or R-GSM

81  1-------  The MS does support any options that are indicated in CM3
    -0------  1 spare bit         : 0
    --0-----  LocationServiceValueAdded Capability  not supported
    ---0----  1 spare bit         : 0
    ----0---  SoLSA Capability    : not supported
    -----0--  Network initiated MO CM connection request not supported.
    ------0-  encryp.algorith.A5/3: not available
    -------1  encryp.algorith.A5/2: available

: Mobile identity

05  00000101  length              : 5

f4  ----0---  No. of ID digits     : even
    -----100  Type of identity     : TMSI/P-TMSI
    1111----  Identity Digit 1     : 95
09  00001001  Identity Digit 2,3   : take hex value
51  01010001  Identity Digit 4,5   : take hex value
47  01000111  Identity Digit 6,7   : take hex value
c4  11000100  Identity Digit 8,9   : take hex value
```

Table 26: The message CM SERVICE REQUEST

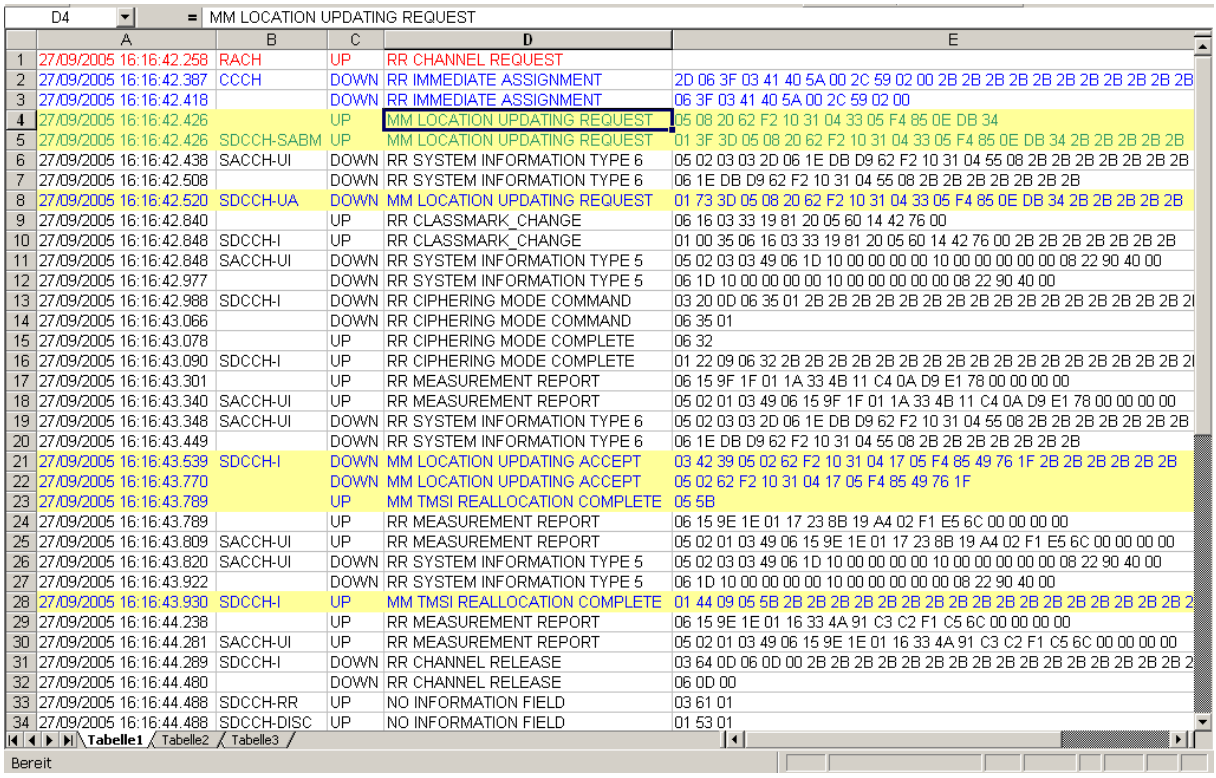
The message CM Service Request appears three times in picture 37, firstly as a layer 3 message when the user who is setting up the call has pressed the enter key.
Following the CHANNEL REQUEST (shown in table 27) and the answer IMMEDIATE ASSIGNMENT, the Mobile sends the CM SERVICE REQUEST again on layer 2 together with SABM to order a protected channel. The network ends this message by sending CM SERVICE REQUEST back on layer 2 with an Unnumbered Acknowledgement.

```
_____[ 4 ]___[ 09:54:32,461 ]___[ UP ]____[ RACH ]_____________________________

ef

L2-RACH Channel Request

ef  111-----  Originating call and TCH/F is needed,
```

Table 27: The message CHANNEL REQUEST ordering a TCH

8.2 The MM messages during Location Update

Picture 38 shows all the messages which appear during Location Update. In order to show all the important frames on one page, some lines have been erased. The full range of messages being transmitted over the air interface can be seen on the exercise stored on the CD.



D4 = MM LOCATION UPDATING REQUEST

	A	B	C	D	E
1	27/09/2005 16:16:42.258	RACH	UP	RR CHANNEL REQUEST	
2	27/09/2005 16:16:42.387	CCCH	DOWN	RR IMMEDIATE ASSIGNMENT	2D 06 3F 03 41 40 5A 00 2C 59 02 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
3	27/09/2005 16:16:42.418		DOWN	RR IMMEDIATE ASSIGNMENT	06 3F 03 41 40 5A 00 2C 59 02 00
4	27/09/2005 16:16:42.426		UP	MM LOCATION UPDATING REQUEST	05 08 20 62 F2 10 31 04 33 05 F4 85 0E DB 34
5	27/09/2005 16:16:42.426	SDCCH-SABM	UP	MM LOCATION UPDATING REQUEST	01 3F 3D 05 08 20 62 F2 10 31 04 33 05 F4 85 0E DB 34 2B 2B 2B 2B 2B
6	27/09/2005 16:16:42.438	SACCH-UI	DOWN	RR SYSTEM INFORMATION TYPE 6	05 02 03 03 2D 06 1E DB D9 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B
7	27/09/2005 16:16:42.508		DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E DB D9 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B
8	27/09/2005 16:16:42.520	SDCCH-UA	DOWN	MM LOCATION UPDATING REQUEST	01 73 3D 05 08 20 62 F2 10 31 04 33 05 F4 85 0E DB 34 2B 2B 2B 2B 2B
9	27/09/2005 16:16:42.840		UP	RR CLASSMARK_CHANGE	06 16 03 33 19 81 20 05 60 14 42 76 00
10	27/09/2005 16:16:42.848	SDCCH-I	UP	RR CLASSMARK_CHANGE	01 00 35 06 16 03 33 19 81 20 05 60 14 42 76 00 2B 2B 2B 2B 2B 2B 2B
11	27/09/2005 16:16:42.848	SACCH-UI	DOWN	RR SYSTEM INFORMATION TYPE 5	05 02 03 03 49 06 1D 10 00 00 00 00 10 00 00 00 00 00 08 22 90 40 00
12	27/09/2005 16:16:42.977		DOWN	RR SYSTEM INFORMATION TYPE 5	06 1D 10 00 00 00 00 10 00 00 00 00 00 08 22 90 40 00
13	27/09/2005 16:16:42.988	SDCCH-I	DOWN	RR CIPHERING MODE COMMAND	03 20 0D 06 35 01 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2I
14	27/09/2005 16:16:43.066		DOWN	RR CIPHERING MODE COMMAND	06 35 01
15	27/09/2005 16:16:43.078		UP	RR CIPHERING MODE COMPLETE	06 32
16	27/09/2005 16:16:43.090	SDCCH-I	UP	RR CIPHERING MODE COMPLETE	01 22 09 06 32 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2I
17	27/09/2005 16:16:43.301		UP	RR MEASUREMENT REPORT	06 15 9F 1F 01 1A 33 4B 11 C4 0A D9 E1 78 00 00 00 00
18	27/09/2005 16:16:43.340	SACCH-UI	UP	RR MEASUREMENT REPORT	05 02 01 03 49 06 15 9F 1F 01 1A 33 4B 11 C4 0A D9 E1 78 00 00 00 00
19	27/09/2005 16:16:43.348	SACCH-UI	DOWN	RR SYSTEM INFORMATION TYPE 6	05 02 03 03 2D 06 1E DB D9 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B
20	27/09/2005 16:16:43.449		DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E DB D9 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 2B
21	27/09/2005 16:16:43.539	SDCCH-I	DOWN	MM LOCATION UPDATING ACCEPT	03 42 39 05 02 62 F2 10 31 04 17 05 F4 85 49 76 1F 2B 2B 2B 2B 2B 2B
22	27/09/2005 16:16:43.770		DOWN	MM LOCATION UPDATING ACCEPT	05 02 62 F2 10 31 04 17 05 F4 85 49 76 1F
23	27/09/2005 16:16:43.789		UP	MM TMSI REALLOCATION COMPLETE	05 5B
24	27/09/2005 16:16:43.789		UP	RR MEASUREMENT REPORT	06 15 9E 1E 01 17 23 8B 19 A4 02 F1 E5 6C 00 00 00 00
25	27/09/2005 16:16:43.809	SACCH-UI	UP	RR MEASUREMENT REPORT	05 02 01 03 49 06 15 9E 1E 01 17 23 8B 19 A4 02 F1 E5 6C 00 00 00 00
26	27/09/2005 16:16:43.820	SACCH-UI	DOWN	RR SYSTEM INFORMATION TYPE 5	05 02 03 03 49 06 1D 10 00 00 00 00 10 00 00 00 00 00 08 22 90 40 00
27	27/09/2005 16:16:43.922		DOWN	RR SYSTEM INFORMATION TYPE 5	06 1D 10 00 00 00 00 10 00 00 00 00 00 08 22 90 40 00
28	27/09/2005 16:16:43.930	SDCCH-I	UP	MM TMSI REALLOCATION COMPLETE	01 44 09 05 5B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
29	27/09/2005 16:16:44.238		UP	RR MEASUREMENT REPORT	06 15 9E 1E 01 16 33 4A 91 C3 C2 F1 C5 6C 00 00 00 00
30	27/09/2005 16:16:44.281	SACCH-UI	UP	RR MEASUREMENT REPORT	05 02 01 03 49 06 15 9E 1E 01 16 33 4A 91 C3 C2 F1 C5 6C 00 00 00 00
31	27/09/2005 16:16:44.289	SDCCH-I	DOWN	RR CHANNEL RELEASE	03 64 0D 06 0D 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2
32	27/09/2005 16:16:44.480		DOWN	RR CHANNEL RELEASE	06 0D 00
33	27/09/2005 16:16:44.488	SDCCH-RR	UP	NO INFORMATION FIELD	03 61 01
34	27/09/2005 16:16:44.488	SDCCH-DISC	UP	NO INFORMATION FIELD	01 53 01

Tabelle1 / Tabelle2 / Tabelle3

Bereit

Picture 38: Messages during Location Updating reported by OTDrivePC

The message CHANNEL REQUEST looks like the following table. ‘NECI’ is an abbreviation for *New Establishment Cause Indicator*. Setting it to one means a new connection is to be set up.

