

## 6 Mobile Station

### Objectives

After this chapter the student will:

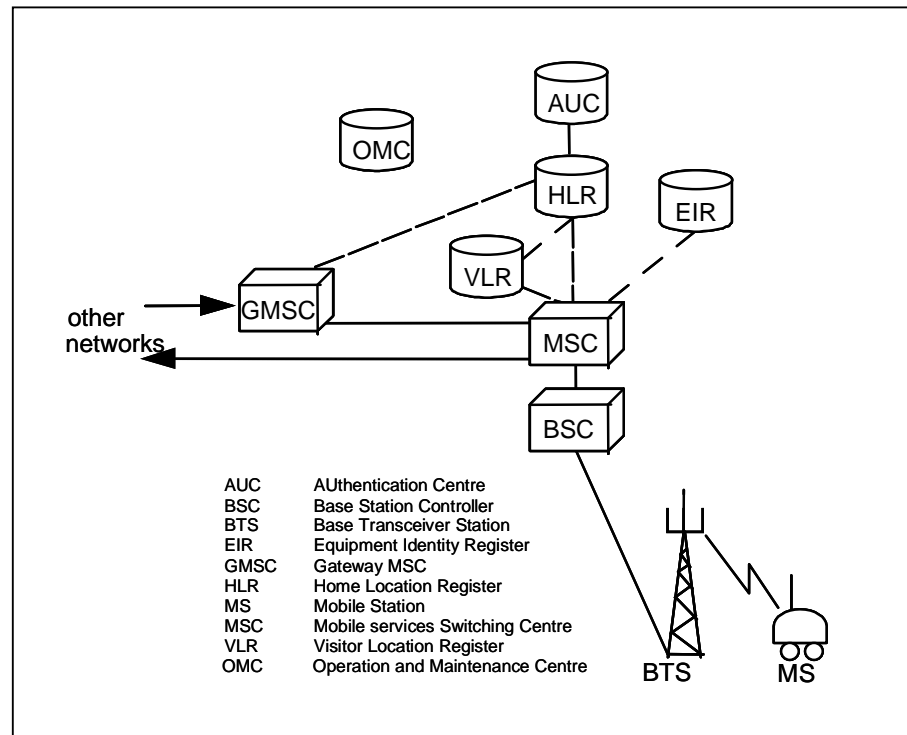
- be able to describe the role of the ME in the Mobile Network.
- be able to describe the characteristics and security aspects of the SIM card.

<b>6.1</b>	<b>INTRODUCTION</b> .....	<b>2</b>
<b>6.2</b>	<b>MOBILE EQUIPMENT - ME</b> .....	<b>3</b>
	<i>Types of Mobile Stations</i> .....	3
	<i>Output Power</i> .....	3
	<i>Frequency bands</i> .....	4
	<i>Full Rate/Half Rate Services</i> .....	4
	<i>SMS Capabilities</i> .....	4
	<i>Mobile Termination - MT</i> .....	4
<b>6.3</b>	<b>SUBSCRIBER IDENTITY MODULE - SIM</b> .....	<b>5</b>
	<i>SIM characteristics</i> .....	6
	<i>SIM information storage</i> .....	6
	<i>Security attributes</i> .....	8
<b>6.4</b>	<b>MOBILE STATION FEATURES</b> .....	<b>9</b>
	<i>Basic MS features</i> .....	9
	<i>Supplementary MS features</i> .....	11
	<i>Additional MS features</i> .....	11

## 6.1 Introduction

The Mobile Station represents the only part the user will probably ever see of the whole system. It is the phone that is carried by the subscriber and used for making and receiving calls. There are different types of Mobile Stations but they all consist of two logical units, the Mobile Equipment and the Subscriber Identity Module.

Mobile stations today offer not only an interface to the user (i.e. microphone, loudspeaker, a display and keyboard for the management of calls and services) but also an interface to personal computer and fax machine (which can be installed in the PC). The range of services and interfaces is left up to the manufacturer of the MS and can thus vary between MSs. This is due to that only a few MS features are mandatory whilst many of them are optional.



