Procedures in GSM

Contents

1 Geographical Network Structures

The GSM system is hierarchically ordered into service areas. To identify and address individual areas, the individual hierarchy levels/service areas have been given types. Every service area (up to location area) is subdivided into one or more service areas of a lower hierarchy level.

1.1 International GSM Service Area

The international GSM service area contains all countries where at least one GSM900, GSM1800 or GSM1900 PLMN is implemented or, to be more precise, the area supplied by these PLMNs, as in many countries the PLMN networks only supply parts of the country with the mobile telephone service. Currently, (12/98) there are 298 GSM-PLMN in service in 129 countries. A GSM subscriber may use all these networks for mobile communications with his SIM card and corresponding mobile equipment, provided that a roaming agreement exists between his home country network (HPLMN) and the network being visited (VPLMN).

1.2 National GSM Service Area

A national GSM service area contains one or more GSM-PLMN. The PLMN of different operators may supplement one another or overlap each other.

The following codes are important to identify a national GSM service area:

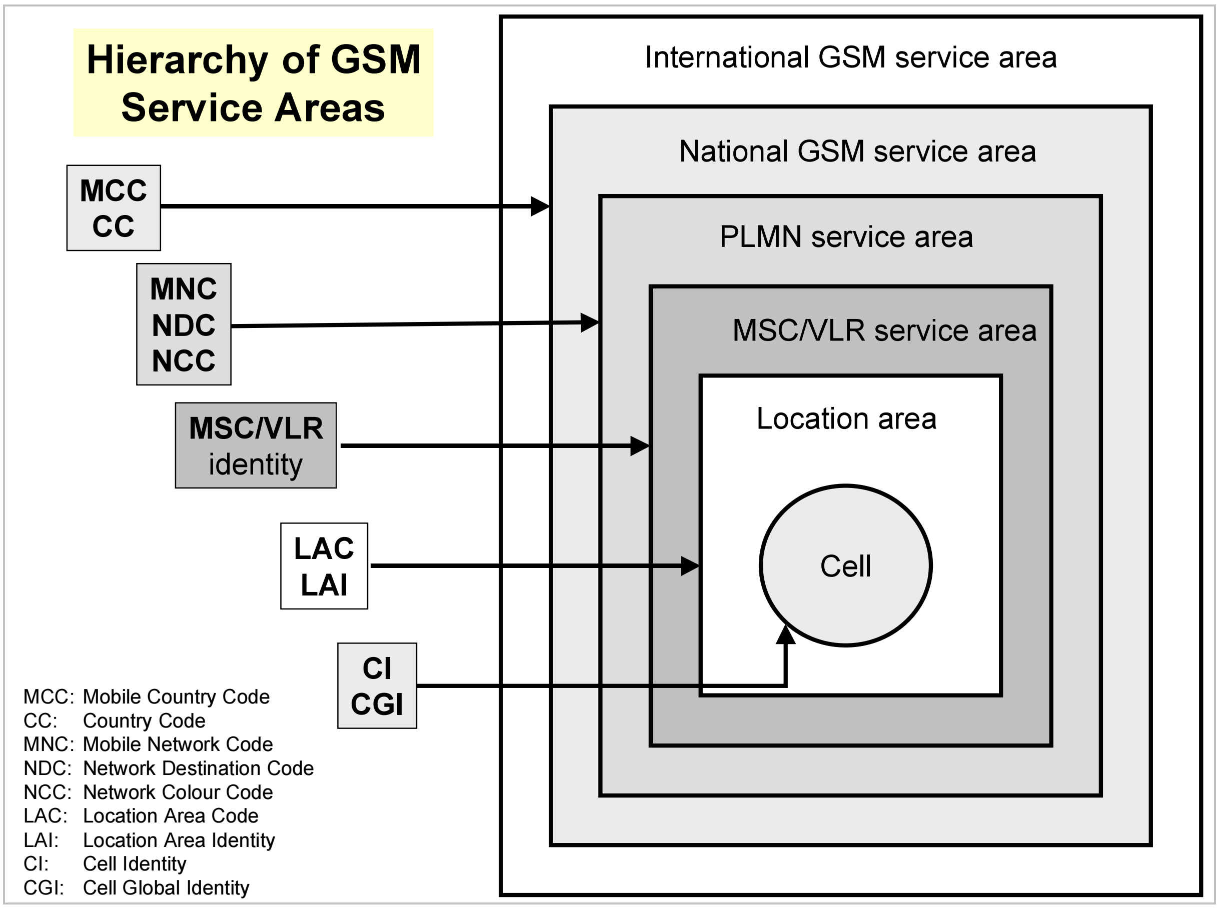
- **Mobile Country Code MCC**

  The MCC consists of 3 digits and is used in IMSI (International Mobile Subscriber Identity), LAI (Location Area Identity) and CGI (Cell Global Identity). A knowledge of the MCC is not necessary for mobile subscribers.

- **Country Code CC**

  The CC is the dialing code of the country in which the mobile subscriber is registered. The CC consists of 2/3 digits and is used in MSISDN (Mobile Subscriber ISDN number).

Examples of MCC and CC can be found in the appendix.



MCC: Mobile Country Code
CC: Country Code
MNC: Mobile Network Code
NDC: Network Destination Code
NCC: Network Colour Code
LAC: Location Area Code
LAI: Location Area Identity
CI: Cell Identity
CGI: Cell Global Identity

Fig. 1

1.3 PLMN Service Area

A PLMN service area is administered by an operator. Two or more PLMN service areas can overlap within a country. Thus the individual PLMNs must have a clear identification:

- **Mobile Network Code MNC**

  The MNC is the mobile phone specific PLMN identification and consists of 2 digits. The MNC is used in IMSI, LAI, CGI.

- **National Destination Code NDC**

  NDCs identify the dialing code of a PLMN and consist of 3 digits. The NDC is used in MSISDN.

- **Network Color Code NCC**

  The NCC is a PLMN discrimination code that is not unambiguous. It is used for short identification (length: 3 bits) of a particular PLMN in overlapping PLMN areas and in border regions and is used in BSIC (Base Station Identity Code).

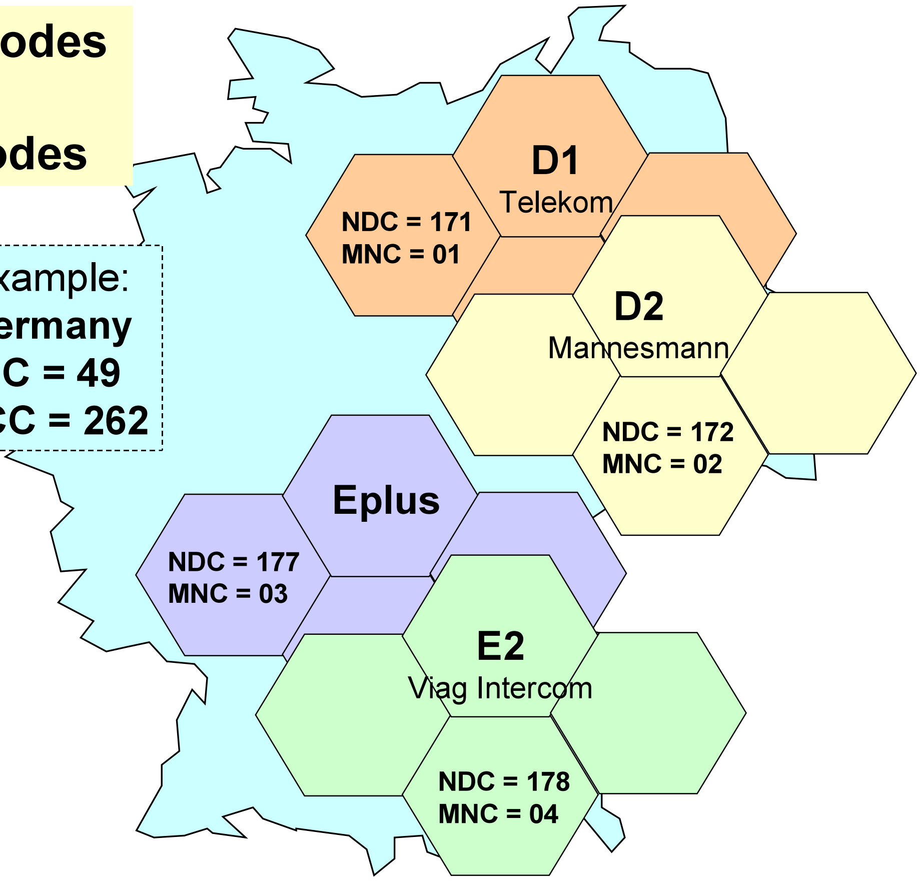
1.4 MSC/VLR Service Area

GSM-PLMN are subdivided into one or more MSC/VLR service areas: mobile subscribers, who have carried out location update/location registration in a MSC area, are registered in the VLR associated to the MSC. A MSC/VLR area may cover a part of a city or also a whole country. A MSC/VLR area may consist of several LAs. MSC and VLR have their own international identity. The code of the VLR, where a MS is currently present, is stored in the HLR so that a connection can be established in the case of MTC.

The following figure illustrates in a diagram the division of Germany into MSC areas. The figure has just an illustrative purpose and does not reflect the actual MSC areas of any German PLMN operator.

National Codes and PLMN Codes

Example:
Germany
CC = 49
MCC = 262



D1
Telekom
NDC = 171
MNC = 01

D2
Mannesmann
NDC = 172
MNC = 02

Eplus
NDC = 177
MNC = 03

E2
Viag Intercom
NDC = 178
MNC = 04

Fig. 2

1.5 Location Area (LA)

The location area is the area in which the MS can move freely without location update being necessary. The size of a LA is established by the operator according to the traffic or population density and the behavior of the mobile subscriber. A LA area can encompass one or more radio cells that are controlled by one or more BSC, but never belong to different MSC areas.

Identifications of the Location Area:

- **Location Area Code LAC**

  The LAC serves to identify a location area within a GSM-PLMN.

- **Location Area Identity LAI**

  LAI = MCC + MNC + LAC

  The LAI serves as an unambiguous international identification of a location area.

1.6 BTS Service Area: The Cell

A BTS service area is the smallest unit in the GSM-PLMN and encompasses the transmission/reception range of a cell. A defined quality of the received signal must be guaranteed within a cell. If a MS leaves the range of a cell while a conversation is being held (dedicated mode), a handover to the next cell is initiated.

Cell identifications are:

- **Cell Identity CI**

  The CI allows identification of a cell within a location area.

- **Cell Global Identity CGI**

  CGI = MCC + MNC + LAC + CI = LAI + CI;

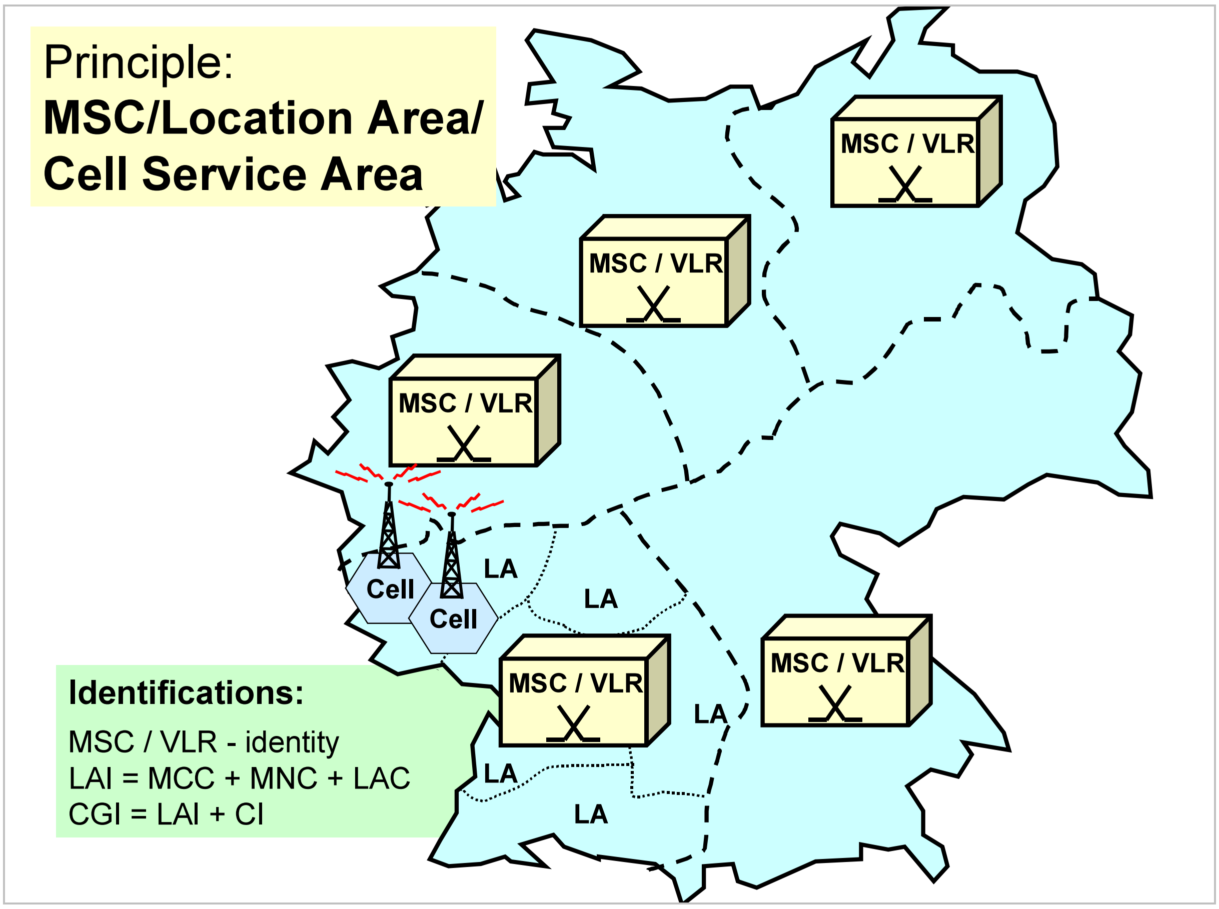
  The CGI represents an international unambiguous identification of a cell and is emitted in regular intervals by the BTS.