```
_____[ 12 ]___[ 14:08:59,660 ]___[ UP ]____[ RACH ]_____________________________

0b

L2-RACH Channel Request

0b  0000----  Location updating and the network sets NECI bit to 1
```

Table 28: The message CHANNEL REQUEST ordering a new Channel

8.2.1 The Message MM LOCATION UPDATING REQUEST

The message LOCATION UPDATING REQUEST appears three times in the illustrated Location Updating procedure. The message issued on layer 3 is shown in table 29. Line 5 in picture 38 shows the message sent to the network with SABM to order a protected connection. In line 8 the network accepts the order by sending back the LOCATION UPDATING REQUEST together with an Unnumbered Acknowledgement UA.

```
_____[ 11 ]___[ 14:08:59,660 ]___[ UP ]_____________________________________________

05 08 22 62 f2 10 31 04 33 05 f4 09 d8 4e 1c

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
08  00------  SendSequenceNumber  : 0

    --001000  MESSAGE TYPE        : LOCATION UPDATING REQUEST

22  ----0---  No follow-on request pending
    -----0--  Spare
    ------10  IMSI attach
    0-------  spare
    -010----  key sequence        : 2

62  ----0010  Mobile CC digit 1   : 2
    0110----  Mobile CC digit 2   : 6
f2  ----0010  Mobile CC digit 3   : 2

    1111----  Mobile NC digit 3   : 15
10  ----0000  Mobile NC digit 1   : 0
    0001----  Mobile NC digit 2   : 1

31  00110001  Loc. area code (LAI) = ID of MSC (hex)
04  00000100  Loc. area code (LAI) = ID of BSC (hex)

33  0-------  Spare
    -01-----  Revision Level      : Used by phase2 mobile stations
    ---1----  "Controlled Early Classmark Sending" option is implemented in the MS
    ----0---  encryption algorithm A5/1 available
    -----011  RF power capability : class4

05  00000101  length of Mob.ident.: 5

f4  1111----  Identity Digit 1    : 15
    ----0---  No. of ID digits    : even
    -----100  Type of identity    : TMSI/P-TMSI
09  00001001  Identity Digit 2,3  : take hex value
d8  11011000  Identity Digit 4,5  : take hex value
4e  01001110  Identity Digit 6,7  : take hex value
1c  00011100  Identity Digit 8,9  : take hex value
```

Table 29: The message LOCATION UPDATING REQUEST

The Message LOCATION UPDATING REQUEST contains the following Information Elements:

a) Location updating type. The IE consists of three different types

```
0 0 Normal location updating
0 1 Periodic updating
1 0 IMSI attach
1 1 Reserved
```

The type “IMSI attach” means that the mobile is registered as present in the VLR. The Mobile can therefore be called by a PAGING REQUEST. If the Mobile is switched off it is registered as absent in the VLR. This means the Mobile will not be searched for in the network and a caller will receive the message “the Mobile is not available”.

b) Ciphering key sequence number. The IE is already known.

c) Location area identification. The IE is already known.
d) Mobile station Classmark 1. That is a short form of Mobile station Classmark 2.
e) Mobile identity. The IE is already known.

In paragraph *6.11.1 About the encryption of the Transport Channel* we discussed the messages MM AUTHENTICATION REQUEST and MM AUTHENTICATION RESPONSE without emphasising that these messages belong to the Mobility Management.

These messages may also appear (although not in this case) during the Location Updating process. It is possible to force this process but the result will be the sending of a strange *Location area identification* (by forcing it with the OT 260).
In picture 38 Authentication does not appear.

8.2.2 The Message MM LOCATION UPDATING ACCEPT

After ciphering, the network sends a LOCATION UPDATING ACCEPT.

```
_____[ 29 ]___[ 11:22:05,094 ]___[ DOWN ]____[ SDCCH ]_____________________________

05 02 62 f2 10 31 04 17 05 f4 64 6f 04 94

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
02  00------  SendSequenceNumber  : 0

    --000010  MESSAGE TYPE        : LOCATION UPDATING ACCEPT

: Location area identification
62  ----0010  Mobile CC digit 1   : 2
    0110----  Mobile CC digit 2   : 6
f2  ----0010  Mobile CC digit 3   : 2

    1111----  Mobile NC digit 3   : 15
10  ----0000  Mobile NC digit 1   : 0
    0001----  Mobile NC digit 2   : 1

31  00110001  Loc. area code (LAI) = ID of MSC (hex)
04  00000100  Loc. area code (LAI) = ID of BSC (hex)


17  00010111  INFORMATIONSELEMET   : Mobile Identity 3

05  00000101  length of Mob.ident.3: 5
f4  1111----  Identity Digit 1     : 15
    ----0---  No. of ID digits     : even
    -----100  Type of identity     : TMSI/P-TMSI
64  0110----  Identity Digit 3     : 6
    ----0100  Identity Digit 2     : 4
6f  0110----  Identity Digit 5     : 6
    ----1111  Identity Digit 4     : 15
04  0000----  Identity Digit 7     : 0
    ----0100  Identity Digit 6     : 4
94  1001----  Identity Digit 9     : 9
    ----0100   Identity Digit 8     : 4
```

Table 30: The message LOCATION UPDATING ACCEPT

The network sends a (possibly new) Location area identification and in all cases a new TMSI.

8.2.3 The Message MM TMSI REALLOCATION COMPLETE

After changing its TMSI to the new value the mobile informs the network that the reallocation has been completed.

```
____[ 30 ]___[ 11:22:05,094 ]___[ UP ]_____________________________________________

05 1b

05  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0101  Protocol Discrim.   : mobility management messages non GPRS
1b  00------  SendSequenceNumber  : 0
    --011011  MESSAGE TYPE        : TMSI REALLOCATION COMPLETE
```

Table 31: The message TMSI REALLOCATION COMPLETE

9. Call Control Messages

Table 32 shows the correspondence of CC-messages in ISDN and Mobile Communication.

Message type	DSS-1 Code	GSM Code, SSN	UMTS Code	Meaning
SETUP	05	05,45	05,45	Initiation of call establishment.
CALL CONFIRMED	-	08,48	08,48	MS confirms incoming call
ALERTING	01	01,41	01,41	MS is ready to receive the call
CALL PROCEEDING	02	02,42	02,42	No more call establishment information accepted
CONNECT	07	07,47	07.47	Indication of call acceptance by the called user
CONNECT ACKNOW.	0F	0F,4F	0F,4F	B-channel is switched through
EMERGENCY SETUP	-	0E,4E	0E,4E	Emergency call wanted
PROGRESS	03	03,43	03,43	Progress of call during interworking
SETUP ACKNOWLEDE	0D	-	-	Call establishment has been initiated
MODIFY	-	17,57	17,57	Demand for change of BC
MODIFY COMPLETE	-	1f,5f	1f,5f	Change of BC done
MODIFY REJECT	-	13,53	13,53	Change of BC failure
USER INFORMATION	20	10,57	10,50	End-to-End transmission of information
HOLD	24	18,58	18,58	Demand for hold the connection
HOLD ACKNOWLEGE	28	19,59	19,59	Confirmation of Hold message
HOLD REJECT	30	1a,5a	1a,5a	Rejection of Hold message
RETRIEVE	31	1c,5c	1c,5c	Demand for retrieve from Hold
RETRIEVE ACKNOWL.	32	1d,5d	1d,5d	Confirmation of Retrieve
RETRIEVE REJECT	33	1e,5e	1e,5e	Rejection of Retrieve message
DISCONNECT	45	25,65	25,65	Demand for call clearing by MS, Indic. of call clearing by Netw.
RELEASE	4d	2d,6d	2d,6d	Reaction to Disconnect by the TE, Release of the transport chain.
RELEASE COMPLETE.	5a	2a,6a	2a,6a	Receipt of Release message, Release of the B(m)-channel
RESTART	46	-	-	ISDN only
RESTART ACK.	4e	-	-	ISDN only
CONGESTION CTRL	-	39,79	39,79	Establ. or term. of flow contrl on the transm. of USR INFO. msg
NOTIFY	6e	3e,7e	3e,7e	Indicates information pertaining to a call,
STATUS	7d	3d,7d	3d,7d	Answer to STATUS ENQUIRY
STATUS ENQUIRY	75	34,74	34,74	Solicits a STATUS message from the peer layer
START DTMF	-	35,75	35,75	Start Dual Tone Multi Frequency
STOP DTMF	-	31,71	31,71	Stop transforming bits in DTMF
STOP DTMF ACK.	-	32,72	32,72	Accept STOP DTMF
START DTMF ACK.	-	36,76	36,76	Accept START DTMF
START DTMF REJ.	-	37,77	37,77	Reject start of DTMF
FACILITY	62	3a,7a	3a,7a	Demand of a connection dependent service attribute

Table 32: CC-Messages in DSS-1, GSM and UMTS

The underlined messages in table 32 will be discussed in this paragraph. If the colour of the message name is red, the message is used in Mobile Communication only, otherwise the message is also used in ISDN.

9.1 The message SETUP

Let's first have a look at a SETUP message in a Mobile Terminated Call. In table 33 you will find all the Information Elements known from the ISDN. The contents of the IEs differ only slightly from those in the ISDN. The possibility of two Bearer Capability IEs occurring and consequently two LLC and HLC is new.

```
_____[ 17 ]___[ 12:02:43,500 ]___[ DOWN ]____[ SDCCH ]_____________________________

13 05 04 01 a0 5c 08 11 81 94 33 57 92 28 f1 7d 02 91 81

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
05  00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
01  00000001  length              : 1
a0  1-------  Extension           : 1
    -01-----  Radio Channel Req.  : full rate support only MS
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech

5c  01011100  INFORMATION ELEMENT : Calling party BCD number
08  00001000  length              : 8
11  0-------  Extension           : 0
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
81  1-------  Extension           : 1
    -00-----  Present.indic.      : Presentation allowed
    ---000--  spare               : 0
    ------01  Present.indic.      : User-provided, verified and passed
94..f1        number              : 49337529821

7d  01111101  INFORMATION ELEMENT : High Layer Compatibility
02  00000010  length              : 2
91  1-------  Extension           : 1
    -00-----  Coding standard     : CCITT standardized coding
    ---100--  Interpret.i.ch.     : First high layer char.id. to be used
    ------01  Present.method      : High Layer protocol profile
81  10000001  High layer char.    : Telephony
```

Table 33: A SETUP message in a MTC

For those readers who do not have active knowledge of ISDN protocols I will repeat some remarks about the Information Elements which appear in our examples.

9.1.1 The Information Element Bearer Capability (BC)

In ISDN this IE is mandatory, in GSM it is not. For an example in which this property appears, please refer to table 36 later in this chapter.
The Bearer Capability tells the network which transmission properties it must guarantee. While the BC in a MTC leaves the problem of adjusting the radio channel to the network, the BC in a MOC delivers a more precise request for channel performance (see table 33).
The IE Bearer Capability describes, alongside the IE's *High Layer Capability* and *Low Layer Capability*, the service which is to be transmitted with the ordered connection.
The writers of GSM Recommendation 04.08 give the possibility of changing the service during an active call. This change may be initiated by the message MODIFY.
In this case the SETUP message must contain two of the IE's BC. The IE's HLC and LLC must also exist twice.

In former times in the (German) ISDN protocol 1TR6 it was possible to start a call as a voice call and then switch to FAX transmission.
I am afraid I cannot think of any example which shows this feature in GSM.

