Switching System

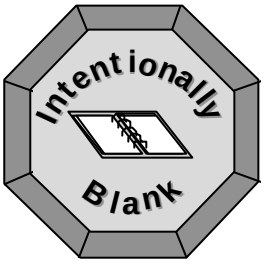
Chapter 6

This chapter is designed to provide the student with an overview of the switching system, including its nodes and their functionality.

OBJECTIVES:

Upon completion of this chapter the student will be able to:

- Name 3 nodes in the Switching System
- List which 2 nodes are contacted for the security procedure in the GSM system
- Briefly explain the purpose of Authentication, Ciphering and Equipment Check


Intentionally
Blank

6 Switching System

Table of Contents

Topic **Page**

INTRODUCTION

The Switching System in Ericsson's GSM systems contains the following components:

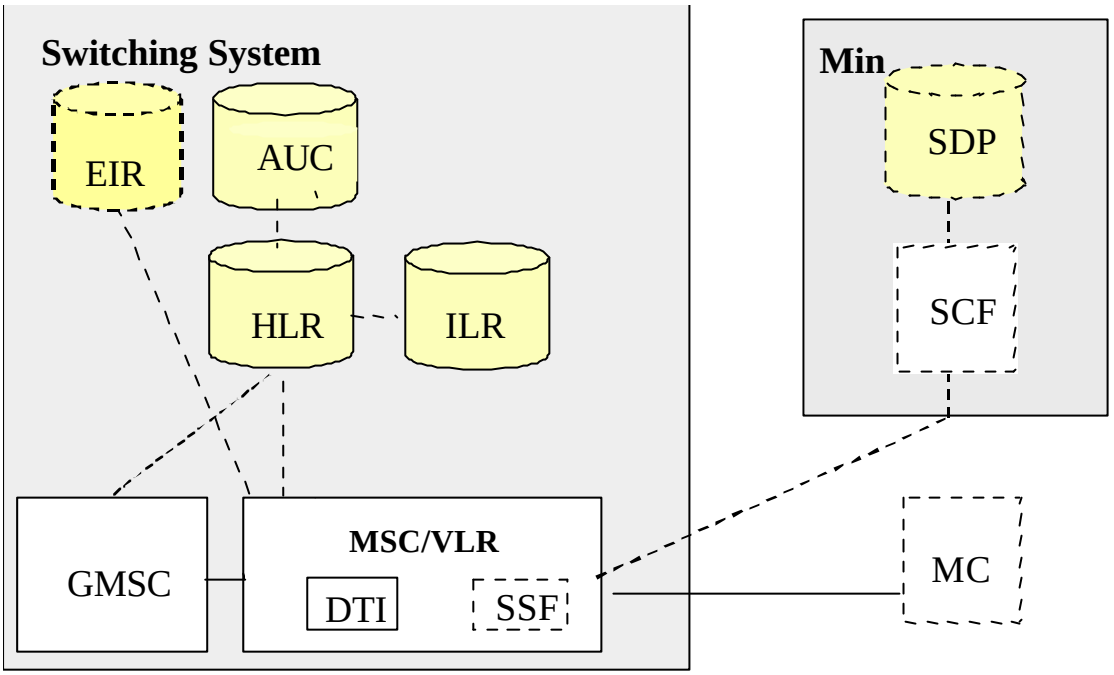


Figure 6-1 Switching System

Type	Abbrev.	Full component name	Platform
Basic	MSC/VLR	Mobile services Switching Center/Visitor Location Register	AXE
	GMSC	Gateway MSC	AXE
	HLR	Home Location Register	AXE
	ILR	Interworking Location Register	AXE
	AUC	AUthentication Center	Unix/AXE
	EIR	Equipment Identity Register	Unix
	DTI	Data Transmission Interface	AXE
Additional	MC	Message Center	MXE
	SSP	Service Switching Function	AXE
	SCP	Service Control Function	AXE
	SDP	Service Data Point	Unix

Table 6-1 Switching System components

Each network component is described in the remainder of this chapter.