*GSM Network*

All Mobile Stations are logically divided into two units. The ME, Mobile Equipment, holds all the radio parts and is also capable of handling the functions required to access the network through the radio interface. This is what the user recognizes as "the phone". The SIM, Subscriber Identity Module, is a small circuit printed on a card which fits into the ME. The SIM provides the ME with subscriber information and thus allows the user to make chargeable calls.

## 6.2 Mobile Equipment - ME

The Mobile Equipment is characterised by its radio and service functions. The ME holds all the necessary functions to access the system, but without the SIM the ME is only allowed to place emergency calls. Some of the radio functions are the output power and the frequency bands that can be handled. The service functions could be e.g. support of full rate and half rate coding and the terminal capabilities. The Mobile Termination (MT) could, apart from the man-machine interface, have different interfaces towards the user such as ISDN or non-ISDN (e.g. for X and V-series) interfaces.

### *Types of Mobile Stations*

The different types of Mobile Stations can be divided into vehicle-mounted and hand-held stations.

- Vehicle-mounted stations are mounted in a vehicle and have the antenna physically mounted on the outside of the vehicle.
- Handheld stations are small and light enough to be carried by hand and typically has the antenna directly attached to it.

### *Output Power*

GSM mobile stations are separated into classes according to their maximum output power.

	GSM 900	GSM 1800
Class1	-	1 Watt
Class2	8 Watt	0.25 Watt
Class3	5 Watt	4 Watt
Class4	2 Watt	-
Class5	0.8 Watt	-

A GSM handheld MS may be of GSM 900 classes 4 and 5 and GSM 1800 handheld MSs can be both class 1 and class 2. Both GSM 900 and GSM 1800 Mobile Stations must be capable of reducing transmitter output power when instructed by the network to do so.

### *Frequency bands*

For the GSM Mobile Stations, three frequency bands are defined:

- Standard GSM Band: 890-915 MHz Uplink and 935-960 MHz downlink
- Extended GSM Band: 880-915 MHz Uplink and 925-960 MHz downlink
- GSM 1800 Band: 1710-1785 MHz Uplink and 1805-1880 MHz downlink

The Mobile Station may be capable of supporting one or more of these bands. However, a procedure to select GSM 1800 operation must be provided internally in the MS if it is capable of handling both. Simultaneous use of GSM 1800 modes is not supported.

### *Full Rate/Half Rate Services*

Both full and half rate services are specified. An MS may support one of these or both, depending on the basic service to be used and the MS capabilities.

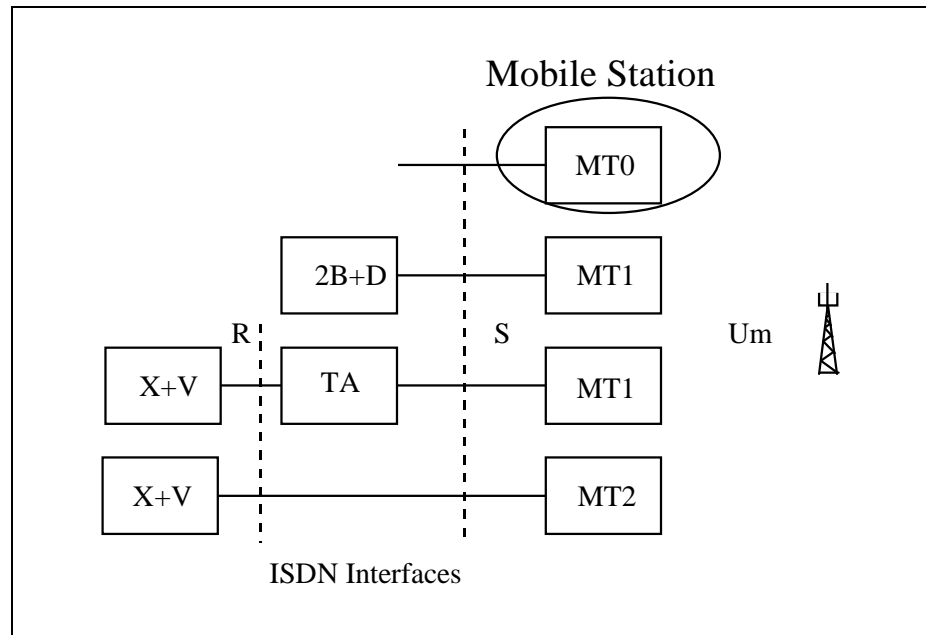
### *SMS Capabilities*

The ME may be able to handle the point-to-point Short Messages Services both mobile originated and mobile terminated.