```
_____[ 14 ]___[ 09:54:33,719 ]___[ UP ]_____________________________________________

03 05 04 04 60 02 00 81 1c 0f a1 0d 02 01 01 02 01 78 30 05 80 01 00 81 00 5e 07 81 30 73 25
01 18 55 7f 01 00

03  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
05  00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
04  00000100  length              : 4
60  0-------  Extension           : 0

    -11-----  Radio Channel Req.  : dual rate support MS/full rate preferred
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
02  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0010  speech Vers. indic. : GSM full rate speech version 2
00  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0000  speech Vers. indic. : GSM full rate speech version 1
81  1-------  Extension           : 1
    -0------  Coding              : octet used for extension of inf. transf. capab.
    --00----  Spare               : 00
    ----0001  speech Vers. indic. : GSM half rate speech version 1

1c  00011100  INFORMATION ELEMENT : Facility
0f  00001111  Lgth of IE FACILITY : 15
a1  10100001  Component           : Invoke
0d  00001101  length              : 13

02  00000010  Type=INTEGER        : Invoke Identifier
01  00000001  length              : 1
01  00000001  Inv.ID. Value       : 1

02  00000010  Type=INTEGER        : Operation Value
01  00000001  length              : 1
78  01111000  Operation           : forwardCUG-Info
30  00110000  SEQUENCE            : forwardCUG-InfoArG
05  00000101  length              : 5
80  10000000  Implicit Integer    : cug-Index
01  00000001  length              : 1
00  00000000  value               : 0
81  10000001  Implicit Null       : suppressPrefCUG
00  00000000  Null

5e  01011110  INFORMATION ELEMENT : CalledPartyBCDNumber
07  00000111  length              : 7
81  1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/teleph. numb. plan (Rec. E.164/E.163) _
30..55        number              : 033752108155
```

Table 34: A SETUP message in a MOC

9.1.2 The Information Element High Layer Compatibility

From paragraph 9.1.1 we know that the BC tells the network which service is to be transmitted. The High Layer Capability is responsible for telling the terminal which service is to be received. In GSM this terminal is usually a Mobile. If the Terminal which receives the HLC is not able to deal with the service it will not accept the call.

9.1.3 The Information Element Low Layer Compatibility

The IE Low Layer Capability tells the Terminal on a communication endpoint which properties it must have on the low layer. The properties are given by the Recommendations issued by the ETSI or the ITU. It has been agreed that in present-day telephony IE LLC must be used.

9.1.4 The Information Elements Calling Party BCD Number/Called Party BCD Number

This IE appears in the SETUP message of a MTC if the caller has elected to display their telephone number at the receiving end. If the permission is not given, the Presentation indicator (see table 32) is set to "0 1 Presentation restricted" and the network suppresses the number, giving it only to the police or other emergency services.

The IE Called Party BCD Number appears in the SETUP message of a MOC.
In a MOC the Calling BCD Number is obsolete because the network knows the number. This is in contrast to the ISDN where up to ten different numbers may be issued from one terminal endpoint.
The restriction of not displaying the number can be given if the IE *CLIR invocation* is inserted in the SETUP message.

9.1.5 Other Information Elements

We shall deal in paragraph "11 SUPPLEMENTARY SERVICES" with the Information Element FACILITY shown in table 32.
As well as the IEs discribed in 9.1.1 to 9.1.4 there are also those shown in table 35. The underlined IEs are used only in a MTC

- BC repeat indicator,
- Facility,
- Progress indicator,
- Signal,
- Calling Party Sub-address,
- Called party BCD number,
- Called party sub-address,
- Redirecting party BCD number,
- Redirecting party sub-address,
- LLC repeat indicator,
- Low Layer Compatibility,
- HLC repeat indicator,
- Priority,
- User-user.
- CLIR suppression
- CLIR invocation

Table 35: Further possible IE in a SETUP message

9.1.6 The Information Element Bearer Capability is not mandatory

A peculiarity exists in GSM which is not present in ISDN: the Information Element Bearer Capability is not mandatory. The trace seen in table 36 is taken from a Mobile equipped with a Prepaid SIM Card. The call was sent by an ISDN-Terminal with the information transfer capability “unrestricted digital information”.

The operator does not allow the transference of data with a prepaid card, therefore the sender will have received the message “bearer capability not authorized”.

```
_____[ 36 ]___[ 11:37:39,039 ]___[ DOWN ]____[ SDCCH ]_____________________________

13 05 5c 08 11 83 94 33 57 92 28 f1

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
05  00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

5c  01011100  INFORMATION ELEMENT : Calling party BCD number
08  00001000  length              : 8
11  0-------  Extension           : 0
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
83  1-------  Extension           : 1
    -00-----  Present.indic.      : Presentation allowed
    ---000--  spare               : 0
    ------11  Present.indic.      : Network provided
94..f1        number              : 49337529821
```

Table 36: A SETUP without the IE Bearer Capability

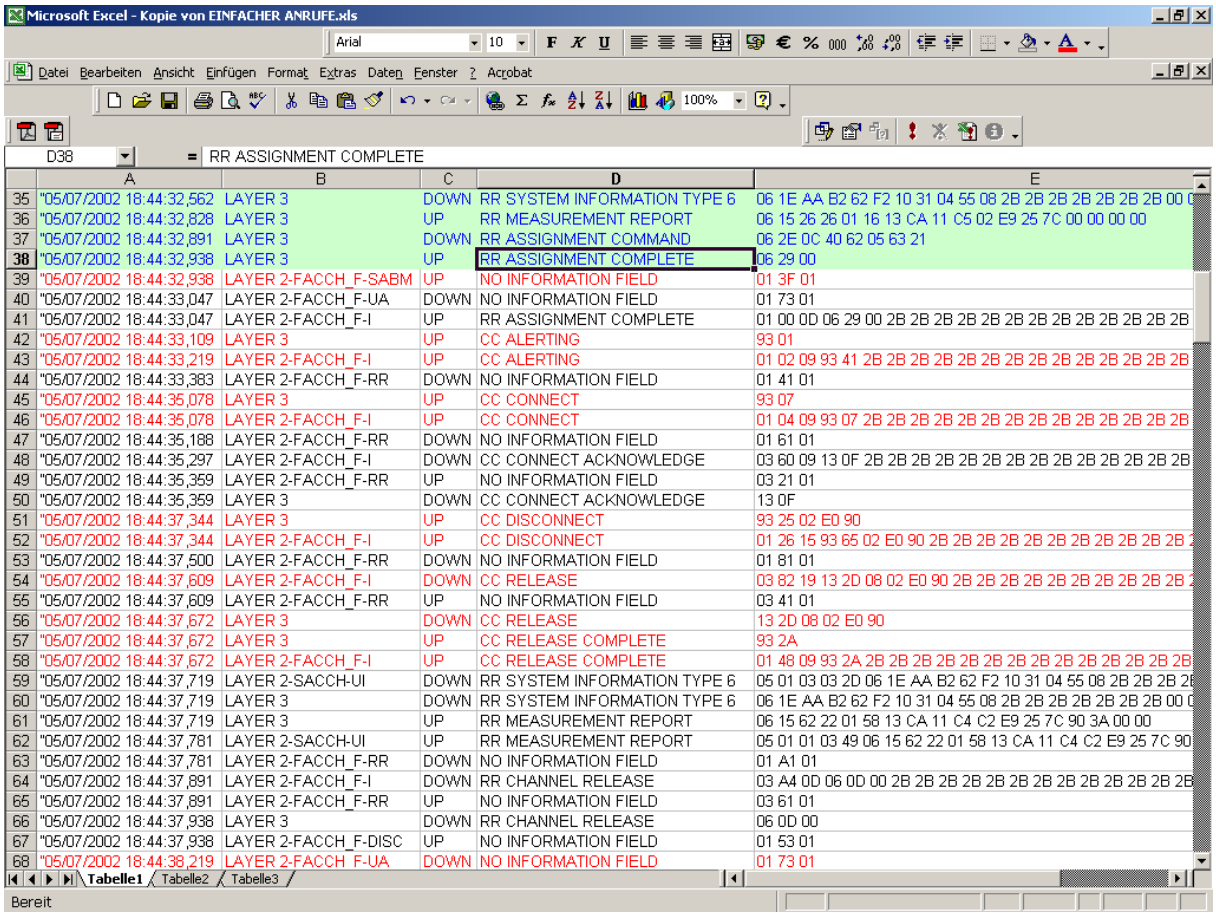
9.2 The message CALL CONFIRMED

The purpose of the message CALL CONFIRMED (shown in table 37) is to confirm a SETUP Message to the network. It reports the BC of the Mobile to the network.

```
_____[ 37 ]___[ 11:37:39,039 ]___[ UP ]_____________________________________________
93 08 04 04 60 02 00 81

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
08  00------  SendSequenceNumber  : 0