MOBILE SERVICES SWITCHING CENTER/VISITOR LOCATION REGISTER (MSC/VLR)

MSC FUNCTIONS

The primary node in a GSM network is the MSC. It is the node which controls calls both to MSs and from MSs. The primary functions of an MSC include the following:

- **Switching and call routing:** An MSC controls call set-up, supervision and release, and may interact with other nodes to successfully establish a call. This includes routing of calls from MSs to other networks such as a PSTN.
- **Charging:** an MSC contains functions for charging mobile calls and information about the particular charge rates to apply to a call at any given time or for a given destination. During a call it records this information and stores it after the call, e.g. for output to a billing center.
- **Service provisioning:** supplementary services are provided and managed by an MSC. In addition, the SMS service is handled by MSCs.
- **Communication with HLR:** the primary occasion on which an MSC and HLR communicate is during the set-up of a call to an MS, when the HLR requests some routing information from the MSC[1].
- **Communication with the VLR:** associated with each MSC is a VLR, with which it communicates for subscription information, especially during call set-up and release.
- **Communication with other MSCs:** it may be necessary for two MSCs to communicate with each other during call set-up or handovers between cells belonging to different MS's.
- **Control of connected BSCs:** as the BSS acts as the interface between the MSs and the SS, the MSC has the function of controlling the primary BSS node: the BSC. Each MSC may control many BSCs, depending on the volume of traffic in a particular MSC service area. An MSC may communicate with its BSCs during, for example, call set-up and handovers between two BSCs.

[1] An MSC may include gateway functionality, in which case there is more communication with HLR's.

- **Direct access to Internet services:** traditionally, an MSC accessed the Internet nodes of an Internet Service Provider (ISP) via existing networks such as the PSTN. However, this function enables an MSC to communicate directly with Internet nodes, thus reducing call set-up time. Direct access can be provided by using an access server called Tigris (from Advanced Computer Communications). This may be integrated in an MSC or stand-alone connected to an MSC.

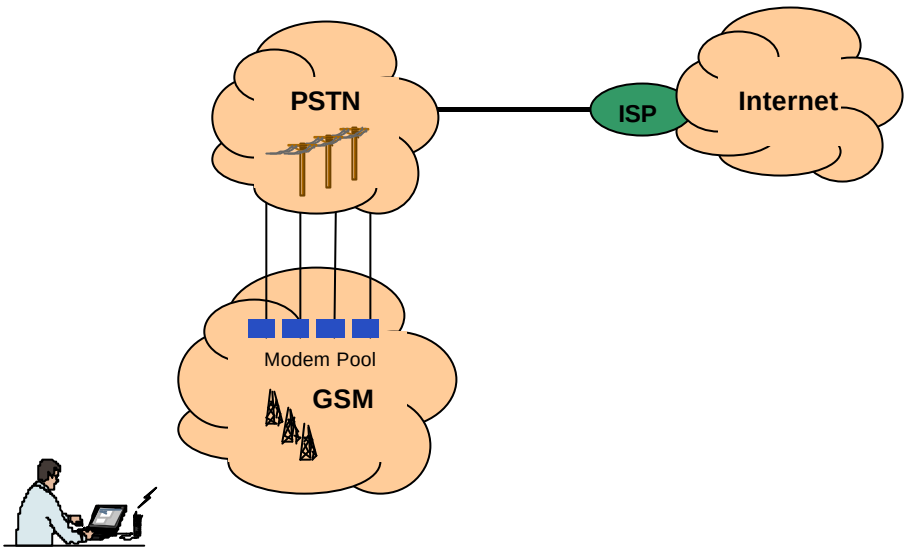


Figure 6-2 Internet access via GSM/PSTN (traditional method)

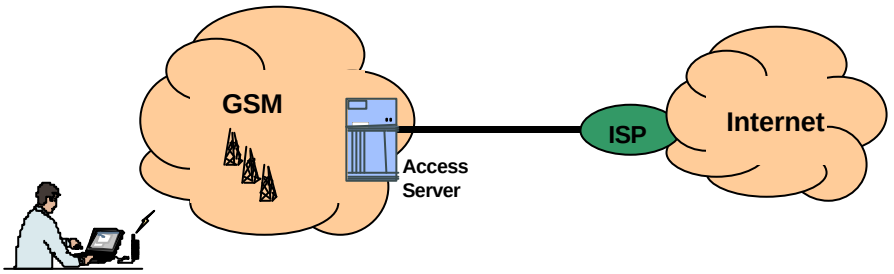


Figure 6-3 Direct access to Internet

- **ISDN Primary Rate Access (PRA):** this function enables an MSC to provide PRA services to subscribers. One network operator can offer PABX connection services, through the PLMN. In this way the operator can compete directly with PSTN operators for ISDN business subscribers.