- **Base Transceiver Station Identity Code (BSIC)**

  BSIC = NCC + BCC (Base Station Color Code)

  The BSIC represents a non-unambiguous short identification of a cell. The BSIC is emitted at a regular rate by the BTS. It enables the MS to differentiate between different surrounding cells.

Note: all the identifications described in this section are summarized again in the appendix and described in more detail there.



Principle:
MSC/Location Area/ Cell Service Area

Identifications:

MSC / VLR - identity
LAI = MCC + MNC + LAC
CGI = LAI + CI

Fig. 3

2 Security Functions

In GSM the security of a mobile subscriber is ensured by several measures.

1) Authentication protects the network operator and mobile subscriber against unauthorized use.
2) Ciphering is used to prevent interception of radio communications.
3) Issue of a Temporary Mobile Subscriber Identity (TMSI) protects the subscriber from an unauthorized identification, as some of the signaling actions are uncoded.
4) IMEI check prevents the usage of stolen/non-authorized mobile equipment.

Security aspects are described in the GSM Recommendations:

02.09:	"Security Aspects"
02.17:	"Subscriber Identity Modules"
03.20:	"Security Related Network Functions"
03.21:	"Security Related Algorithm".

2.1 Prerequisites for Authentication and Ciphering

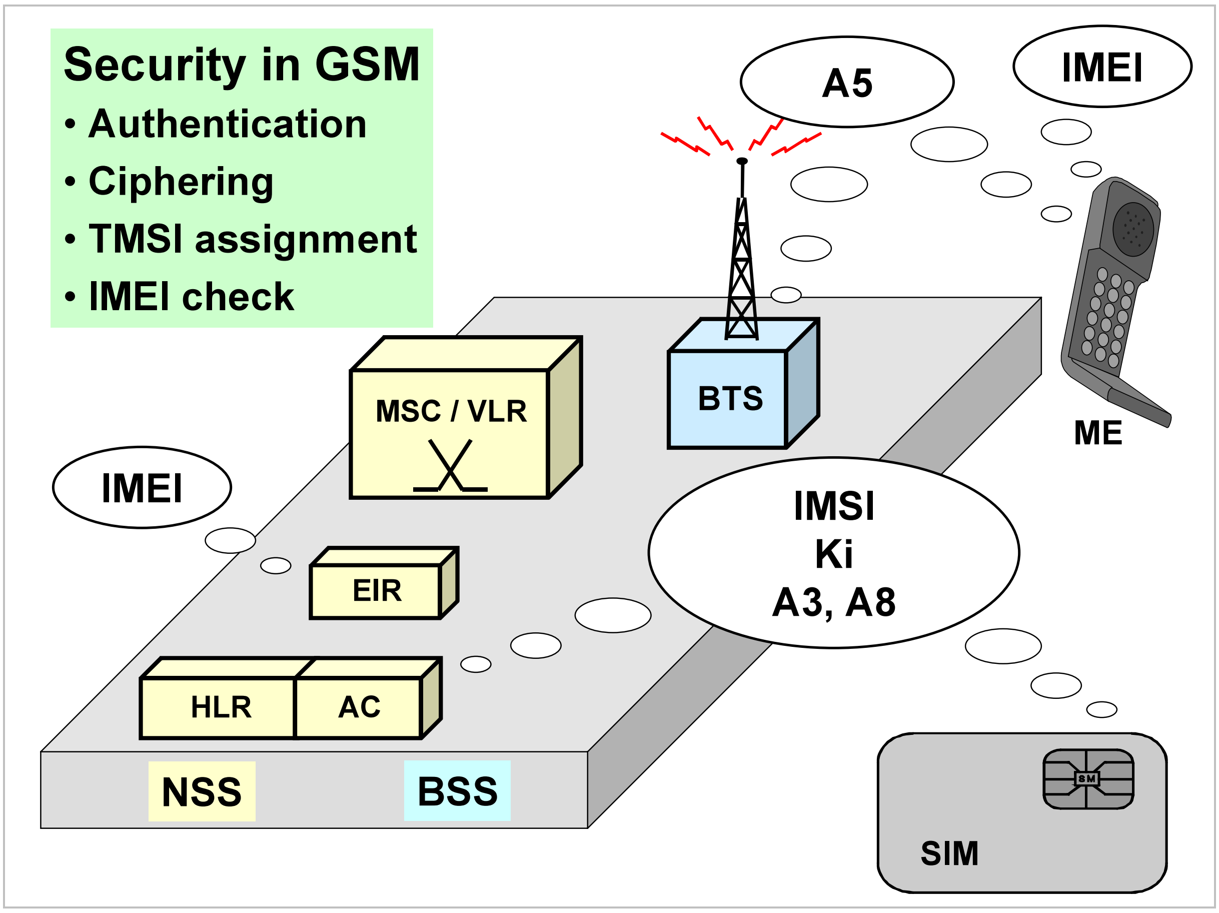
For authentication (proof of authorization) and ciphering, the Authentication Center **AC** and the **SIM** card are important.

For authentication and ciphering purposes AC and the SIM card store the following data:

- **IMSI** (International Mobile Subscriber Identity)
- **Ki** (Individual Subscriber Authentication Key)
- **A3, A8**: Algorithms for the creation of authentication and encipherment parameters.

IMSI, Ki, A3 and A8 are used to calculate the authentication parameters (**Triples**).

Further, for ciphering purposes another encipherment algorithm, **A5**, is stored in the SIM card. This algorithm can be found in the BTS on the fixed network side of the PLMN.



Security in GSM

- Authentication
- Ciphering
- TMSI assignment
- IMEI check

Fig. 4

2.2 Triples

The triples (authentication parameters) are produced in the Authentication Center AC and consist of:

- **RAND** (RANDom number)
- **SRES** (Signed RESponse): the reference value for the authentication
- **Kc** (Cipher Key): code for radio transmission encipherment.

The **calculation of a triple in the AC** occurs in the following manner:

- For the subscriber with a particular IMSI the reference value of authentication SRES is calculated by the algorithm A3 from the individual key Ki and the random number RAND produced by a random number generator.
- The cipher key Kc is calculated by the algorithm A8 from the individual key Ki and the random number RAND.
- RAND, Kc and SRES make together a complete triple.

At the request of the VLR, several triples are generated for each mobile subscriber in the AC and transferred to the VLR via the HLR on request.

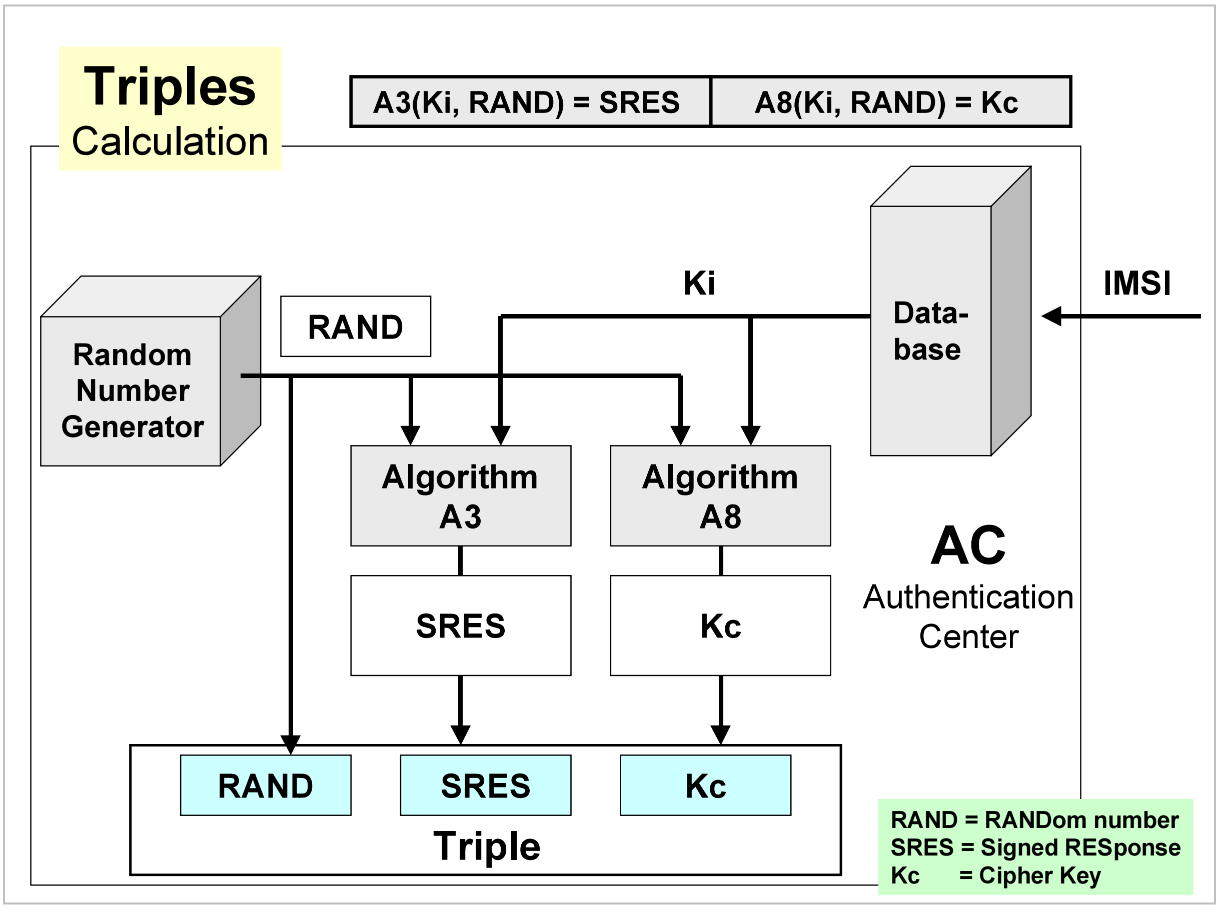

Triples
Calculation
A3(Ki, RAND) = SRES
A8(Ki, RAND) = Kc
Random Number Generator
RAND
Ki
Data-base
IMSI
Algorithm A3
Algorithm A8
SRES
Kc
AC
Authentication Center
RAND
SRES
Kc
Triple
RAND = RANDom number
SRES = Signed RESponse
Kc = Cipher Key

Fig. 5

2.3 Authentication

The authentication (authorization check) protects network operators and mobile subscribers against unauthorized use. The authentication is an essential part during the call setup of a MOC (Mobile Originating Call).

The authentication procedure is initiated by a VLR during:

- location registration (initial)
- call setup
- activation of connection-less supplementary services
- Short Message Service (SMS)
- location update with VLR change.