    --001000  MESSAGE TYPE        : CALL CONFIRMED

04  00000100  INFORMATION ELEMENT : Bearer capability
04  00000100  length              : 4
60  0-------  Extension           : 0
    -11-----  Radio Channel Req.  : dual rate support MS/full rate preferred
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----000  Info Transfer Cap.  : speech
02  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. Transfer capability.
    --00----  Spare               : 00
    ----0010  speech Vers. indic. : GSM full rate speech version 2
00  0-------  Extension           : 0
    -0------  Coding              : octet used for extension of inf. Transfer capability.
    --00----  Spare               : 00
    ----0000  speech Vers. indic. : GSM full rate speech version 1
81  1-------  Extension           : 1
    -0------  Coding              : octet used for extension of inf. Transfer capability
    --00----  Spare               : 00
    ----0001  speech Vers. indic. : GSM half rate speech version 1
```

Table 37: The message CALL CONFIRMED

.



	A	B	C	D	E
35	"05/07/2002 18:44:32,562	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 00
36	"05/07/2002 18:44:32,828	LAYER 3	UP	RR MEASUREMENT REPORT	06 15 26 26 01 16 13 CA 11 C5 02 E9 25 7C 00 00 00 00
37	"05/07/2002 18:44:32,891	LAYER 3	DOWN	RR ASSIGNMENT COMMAND	06 2E 0C 40 62 05 63 21
38	"05/07/2002 18:44:32,938	LAYER 3	UP	RR ASSIGNMENT COMPLETE	06 29 00
39	"05/07/2002 18:44:32,938	LAYER 2-FACCH_F-SABM	UP	NO INFORMATION FIELD	01 3F 01
40	"05/07/2002 18:44:33,047	LAYER 2-FACCH_F-UA	DOWN	NO INFORMATION FIELD	01 73 01
41	"05/07/2002 18:44:33,047	LAYER 2-FACCH_F-I	UP	RR ASSIGNMENT COMPLETE	01 00 0D 06 29 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
42	"05/07/2002 18:44:33,109	LAYER 3	UP	CC ALERTING	93 01
43	"05/07/2002 18:44:33,219	LAYER 2-FACCH_F-I	UP	CC ALERTING	01 02 09 93 41 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
44	"05/07/2002 18:44:33,383	LAYER 2-FACCH_F-RR	DOWN	NO INFORMATION FIELD	01 41 01
45	"05/07/2002 18:44:35,078	LAYER 3	UP	CC CONNECT	93 07
46	"05/07/2002 18:44:35,078	LAYER 2-FACCH_F-I	UP	CC CONNECT	01 04 09 93 07 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
47	"05/07/2002 18:44:35,188	LAYER 2-FACCH_F-RR	DOWN	NO INFORMATION FIELD	01 61 01
48	"05/07/2002 18:44:35,297	LAYER 2-FACCH_F-I	DOWN	CC CONNECT ACKNOWLEDGE	03 60 09 13 0F 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
49	"05/07/2002 18:44:35,359	LAYER 2-FACCH_F-RR	UP	NO INFORMATION FIELD	03 21 01
50	"05/07/2002 18:44:35,359	LAYER 3	DOWN	CC CONNECT ACKNOWLEDGE	13 0F
51	"05/07/2002 18:44:37,344	LAYER 3	UP	CC DISCONNECT	93 25 02 E0 90
52	"05/07/2002 18:44:37,344	LAYER 2-FACCH_F-I	UP	CC DISCONNECT	01 26 15 93 65 02 E0 90 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
53	"05/07/2002 18:44:37,500	LAYER 2-FACCH_F-RR	DOWN	NO INFORMATION FIELD	01 81 01
54	"05/07/2002 18:44:37,609	LAYER 2-FACCH_F-I	DOWN	CC RELEASE	03 82 19 13 2D 08 02 E0 90 2B 2B 2B 2B 2B 2B 2B 2B 2B
55	"05/07/2002 18:44:37,609	LAYER 2-FACCH_F-RR	UP	NO INFORMATION FIELD	03 41 01
56	"05/07/2002 18:44:37,672	LAYER 3	DOWN	CC RELEASE	13 2D 08 02 E0 90
57	"05/07/2002 18:44:37,672	LAYER 3	UP	CC RELEASE COMPLETE	93 2A
58	"05/07/2002 18:44:37,672	LAYER 2-FACCH_F-I	UP	CC RELEASE COMPLETE	01 48 09 93 2A 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
59	"05/07/2002 18:44:37,719	LAYER 2-SACCH-UI	DOWN	RR SYSTEM INFORMATION TYPE 6	05 01 03 03 2D 06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B
60	"05/07/2002 18:44:37,719	LAYER 3	DOWN	RR SYSTEM INFORMATION TYPE 6	06 1E AA B2 62 F2 10 31 04 55 08 2B 2B 2B 2B 2B 2B 00
61	"05/07/2002 18:44:37,719	LAYER 3	UP	RR MEASUREMENT REPORT	06 15 62 22 01 58 13 CA 11 C4 C2 E9 25 7C 90 3A 00 00
62	"05/07/2002 18:44:37,781	LAYER 2-SACCH-UI	UP	RR MEASUREMENT REPORT	05 01 01 03 49 06 15 62 22 01 58 13 CA 11 C4 C2 E9 25 7C 90
63	"05/07/2002 18:44:37,781	LAYER 2-FACCH_F-RR	DOWN	NO INFORMATION FIELD	01 A1 01
64	"05/07/2002 18:44:37,891	LAYER 2-FACCH_F-I	DOWN	RR CHANNEL RELEASE	03 A4 0D 06 0D 00 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B 2B
65	"05/07/2002 18:44:37,891	LAYER 2-FACCH_F-RR	UP	NO INFORMATION FIELD	03 61 01
66	"05/07/2002 18:44:37,938	LAYER 3	DOWN	RR CHANNEL RELEASE	06 0D 00
67	"05/07/2002 18:44:37,938	LAYER 2-FACCH_F-DISC	UP	NO INFORMATION FIELD	01 53 01
68	"05/07/2002 18:44:38,219	LAYER 2-FACCH_F-UA	DOWN	NO INFORMATION FIELD	01 73 01

Picture 39: CC-Messages in a MTC registered with OTDrivePC

9.3 The message ALERTING

The purpose of the message ALERTING is to inform the user issuing the SETUP of the possibility of accepting the call. The Information Elements in the ALERTING message are Facility, Progress Indicator and User-user.
We will deal with the IE Facility in paragraph 11. The IE User-user is not yet used in GSM .

```
_____[ 25 ]___[ 12:02:44,652 ]___[ UP ]____[ FACCH_F ]_____________________________

93 01

93  1-------  direction to         : originating site
    -001----  TransactionID        : 1
    ----0011  Protocol Discrim.    : Call control and call related SS messages
01  00------  SendSequenceNumber   : 0

    --000001  MESSAGE TYPE         : ALERTING
```

Table 38: The message ALERTING in a MTC

The IE Progress Indicator is sent by the network. In table 39 during a MTC the network reports that the call was issued beyond the interworking point in the ISDN.

```
_____[ 31 ]___[ 09:54:36,352 ]___[ DOWN ]____[ FACCH_F ]_____________________________

83 01 1e 02 ea 81

83  1-------  direction to        : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
01  00------  SendSequenceNumber  : 0

    --000001  MESSAGE TYPE        : ALERTING

1e  00011110  INFORMATION ELEMENT : Progress indicator
02  00000010  L. OF IE PROG.IND.  : 2
ea  1-------  Extension           : 1
    -11-----  Coding standard     : Standard Definition for the GSM-PLMNS as described.
    ---0----  Spare               : 0
    ----1010  Location            : Network beyond interworking point
81  1-------  Extension           : 1
    -0000001  Progress descr.     : Call is not end-to-end PLMN/ISDN,
```

Table 39: The message ALERTING in a MOC

There is another feature seen in tables 38, 39 and picture 39. While the messages SETUP and CALL CONFIRMED are exchanged on the SDCCH, the message ALERTING is not.
The message ASSIGNMENT COMMAND assigns a transport channel. Therefore from line 39 to 68 in picture 39 all messages are sent and received on the FACCH.

9.4 The message CONNECT

This message is sent either by the network to the calling mobile station, or is sent by the called mobile station to the network, in order to indicate the call has been accepted by the called user.

```
_____[ 43 ]___[ 12:02:49,309 ]___[ UP ]____[ SACCH ]_____________________________

93 07

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
07  00------  SendSequenceNumber  : 0

    --000111  MESSAGE TYPE        : CONNECT
```

Table 40: The message CONNECT

The message CONNECT can consist of the following Information Elements:
- from the mobile to network: Facility, Connected Subaddress, User-user; SS-Version (only if Facility is used),
- from the network to mobile: Facility, Connected number, Connected Subaddress, User-user.
A Connected Subaddress IE can contain a minimum of 2 octets and a maximum length of 23 octets (I don't know of any mobile which allows the insertion of Sub-addresses).

9.5 The message CONNECT ACKNOWLEDGE

This message is either sent by the called mobile station to the network to acknowledge the offered connection, or is sent by the network to the calling mobile to indicate the B-channel is switched on.

```
_____[ 46 ]___[ 12:02:49,629 ]___[ DOWN ]____[ FACCH_F ]_____________________________

13 0f

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
0f  00------  SendSequenceNumber  : 0

    --001111  MESSAGE TYPE        :CONNECT ACKNOWLEDGE
```

Table 41: The message CONNECT ACKNOWLEDGE

There are no Information Elements in this message.

9.6 The message DISCONNECT

This message is either sent by the mobile station to request that the network clears an end-to-end connection, or by the network to indicate that the end-to-end connection has been cleared.

```
_____[ 63 ]___[ 12:02:53,523 ]___[ UP ]____[ SACCH ]_____________________________

93 25 02 e0 90

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
25  00------  SendSequenceNumber  : 0

    --100101  MESSAGE TYPE        : DISCONNECT

02  00000010  LENGTH OF IE CAUSE  : 2
e0  1-------  Extension Bit       : 1
    -11-----  Coding stand.       : Standard defined for the GSM-PLMNS
    ---0----  spare               : 0
    ----0000  location            : user
90  -0010000  cause               : Normal call clearing
```

Table 42: The message DISCONNECT

Possible Information Elements are
- from the mobile to network: Facility, User-user, SS-Version (only if Facility is used),
- from the network to mobile: Cause, Facility, Progress indicator, User-user, Allowed actions $(CCBS)$

The IE “Allowed actions $(CCBS)$“ can be used if the called user is busy and the network is able to offer the Supplementary Service “Completion of Calls to Busy Subscribers”.

The IE Causes are mandatory and of type LV. This message is well suited to trouble-shooting because the location and the cause are given.

0------- Extension Bit : 0
1------- Extension Bit : 1
-00----- Coding stand. : Coding as specified in CCITT Rec. Q.931
-01----- Coding stand. : Reserved for other international standards
-10----- Coding stand. : National standard
-11----- Coding stand. : Standard defined for the GSM-PLMNS
---0---- spare : 0
----0000 location : user
----0001 location : private network serving the local user
----0010 location : public network serving the local user
----0011 location : transit network
----0100 location : public network serving the remote user
----0101 location : private network serving the remote user
----0111 location : international network
----1010 location : network beyond interworking point
-0000001 cause : Unassigned (unallocated) number
-0000011 cause : No route to destination
-0000110 cause : Channel unacceptable
-0001000 cause : Operator determined barring
-0010000 cause : Normal call clearing
-0010001 cause : User busy
-0010010 cause : No user responding
-0010011 cause : User alerting, no answer
-0010101 cause : Call rejected
-0010110 cause : Number changed, New destination
-0011001 cause : Pre-emption
-0011010 cause : Non selected user clearing
-0011011 cause : Destination out of order
-0011100 cause : Invalid number format (incomplete number)
-0011101 cause : Facility rejected
-0011110 cause : Response to STATUS ENQUIRY
-0011111 cause : Normal, unspecified
-0100010 cause : No circuit/channel available
-0100110 cause : Network out of order
-0101001 cause : Temporary failure
-0101010 cause : Switching equipment congestion
-0101011 cause : Access information discarded
-0101100 cause : requested circuit/channel
-0101111 cause : Resources unavailable, unspecified
-0110001 cause : Quality of service unavailable
-0110010 cause : Requested facility not subscribed
-0110111 cause : Incoming calls barred within the CUG
-0111001 cause : Bearer capability not authorized
-0111010 cause : Bearer capability. not presently available
-0111111 cause : Service or option not available .unspecified
-1000001 cause : Bearer service not implemented
-1000100 cause : ACM equal to or greater than ACMmax
-1000101 cause : Requested facility not implemented
-1000110 cause : Only restricted digital information bearer capability is available.
-1001111 cause : Service or option not implemented, unspecified
-1010001 cause : Invalid transaction identifier value
-1010111 cause : User not member of CUG
-1011000 cause : Incompatible destination Incompatible parameter
-1011011 cause : Invalid transit network selection
-1011111 cause : Semantically incorrect message
-1100000 cause : Invalid mandatory information
-1100001 cause : Message type non-existent or not implemented
-1100010 cause : Message type not compatible with protocol state
-1100011 cause : Information element non-existent or not implemented
-1100100 cause : Conditional IE error
-1100101 cause : Message not compatible with protocol state
-1100110 cause : Recovery on timer expiry
-1101111 cause : Protocol error, unspecified
-1111111 cause : Interworking, unspecified

Table 43: Causes for disconnection of a message.

9.7 The message RELEASE

This message is either sent from network to mobile if the network intends to release the transaction identifier, or from mobile to network if the mobile station intends to release the transaction identifier.