VLR FUNCTIONS

The role of a VLR in a GSM network is to act as a temporary storage location for subscription information for MSs which are within a particular MSC service area. Thus, there is one VLR for each MSC service area. This means that the MSC does not have to contact the HLR (which may be located in another country) every time the subscriber uses a service or changes its status.

The following occurs when MSs move into a new service area:

1. The VLR checks its database to determine whether or not it has a record for the MS (based on the subscriber's IMSI)

2. When the VLR finds no record for the MS, it sends a request to the subscriber's HLR for a copy of the MS's subscription

3. The HLR passes the information to the VLR and updates its location information for the subscriber. The HLR instructs the old VLR to delete the information it has on the MS

4. The VLR stores its subscription information for the MS, including the latest location and status (idle)

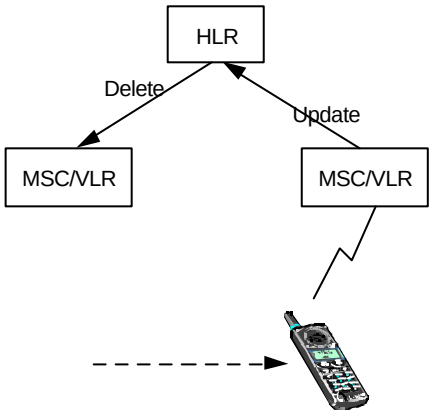


Figure 6-4 VLR-HLR interaction

While the MS is within one MSC service area, the VLR contains a complete copy of the necessary subscription details, including the following information:

- Identity numbers for the subscriber
- Supplementary service information (e.g. whether the subscriber has call forwarding on busy activated or not)
- Activity of MS (e.g. idle)
- Current LA of MS

MSC/VLR IMPLEMENTATION

In Ericsson's GSM systems, the MSC and VLR are integrated in the same AXE-based node. The reason for this is that there is an extensive amount of information exchange between the two nodes for every call, particularly during call set-up. The MSC-VLR interface is completely internal within the AXE, but each is treated as a distinct and separate function.

An MSC/VLR contains the common APZ and APT subsystems described previously, along with the subsystems in the following table, each of which is implemented in software only.

Subsystem	Functions
Mobile Data Subsystem (MDS)	• VLR functions
Mobile Mobility and radio Subsystem (MMS)	• Control of BSCs • Control of handovers involving the MSC
Mobile Switching Subsystem (MSS)	• Switching and call routing • Communication with HLRs • Communication with other MSCs
Short message Handling Subsystem (SHS)	• Handling of SMS messages

Table 6-2 MSC/VLR Subsystems

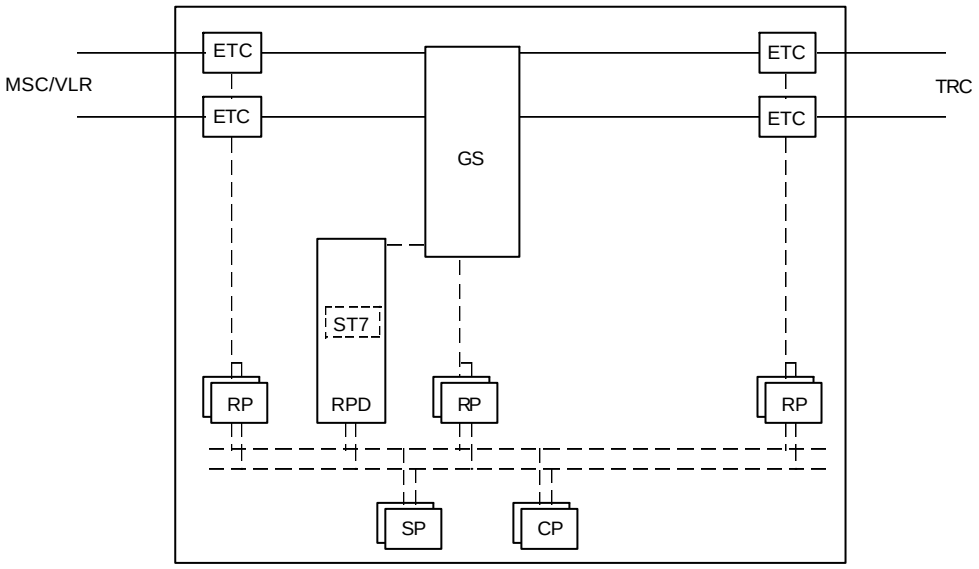


Figure 6-5 MSC/VLR hardware

GATEWAY MSC (GMSC)

GMSC FUNCTIONS

Gateway functionality enables an MSC to interrogate a HLR in order to route a mobile terminating call. It is not used in calls from MSs to any terminal other than another MS.