Authentication Procedure

1) VLR requests triples from the HLR
2) Triples are generated (see above) and are sent to VLR by the HLR
3) VLR sends RAND to the MS, SIM card calculates SRES using Ki, A3 and RAND
4) MS sends SRES back; VLR compares the SRES in the triple with the SRES sent by the MS; if they coincide, network access will be authorized, otherwise
5) access will be refused and the "Authentication Refused" message will be sent to the MS.

Authentication

basic sequence

with:

- Location Registration LR
- LUP with VLR change
- MOC / MTC / SMS
- Activation of connection-less supplementary services

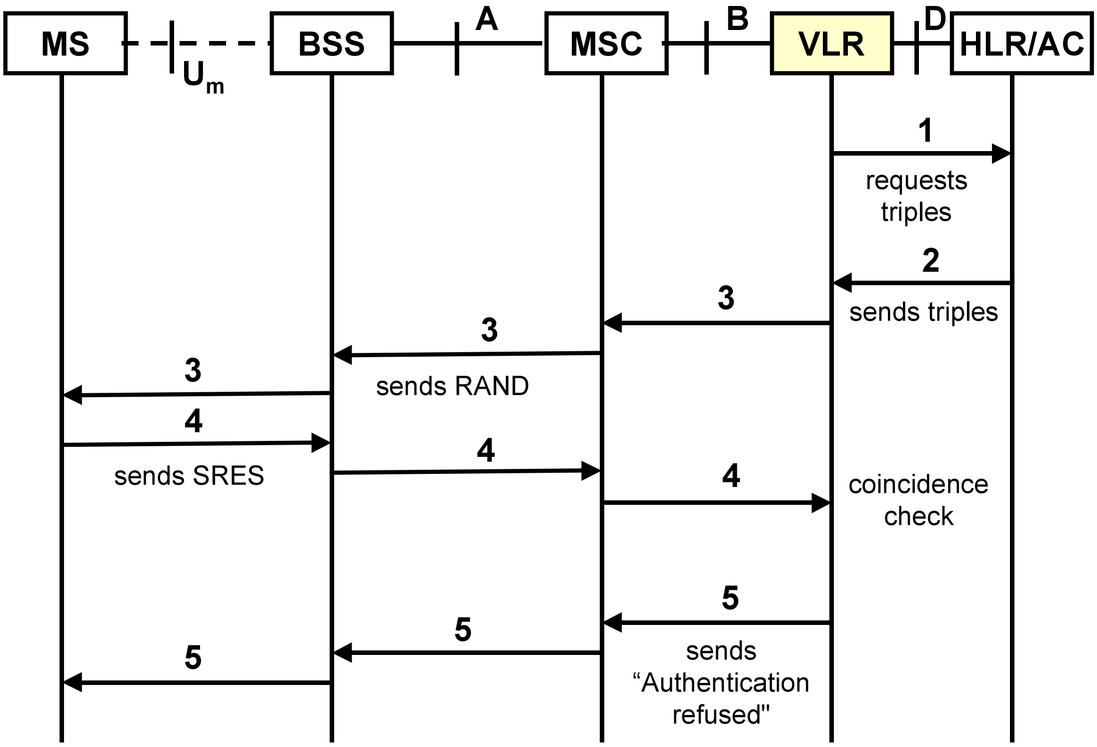


Fig. 6

2.4 Ciphering

Ciphering regards the security aspects of the information exchange between the Mobile Station (MS) and the Base Station (BTS) on the air interface Um. User information (speech/data) and signaling information are encrypted on the air interface Um (uplink and downlink). An exception is given by the initial signaling. The encryption and decryption procedures are carried out in the BTS and in the MS.

The GSM Recommendation (02.16) of Phase 2 states that up to 8 logically different encryption algorithms (incl. "no ciphering") should be used. The reason for this is the intention:

a):to assign different algorithms to different countries and

b):to provide MS, which do not use the A5-1 algorithm, with the possibility of roaming in different GSM-PLMN networks.

Currently 3 algorithms are defined:

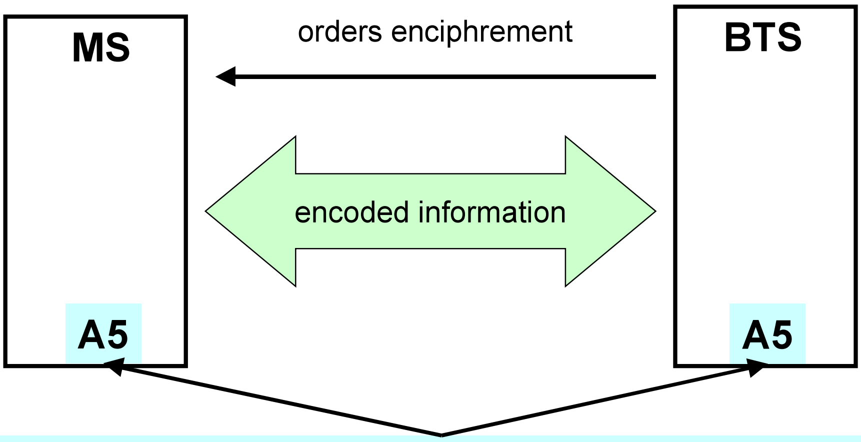
1. A5-0: no ciphering for COCOM countries1
2. A5-1: "strict" encipherment (originally MoU algorithm) for MoU-1 countries2, A5-1comes from GB; due to military usage, high security arrangements;
3. A5-2: "simplified" encipherment for MoU-2 countries (without COCOM countries).

[1] For the countries affected by the COCOM list, countries in which monitoring is compulsory, e.g. the former Eastern Block states (no export of so-called "sensitive technology")

[2] MoU-1 countries: countries which have signed the original Memorandum of Understanding (MoU)

Ciphering

- Prevents eavesdropping in Um
- Application in user information and signaling
- Exception: initial signaling



Rec. 02.16: max. 8 encoding algorithms

A5-0: no ciphering; COCOM countries
A5-1: "strict" enciphrement; MoU-1 countries
A5-2: "simple" enciphrement; MoU-2 countries (except COCOM)

Fig. 7

Encipherment Procedure

Transmitter/receiver must use the same encipherment algorithms.

In order to handle every encipherment procedure individually, the individual key Ki (stored in the SIM card and the AC) is used. Together with the encipherment algorithm A5, this should prevent interception.

The cipher key Kc is calculated by algorithm A8 from RAND and Ki.

The data are enciphered and deciphered together with Kc and the encipherment algorithm A5 (in MS and BTS).

To start the encipherment procedure, the network sends a start command to the MS. From this point onward, the MS begins to use the algorithm A5 together with cipher key Kc to encipher the data.

Encipherment and Decipherment Mechanism

One of the important advantages of digital transmission is the comparatively simple encipherment of the transmitted information. The type of information transmitted (speech, data, signaling) is irrelevant. Only the "normal burst" is enciphered.

The encipherment is achieved as follows:

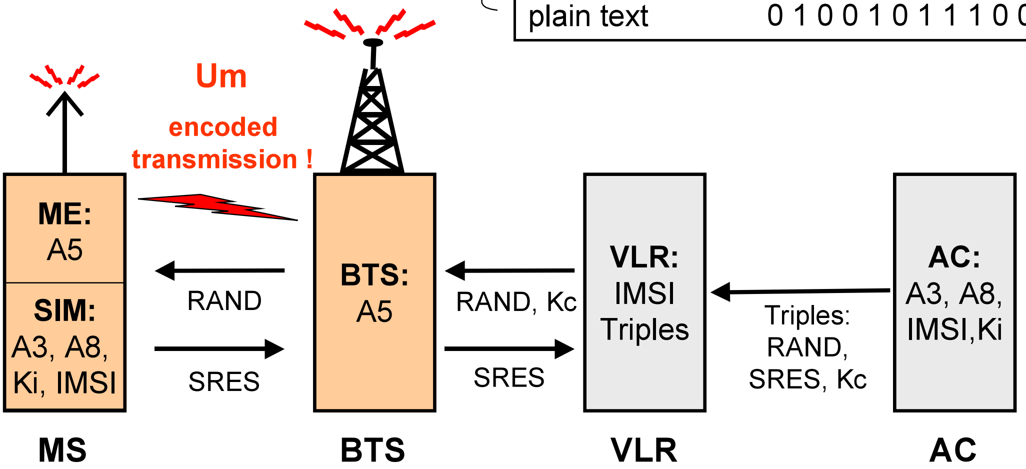
the bit sequence to be enciphered (all 114 "useful bits" of a normal burst) is connected to one of the enciphering bit sequences in a so-called "eXclusive OR" (XOR) operation.

Deciphering follows exactly the same scheme as enciphering, as the XOR operation yields the original values after double application of XOR.

The encipherment bit sequence is produced via the A5 algorithm by using Kc.

Ciphering & Authentication

	plain text	0 1 0 0 1 0 1 1 1 0 0 1...
XOR	ciphering seq.	0 0 1 0 1 1 0 0 1 1 1 0...
	ciphered text	0 1 1 0 0 1 1 1 0 1 1 1...
XOR	ciphering seq.	0 0 1 0 1 1 0 0 1 1 1 0...
	plain text	0 1 0 0 1 0 1 1 1 0 0 1...



Authentication:
A3(Ki, RAND) = SRES

Ciphering:
A8(Ki, RAND) = Kc
A5(Kc,TDMA-No.) = CS
text XOR CS = ciphered text

Ciphering:
A5(Kc,TDMA-No.) = CS
text XOR CS = ciphered text

Authentication:
SRES comparison

Authentication & ciphering:
generates RAND
A3(Ki, RAND) = SRES
A8(Ki, RAND) = Kc

CS: ciphering sequence

Fig. 8

2.5 TMSI Allocation

The encipherment protects the user from unauthorized interception. However the encipherment with Kc requires that the network is aware of the identity of the mobile subscriber with whom it is in contact. Thus the start phase of communication setup, when the identity of the mobile subscriber is still unknown, has to occur without use of a cipher. During this phase a third party may identify a subscriber and the desired method of communication.

In order to protect the identity of the subscriber in this phase, a temporary identification of the subscriber is distributed: the Temporary Mobile Subscriber Identity TMSI.

The TMSI is used instead of the International Mobile Subscriber Identity, which is stored permanently on the SIM card; it is stored temporarily on the SIM card and in the current VLR. The MS is usually identified with the TMSI. Single exception: the IMSI itself must be used during first registration in PLMN (location registration).

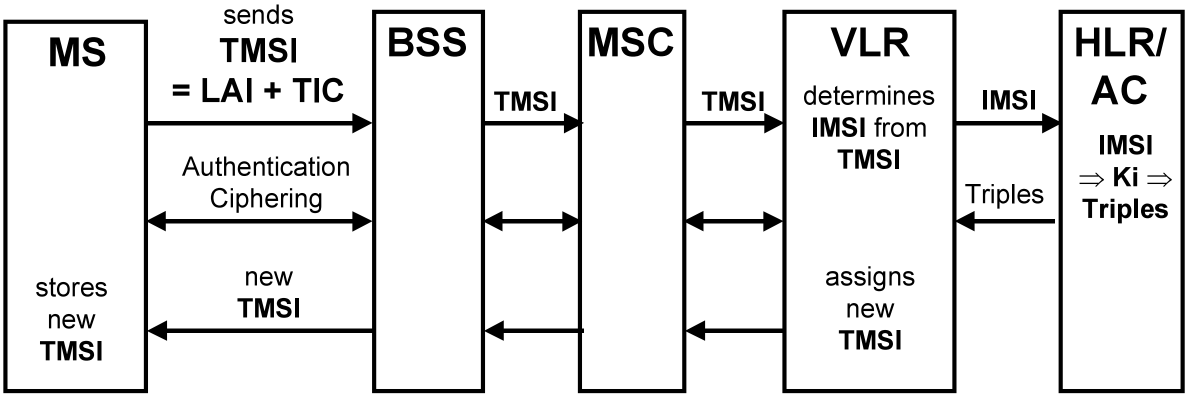
The TMSI is used in connection with the LAI, i.e. to identify the location area. The TMSI may, in principle, be regarded as consisting of two components: the LAI and a TMSI code, which is briefly called TIC. Its structure is chosen by the operator.