```
_____[ 66 ]___[ 12:02:53,867 ]___[ DOWN ]____[ FACCH_F ]_____________________________

13 2d 08 02 e0 90

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
2d  00------  SendSequenceNumber  : 0

    --101101  MESSAGE TYPE            : RELEASE

08  00001000  INFORMATION ELEMENT : Cause
02  00000010  LENGTH OF IE CAUSE  : 2
e0  1-------  Extension Bit       : 1
    -11-----  Coding stand.       : Standard defined for the GSM-PLMNS
    ---0----  spare               : 0
    ----0000  location            : user
90  -0010000  cause               : Normal call clearing
```

Table 44: The message RELEASE

Possible Information Elements are
- from the mobile to network: Cause, Second cause (in case of abnormal call clearing), Facility, User-user, SS-Version (only if Facility is used),
- from the network to mobile: Cause, Second cause (in case of abnormal call clearing), Facility, User-user.

9.8 The message RELEASE COMPLETE

This mesage is either sent from network to mobile if the network has released the transaction identifier, or from mobile to network if the mobile station has released the transaction identifier.

```
_____[ 67 ]___[ 12:02:53,867 ]___[ UP ]_____________________________________________

93 2a

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
2a  00------  SendSequenceNumber  : 0

    --101010  MESSAGE TYPE        : RELEASE COMPLETE
```

Table 45: The message RELEASE COMPLETE

Possible Information Elements are
- from the mobile to network: Cause, Facility, User-user, SS-Version (only if Facility is used),
- from the network to mobile: Cause, Facility, User-user

While talking about Supplementary Services we shall see that RELEASE COMPLETE is used by the network as an answer to the message FACILITY REGISTER.

9.9 The line NO INFORMATION FIELD in the window Layer Messages

Please have a look at “Picture 39: CC-Messages in a MTC registered with OTDrivePC”. In line 39 you can see a layer 2 frame issued on a FACCH with the unnumbered element SABM. In line 40 there follows a layer 2 frame issued on a FACCH with the unnumbered element UA.

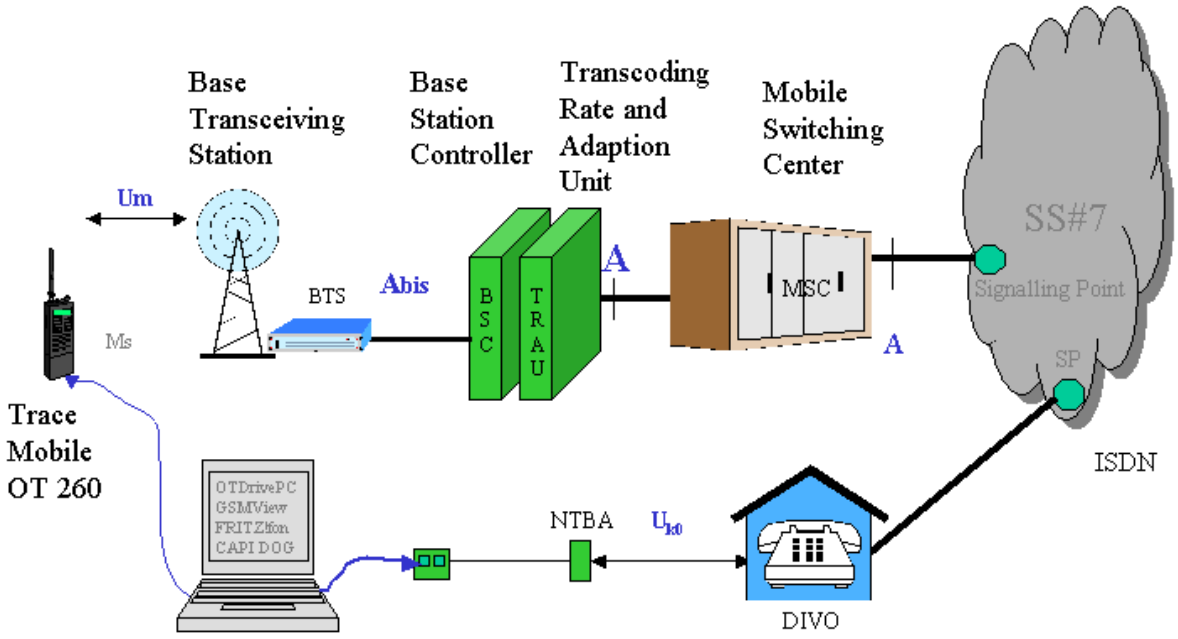
```
_____[ 27 ]___[ 09:54:35,309 ]___[ UP ]____[ FACCH_F ]_____________________________

01 3f 01

01  0-------  Spare               : 0
    -00-----  Link Prot. Disc.    : 0
    ---000--  SAPI                : 0
    ------0-  C/R Flag            : 0, MS side to BS side
    -------1  EA                  : 1
3f  00111111  Unnumbered          : SABM                      P=1
01  000000--  length              : 0
    ------0-  M                   : 0
    -------1  EL                  : 1

_____[ 28 ]___[ 09:54:35,480 ]___[ DOWN ]____[ FACCH_F ]_____________________________

01 73 01

01  0-------  Spare               : 0
    -00-----  Link Prot. Disc.    : 0
    ---000--  SAPI                : 0
    ------0-  C/R Flag            : 0, MS side to BS side
    -------1  EA                  : 1
73  01110011  Unnumbered          : UNNUMBERED ACKNOWLEDGE    F=1
01  000000--  length              : 0
    ------0-  M                   : 0
    -------1  EL                  : 1
```

Table 46: SABM and UA as a NO INFORMATION FIELD

The name NO INFORMATION FIELD is somewhat strange: it would be more precise to write LAYER 2 ONLY FIELD.
As is known from the ISDN, in protected mode all messages are protected by numbering. A numbered frame (a so-called ‘I-frame’) first receives a receipt on layer 2 from a Supervisory octet named Receiver Ready. This field is called a NO INFORMATION FIELD. Following that the next I-frame in the opposite direction gives another receipt.
You must note that the receiver counter does not register the send-number of the I-frame but instead counts the expected number of the I-frame.
For example, if the I-frame is sent with N(S) = 0, the receipt is “I received the number 0 therefore I expect the number 1” N(R) = 1.

10. Services in GSM

On the CD issued with the booklet [4] are exercises which allow you to investigate the behaviour of a mobile (Trace Mobile OT260) in an environment shown in the following picture.



Picture 40: Measurement equipment for exercises with Trace Mobile OT260

The Laptop shown in picture 40 captures traces from the OT260 combined with OTDrivePC and ISDN-traces gathered with a FRITZ!Card and CAPIDOG.
The raw traces can be translated by GSMView and ISDNView.

10.1 Exercise: Call ISDN-Phone to Trace Mobile (MTC)

If you compare the CC-messages of the ISDN and the GSM Trace you can see they are very similar. We can now measure the time duration from a call set up on the ISDN site to the ringing of the mobile. Please imagine that the time difference is calculated by subtracting the SETUP time on the ISDN site from the ALERTING time on the Mobile site.

10.2 Exercise: Call Trace Mobile to ISDN-Phone (MOC)

Please look at the differences, if any, between the results of this exercise and those gathered in exercise 10.1.

10.3 Exercise: Call with BC “facsimile group3” and HLC “Fax Gr2/3”

The Facsimile operation mode is a very interesting one. In GSM only Fax Group 3 is allowed. A FAX is often a document which contains text and pictures. It is obvious that such a

document cannot be displayed on the screen of a mobile and the operators use some tricks to bypass this handicap.
In the exercise given on the aforementioned CD you are required to send a fax document to a mobile using the FRITZ!fax client. The BTS has to recognize the message is a fax by reading the bearer of the incoming SETUP.
The network will store this message and then call the mobile user and ask him for the telephone number of an actual fax device. The network will then send the stored fax to the given fax device.
If you do not use the ISDN-fax operation mode the bearer will be the same as the one sent by an analogue telephone: the mobile will ring but there is no call.
The operator t-mobile (D1) provides a special service: it is possible to use the menu-entry *Special>Mail& Fax*. A SMS written here can then be sent to a Fax device.

10.4 Remarks about Data transfer in GSM

Data transfer in GSM is possible in CSD-mode. This means data links are switched in the same way as speech by the Mobile Switching Center.
If you want a connection with the Internet you must install special software (e.g. WellPhone by RTE). This software generates a modem and provides a communication end point suited to contact with the WEB.
It is possible to send a data message using FRITZ!data over a standard GSM-Phone connection. The operators do not like to transfer such messages using a normal telephone number and so these messages are refused by the GMSC.
However, if you use a MSISDN admissible for data transfer, the connection will work.

10.5 Exercise: Call using BC “unrestricted digital information”

If you set up a call by FRITZ!data to a mobile you will receive a DISCONNECT message with the cause “Bearer capability not authorised” i.e. the operator does not allow a data connection on a line commissioned for telephony.
If you commission a data transmission service from the operator you will receive a special telephone number.
Data transmission is always organised using GPRS (UMTS).

10.6 Exercise: Call with mobile to the internet

Whilst data transmission with your mobile is mostly forbidden (with the aforementioned exception), the connection to WAP is always allowed. A SETUP message to WAP is shown in the following table. Please have a look at the extensive Bearer with a length of 7 octets and the extensive Information Element Low Layer Capability.

```
____[ 95 ]___[ 16:03:29.930 ]___[ UP ]_____________________________________________

03 05 04 07 a1 88 89 21 15 63 a0 5e 07 91 94 71 21 25 14 02 7c 06 88 90 21 48 40 bb a1

03  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----0011  Protocol Discrim.   : Call control and call related SS messages
05  00------  SendSequenceNumber  : 0

    --000101  MESSAGE TYPE        : SETUP

04  00000100  INFORMATION ELEMENT : Bearer capability
```

```
07  00000111  length              : 7
a1  1-------  Extension           : 1
    -01-----  Radio Channel Req.  : full rate support only MS
    ---0----  Coding Standard     : GSM standard coding
    ----0---  Transfer Mode       : Circuit Mode
    -----001  Info Transfer Cap.  : unrestricted digital information
88  1-------  Extension           : 1
    -0------  Compression         : data compression not possible
    --00----  Structure           : service data unit integrity
    ----1---  Duplex Mode         : full duplex
    -----0--  Configuration       : point-to-point
    ------0-  Negot. of Int.      : No meaning is associated with this value.
    -------0  Establishment       : demand
89  1-------  Extension           : 1
    -00-----  Access ID           : octet identifier
    ---01---  Rate Adaptation     : V.110/X.30
    -----001  Signalling Acc.Prot : I.440/450
21  0-------  Extension           : 0
    -01-----  Layer 1 ID
    ---0000-  User Info L1 Prot   : Default layer1 protocol
    -------1  Sync/async          : asynchronous
15  0-------  Extension           : 0
    -0------  Numb Stop Bits      : 1 bit (also used in the case of synchr mode)
    --0-----  Negotiation         : in-band negotiation not possible
    ---1----  Numb Data Bits      : 8 bits (also used in case of bit oriented protocols)
    ----0101  User Rate           : 9.6 kbit/s Recommendation X.1 and V.110
63  0-------  Extension           : 0
    -11-----  Intermediate Rate   : 16 kbit/s
    ---0----  NIC On Tx           : not require to send data with network  indep.clock
    ----0---  NIC On Rx           : can't accept data with network indep. clock
    -----011  Parity              : none
a0  1-------  Extension           : 1
    -01-----  Connect Element     : non transparent (RLP)
    ---00000  Modem Type          : none

5e  01011110  INFORMATION ELEMENT : CalledPartyBCDNumber
07  00000111  length              : 7
91  1-------  Extension           : 1
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/teleph. numb. plan (Rec. E.164/E.163) _
94..02        number              : 491712524120

