

# 8 Switching system

## Objectives

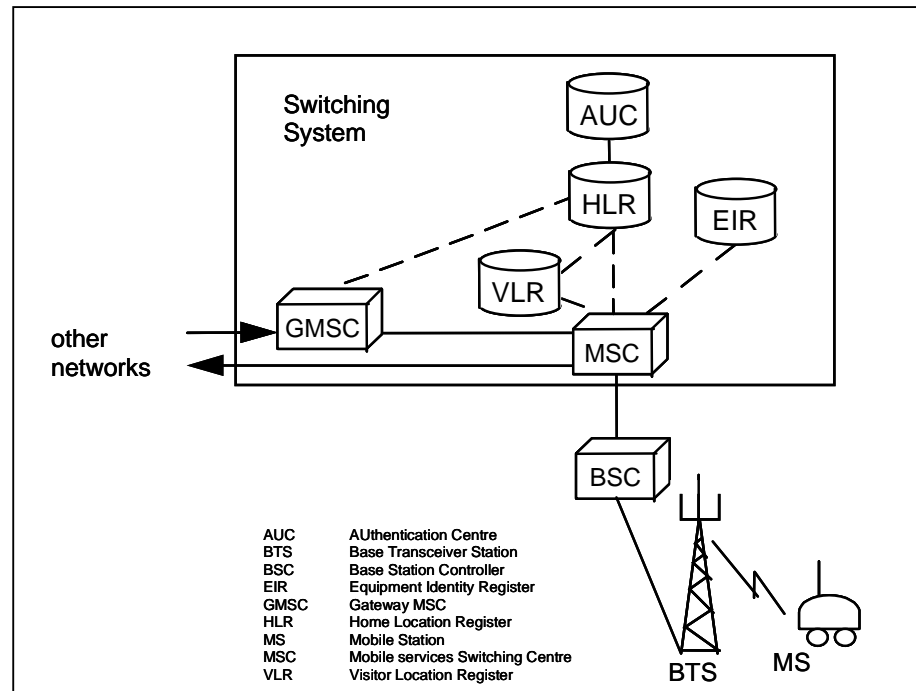
After this chapter the student will:

- be able to describe the functionality of MSC/VLR, GMSC and HLR.
- understand the procedures for authentication, ciphering and identification.
- be familiar with the nodes handling SMS and data transmission.

|            |   |   |
|------------|---|---|
| <b>8.1</b> | INTRODUCTION .....                                  | 2 |
| <b>8.2</b> | MSC/VLR.....  | 3 |
|            | <i>General</i> .....                                | 3 |
|            | <i>Mobile services Switching Centre (MSC)</i> ..... | 3 |
|            | <i>Visitor Location Register (VLR)</i> .....        | 3 |
|            | <i>MSC/VLR functions</i> .....                      | 3 |
| <b>8.3</b> | GATEWAY MSC (GMSC).....                             | 5 |
| <b>8.4</b> | HOME LOCATION REGISTER (HLR) .....                  | 5 |
| <b>8.5</b> | AUC AND EIR.....                                    | 6 |
|            | <i>General</i> .....                                | 6 |
|            | <i>AUC - Authentication Centre</i> .....            | 6 |
|            | <i>EIR - Equipment Identity Register</i> .....      | 7 |
|            | <i>TMSI</i> .....                                   | 7 |
| <b>8.6</b> | SHORT MESSAGE SERVICES CENTRE (SMS-C).....          | 8 |
| <b>8.7</b> | INTER WORKING FUNCTIONS (IWF) .....                 | 8 |

## 8.1 Introduction

The switching system is the GSM connection to other networks and allows calls to be set up to and from the MS. This involves switching and routing as well as checking different registers for location, subscription and equipment of the MS.



*GSM Network*

### Switching and routing

MSC - Mobile services Switching Centre

GMSC - Gateway MSC

### Subscriber registers

VLR - Visitor Location Register

HLR - Home Location Register

### Security functions

AUC - AUthentication Centre

EIR - Equipment Identity Register

### Non-voice traffic

SMS-C - Short Message Services Centre

IWF – Inter Working Functions

## 8.2 MSC/VLR

### *General*

The main responsibility of the MSC is to route and set up calls to and from the MS. For this it needs subscriber information which is stored in the VLR. In every MS activity involving the network the MSC and VLR has to communicate. The amount of signalling between these nodes has practically lead to an integration. Still they are two logical units specified by GSM but in the existing implementations the interface between them is internal following the standard of the supplier.

### *Mobile services Switching Centre (MSC)*

The MSC is mainly an exchange with switching capacity. It handles in- and outgoing trunks, the PCM-links and the functions for signalling to other switches in GSM as well as other networks. It also has functions for supervision of the calls and routines for charging and statistics. So far the MSC can be compared with any ordinary switch in the fixed network. It is the ability to handle mobile calls that turns it into an MSC.