For example, if a person connected to the PSTN wants to make a call to a GSM mobile subscriber, then the PSTN exchange will access the GSM network by first connecting the call to a GMSC. The GMSC requests call routing information from the HLR that provides information about which MSC/VLR to route the call to. The same is true of a call from an MS to another MS.

GMSC IMPLEMENTATION

Any MSC in the mobile network can function as a gateway by integration of the appropriate software and definition of HLR interrogation information. In effect it then becomes a GMSC/VLR.

In Ericsson's GSM systems, gateway functions are provided within the subsystem MSS. The only additional hardware required is hardware to interface the signaling link to the HLR.

Gateway Function:

1. Find and interrogate HLR for roaming number.
2. Route the call according to the interrogation.

HOME LOCATION REGISTER (HLR)

HLR FUNCTIONS

The HLR is a centralized network database that stores and manages all mobile subscriptions belonging to a specific operator. It acts as a permanent store for a person's subscription information until that subscription is cancelled. The information stored includes:

- Subscriber identity (i.e. IMSI, MSISDN)
- Subscriber supplementary services
- Subscriber location information (i.e. MSC service area)
- Subscriber authentication information

The primary functions of the HLR include:

- **Subscription database management:** as a database, the HLR must be able to process data quickly in response to data retrieval and update requests from other network nodes. For this reason it acts as a database management system. Each subscriber record contains a substantial amount of parameters.
- **Communication with MSCs:** when setting up calls to an MS, it is necessary for the HLR to contact the MSC serving the MS for routing information. By analyzing the MSISDN, MSC knows which HLR to contact worldwide for that MS's subscription.
- **Communication with GMSCs:** during call set-up to an MS, the GMSC requests MS location information from the HLR, which then provides this in the form of routing information. Also, if the subscriber is detached the HLR will inform the GMSC that there is no need to perform further routing of the call.
- **Communication with AUCs:** before any activity involving change or use of subscription information takes place, the HLR must retrieve new authentication parameters from an AUC.
- **Communication with VLRs/ILRs:** when an MS moves into a new MSC service area the VLR for that area requests information about the MS from the HLR of the subscriber. The HLR provides a copy of the subscription details, updates its MS location information and instructs the old VLR to delete the information it has about that MS. As the ILR acts as a VLR for AMPS subscribers, the HLR communicates with it in a similar way.

HLR IMPLEMENTATION

The HLR can be implemented in the same network node as the MSC/VLR (i.e. MSC/VLR/HLR) or as a stand-alone database. An MSC/VLR/HLR node is a suitable solution for a small start-up GSM network as it saves hardware and signaling load on the links between MSC/VLR and HLR.

A stand-alone HLR is a suitable solution for large networks. It has the following advantages:

- There are no traffic disturbances creating better reliability
- When the HLR is separate from the MSC/VLR, there is more capacity available for call handling in the MSC/VLR

If the number of subscribers exceeds the capacity of a HLR, additional HLR's may be added.

HLR Redundancy

In order to provide additional network reliability, an additional “mated” HLR is used to mirror the data in a HLR and can automatically take over if required.

System Structure

In Ericsson’s GSM systems the HLR is an AXE-based AM called HLRAM. Along with the standard APZ and APT subsystems the HLR includes the APT subsystem Home location Register Subsystem (HRS) which performs the necessary subscription management.

INTERWORKING LOCATION REGISTER (ILR)

ILR FUNCTIONS

Ericsson's ILR offers roaming capabilities between mobile telephony systems complying with different standards. The ILR is specific to the GSM1900 product portfolio and enables AMPS network subscribers to roam to a GSM 1900 network.

For AMPS subscribers who wish to avail of this roaming functionality, their AMPS network subscriptions are copied into the HLR side of the ILR. When they roam into the GSM 1900 network, the HLR copies this information into the VLR side of the ILR, as occurs for normal GSM roaming subscribers.

From the subscriber's point of view however, there is only one subscription.