### *Mobile Termination - MT*

There are three types of MT:

- MT0 consists of the functions belonging to the functional group MT, with support of no terminal interfaces.
- MT1 consists of the functions belonging to the functional group MT, and an interface with the GSM recommended subset of the ISDN user-network interface recommendations.
- MT2 consists of the functions belonging to the functional group MT, and with an interface that complies with the GSM recommended subset of the CCITT X or V series interface recommendations.



Connection points for MTs

MT plus any TE (Terminal Equipment) or TE+TA (Terminal Adapter) will constitute the mobile station.

### 6.3 Subscriber Identity Module - SIM

In order for the ME to operate in a GSM network for services other than emergency services, a valid SIM-card with a valid IMSI stored on it must be present. With the insertion of the SIM card the ME will become a fully functional Mobile Station.

Certain subscriber parameters together with personal data used by the subscriber, e.g. frequently called numbers will be stored on the SIM. Since only the SIM is required to personalise a phone it is therefore possible to rent a phone and personalise its operation with the insertion of the SIM card. This way all calls will be diverted to the new location of the SIM card wherever it is in the global GSM network. Every call placed from this phone will be billed to the subscriber's home account.

There are three types of subscriber related information that is stored on the SIM:

- Data fixed before the personalisation of the SIM, e.g. IMSI, subscriber authentication key (Ki), access control class.
- Temporary network data, e.g. TMSI, LAI, Kc, forbidden PLMNs.
- Service related data, e.g. language preference, advice of charge.

The GSM application may be one of several applications on a multi-application IC card.

### *SIM characteristics*

Two types of SIM exist, "ID-1 SIM" and the "Plug-in SIM". The information on the exterior of either SIM should include at least the account identifier and the check digit of the IC Card identification. Both types of SIM are often issued to the user to enable the choice of operating either type of ME. An ME able to accept a Plug-in SIM may also be capable of accepting the ID-1 SIM.

If a SIM is removed, any call in progress made using that SIM is terminated immediately.

#### ID-1 SIM

The size of this SIM-card is the same as that of any credit card. Format and layout is in accordance with ISO standards. The card will also have a polarisation mark which will indicate how the card should be inserted into the ME by the user.

#### Plug-in SIM

The Plug-in SIM is a cut out version of ID-1 SIM which contains the IC and will be cut on one corner to prevent the user from inserting it incorrectly.

### *SIM information storage*

The SIM will contain information elements for GSM network operations. The SIM may contain information elements related to the mobile subscriber, GSM services and PLMN related information, e.g. PLMN Selector. All subscriber related information transferred into the ME during GSM network operations is deleted from the ME after removal of the SIM or deactivation of the MS.

#### Mandatory storage

The SIM card will store the following information:

- IC card identification: a number uniquely identifying the SIM and the card issuer
- Administrative information: indicates mode of operation of the SIM, e.g. normal, type approval
- International Mobile Subscriber Identity (IMSI)
- Location information: comprising Temporary Mobile Subscriber Identity (TMSI), Location Area Information (LAI), Current value of Periodic Location Updating Timer (T3212) and the Location Update status
- Cipher Key (Kc) and cipher key sequence number

Location Information, Cipher key and Cipher Key Sequence Number are updated on the SIM after each call termination and when the MS is correctly deactivated in accordance with the manufacturers instructions.

In addition the SIM will manage and provide storage for the following information in accordance with the security requirements:

- PIN
- PIN enable/disable indicator
- PIN error counter
- PUK
- PUK error counter
- Subscriber authentication key

Other mandatory features stored on the SIM card are:

- BCCH information: list of carrier frequencies to be used for cell selection
- HPLMN search period: used to control the time interval between HPLMN searches
- Forbidden PLMNs
- Language preference: subscriber preferred language(s) of MMI
- Phase identification
- Access control class(es)
- SIM service table: indicates which optional services are provided by the SIM

#### Optional storage

In addition to the above the SIM may provide storage capabilities for the following:

- Abbreviated Dialling Numbers
- Fixed Dialling Numbers
- Last number(s) dialled
- Short messages and associated parameters
- Capability configuration parameters: Provides the parameters of required bearer capabilities associated with dialling numbers
- Cell Broadcast Message Identifier Selection
- Accumulated call meter, Accumulated call meter maximum value and Price per unit & currency table
- PLMN selector: for automatic PLMN selection
- Called party sub address

In addition, if the SIM supports PIN2, the following information will be managed and stored by the SIM:

- PIN2 and PIN2 error counter
- PUK2 and PUK2 error counter

## *Security attributes*

The GSM security attributes to be supported by the SIM are:

- authentication algorithm (A3)
- subscriber authentication key (Ki)
- cipher key generation algorithm (A8)
- cipher key (Kc)
- control of access to data stored (PIN and PUK), and functions performed, in the SIM

(An algorithm A38 may perform the combined functions of A3 and A8.)

All reasonable steps are taken to ensure that the algorithms (A3 and A8) and subscriber authentication key (Ki) cannot be read, altered, manipulated or bypassed in such a way as to reveal secret information.

Every MS process which require the use of the subscriber authentication key are performed internally by the SIM.

### Authentication

A security function for authenticating the SIM, which is mandatory for any MS, is based on a cryptographic algorithm A3, and the secret subscriber authentication key Ki. Both A3 and Ki are located on the SIM.

### Ciphering

The security function that ciphers the information sent and received by the MS, requires a cipher key Kc. The generation of the Kc is based on a cryptographic algorithm A8, and the Ki. Also A8 is located on the SIM.

### SIM-control

To provide protection against the use of stolen cards PIN and PUK codes are issued.

The SIM contains a PIN number (Personal Identification Number) which will provide protection against unauthorised use as the PIN number is requested each time the MS is switched on. The PIN could be disabled by the subscriber or by the operator at start of subscription. For the use of some optional features a second PIN number (PIN2) will be requested.

The PIN numbers are stored and verified in the SIM card. Both PINs take the form of a numeric value of 4 to 8 decimal digits.

If an incorrect PIN or PIN2 is entered, that will be indicated to the user. The relevant PIN will be blocked after the three consecutive incorrect entries, i.e. functions and actions on data protected by the PIN access condition are no longer possible. Removing/inserting the SIM or switching the MS off/on has no effect.

Unblocking of a PIN is performed using the relevant PIN Unblocking Key (PUK/PUK2). The PUKs consist of 8 decimals and are not changeable by

the user. If an incorrect PUK is entered, that will be indicated to the user. After 10 consecutive incorrect entries, the PUK is itself blocked, even if between attempts the SIM has been removed or the MS has been switched off. It is not possible to read the PINs or PUKs from the ME.

## 6.4 Mobile Station features

Three categories of features can be distinguished:

1. Basic MS features are directly related to the operation of basic telecommunication services (e.g. key-pad functions).
2. Supplementary MS features are directly related to the operation of supplementary services (e.g. display of calling line number).
3. Additional MS features are features which are neither a basic nor a supplementary feature (e.g. abbreviated dialling).

### *Basic MS features*

<b>Function</b>	<b>(M - Mandatory, O - Optional)</b>
Display of Called Number	M
Indication of Call Progress Signals	M
Country / PLMN Indication	M
Country / PLMN Selection	M
Keypad	O
IMEI	M
Short Message	M
Short Message Overflow Indication	M
DTE / DCE Interface	O
ISDN "S" Interface	O
International Access Function ("+" Key)	O
Service Indicator	M
Autocalling restriction capabilities	--
Emergency Calls capabilities	M
Dual Tone Multi Frequency function (DTMF)	M
Subscription Identity Management	M
On / Off switch	O
Subaddress	O
Support of Encryption A5/1 and A5/2	M
Short Message Service Cell Broadcast DRX	M
Service provider Indication	M

*Table of Basic MS features*

#### Display of Called Number

This feature allows the user to check if the number is correct before call set-up.

#### Indication of Call Progress Signals

These indications are based on signalling information returned from the PLMN. They can be shown on visual display or as recorded message or simply as tones.

#### Country / PLMN Indication

The Country / PLMN indicator simply indicates in which GSM PLMN that the MS is roaming. It is necessary that this information is displayed so that the user is aware that "roaming" is taking place.