The storage and assignment, i.e. the "management" of the TMSI, occurs in the VLR. The assignment of a TMSI occurs for the first time, when the MS is initially registered in a Location Area (LA). The erasure of the TMSI occurs when the VLR area is left, after the MS has been registered in a new VLR area. The erasure of the old TMSI on the SIM card occurs by overwriting with a new TMSI. The new VLR receives the IMSI by referring back to the old VLR after the old TMSI was sent by the MS. This is possible as the LAI is always transmitted together with the TMSI or as a component of the TMSI together with the TIC (i.e. as LAI + TIC).

Further, a new assignment of a TMSI usually occurs within the framework of every new call setup. Thus the frequent changing of the subscriber identity makes the detection/identification of a subscriber via the radio interface substantially more difficult.

TMSI Allocation

- Network requires subscriber identification for call setup
- Identity necessary for triples calculation
- Transmission of identity uncoded
- TMSI prevents subscriber identification
- New TMSI with VLR change & usually at call setup



MS

sends **TMSI = LAI + TIC**

BSS

TMSI

MSC

TMSI

VLR

determines **IMSI** from **TMSI**

IMSI

HLR/ AC

IMSI ⇒ Ki ⇒ Triples

Authentication Ciphering

Triples

stores new **TMSI**

new **TMSI**

assigns new **TMSI**

For LA change with MSC/VLR change:

- New VLR identifies old VLR by TMSI
- Subscriber data: query of old VLR

Fig. 9

2.6 IMEI Check

In contrast to authentication, encipherment and TMSI issue, the check of international mobile equipment identity IMEI is not obligatory, but depends on the operator.

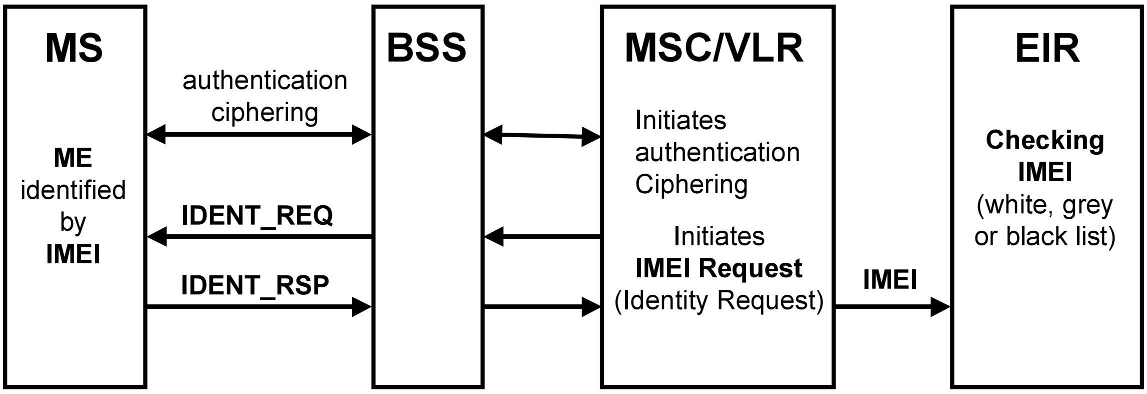
IMEI check serves to identify stolen, expired or faulty mobile equipment. A IMEI clearly identifies a particular mobile device and contains information about the place of manufacture, type approval code and the serial number of the equipment.

If a IMEI check in the PLMN of an operator is intended, the Mobile Station MS will be required to submit the IMEI (identify request) during call setup after the ciphering command of the MSC/VLR was delivered. The mobile station sends IMEI to the network as identity response. The IMEI is routed to the EIR of the PLMN. A check occurs here to find out whether the IMEI is registered on the black or gray list, i.e. whether the MS is barred from further use of the PLMN, or whether it is to be kept under observation.

IMEI Check

- Recognizing stolen, expired and faulty MEs

TAC	FAC	SNR	SVN
Type Approval Code	Final Assembly Code	Serial Number	Software Version Number
24 Bit	8 Bit	24 Bit	(spare) 4 Bit



MS

ME identified by IMEI

authentication ciphering

IDENT_REQ

IDENT_RSP

BSS

MSC/VLR

Initiates authentication Ciphering

Initiates **IMEI Request** (Identity Request)

IMEI

EIR

Checking IMEI (white, grey or black list)

Fig. 10

3 Location Registration/Location Update

The registration of the location of the mobile station enables the mobile subscriber to move freely within the GSM service area, without losing the ability to build up connections or to receive information (speech/data), i.e. to be reachable. The corresponding location data are stored in the currently responsible Visitor Location Register (VLR), whose identity is stored in the Home Location Register (HLR).

The purpose of **location registration** and/or **location update** is to supply/update subscriber and location information to set up connections for the mobile subscriber (MTC), supplementary service functions, etc. For provisioning this information, the PLMN must trace the location area of the MS.

A location update only occurs when there is currently no conversation taking place!

3.1 Location Update Types

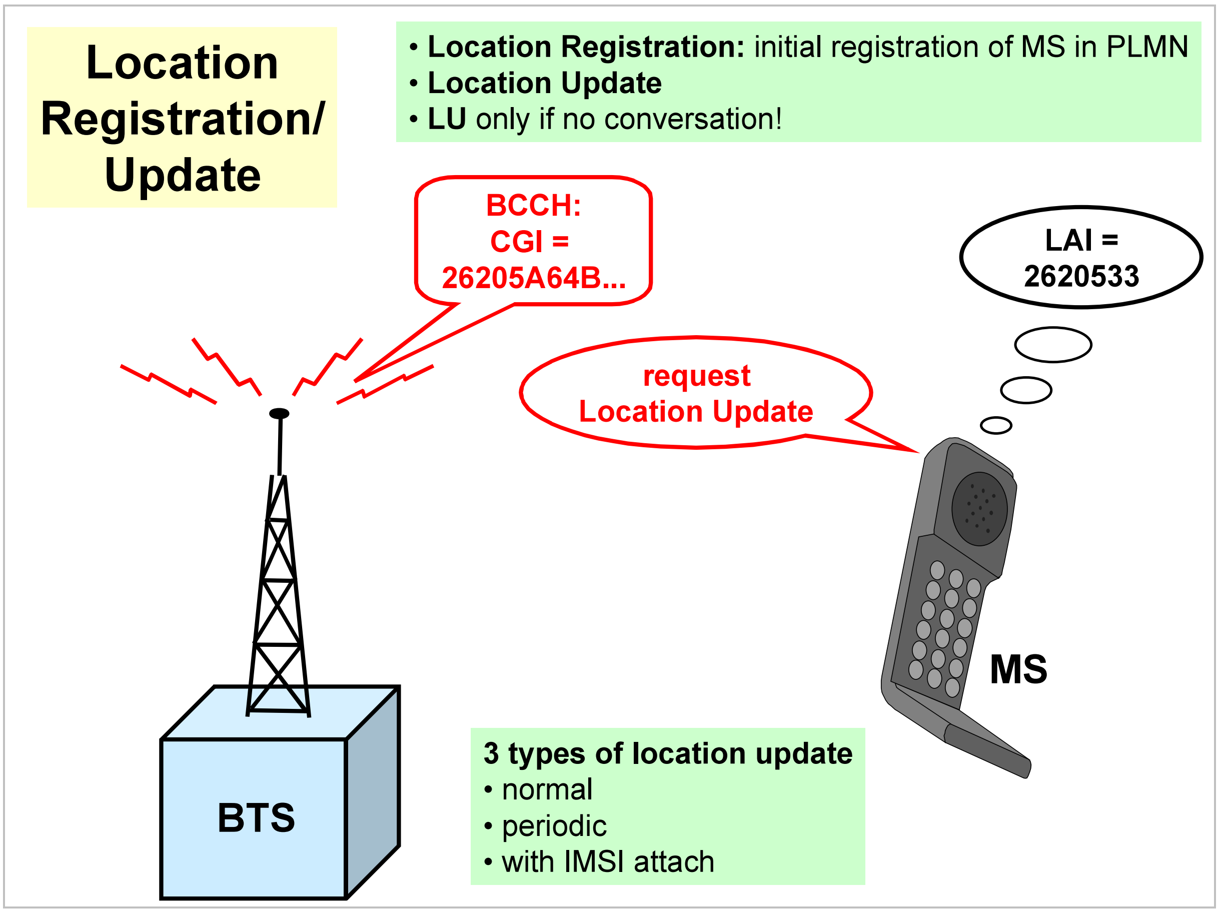
There are 3 kinds of Location Update (LU):

1) **Normal Location Update** is initiated by a MS, when the LAI (temporally) stored on the SIM card differs from the LAI of the best cell (strongest signal). This occurs e.g. when the MS moves from one LA (Location Area) to another, when the MS has lost the current location information and when the MS is switched on and the stored LAI does not correspond with the current location.

2) **Periodical Location Update** is initiated by a MS at regular intervals.

3) **Location Update with IMSI attach** occurs when a MS is "activated" again.

Explanation of the term **"IMSI attach"**: if a MS is deactivated the MS can indicate this to the PLMN. The subsequent procedure is described as IMSI detach. This information is necessary for rejection of incoming calls (MTC), without occupying radio resources. When the MS is activated again, this is displayed by the **IMSI attach** procedure.



Location Registration/ Update

- **Location Registration:** initial registration of MS in PLMN
- **Location Update**
- **LU** only if no conversation!

3 types of location update
- normal
- periodic
- with IMSI attach

Fig. 11

3.2 Location Registration/Location Update Procedure

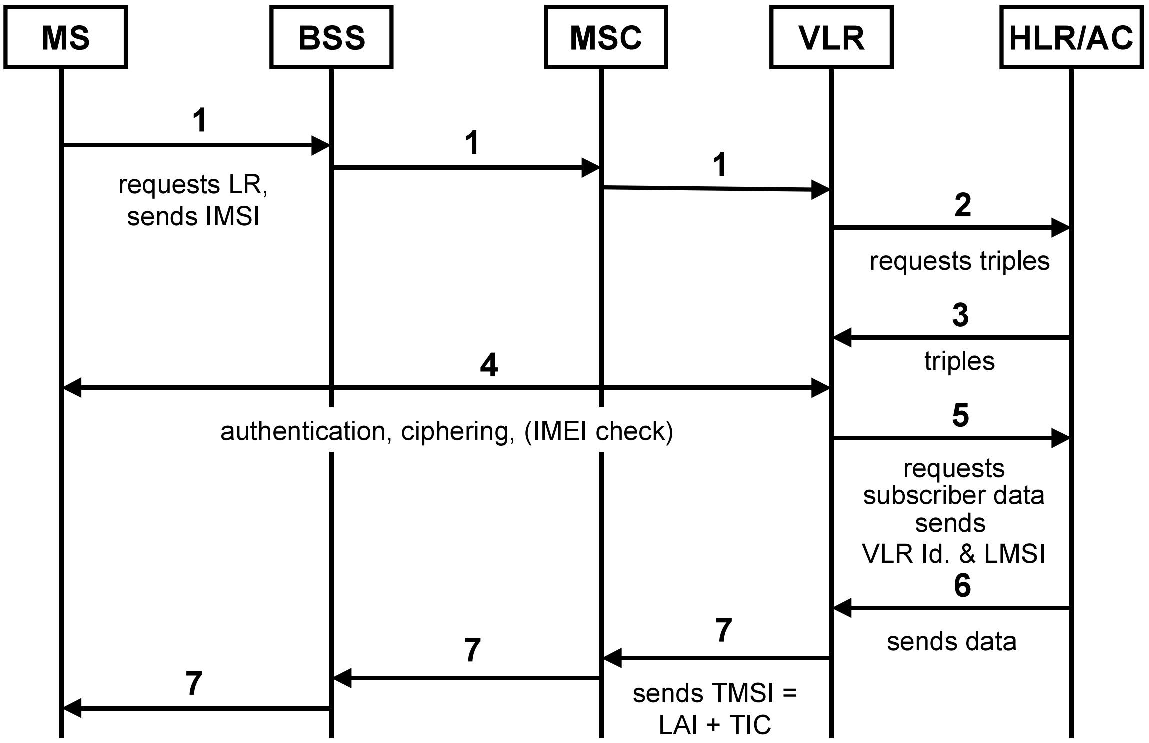
Location Registration

- SIM does not contain LAI (new card) or foreign LAI (PLMN change)
- MS requests location registration with IMSI (1): Location Request
- VLR stores IMSI and requests triples from AC via the HLR (2)
- AC supplies several triples via HLR (3)
- VLR stores triples and initiates authentication procedure, ciphering and, if necessary, an IMEI check (4)
- If the authentication, ciphering and IMEI check are successful, the VLR requests subscriber data from HLR and transmits the VLR identity[3] and a LMSI (5)
- HLR stores VLR identity and LMSI and transmits the requested subscriber data to the VLR (6)
- VLR stores the subscriber data and assigns a TMSI to the subscriber
- VLR transmits TMSI to the MS (7)
- TMSI and new LAI are stored on SIM card.