In the near future, the ILR will make intersystem roaming possible in both directions between all GSM, AMPS/TDMA-networks

ILR IMPLEMENTATION

In Ericsson's GSM systems the ILR is AXE-based. It includes the common APZ and APT subsystems outlined previously and the following additional subsystems:

Subsystem	Functions
Home location Register Subsystem (HRS)	• AMPS Subscriber database management
Mobile Intersystem roaming Subsystem (MIS)	• Mapping and translation of services and protocols • Communication with other nodes

Table 6-3 ILR subsystems

ILR hardware is similar to HLR hardware.

AUTHENTICATION CENTER (AUC) AND EQUIPMENT IDENTITY REGISTER (EIR)

PLMNs need a higher level of protection than traditional telecommunication networks. Therefore, to protect GSM systems, the following security functions have been defined:

- **Subscriber authentication:** by performing authentication, the network ensures that no unauthorized users can access the network, including those that are attempting to impersonate others.
- **Radio information ciphering:** the information sent between the network and an MS is ciphered. An MS can only decipher information intended for itself.
- **Mobile equipment identification:** because the subscriber and equipment are separate in GSM, it is necessary to have a separate authentication process for the MS equipment. This ensures, e.g. that a mobile terminal, which has been stolen, is not able to access the network.
- **Subscriber identity confidentiality:** during communication with an MS over a radio link, it is desirable that the real identity (IMSI) of the MS is not always transmitted. Instead a temporary identity (TMSI) can be used. This helps to avoid subscription fraud.

The AUC and EIR are involved in the first three of the above features, while the last is handled by MSC/VLRs (and is described in the “Traffic Cases” chapter).

AUC FUNCTIONS

The primary function of an AUC is to provide information, which is then used by an MSC/VLR to perform subscriber authentication and to establish ciphering procedures on the radio link between the network and MSs.

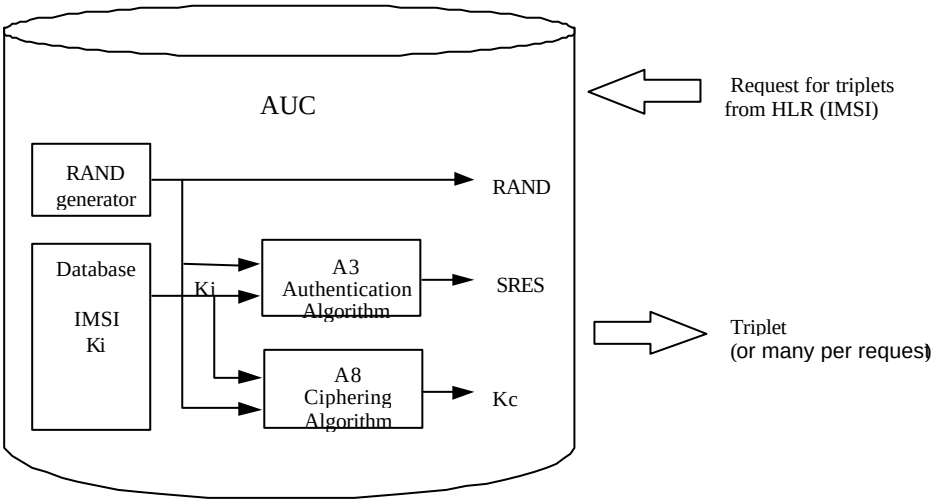
The information provided is called a triplet and consists of:

1. A non predictable RANDom number (RAND)
2. A Signed RESponse (SRES)
3. A ciphering Key (Kc)

Provision of Triplets

At subscription time, each subscriber is assigned a subscriber authentication Key (Ki). Ki is stored in the AUC along with the subscriber's IMSI. Both are used in the process of providing a triplet. The same Ki and IMSI are also stored in the SIM. In an AUC the following steps are carried out to produce one triplet:

1. A non-predictable random number, RAND, is generated
2. RAND and Ki are used to calculate SRES and Kc, using two different algorithms, A3 and A8 respectively
3. RAND, SRES and Kc are delivered together to the HLR as a triplet



RAND Random number
SRES Signed Response
Kc Ciphering key
Ki Subscriber authentication key
IMSI International Mobile Subscriber Identity

Figure 6-6 Provision of triplets

Authentication Procedure

1. The MSC/VLR transmits the RAND to the MS.
2. The MS computes the signature SRES using RAND and the subscriber authentication key (Ki) through the A3 algorithm.
3. The MS computes the Kc by using Ki and RAND through A8 algorithm. Kc will thereafter be used for ciphering and deciphering in MS.
4. The signature SRES is sent back to MSC/VLR, which performs authentication, by checking whether, the SRES from the MS and the SRES from the AUC match. If so, the subscriber is permitted to use the network. If not, the subscriber is barred from network access.