7c  01111100  INFORMATION ELEMENT : Low Layer Compatibility
06  00000110  length              : 6
88  1-------  Extension           : 1
    -00-----  coding standard     : CCITT standardized coding as described below
    ---01000  inform. transf. cap : unrestricted digital information
90  1-------  Extension           : 1
    -00-----  transfer mode       : circuit mode
    ---10000  transfer rate       : 64 kbit/s -
21  0-------  Extension           : 0
    -01-----  layer1,ident
    ---00001  CCITT standardized rate adaption V.110/X.30. This implies the presence of octet
5a and optionally octet 5b, 5c and 5d as defined below
48  0-------  Extension           : 0
    -1------  synch./ansynch      : asynchronous
    --0-----  negotiation         : in-band negotiation not possible
    ---01000  user rate           : 9.6 kbit/s Recommendations V.6 and X.1
40  0-------  Extension           : 0
    -10-----  intermediate rate   : 16 kbit/s
    ---0----  NIC on Tx           : not required to send data with Network Independent Clock
    ----0---  NIC on Rx           : cannot accept data with Network Independent Clock (i.e.
sender does not support this optional procedure)
    -----0--  Flow control on Tx  : Not required to send data with flow control mechanism
    ------0-  Flow control on Rx  : cannot accept data with flow control mechanism (i.e.
sender does not support this optional procedure)
    -------0  Spare               : 0
bb  1-------  Extension           : 1
    -01-----  number of stop bits : 1 bit
    ---11---  number of data bits : 8 bits
    -----011  Parity              : none

a1  10100001  Information Element : CLIR suppression
```

Table 47: The SETUP message to connect to the WAP

11. Supplementary Services in GSM

Supplementary Services in GSM can be realized in three different ways:

1. By Information Elements.
Information Elements are
- *Calling Line Identification Restriction (CLIR)*: i.e. the subscriber does not allow his *calling party number* to be displayed in the mobile or telephone of the person he is calling. The Information Element is called *CLIR invocation*. If this IE is a component of the SETUP message the telephone number is suppressed.
- *Subaddressing*: A Sub-address consisting of up to 20 digits can be a component of the SETUP message in a MOC or MTC. GSM Recommendation 04.08 permits sub-addresses. However, up to this point I have not found any.

2. By messages
Messages without coding in ASN.1 are HOLD and RETRIEVE. They are used to realize the *Brokers Call,* or to handle the subscriber in *Multiple Party Service*.

3. By using the messages FACILITY and FACILITY REGISTER.
As in the ISDN-protocol 1TR6, GSM distinguishes between call-related and none call-related Supplementary Services.
The Protocol discriminator of Call Control and call-related SS messages is equal 3.
The Protocol discriminator of none call-related SS messages is equal B.
The construction of the messages is very similar to those of the ISDN. The messages are coded using the language ASN.1.

Messages :	FACILITY,	FACILITY REGISTER,	RELEASE COMPLETE.
PD :	3	B	B
IE :	Type LV	Facility	Facility
Length:	Length of the whole Information Element		
Component:	a1 = Invoke,	a2 = Return Result,	a3 = Error, a4 = Reject
Length:	Length of the Component		
Invoke Identifier:	Type, Length, Value		
Operation Value:	Type, Length, Value		

Table 48: Types of FACILITY messages

On the CD issued with this booklet are exercises which allow you to investigate the behaviour of a mobile (Trace Mobile OT260) in an environment shown in picture 40.
The exercises are:

11.1 Exercise: CLIR and CLIP

By performing the exercises CLIR and CLIP you switch the behaviour of the OT260 to *Settings -> Calls -> Display number-> Anonymous->NO* or to **"***Anonymous->YES***".** In the first case the IE *A1 CLIR suppression* is a component of the message SETUP (see table 46). In the second case the IE *A2 CLIR invocation* has to be a component of the message SETUP.

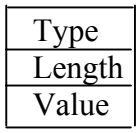
11.2 Exercise: HOLD and broker's call

Using the Trace Mobile set up a call to FRITZ!fon (subscriber 1)
If the connection is established press the "MENU" button on the mobile and select "**Hold call**".
Now dial the phone number of a second telephone on the mobile. Accept the call and talk with subscriber 2.
Press the "MENU" button on the mobile again, select **"Take another call"** from the display and press "OK". You can now talk to subscriber 1 again.
Close both connections by hanging up the mobile.
Stop recording, disconnect OTDrivePC from the mobile and export the trace *HOLD*.
If you have a closer look at the translated trace you can verify that the connection to be held is selected by the *Transactions ID*.

11.3 Some remarks about ASN.1

"ASN.1 is the acronym for Abstract Syntax Notation One, a language for describing structured information; typically, information intended to be conveyed across some interface or communication medium……." (Douglas Steedman, ASN1..)
An ASN.1 Type is a set of values and represents a potential for conveying information.

In ISDN and GSM ASN.1 is used to describe Supplementary Services. The Radio Resource Control messages in UMTS are written exclusively in the Packet encoding rules of ASN.1.
It is not our task to deal with the latter here.
In our application we always have the notation



Defined by the Basic Encoding Rules BER, a type is represented by a Tag. A Tag can be compared to a label which is printed on a box describing the contents of the box . For our purposes we shall only look for tags of one octet in length.
A Tag is a combination of the Tag **C**lass, the **F**orm and the **T**ype.

Bit	87654321
Value	CCFTTTTT

CC	TAG CLASS	F	Form	TTTTT	Type(selection)
00	**universal**	0	primitive	00001	Boolean
01	application-wide	1	constructed	00010	Integer
10	**context-specific**			00100	Octet string
11	private-use			00110	Object identifier
				01010	Enumerated
				10000	Sequence
				10010	Numeric String

Table 49: Description of a Tag

For example in table 50 you find the lines

```
02  00000010  Type=INTEGER        : Invoke Identifier
01  00000001  length              : 1
01  00000001  Invoke ID Value     : 1
```

describing the Invoke Identifier. The Invoke Identifier gives the message a number. For example, the message shown in table 50 is numbered with Invoke ID Value one. It only allows the network to answer the call if it returns that Invoke Identifier (see table 51)

Another example are the lines

```
02  00000010  Type=INTEGER        : Operation Value
01  00000001  length              : 1
7c  01111100  Operation Value     : buildMPTY
```

defining an Operation Value. This Value is taken from the list shown in table 51.

Somewhat more sophisticated is the construction in table 52 using the type SEQUENCE

```
30  00110000  SEQUENCE            : registerSS-Arg
0f  00001111  length              : 15

04  00000100  OCTETSTRING         : ss-code
01  00000001  length              : 1
21  00100001  ss-code Value       : cfu

83  10000011  IMPL. OCTETSTRING   : teleservice
01  00000001  length              : 1
11  00010001  Teleservice         : telefony

84  10000100  INFORMATION ELEMENT : forwardedToNumber
07  00000111  length              : 7
81  1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/telephony numbering plan (Rec. E.164/E.163)
30..f9        number              : 03375295837
```

A SEQUENCE is a structured type which is defined in terms of a list of other types, or, more colloquially, the SEQUENCE builds brackets around some other types.

The last type we will consider here is the Choice Type which is constructed in a context-specific way. Choice is used for selections from a list of alternatives. A key element of this type is the *Component,* the first type which appears in the Information Element Facility.

```
Components    ::= CHOICE {
                    invokeComp [1] IMPLICIT Invoke Component,
                    returnResultComp [2] IMPLICIT ReturnResultComponent,
                    returnErrorComp [3] IMPLICIT ReturnErrorComponent,
                    rejectComp [4] IMPLICIT RejectComponent
                  }
```

There exist primitive choice types encoded 8x and constructed choice types encoded ax. Therefore the Invoke Component is written a1, the ReturnResultComponent is written a2. In our examples we shall deal only with the Invoke Component and the ReturnResult Component.
We are now able to understand the following traces:

11.4 Call related SS messages

Call related SS messages are issued whilst a call is performed. If you are not familiar with the use of Supplementary Services in ISDN please have a look at the following example.

- A mobile receives a call from the ISDN (subscriber 1) and accepts it.
- During the communication the user receives a *Call Waiting Signal* (possibly a tone).
- The subscriber decides to accept the incoming call (subscriber 2) and send the signal *HOLD* to the existing call.
- The network sends *HOLD ACKNOWLEDGE*.
- Now the second call can be taken by the user.
- The user decides to have a Multiple Party, that is to communicate with both subscribers and sends the message FACILITY. The message FACILTITY is structured as shown in table 50.

```
_____[ 260 ]___[ 10:49:13,152 ]___[ UP ]_____________________________________________

93 3a 08 a1 06 02 01 01 02 01 7c 7f 01 00

93  1-------  direction to        : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
3a  00------  SendSequenceNumber  : 0

    --111010  MESSAGE TYPE        : FACILITY
08  00001000  Lgth OF IE FACILITY : 8
a1  10100001  Component           : Invoke
06  00000110  length              : 6
02  00000010  Type=INTEGER        : Invoke Identifier
01  00000001  length              : 1
01  00000001  Invoke ID Value     : 1
02  00000010  Type=INTEGER        : Operation Value
01  00000001  length              : 1
7c  01111100  Operation Value     : buildMPTY

7f  01111111  Information Element : SS-Version
01  00000001  length              : 1
00  00000000  SS-Version indicator: 0
```

Table 50: Invocation of the Supplementary Service MTPY

- The network accepts this order by returning the Invoke Identifier (see table 51).

```
_____[ 264 ]___[ 10:49:13,902 ]___[ DOWN ]____[ FACCH_F ]_____________________________

13 3a 05 a2 03 02 01 01

13  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----0011  Protocol Discrim.   : Call control and call related SS messages
3a  00------  SendSequenceNumber  : 0

    --111010  MESSAGE TYPE        : FACILITY
05  00000101  Lgth OF IE FACILITY : 5
a2  10100010  Component           : Return Result
03  00000011  length              : 3

02  00000010  Type=INTEGER        : Invoke Identifier
01  00000001  length              : 1
01  00000001  Invoke ID Value     : 1
```

Table 51: The Supplementary Service MTPY is accepted by the network

- The three calls are connected by the *conference bridge*. The user and subscribers 1 and 2 can now all talk to one another.

The principle of invoking a call-related supplementary service is always the same but the Invoke Identifier may differ (see table 52).

RegisterSS	10
EraseSS	11
ActivateSS	12
DeactivateSS	13
InterrogateSS	14
NotifySS	16
RegisterPassword	17
GetPassword	18
ProcessUnstructuredSS-Data	19
ForwardCheckSS-Indication	38
ProcessUnstructuredSS-Request	59
UnstructuredSS-Request	60
UnstructuredSS-Notify	61
EraseCC-Entry	77
CallDeflection	117
UserUserService	118
AccessRegisterCCEntry	119
ForwardCUG-Info	120
SplitMPTY	121
RetrieveMPTY	122
HoldMPTY	123
BuildMPTY	124
ForwardChargeAdvice	125
ExplicitCT	126
LCS-LocationNotification	116
LCS-MOLR	115

Table 52: Operation Values defined by ETS TS 124080

11.5 None Call-related SS messages

Possibly the most familiar *None Call-related SS message* is CALL FORWARDING.
Call Forwarding exists in three modes:
- Call Forwarding Unconditional (cfu), i.e. a call to a mobile subscriber is immediately diverted in the MSC to another number given by the command cfu.
- Call Forwarding Busy (cfb), i.e. a call to a number is diverted in the MSC to another number given by the command cfb only if the called user is busy.
- Call Forwarding No Reply (cfnr), i.e. a call to a mobile subscriber is diverted in the MSC to another number given by the command cfnr only if the called party does not react.

The message to install a *None Call-related SS message* is FACILITY REGISTER. See the example shown in table 53.