[3] International signal number of the VLR; is needed in the case of MTC.

Location Registration LR

basic sequence



MS

BSS

MSC

VLR

HLR/AC

1

requests LR,
sends IMSI

1

1

2

requests triples

3

triples

4

authentication, ciphering, (IMEI check)

5

requests
subscriber data
sends
VLR Id. & LMSI

6

sends data

7

sends TMSI =
LAI + TIC

7

7

Fig. 12

Location Update Procedure (here: with VLR change)

- SIM contains incorrect LAI
- Location Request: MS requests location update with old TMSI (1)
- The new VLR receives TMSI, recognizes that TMSI has been allocated by another VLR. VLR requires IMSI and other subscriber data in order to complete location update
- VLR uses the first component of the TMSI, the LAI, to identify the previous VLR from which requests the IMSI as well as, if possible, unused triples (2); the old VLR supplies this data (2)
- The new VLR informs the HLR about the location update with MSC/VLR change, provides the VLR identity and the LMSI; if necessary new triples can be requested from the HLR/AC (3)
- The HLR confirms the information, supplies the subscriber data and, if necessary, triples (4)
- and informs the old VLR, that it may now erase the subscriber data (5)
- The VLR now realizes authentication, ciphering and IMEI check, if required (6)
- The VLR supplies a new TMSI (7).

Note: if (2) is not possible or an IMSI cannot be received by a the new VLR, the VLR initiates a MS identifying procedure with the MS itself (LR).

Note: in the case of a location update without a MSC/VLR change, no contact between VLR and HLR is necessary. The HLR only knows the VLR area of the MS, not the location area.

Location Update Procedure LUP

(incl. MSC - VLR change) basic sequence

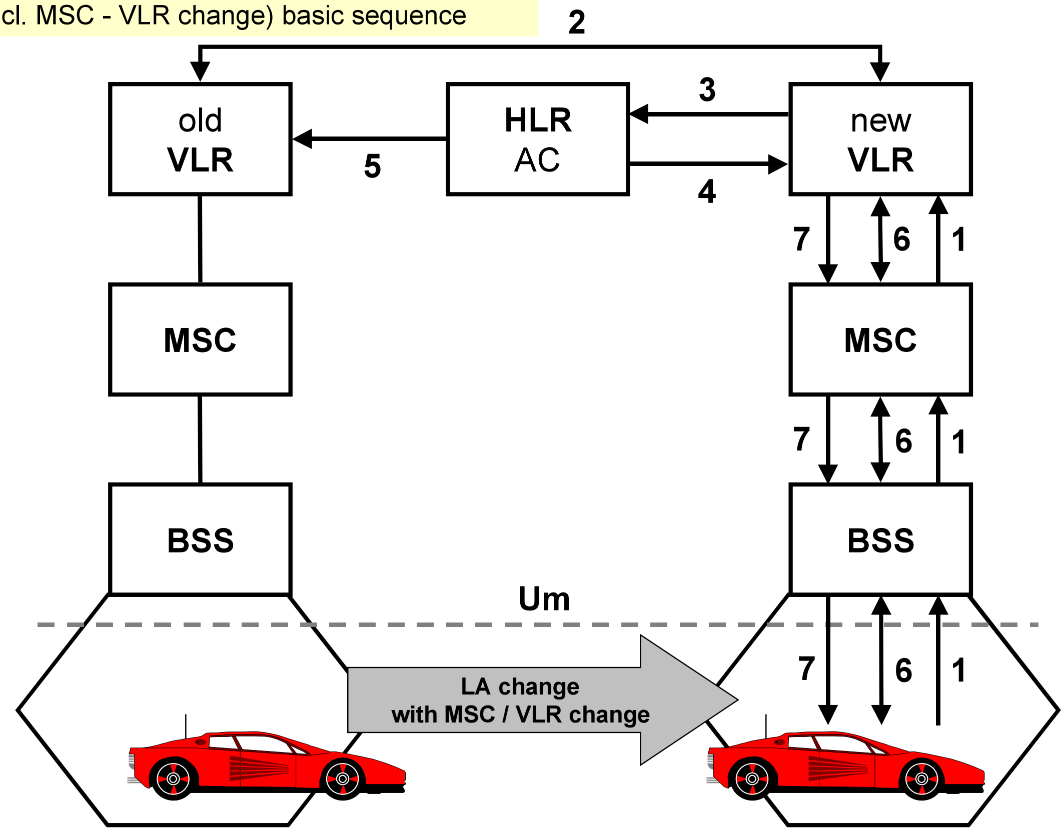


Fig. 13

4 Call Setup

Mobile Originating Call MOC

Calls which are initiated by the MS as a calling party.

- Call from a MS registered in VLR:

  the incoming call is routed according to the dialed number. When the connection is finished, the MSC sends the related charging information to the HLR, to a billing unit and/or stores it on magnetic tapes or disks.

- Call from a MS not registered in VLR:

  if the VLR of a MSC receives a request for call setup from a MS, that is not registered in the VLR, the VLR starts a location update to the HLR. The response is send as parameters relating to category, service(s) and restraints of the subscriber. Then the connection is set up as normal.

Mobile Terminating Call MTC

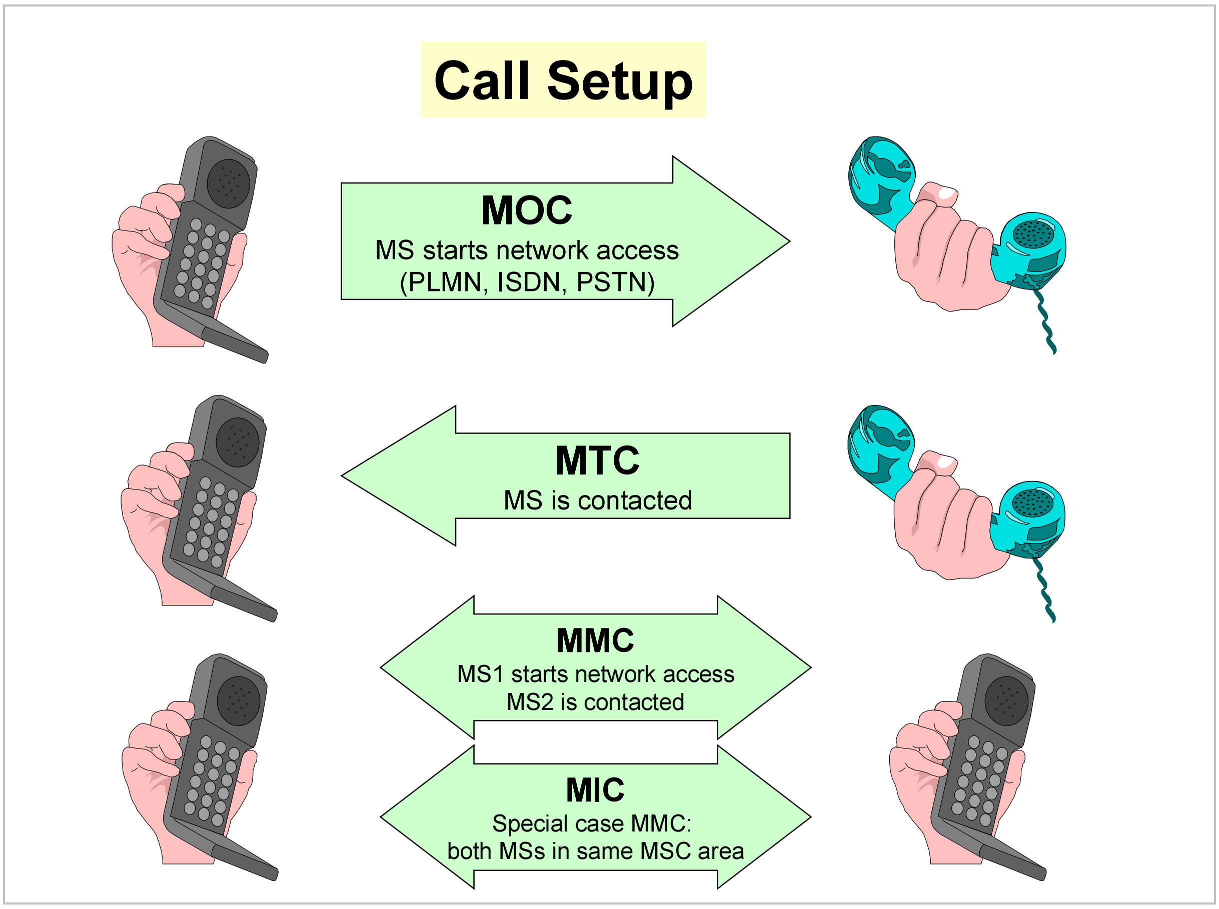
Calls which are sent to the MS as the called party. The call is routed according to the location data received from the HLR to the serving MSC.

Mobile Mobile Call MMC

Calls between two mobile subscribers; MMC thus consists of the execution of a MOC and a MTC one after the other.

Mobile Internal Call MIC

A MMC special case: both MSs are in the same MSC area, possibly even in the same cell.



Call Setup

MOC
MS starts network access
(PLMN, ISDN, PSTN)

MTC
MS is contacted

MMC
MS1 starts network access
MS2 is contacted

MIC
Special case MMC:
both MSs in same MSC area

Fig. 14

4.1 Mobile Originating Call MOC

- Mobile subscriber (calling party) dials a number
- MS requests provisioning of a traffic channel
- VLR carries out authentication
- VLR assigns new TMSI
- VLR checks authorization of subscriber for requested service: Subscription Check
- MSC sets up a connection to BSC and to requested number (called party)

(1) Channel request

(2) Sending of subscriber identity (TMSI or IMSI)

(3) Initiation of authentication procedure (request for triples)

(4) Authentication procedure and encipherment (possible IMEI check and new TMSI)

(5) MS sends call setup information (number of requested subscriber)

(6) MSC requests connection information from the VLR; VLR sends MS data back

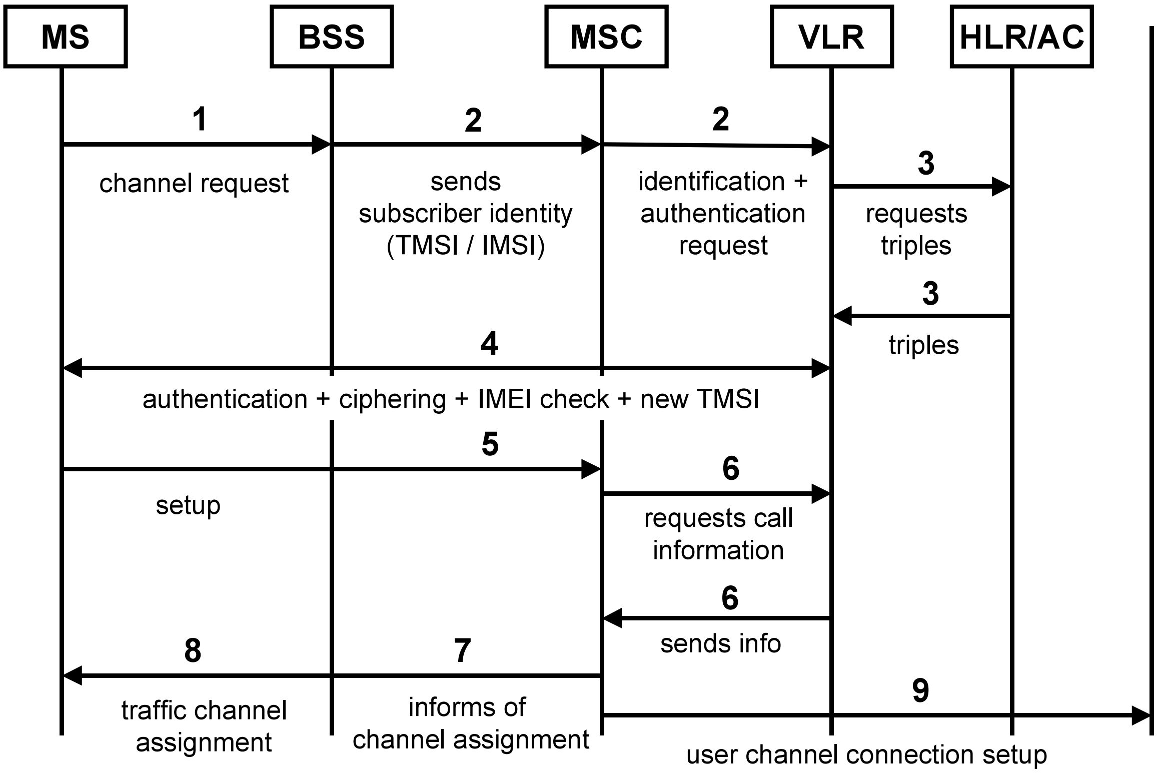
(7) MSC informs BSC of channel assignment

(8) BSC supplies a traffic channel (TCH)

(9) MSC sets up the connection to requested number (called party).