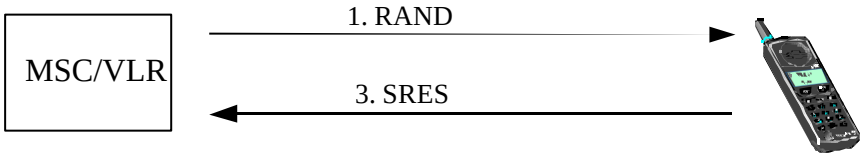


Figure 6-7 Authentication procedure

Authentication can by operator's choice be performed during:

- Each registration
- Each call setup attempt
- Location updating
- Before supplementary service activation and deactivation

There can be exceptions for subscribers belonging to other PLMN's.

Ciphering Procedure

☞ Did you know?

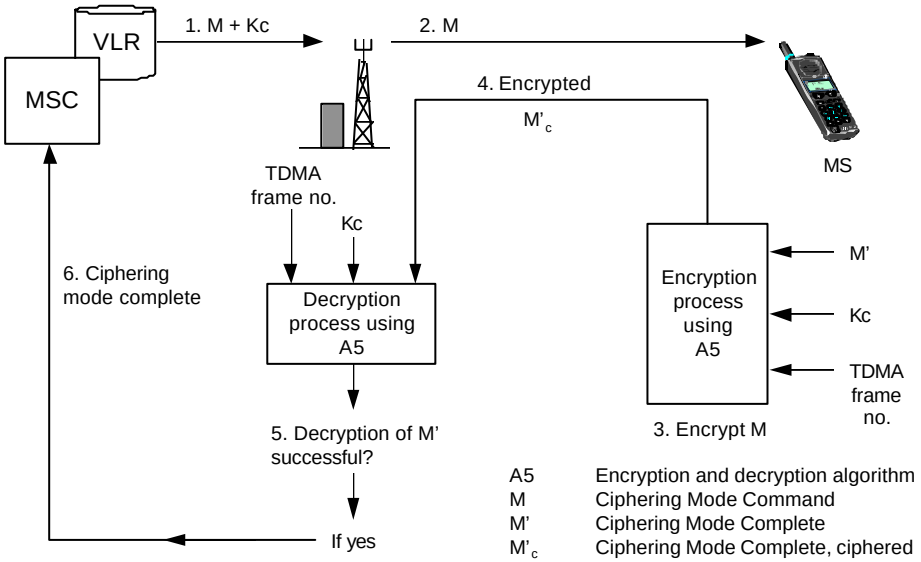
There are actually 2 A5 algorithms. The A51 algorithm was of military grade and could only be used in NATO countries. This has been replaced by a non-military grade general GSM algorithm called A52.

Confidentiality means that user information and signaling exchanged between BTS's and MS's is not disclosed to unauthorized individuals, entities or processes.

A ciphering sequence is produced using Kc and the TDMA frame number as inputs in the encryption algorithm A5. The purpose of this is to ensure privacy concerning user information (speech and data) as well as user related signaling elements.

In order to test the ciphering procedure some sample of information must be used. For this purpose the actual ciphering mode command (M) is used.

1. M and Kc are sent from the MSC/VLR to the BTS.
2. M is forwarded to the MS.
3. M is encrypted using Kc (calculated earlier with SRES in the authentication procedure) and the TDMA frame number which are fed through the encryption algorithm, A5.
4. The encrypted message is sent to the BTS.
5. Encrypted M is decrypted in the BTS using Kc, the TDMA frame number and the decryption algorithm, A5.
6. If the decryption of M was successful, the ciphering mode completed message is sent to the MSC. All information over the air interface is ciphered from this point on.



A5	Encryption and decryption algorithm
M	Ciphering Mode Command
M'	Ciphering Mode Complete
M'_c	Ciphering Mode Complete, ciphered
Kc	Ciphering key
MSC	Mobile services Switching Center
VLR	Visitor Location Register

Figure 6-8 Ciphering procedure

EIR FUNCTIONS

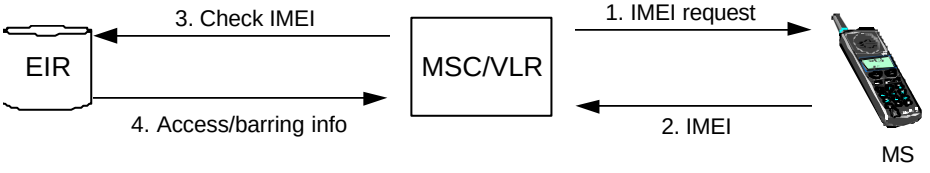
Equipment Identification Procedure

☞ Did you know?