```
_____[ 1 ]___[ 12:41:51,410 ]___[ UP ]_____________________________________________

0b 3b 1c 19 a1 17 02 01 01 02 01 0a 30 0f 04 01 21 83 01 11 84 07 81 30 73 25 59 38 f9 7f 01
00

0b  0-------  direction from      : originating site
    -000----  TransactionID       : 0
    ----1011  Protocol Discrim.   : non call related SS messages
3b  00------  SendSequenceNumber  : 0

    --111011  MESSAGE TYPE        : FACILITY REGISTER

1c  00011100  INFORMATION ELEMENT : Facility
19  00011001  length              : 25
a1  10100001  Component           : Invoke
17  00010111  length              : 23

02  00000010  Type=INTEGER        : Invoke Identifier
01  00000001  length              : 1
01  00000001  Invoke ID Value     : 1

02  00000010  Type=INTEGER        : Operation Value
01  00000001  length              : 1
0a  00001010  Operation Value     : registerSS

30  00110000  SEQUENCE            : registerSS-Arg
0f  00001111  length              : 15

04  00000100  OCTETSTRING         : ss-code
01  00000001  length              : 1
21  00100001  ss-code Value       : cfu

83  10000011  IMPL. OCTETSTRING   : teleservice
01  00000001  length              : 1
11  00010001  Teleservice         : telefony

84  10000100  INFORMATION ELEMENT : forwardedToNumber
07  00000111  length              : 7
81  1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/telephony numbering plan (Rec. E.164/E.163)
30..f9        number              : 03375295837

7f  01111111  INFORMATIONSELEMENT : SS Version Indicator
01  00000001  length              : 1
00  00000000  SS-Versions Info.   : 0
```

Table 53: A Supplementary Service CFU set-up call

The network answers with the message RELEASE COMPLETE and repeats all features given in the command FACILITY REGISTER. There is a slight difference if the mobile orders the teleservice *telephony*. In this case the network confirms the teleservice *speech*.

```
_____[ 2 ]___[ 12:41:53,051 ]___[ DOWN ]____[ SDCCH ]_____________________________

8b 2a 1c 22 a2 20 02 01 01 30 1b 02 01 0a a0 16 04 01 21 30 11 30 0f 83 01 10 84 01 07 85 07
91 94 33 57 92 85 93

8b  1-------  direction to         : originating site
    -000----  TransactionID        : 0
    ----1011  Protocol Discrim.    : non call related SS messages
2a  00------  SendSequenceNumber   : 0

    --101010  MESSAGE TYPE         : RELEASE COMPLETE

1c  00011100  INFORMATION ELEMENT  : Facility
22  00100010  Lgth of IE FACILITY  : 34
a2  10100010  Component            : ReturnResult
20  00100000  length               : 32

02  00000010  Type=INTEGER         : Invoke Identifier
01  00000001  length               : 1
01  00000001  Invoke ID value      : 1

30  00110000  SEQUENCE             : Resultinfo
1b  00011011  length               : 27
02  00000010  INTEGER              : OperationValue
01  00000001  length               : 1
0a  00001010  Operation Value      : RegisterSS

a0  10100000  IMPLICIT SEQUENCE    : Forwarding Info
16  00010110  length               : 22

04  00000100  IMPL.OCTETSTRING     : ss-code
01  00000001  length               : 1
21  00100001  ss-code Value        : cfu

30  00110000  SEQUENCE             : forwardingFeatureList
11  00010001  length               : 17
30  00110000  SEQUENCE             : basicService
0f  00001111  length               : 15

83  10000011  IMPL. OCTETSTRING    : teleservice
01  00000001  length               : 1
10  00010000  Teleservice          : speech

84  10000100  OCTETSTRING          : ss-status
01  00000001  length               : 1
07  00000111  P,R und A-bit        : Active and Operative, Registered, Provisioned

85  10000101  IMPL. OCTETSTRING    : forwardedToNumber
07  00000111  length               : 7
91  1-------  Extension            : 1
    -001----  Type of number       : international number
    ----0001  Numb. plan id.       : ISDN/telephony numb. pl. (Rec. E.164/E.163)
94  1-------  Extension            : 1
    -00-----  Present.indic.       : Presentation allowed
    ------00  Screening ind.       : User-provided, not screened
33..93        number               : 3375295839
```

Table 54: The Supplementary Service cfu is accepted by the network

In the tables 53 and 54 the element ss-code appears, that is the code of the used supplementary service.

```
00010001  ss-code Value       : clip
00010010  ss-code Value       : clir
00010011  ss-code Value       : colp
00010100  ss-code Value       : colr
00100000  ss-code Value       : all Call Forwarding Services
00100001  ss-code Value       : cfu
00101000  ss-code Value       : allCondForwardingSS
00101001  ss-code Value       : cfb
00101010  ss-code Value       : cfnry
00101011  ss-code Value       : cfnrc
00100100  ss-code Value       : cd
00110001  ss-code Value       : ect
01000001  ss-code Value       : cw
01000011  ss-code Value       : ccbs-A(origination side)
01000100  ss-code Value       : ccbs-B(destination side)
01000010  ss-code Value       : hold
01010001  ss-code Value       : multiPTY
01110001  ss-code Value       : aoci (information)
01110010  ss-code Value       : aocc (charging)
10000001  ss-code Value       : uus1
10000010  ss-code Value       : uus2
10000011  ss-code Value       : uus3
10010000  ss-code Value       : allBarringSS
10010001  ss-code Value       : barrinOfOutgoingCalls
10010010  ss-code Value       : baoc
10010011  ss-code Value       : boic
10010100  ss-code Value       : boicExHC
10011001  ss-code Value       : barringOfincomingCalls
10011010  ss-code Value       : baic
10011011  ss-code Value       : bicRoam
```

Table 55: Selected part of ss-code values from GSM 09.02

12. The transmission of SMS

Whilst transmitting a SMS the channel request the dedication of a channel, the authentification, the encryption, the Message Reports and so on, are the same as during a voice call set up.
There are two new messages: RP_DATA, which consists of the contents of the SMS, and CP-ACK which is used to receipt the message. For reasons of length the message RP_DATA is often segmented.
It is to be emphasized that only a SDCCH and no Transport Channel is used to transport a SMS.

It is an interesting idea to save channel capacity whilst transmitting the user data of a SMS. The octets are arranged into a bit string and the message is performed by 7 bit characters.

: User Data 04 00000100 length of 7 bit char : 4
f4 11110100 t
f2 11110010 e
9c 10011100 s
0e 00001110 t

12.1 Receiving a SMS

In this exercise you must receive a SMS with the Trace Mobile. To keep the trace easy to read please clear all check boxes which do not contain “SMS” and “Layer3”.Only the first message-frame is of interest. The frame is concatenated by GSMView using the segmented parts of the SMS.

```
_____[ 1 ]___[ 17:30:28,980 ]___[ DOWN ]____[ SDCCH ]_____________________________

0f 00 53 19 01 2d 01 00 07 91 94 71 01 67 05 00 00 21 04 0c 91 94 61 20 05 95 89 32 00 20 70
81 71 03 22 40 10 c4 f0 1c 94 9e d3 41 e5 b4 bb 0c 9a 36 a7

0f  0-------  Spare               : 0
    -00-----  Link Prot. Disc.    : 7
    ---011--  SAPI                : 3
    ------1-  C/R Flag            : 1, BS side to MS side
    -------1  EA                  : 1
00  00000000  Information Transf. : INFORMATION         N(R)=0, N(S)=0, P=0
53  010100--  length              : 20
    ------1-  M                   : 1
    -------1  EL                  : 1
19  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----1001  Protocol Discrim.   : SMS messages


01  00000001  MESSAGE TYPE        : RP_DATA

: Length of SMS
2d  00101101  lenght              : 45
: Parameter
01  00000001  Parameter           : 1
00  00000000  Parameter           : 0

: SMSC Address
07  00000111  lenght              : 7
91  1-------  Extension
    -001----  Type of number      : International number
    ----0001  Numbering plan      : ISDN/telephone numberingplan(E.164/E.163)
94..00        number              : 491710765000

: Message Flags
00  00000000  TP-MTI, TP-MMS, TP-SRI, TP-UDIH, TP-RP

: Message Reference Number
21  00100001  Reference Number    : 33

04  00000100  Parameter

: Destination address

0c  00001100  length              : 12
91  1-------  Extension           : 1
    -001----  Type of number      : international number
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
94..89        number              : 491602505998

: Protocol Identifier
32  00110010  Protocol Identifier
: Data Coding Sheme
00  00000000  Data Coding Sheme
: Parameter
20  00100000  Parameter1
70  01110000  Parameter2
81  10000001  Parameter3
71  01110001  Parameter4
03  00000011  Parameter5
22  00100010  Parameter6
40  01000000  Parameter7

: User Data
10  00010000  SMS_LENGTH          : 16
              SMS_TEXT            : That is a SMS
```

Table 56: Concatenated trace of incoming SMS

There are two addresses in an SMS-message: the SMS-Control Centre and the Destination Address. There are also many Message Flags and Parameters which we will not discuss.

12.2 Sending a SMS

```
_____[ 1 ]___[ 16:01:55.633 ]___[ UP ]____[ SDCCH ]_____________________________

19 01 4c 00 00 00 07 91 94 71 07 16 00 00 40 b1 04 0b 81 10 37 26 33 01 f6 00 00 a7 39 e4 72
58 0e 32 cb d3 65 37 d9 05 4a 83 c2 6d d0 99 1d 26 83 e8 6f 90 b8 0c 0a 8b d9 65 10 fd 0d 9a
97 dd 64 50 fe 5d 07 85 41 ed f2 7c 1e 3e 97 5d 20

19  0-------  direction from      : originating site
    -001----  TransactionID       : 1
    ----1001  Protocol Discrimin. : SMS messages


01  00000001  MESSAGE TYPE        : RP_DATA

: Length of SMS
4c  01001100  length              : 76
: Parameter
00  00000000  Parameter           : 0
00  00000000  Parameter           : 0
00  00000000  Parameter           : 0

: SMSC Address

07  00000111  length              : 7
91  1-------  Extension
    -001----  Type of number      : International number
    ----0001  Numbering plan      : ISDN/telephone numbering plan(E.164/E.163)
94..00        number              : 491770610000

40  0-------  TP-Reply-Path       : parameter is not set in this SMS-SUBMIT/DELIVER
    -1------  TP-UDHI             : The beginning of the TP-UD field contains a
                                    Header in addition to the s. m.
    --0-----  TP-SRR              : A status report will not be returned to the SME
    ---00---  TP-VPF              : field not present
    -----0--  TP-RD               : Instruct the SC to accept an SMS-SUBMIT for an
                                    SM still held in the SC
    ------00  TP-MTI              : SMS-DELIVER REPORT (in the direction MS to SC)

b1  ----000-  Reference Number  high part
04  00000100  Reference Number  low part

: Destination address

0b  00001011  length              : 11
81  1-------  Extension           : 1
    -000----  Type of number      : unknown
    ----0001  Numb. plan id.      : ISDN/telephony numb. pl. (Rec. E.164/E.163)
10..f6        number              : 01736233106