Mobile Originating Call MOC

basic sequence



MS BSS MSC VLR HLR/AC

1 channel request

2 sends subscriber identity (TMSI / IMSI)

2 identification + authentication request

3 requests triples

3 triples

4 authentication + ciphering + IMEI check + new TMSI

5 setup

6 requests call information

6 sends info

7 informs of channel assignment

8 traffic channel assignment

9 user channel connection setup

Fig. 15

4.2 Mobile Terminating Call MTC

In the case of a MTC, another subscriber (from PSTN, ISDN, their own or other PLMN) is trying to reach a mobile subscriber. The main difference in the procedure is the routing to the MSC visited by the subscriber, Visited MSC (VMSC). In the case of external contact the Gateway MSC (GMSC) is responsible for the further procedure, in the case of internal calls MMC/MIC a different/the same MSC.

In the following example, a typical case of a call setup from an external network is described.

- other subscriber dials MSISDN
- user connection: original exchange to GMSC

(1) call request to GMSC: GMSC identifies HLR from MSISDN

(2) GMSC requests **MSRN**[4] from HLR: **Interrogation**[5]

(3) HLR sends IMSI to VLR and requests MSRN

(4) VLR sends MSRN via HLR to GMSC

(5) GMSC routes the connection request to VMSC

(6) VMSC requests data (LAI, TMSI) for call setup from VLR

(7) VLR sends these data

(8) VMSC knows LAI, but not the cell; therefore the searched MS is called via all BTSs of the LA: **Paging**

(9) MS responses the paging: localization of current BTS

(10) authentication, ciphering, if necessary, IMEI check, new allocation of TMSI

(11) the call is switched through.

[4] MSRN (Mobile Station Roaming Number): Number, that enables the GMSC to transfer an incoming call to the corresponding VMSC. MSRN = CC + NDC + temporary Subscriber Number SN (is released again after paging).

[5] Interrogation: Request of a MSRN from VLR associated with VMSC (via HLR).

Mobile Terminating Call MTC

basic sequence

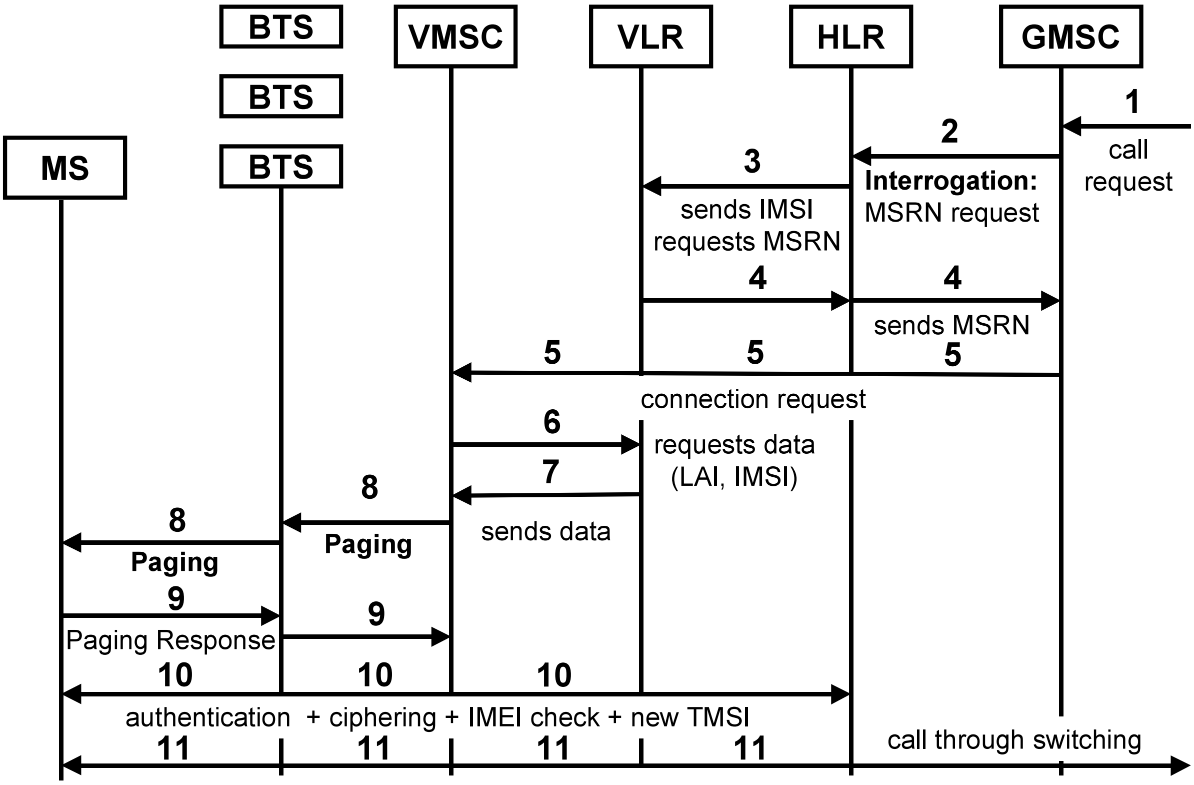


Fig. 16

4.3 Mobile Mobile Call MMC/Mobile Internal Call MIC

Mobile Mobile Call MMC

MMC stands for Mobile Mobile Call, i.e. a conversation between two mobile subscribers. MM. thus consists of the execution of a MOC (for the calling party) and a MTC (for the called party) one after the other.

For the call setup of a MMC the same procedures are valid as in the case of MOC and MTC for the call setup between a mobile subscriber and a fixed subscriber. In the case of PLMN internal MMC, instead of inquiring the GMSC the MSC, visited by the calling party, queries the HLR of the called party.

Mobile Internal Call MIC

A special case in the MMC is represented by the MIC (Mobile Internal Call), in which both mobile subscribers are in the same MSC area or even in the same cell. No shortening of the procedure takes place here.

MOC and MTC procedures are executed after each other and two different MSCs (VMSC from subscriber 1 and 2) are simulated via a trunk-loop-function of the MSC.

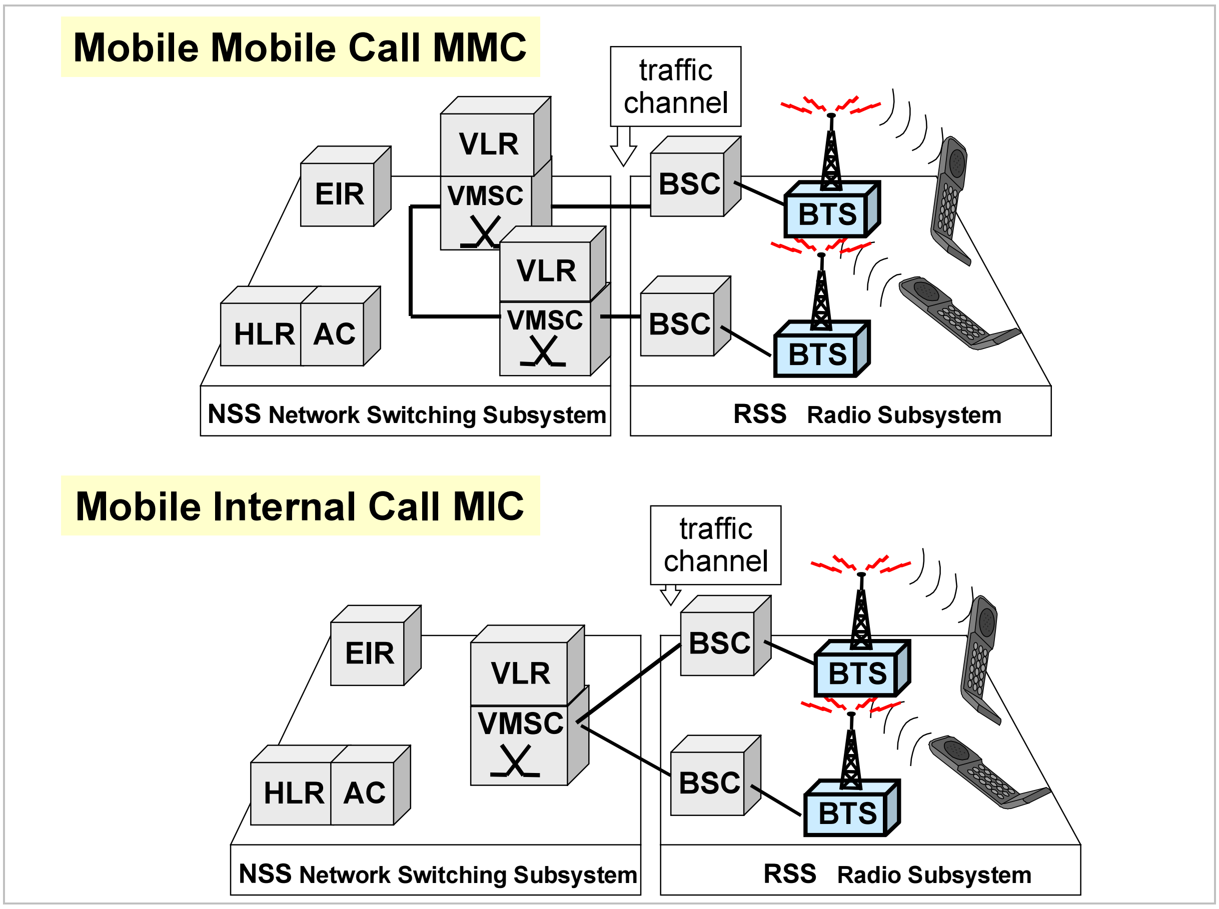

Mobile Mobile Call MMC
traffic channel
VLR
EIR
VMSC
VLR
VMSC
HLR
AC
BSC
BTS
BSC
BTS
NSS Network Switching Subsystem
RSS Radio Subsystem
Mobile Internal Call MIC
traffic channel
EIR
VLR
VMSC
HLR
AC
BSC
BTS
BSC
BTS
NSS Network Switching Subsystem
RSS Radio Subsystem

Fig. 17

4.4 OACSU (Off Air Call Set Up)

The OACSU represents a call setup procedure in which the traffic channel (TCH), via the radio interface Um, is allocated after the called subscriber (called party) has answered. This allows a particularly good utilization of the traffic channels. The OACSU can be applied in the case of overloading of the radio interface, when during the call setup (only signaling) all traffic channels are occupied. Because it is highly probable that, until the called subscriber answered, another subscriber ends his call, a traffic channel will be available and can be assigned to the subscriber.

OACSU can theoretically be used for MOC and MTC.