#### Country / PLMN selection

If more than one GSM PLMN exists in a given area the user will have the ability to select which operator to be connected.

#### IMEI

Each MS has a unique ME identity and will transmit this when requested to do so by the PLMN. The IMEI is stored on a module which is physically secured in the MS and not accessible to the user.

#### Short message indication and acknowledgement

Messages submitted to the service centre by a telecommunications network user will be delivered to the MS shortly after the MS accesses the system. The MS will provide an indication to the user that a message has been received from the service centre and must also send an acknowledgement signal to the PLMN to show that this indication has been activated. The PLMN will then return this acknowledgement to the service centre.

#### Short message overflow indication

When an incoming message cannot be received due to insufficient available memory it will be indicated to the MS user.

#### DTE / DCE

This is a standard interface for attachment of a DTE (Data Terminal Equipment) to the MS and used in conjunction with data services, DCE (Data Communication Equipment).

#### ISDN "S" terminal Interface

This is a standard interface for attachment of equipment to ISDN.

#### International access function

For the purpose of gaining international access from an MS a key with a function "+" is used. When this is signalled over the air interface it has the function of generating the international access code in the network.

#### Service Indicator (SI)

When there is adequate signal strength to allow a call to be made and the MS has successfully registered on the selected PLMN it will be indicated to the user.

#### Dual Tone Multi Frequency (DTMF)

The MS is capable of initiating DTMF in accordance with GSM specifications.

Subscription identity management

The SIM (Subscriber Identity Module) contains the IMSI. The result of the SIM card being removed is that a call in progress will be terminated and no further calls should be allowed to be initiated. Emergency calls may still be made by dialling 112.

Support of Encryption A5/1 and A5/2

Support of A5/1, A5/2 and non encrypted mode is mandatory. The specification allows the use of 7 different algorithms and the non encrypted case.

Service provider Indication

Whilst in idle mode the Service providers name along with the current PLMN can be displayed. The SIM should support two options in parallel and alternatively.

*Supplementary MS features*

<b>Function</b>	<b>(M - Mandatory, O - Optional)</b>
Control of Supplementary Services	--
Call Barring and Call Forwarding	M
Others	O

Table of *Supplementary MS features*

Control of Supplementary Services

The support of Call Barring and Call Forwarding Supplementary Services is mandatory. The support of other Supplementary Services is up to the manufacturer.

*Additional MS features*

<b>Function</b>	<b>(M - Mandatory, O - Optional)</b>
Abbreviated Dialling	O
Fixed Number Dialling	O
Barring of Outgoing Calls	O
DTMF Control Digits Separator	O
Selection of Directory No in Short Messages	O
Last Numbers Dialed	O

Table of *Additional MS features*

Abbreviated Dialling

The directory number or part thereof is stored in the MS together with the abbreviated address. After retrieval the number may appear on the display. Abbreviated numbers stored in the ME or SIM may contain wild characters. The completed number is transmitted on the radio path.

#### Fixed Number Dialling

Utilising this feature in conjunction with an electronic lock makes it possible to place a bar on calling any numbers other than those pre-programmed in the SIM. "Fixed Dialling Mode" under control of PIN 2, may be enabled or disabled, the mode selected will then be stored in the SIM.

#### Barring of outgoing calls

This feature allows outgoing calls to be blocked. The barring condition can be activated/deactivated by using a key, keyword etc. The barring may be selective and applied to individual services or individual call types. This is set in the ME only.

#### DTMF control digits separator

Provision has been made to enter DTMF digits with a telephone number, and upon the called party answering the ME will send the DTMF digits automatically to the network.

#### Selection of directory number in short messages

The Short Message may be used to convey a Directory Number which the user may wish to call. This can be indicated by enclosing the directory number in a pair of inverted commas (" "). If the displayed message contains these characters enclosing a directory number, a call can be set up by user action. Normal (unspecified) or International format (+) may be used.

#### Last numbers dialled

The MS may store the Last "N" Numbers dialled in the SIM and/or the ME. "N" may take the value up to 10 in the SIM. It may be any value in the ME. If these numbers are stored in both the SIM and the ME, those from the SIM will take precedence.