### *Visitor Location Register (VLR)*

Due to the fact that the MS can roam in a large geographical area it is necessary to have a distributed register for the subscriber information. The VLR is a database that holds a file for the MSs present in the area controlled by the connected MSC, a file which will be erased in that specific VLR when the MS leaves that area. The files are registered on IMSI and contains information about the subscription, classmark of MS, the address to the HLR where the MS is registered, parameters for authentication, ciphering as well as dynamic data such as location, state of MS and status of services. The information is fetched from the HLR on request from the VLR e.g. during the location updating.

### *MSC/VLR functions*

To handle mobile calls the following functions are needed in the MSC/VLR

- call setup and supervision, special for mobile calls
- authentication and identification
- establishing and maintaining a continuous speech path to a moving subscriber
- privacy on the air
- handling subscriber data and updating registers

These functions can be related to two different areas.

### 1. MS connection

The signalling to establish and maintain a connection with the MS is done with a protocol developed for GSM called BSSAP (Base Station System Application Part). This protocol consists of different entities, each with its own functions.

**CM** - Connection Management - is responsible for the call control i.e. call establishment, supervision and clearing. It also handles supplementary services and functions for short messages.

**MM** - Mobility Management - deals with the consequences of mobility i.e. registration and security. Registration is the different types of location updating initiated by the MS. Security functions means the procedures for authentication, identification and TMSI assignment.

**RR** - Radio Resource management - is handled through the BSS and concerns the establishing and maintaining of the radio channel. It coordinates paging and different handover procedures and also keeps translation tables for cell or location area identity into BSC identity. The start of ciphering is also handled by this entity. The MSC/VLR also needs the ability to assign and clear call paths on the trunks to the BSC, and handle the associated signalling.

### 2. Switching system connection

The signalling to and from the HLR could e.g. be concerning an entering or leaving MS when the HLR or the VLR has to be updated with new subscriber information. Another reason is a request sent from the VLR to the HLR, for new triplets for authentication. During the setup of a mobile terminated call signalling is needed for the provision of a roaming number for the GMSC to route the call.

MSC/VLR also has to communicate with other MSC/VLRs during some handover procedures. The signalling between the nodes in the switching system to keep the registers updated is done with a protocol developed for GSM called MAP (Mobile Application part).

### 8.3 Gateway MSC (GMSC)

A mobile terminated call is always routed to a GMSC, specific for that MS operator. The task for the GMSC is to find the MS and route the call to the MSC/VLR controlling that area. The GMSC will ask the HLR for routing information and then reroute the call to the MSC/VLR using the roaming number in the reply. The gateway function could be implemented in an ordinary MSC/VLR

### 8.4 Home Location Register (HLR)

The HLR is the main database that holds files for all the MSs in an operator's network. There is one HLR per operator but it can be separated geographically into smaller units. The files are registered on IMSI and contains information about the subscription, MSISDN, parameters for authentication and ciphering as well as dynamic data such as the address to the present MSC/VLR, status of supplementary services and in some cases state of MS.

The HLR uses the MAP protocol to communicate with the MSC/VLR, GMSC and in some networks also the AUC. On a location updating request from a MSC/VLR concerning an entering MS, i.e. a new visitor, the HLR will execute several operations. It will register the new VLR address in the database, send the subscriber information to that new VLR and also tell the old VLR to erase that subscriber's information. The VLR can thus be seen as a distributed HLR holding information only about the MSs served by that MSC/VLR.

During the setup of a mobile terminated call the HLR will be requested by the GMSC to provide routing information for rerouting. The HLR will fetch that information from the correct MSC/VLR, or the database in case of a forwarding number, and send it to the GMSC.

The HLR will also provide triplets for authentication and ciphering on request from VLR. These triplets have been produced in AUC and fetched by the HLR and stored in the database.