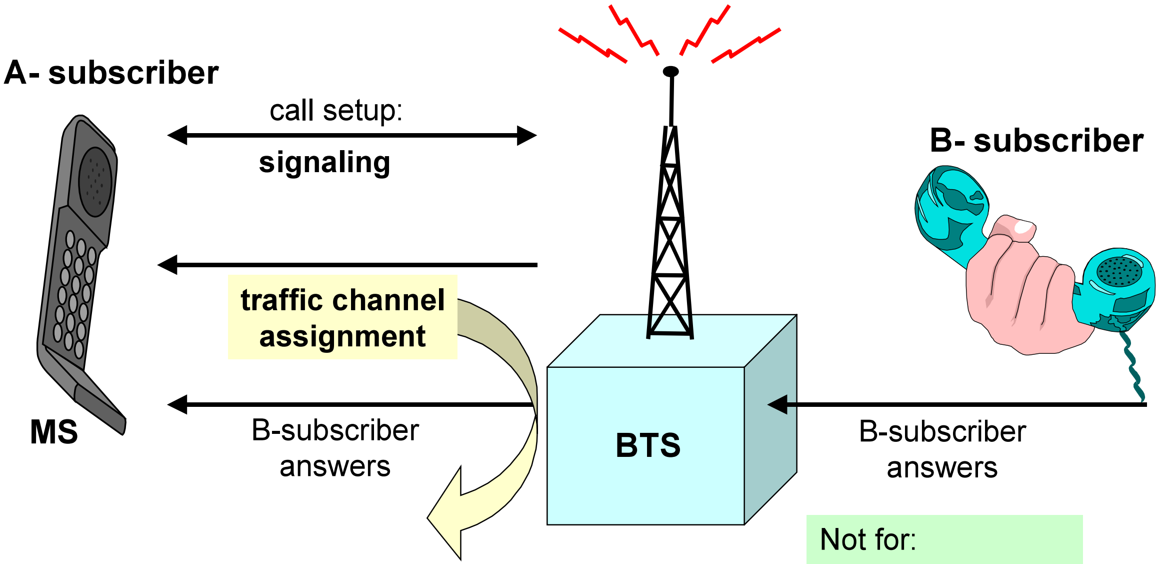
In the case of OACSU so-called partial connections are set up. After the TCH is assigned, the partial connection is completed. The delay of the TCH assignment is monitored by a timer. When the time frame has run out, a TCH is assigned. The OACSU can lead to an announcement for the called party, if he/she picks up the phone before the delayed assignment of the TCH.

Restraints for OACSU:

- not for international calls
- not for data connection
- not for emergency calls.

OACSU
Off Air Call Set Up

- Delayed call setup
- No traffic channel assignment until B-subscriber answers / timer expires



A- subscriber

call setup:

signaling

traffic channel assignment

MS

B-subscriber answers

BTS

B- subscriber

B-subscriber answers

Not for:

- International calls
- Data connection
- Emergency calls

Fig. 18

5 Handover (HO)

5.1 Handover Types

Handover (HO) refers to the changing of a physical channel during a current connection. There are various types of handover:

- **Intra-Cell Handover**: in the case of intra-cell handover, a physical channel within a cell is changed. A reason for this may be an interference in the frequency currently being used. The internal channel change consists of a change in frequency and/or time slot and therefore differs from the feature "frequency hopping", in which the frequency is changed after a certain algorithm, but the time slot is never changed. The intra-cell handover is realized internally in the BSS, i.e. the BSC decides without MSC involvement. Only the message "handover performed" is sent to the MSC after the handover.
- **Intra-BSS Handover**: an intra-BSS handover is carried out between two cells of the same BSS. The procedure is decided and performed by the BSC (no MSC involvement). The MSC is informed only after the handover ("handover performed").
- **Intra-MSC Handover**: an intra-MSC handover is a handover between two BSSs of one MSC. The MSC switches between the two BSCs.
- **Inter-MSC Handover**: a inter-MSC handover affects handovers which include at least two MSCs. Inter-MSC handovers are one of the most complicated GSM procedures, in particular in the case of MSCs made by different manufacturers. One has to distinguish between "basic handover" and "subsequent handover".
- **Basic Handover**: if, during a running connection, a MS changes for the first time from the area of an MSC (A) to the area of a MSC (B), this is described as Basic Handover.
- **Subsequent Handover**: if, during the same connection, the MS also leaves the MSC (B) area and moves into the area of a further MSC (C) or returns to the area of the old MSC (A), this follow-on handover is called Subsequent Handover. The handovers are controlled by the original MSC (MSC (A) = Anchor MSC). The connection MSC (A) - MSC (B) is set off when the connection MSC (A) -MSC (C) is successfully set up.

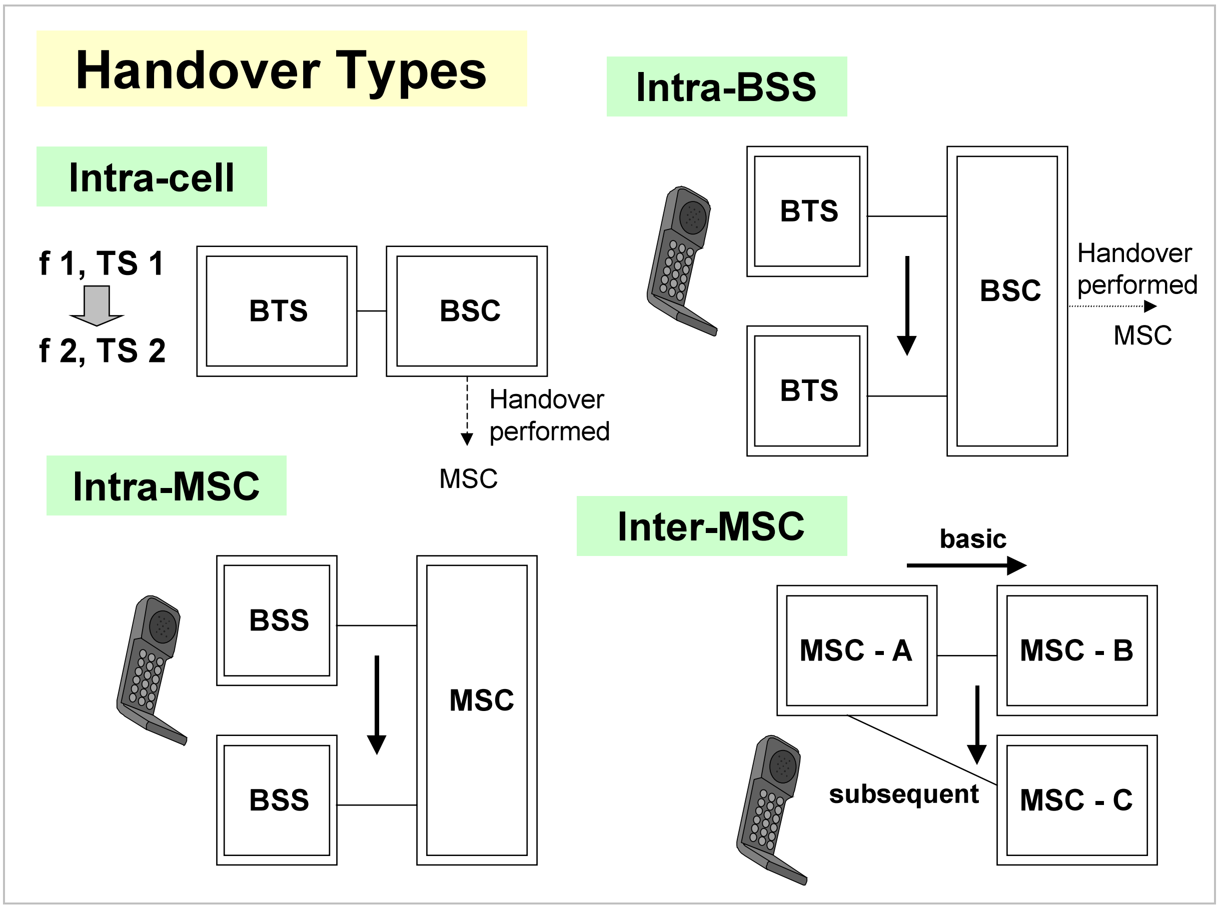

Handover Types
Intra-cell
f 1, TS 1
f 2, TS 2
BTS
BSC
Handover performed
MSC
Intra-BSS
BTS
BTS
BSC
Handover performed
MSC
Intra-MSC
BSS
BSS
MSC
Inter-MSC
basic
MSC - A
MSC - B
subsequent
MSC - C

Fig. 19

5.2 Handover Procedure

The handover algorithm is based on periodically measurements of MS and BTS concerning the strength and quality of the received signals. The initiation of a handover (HO) is caused by:

- Downlink measurements (DL): performed by the MS and periodically transmitted via the BTS to the BSC. The MS measures quality and strength of the connection and the strength of the serving BTS and that of the surrounding BTSs.
- Uplink measurements (UL): carried out by the BTS. The BTS measures quality and strength of the connection as well as the distance MS - BTS (Timing Advance TA).

The decision, whether a handover is necessary, is determined by the comparison between the current measured values and the threshold values. The threshold values are previously specified and are based on the evaluation of previous measurement processes. If an inter-cell handover is initiated, the criterion of availability of surrounding cells is used to set up a list of suitable handover destinations in a declining order of priority. This list forms the basis for the final handover decision that is carried out by the BSC or by MSC.

Handover Criteria

1) Strength of the received signal (UL and DL)

2) Quality of the received signal (UL and DL)

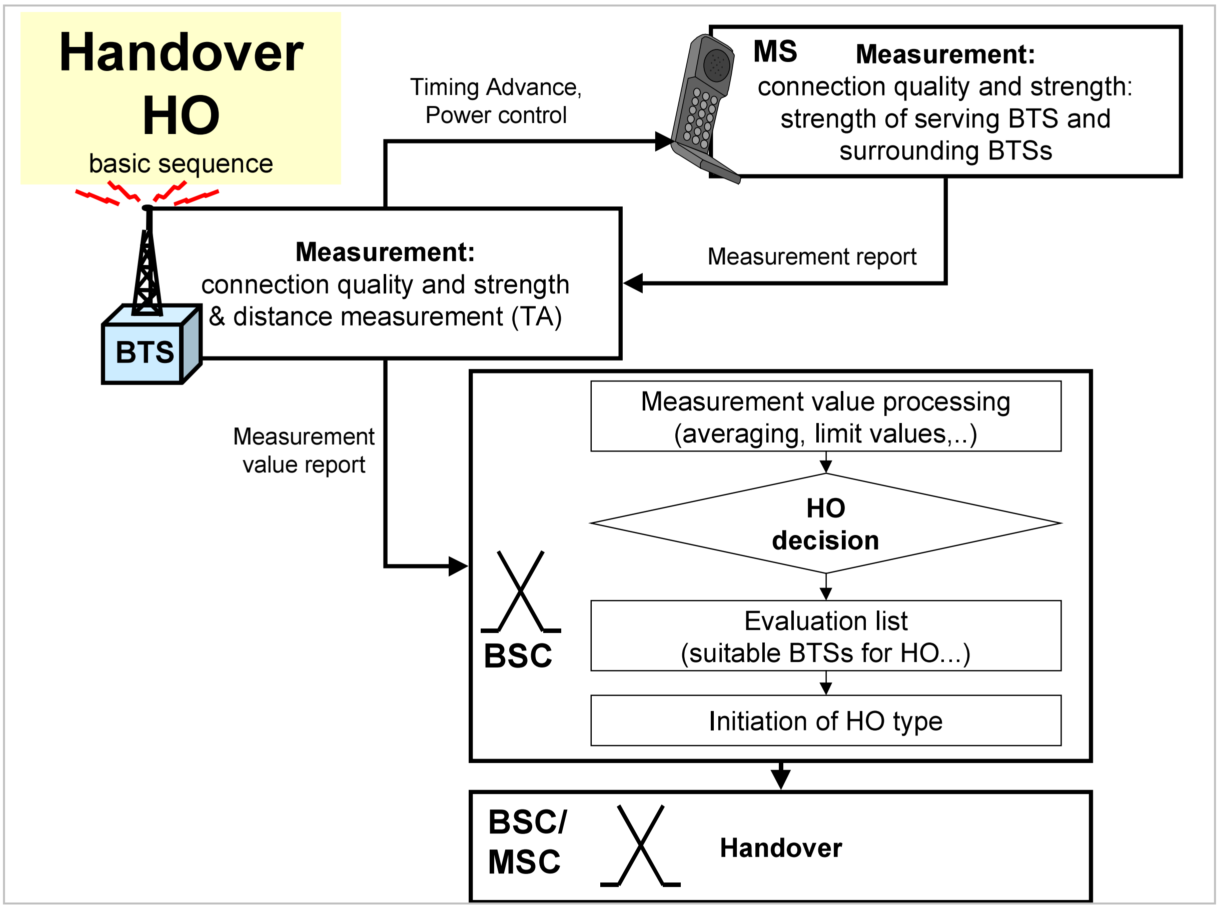
3) Distance MS - BTS (Timing Advance, UL)

4) Signal strength of suitable surrounding cells (UL, BCCH)

5) Interferences that decrease the signal quality (UL and DL).

1) - 4) Is an inter-cell handover required?

5) Is an intra-cell handover required?