00  00000000  TP-Protocol Identifier
00  00000000  TP-Data-Coding-Scheme
a7  10100111  TP-Validity-Period

: User Data

39  00111001  SMS_LENGTH          : 57
              SMS_TEXT            : dear friend. i am glad to be able to send
                                    you a message.
```

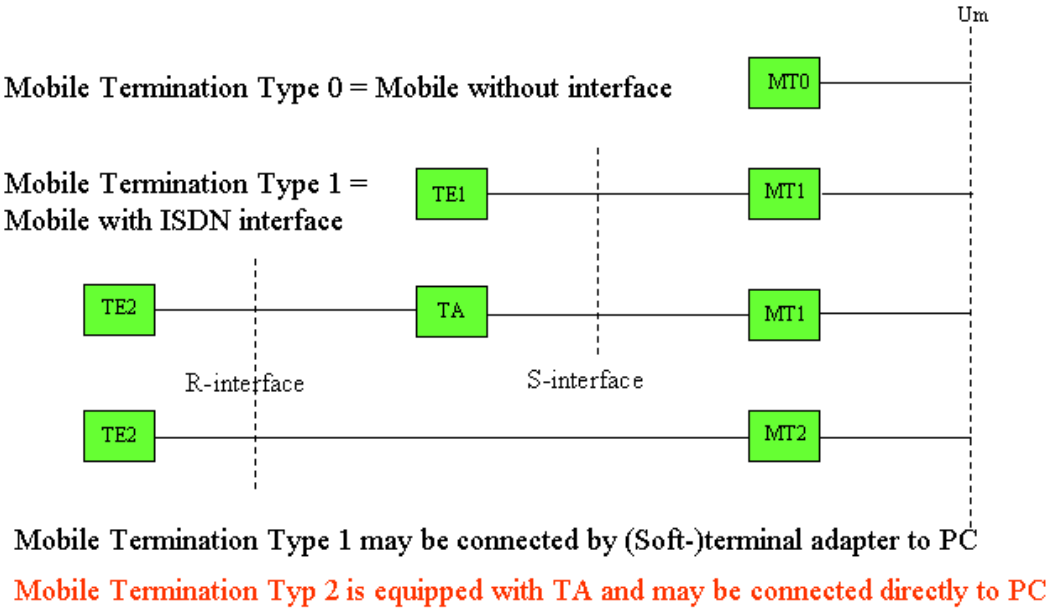
Table 57: Concatenated trace of an outgoing SMS

In addition to the term SMS there are also the concepts of EMS and MMS.

The **E**xtended **M**essage **S**ervice is defined in ETS TS 123 040. This service allows to concatenate up to 255 SMS to an EMS. Control elements exist to allow the translation of sound, pictures and animations.
The EMS service is used in newer mobiles to enable SMS of more than 160 characters to be sent.
Pictures, sounds and animations (videos) are conveyed with MMS. MMS are data strings which are transported using data channels of GPRS or UMTS connections.

13 Controlling mobiles by AT-commands

13.1 Mobile station interfaces



Picture 41: Mobile station interfaces

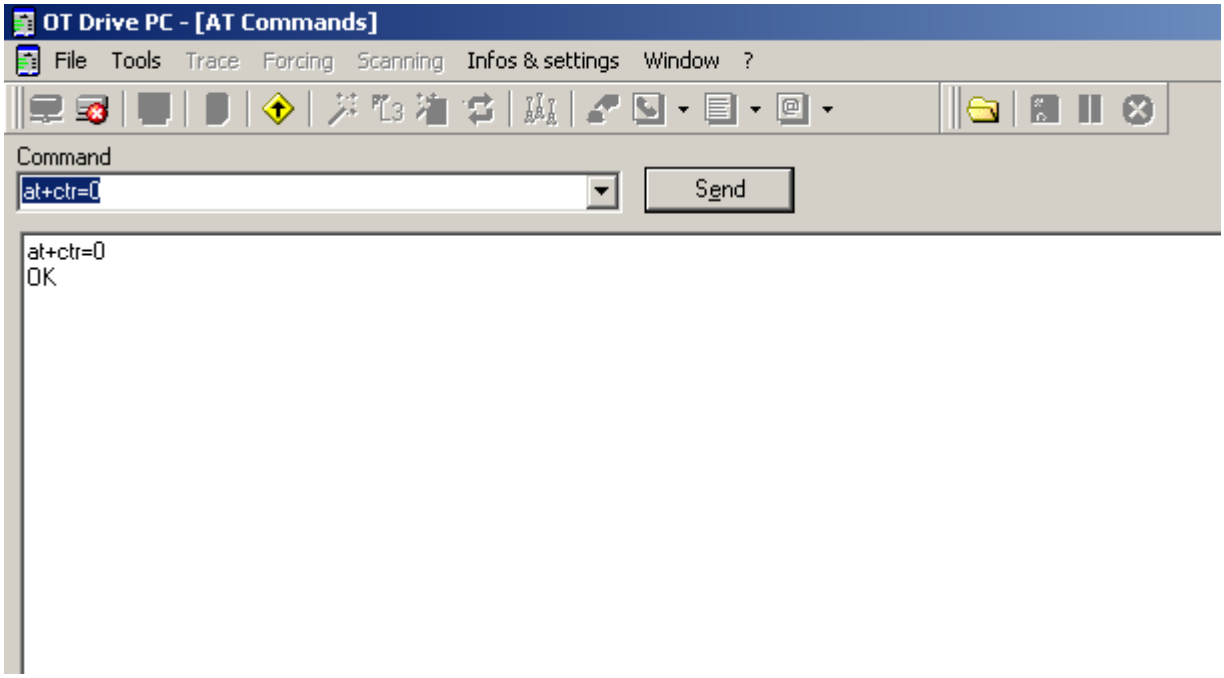
At present three Mobile Termination Types are in use:
- Type 0 is a mobile which possesses only a socket for connecting a charging cable
- I could not find any mobile of Type 1 with an ISDN-Interface
- Type 2 with S-Interface allows connection to a TE2 (possibly a computer) but there has to be a Terminal Adapter between MT1 and TE2.
- Type 2 with R-Interface is a mobile with a socket to connect the mobile to a COM-port of a computer with a cable.

The Trace Mobile OT260 is of Type 1 with S-Interface because in the cable there is a small circuit which works as a TA.
Many mobiles in use can be connected to a computer by Infra Red (IrDA) or Bluetooth. I would like to designate them MT1.

13.2 Controlling a mobile using AT-Commands

Mobiles of type MT1 or MT2 can be controlled like modems by using AT-Commands. The Possible AT-Commands are defined in ETSI TS 100 916 i.e. GSM 07.07.
If you read this ETS you must bear in mind that not all definitions are mandatory. In addition, every producer of mobiles has additional AT-Commands which work only with their products. To communicate with a mobile using an AT-Command you should use the Hyper Terminal of MS Windows.

In our case, because we use an OT260, it is convenient to use OTDrivePC for communication with AT-Commands. To do so open OTDrivePC. Click *File -> Connect* and then *Tools-> AT commands* ... If your mobile is in Trace-mode write the command at+ctr=0. The reaction of the mobile is seen in picture 42: the mobile has changed to Data-mode



Picture 42: OTDrivePC in AT-mode

13.3 AT-Commands for controlling services.

As we know from our exercise in paragraph 9 the service is determined by the BC.
For speech communication the bearer can be set very simply: we have to write ATD (D means Dialling), the telephone number of the remote terminal and finally a semicolon.
e.g.

ATD03375203716;

You may test this by calling your FRITZ!fon. Catch the trace with CAPIDOG and translate it with ISDNView.
The question is how do we set up a call in data mode? GSM 07.07. paragraph 6. gives a method of selecting a bearer service type.
Let's ask the mobile which BC parameter can be used with the OT260.
Our question:

AT+CBST=?

The answer:

+CBST: (0,4,6,7,68,70,71),(0),(0,1)

OK
If we now look at the recommendation GSM 07.07. paragraph 6.7 we find:

<speed>:
0 autobauding
1 300 bps (V.21)
2 1200 bps (V.22)
3 1200/75 bps (V.23)
4 2400 bps (V.22bis)
5 2400 bps (V.26ter)
6 4800 bps (V.32)
7 9600 bps (V.32)
...
68 2400 bps (V.110 or X.31 flag stuffing)
70 4800 bps (V.110 or X.31 flag stuffing)
71 9600 bps (V.110 or X.31 flag stuffing)
<name>:
0 data circuit asynchronous (UDI or 3.1 kHz modem)
<ce>:
0 transparent
1 non-transparent

If you want to build an analogue modem you can enter:
AT+CBST=7,0,1 <ENTER>
ATD<YourNumberOfFRITZ!fon> <ENTER>
If you want to build a digital modem you can enter:
AT+CBST=71,0,1 <ENTER>
ATD<YourNumberOfFRITZ!fon> <ENTER>

13.4 AT-Commands for controlling supplementary services.

In paragraph 11.1 Exercise: CLIR and CLIP we learned about suppressing the caller's telephone number in a call.
GSM 07.07 paragraph 7.7 tells us how to do this with AT-Commands by calling line identification restriction +CLIR:
By keying in: AT +CLIR? We receive the Answer +CLIR: <n>,<m>

In the above ETS the defined values are:

<n> (parameter sets the adjustment for outgoing calls):
0 presentation indicator is used according to the subscription of the CLIR service
1 CLIR invocation
2 CLIR suppression
<m> (parameter shows the subscriber CLIR service status in the network):
0 CLIR not provisioned
1 CLIR provisioned in permanent mode
2 unknown (e.g. no network, etc.)
3 CLIR temporary mode presentation restricted
4 CLIR temporary mode presentation allowed

If we write into the AT-command window of OTDrivePC

At+clir?

We get

+CLIR: 1,3

OK

That is n=1 CLIR invocation

m=3 CLIR temporary mode presentation restricted

Our telephone number will be suppressed

Now if we write into the AT-command window of OTDrivePC

At+clir=2

We get OK

Reading the status of the suppression mode by writing at+clir? we get +CLIR: 2,3 OK.

i.e. CLIR is now suppressed, the person we are calling can see our number. You can test this if you wish.

14 Bibliography

14.1 Books

[1] The GSM System for Mobile Communication by Michel MOULY and Marie-Bernadette PAUTET, publisher CELL &SYS, ISBN 2-9507190-0-7

[2] GSM Networks: Protocols, Terminology, and Implementation by Gunnar Heine Artech. House Publishers, Boston, London, ISBN 0-89006-471-7

[3] ISDN D-Channel in Dialogue by Joachim Göller, Narosa Publishing House New Dehli, Chennai Mumbai, Calcutta, London, ISBN 81-7319-535-3

[4] Signaling in Mobile Radio Communication by Joachim Göller, publisher EPV-Verlag, ISBN –10: 3-936318-24-7

14.2 Recommendations

[1] TS_100940v070800p GSM 04.08 Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification

[2] ETS_300938 . GSM 04.06 Digital cellular telecommunications system (Phase 2+); Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification

[3] TS_124080v030300p Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Mobile radio interface layer 3 supplementary services specification; Formats and coding

[4] TS_123040v050400p Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Technical realization of Short Message Service (SMS)

[5] TS_100916v070600p GSM 07.07 Digital cellular telecommunications system (Phase 2+); AT command set for GSM Mobile Equipment (ME)