## 8.5 AUC and EIR

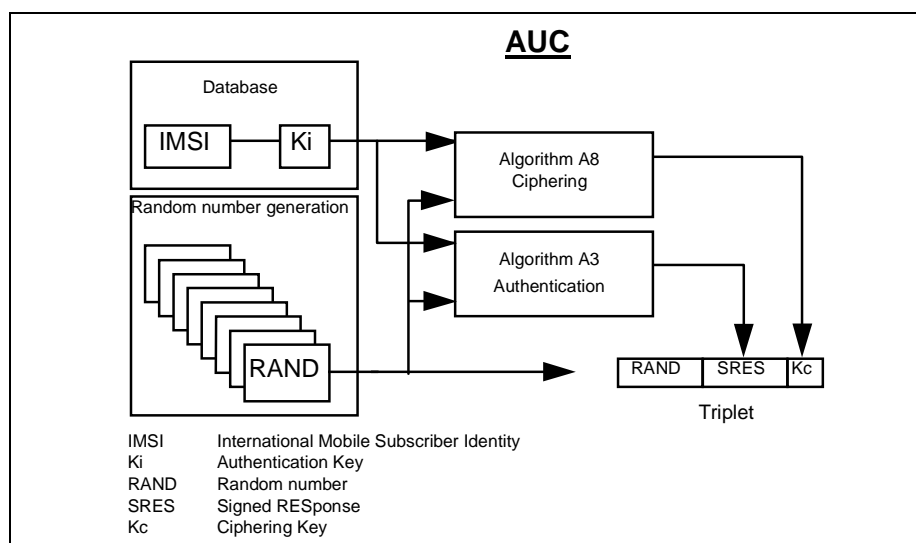
### *General*

Much effort has been put into security in GSM due to problems in older mobile systems. The security aspects can be divided into first identification and verification of a correct MS so that unauthorised, barred or stolen equipment cannot be used and second privacy on the radio channel.

The MS is checked by the authentication procedure for the subscription - the SIM-card - and the identification procedure for the phone - the mobile equipment (ME). The privacy on the air is achieved by ciphering the information, speech and data, and by using a Temporary Mobile Subscriber Identity (TMSI) for the subscriber. The AUC is the node that generates parameters, triplets, for authentication of the subscriber and ciphering while the EIR is a database for the identification of the mobile equipment.

### *AUC - AUthentication Centre*

The authentication centre produces triplets for each and every subscriber in that operators network and the triplets will be sent to the HLR on request. The AUC contains a database with IMSI and Ki, the authentication key. IMSI and Ki are also stored on the SIM-card in the MS. These two parameters together with a random number, (RAND), generated in the AUC will be input data to algorithms. This will produce the "Signed RESponse" (SRES) and the key for ciphering (Kc). RAND, SRES and Kc will form a triplet.



*Generation of triplets in AUC*

### Authentication procedure

The authentication procedure is initiated from the MSC/VLR by sending RAND to the MS. The MSC/VLR has fetched the triplets from the HLR. Now the MS calculates the SRES and Kc using the same algorithms as the AUC. The calculated SRES will be sent to the MSC/VLR which compares the SRES received from the MS with the one in the triplet from the AUC. If the two are the same access will be granted. The calculated Kc will be stored on the SIM-card.

### Ciphering start procedure

The ciphering start procedure is initiated from the MSC/VLR by sending a message Cipher Mode Command containing the Kc. The Kc will be removed from the message by the BTS before sending it on to the MS, so that the Kc will never be sent on the air. When the MS receives this message it will send the message Cipher Mode Complete in cipher mode using the calculated Kc stored on the SIM-card. If the BTS can decipher this message it will inform the MSC/VLR that ciphering has started.

### *EIR - Equipment Identity Register*

The EIR is a database containing the identity numbers for the mobile equipment, IMEI. These numbers are put on a black list if the equipment has been barred for some reason, on a grey list if it is not yet type approved or has bad behaviour and on the white list if there is no restrictions in using the equipment.

### Equipment identification procedure

The equipment identification procedure is initiated from the MSC/VLR by sending a message Identity Request for the IMEI. The MS is now forced to reply by sending the IMEI which will be sent to the EIR by the MSC/VLR. Depending on the result from the EIR i.e. on what list the IMEI was found, the MSC/VLR will grant or deny access.

### *TMSI*

The Temporary Mobile Subscriber Identity number is used to cover IMSI, the real identity, so that no tracing and identification can be done by listening to the traffic on the air. TMSI is allocated by the MSC/VLR and is only valid in one MSC Service area. This means that when the MS changes MSC Service area the MS need a new TMSI allocated by the new MSC/VLR. After the allocation, which could be done during location updating, the MS should use TMSI instead of IMSI in any connection with the network.

There is also a gain from the operators point of view in using TMSI because it is only half the length of IMSI. This doubles the paging capacity in the network.

## 8.6 Short Message Services Centre (SMS-C)

The short messages point-to-point are handled by a SMS-C. Short messages can have the length of up to 160 alphanumerical characters and can be sent to and from the MS.

The SMS-C works together with the HLR and MSC/VLR and a gateway function for SMS in the same way as for setting up calls. The short messages can be buffered in the SMS-C and sent again if the MS cannot receive the message the first time.

## 8.7 Inter Working Functions (IWF)

GSM is capable of handling not only speech but also data. In order to handle the different bit rates there is a need for modems. These, placed in the IWF, can be used by a MSC/VLR when setting up a data call and will then be connected through the switch.

The data services that the IWF shall be able to handle according to the GSM specification is synchronous 1,2 - 9,6 kbit/s and asynchronous 0.3 - 9,6 kbit/s. Also, it must be able to handle different access protocols (e.g. X.28 and X.32) used in data networks and different modem type standards (e.g. V.21 and V.22).

From GSM point of view the transmission can be transparent or non-transparent which implies that signal processing is being used or not. The IWF also has to perform the rate adaptation from bit rate used on the air interface to the wanted bit rate.