Handover HO

basic sequence

Timing Advance, Power control

MS **Measurement:** connection quality and strength: strength of serving BTS and surrounding BTSs

Measurement report

Measurement: connection quality and strength & distance measurement (TA)

BTS
Measurement value report
BSC
Measurement value processing (averaging, limit values,..)
HO decision
Evaluation list (suitable BTSs for HO...)
Initiation of HO type
BSC/ MSC
Handover

Fig. 20

5.3 Handover Functional Sequence

1. Phase: the BSC decides that a handover is necessary.
2. Phase: a second connection is built up parallel to the existing connection.
3. Phase: the MS switches over to the new connection.
4. Phase: the original connection is released.

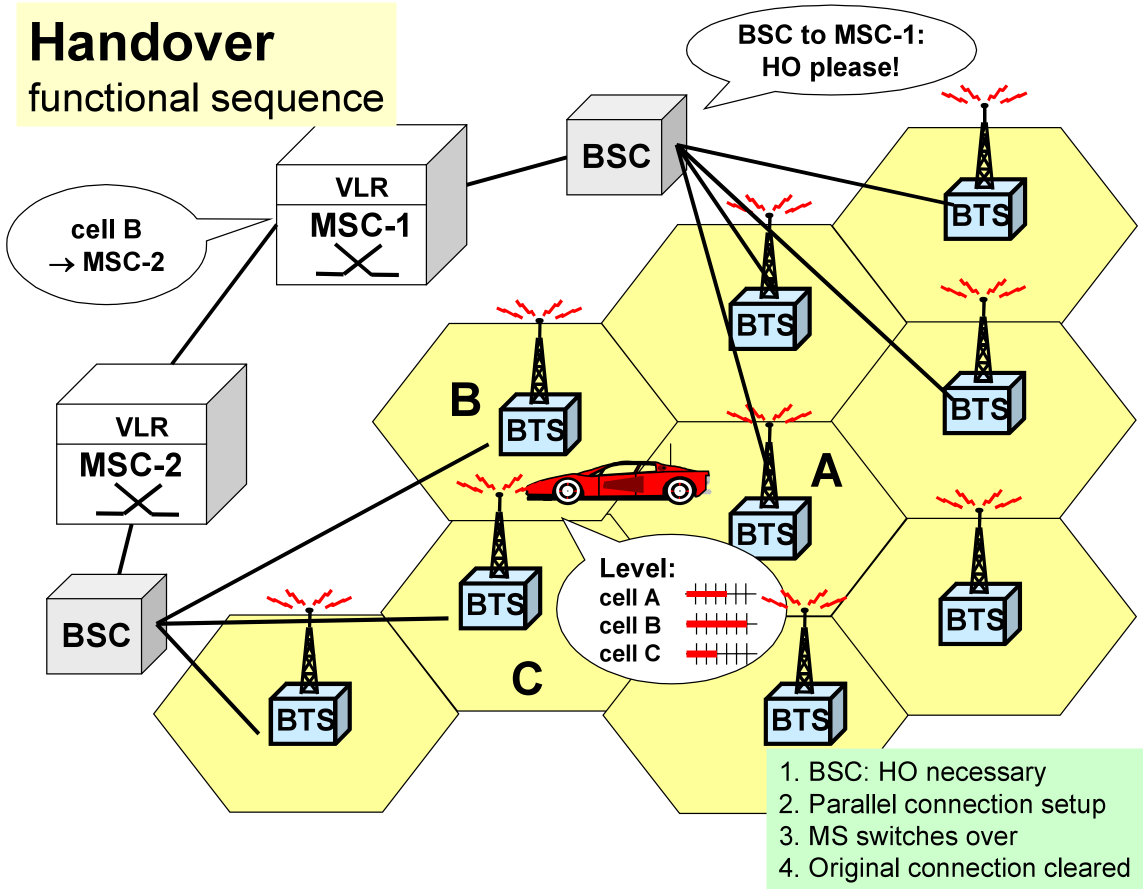
Example: Inter-MSC Handover (Basic Handover)

1. Phase:
   during an existing connection, the MS permanently measures the receive level and the receive quality of the serving cell and the receive level of the surrounding cells. The results are transmitted to the BSC, which initiates a handover, if another cell offers a better signal quality, i.e. subscriber goes from cell A to B. The BSC recognizes, that a handover is necessary which needs to be controlled by a MSC and informs MSC-1.
2. Phase:
   the MSC-1 requests a Handover Number (HOVN) from MSC-2 and informs MSC-2 about cell B. MSC-2 requests a HOVN from the VLR and provisioning of radio channels from BSC[6]. The information about the radio channel and the HOVN are sent back to the MSC-1.
3. Phase:
   the MSC-1 can set up the connection to the MSC-2 with the HOVN. The connection is completed up to the BTS. The MSC-1 informs the MS about the new radio channel and requests the switchover.
4. Phase:
   the connection to the old BTS is released.

[6] If no radio resource is available in the new BTS, then the handover procedure is aborted or, if necessary, put into the queue. In this case, the old MS-BTS connection is not released.

Handover

functional sequence



1. BSC: HO necessary
2. Parallel connection setup
3. MS switches over
4. Original connection cleared

Fig. 21

6 Emergency Call

The (basic) teleservice "emergency call" uses the method of the Mobile Originating Calls (MOC).

The mobile subscriber starts this service either by using a SOS key or by dialing an emergency service number.

The BSS always delivers the geographic location of the emergency call to the MSC. Depending on this origin, the emergency connection is then transmitted from the MSC to the regionally responsible emergency call exchange.

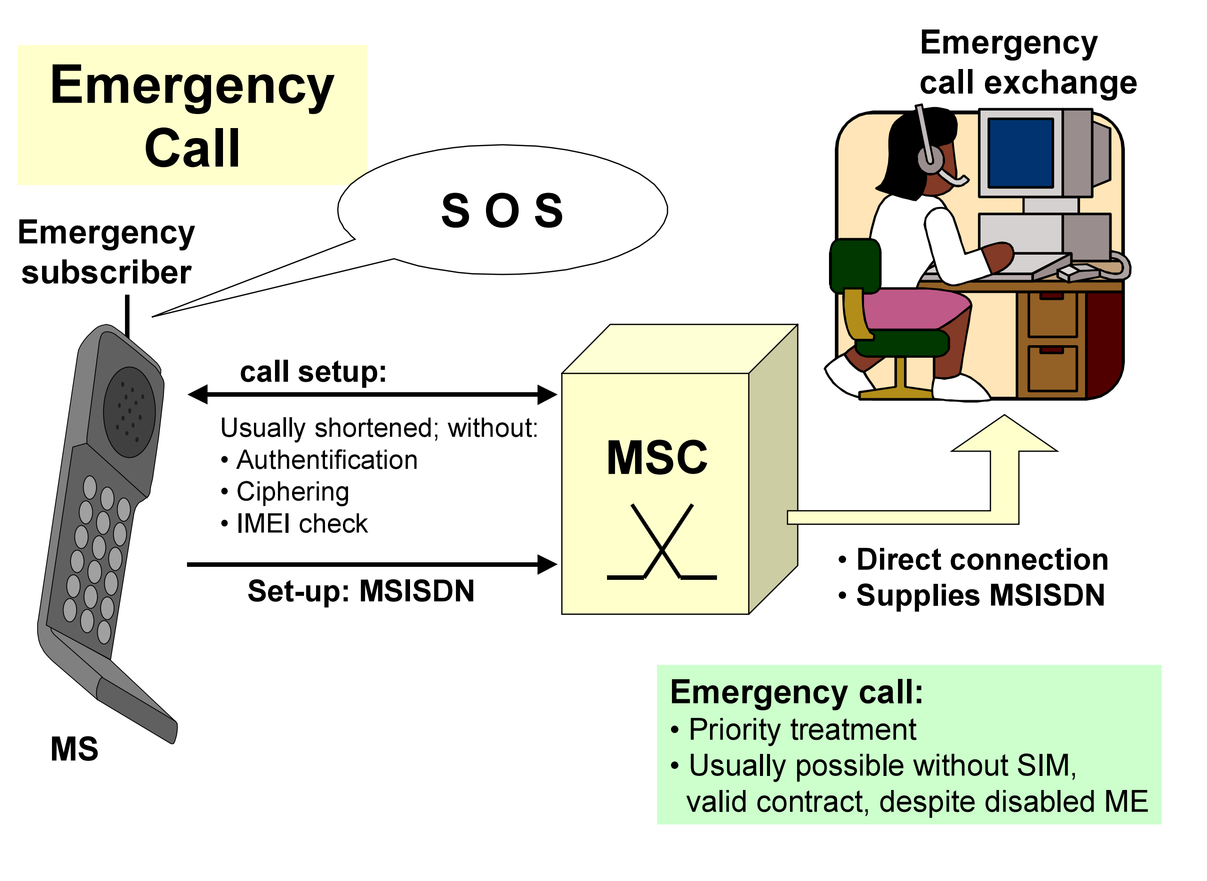
It can be administered whether emergency calls may also be made without a SIM card/valid contract/IMEI check. Normally, emergency calls are processed without taking otherwise applicable restraints such as missing subscriber recognition (no SIM card necessary), subscriber cancellation, etc. into account.

Emergency calls are treated with precedence. This may also lead to the release of other existing connections.

The setup may be shortened, i.e. without authentication procedure, ciphering, IMEI check and new TMSI allocation.

If the MSC receives the MSISDN of the emergency call subscriber (in the setup information), this is transmitted to the emergency service central office. The Location Area Identification (LAI) is not given to the emergency call exchange.

Emergency Call



Emergency subscriber

S O S

MS

call setup:

Usually shortened; without:

- Authentification
- Ciphering
- IMEI check

Set-up: MSISDN

MSC

Emergency call exchange

- **Direct connection**
- **Supplies MSISDN**

Emergency call:

- Priority treatment
- Usually possible without SIM, valid contract, despite disabled ME

Fig. 22

7 SMS (Short Message Service)

Mobile Terminated SMS (MT-SMS)

1) a service center sends the "short message" to the (SMS-)GMSC.

2) an interrogation is carried out with the HLR to receive current routing information.

3) after this, the "short message" can be switched to VMSC (possibly also via other networks).

4) the VMSC sends the "short message" to the BSS.

5) the BSS sends the "short message" via the SDCCH (Stand Alone Dedicated Control CHannel) of the radio interface Um to the MS.

If the addressee of the short message (called party) is not reachable, the short message is stored in the Short Message Service Center SMS-C and a notification is left in the HLR ("HLR flag"). When the subscriber is reachable again, the HLR sends a message (MAP/C Alert Service Center Message) to the GMSC of the SMS-C, so that a new transfer may be initiated.

SMS
Short Message Service

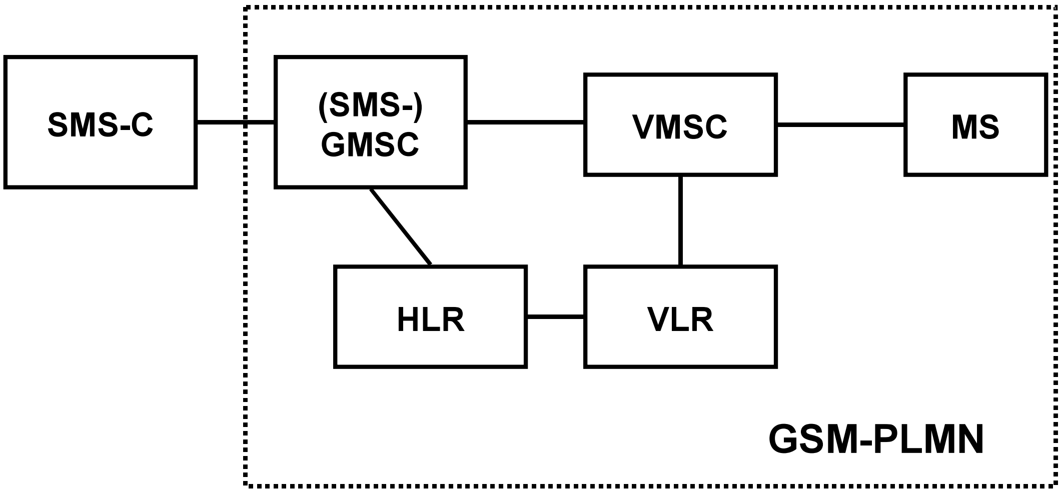


Fig. 23