Up to recently, many networks did not use an EIR. However, a Centralised EIR (CEIR) has been set-up in Europe (located in Ireland) which is used by many European network operators.

The equipment identification procedure uses the identity of the equipment itself (IMEI) to ensure that the MS terminal equipment is valid.

1. The MSC/VLR requests the IMEI from the MS.
2. MS sends IMEI to MSC.
3. MSC/VLR sends IMEI to EIR.
4. On reception of IMEI, the EIR examines three lists:
   - A **white list** containing all number series of all equipment identities that have been allocated in the different participating GSM countries.
   - A **black list** containing all equipment identities that has been barred.
   - A **gray list** (on operator level) containing faulty or non - approved mobile equipment.
5. The result is sent to MSC/VLR, which then decides whether or not to allow network access for the terminal equipment.



IMEI	International Mobile station Equipment Identity
EIR	Equipment Identity Register
MSC/VLR	Mobile services Switching Center

Figure 6-9 Equipment identification

The decision to identify equipment remains with individual operators. GSM specifications recommend identification for each attempted call set-up.

AUC AND EIR IMPLEMENTATION

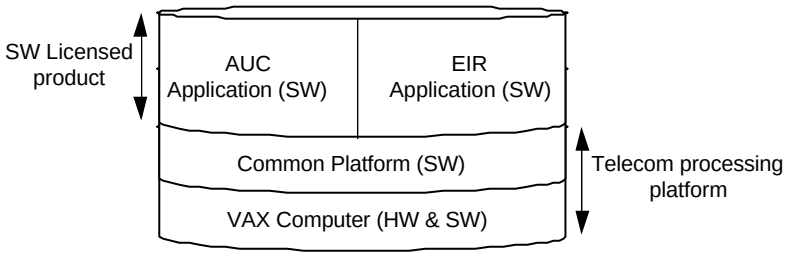
In a GSM network the AUC is connected directly to a HLR. The EIR is connected to an MSC/VLR.

In Ericsson's GSM systems the AUC may be implemented on either AXE or Unix (from Sema Group). The EIR is implemented on a Unix platform from Sema Group.

If implemented on AXE, the most common configuration for an AUC is integrated with a HLR as an AUC/HLR node. This reduces the signal processing requirements of both. The AUC is implemented using the AUC Application Module (AUCAM).

The most common implementation is a Unix-based AUC/EIR node, which provides the following benefits to the operator:

- AUC and EIR processing is physically separated from the switching function in the MSC. This provides better network planning flexibility when the network needs to be expanded.
- The common platform is based on standard industry computer hardware (HW) and software (SW).



AUC Authentication Center
EIR Equipment Identity Register
HW Hardware
SW Software

Figure 6-10 AUC/EIR product structure

DATA TRANSMISSION INTERFACE (DTI)

This section gives a brief introduction to the data handling capabilities of Ericsson's GSM systems. For a more detailed survey of such functions, please refer to the appendix titled "Data Services".

DTI FUNCTIONS

☞ Did you know?

In previous versions of CME20/CMS 40 the functions of the DTI were implemented using a GSM Inter-Working Unit (GIWU), separate from the MSC/VLR.

The DTI implements the GSM Inter-Working Function (IWF). It performs data handling functions such as data rate conversion and provides the functions necessary for data interworking between GSM networks and other networks, including:

- **Data Traffic to/from PSTN:** this involves modem and fax calls. For connections to the PSTN a modem is selected by the DTI to perform the necessary rate and format conversions.
- **Data Traffic to/from ISDN:** the whole set of data communications towards ISDN is available, since the MSC/DTI is capable of signaling and mapping basic service information between the ISDN and the GSM network.
- **Data Traffic to/from PDNs:** the DTI handles data traffic to and from Public Data Networks (PDNs) such as the Packet Switched PDN (PSPDN) and Circuit Switched PDN (CSPDN).
- **Data Traffic between mobiles:** the data traffic inside the PLMN must pass through the DTI to handle the protocol used for rate adaptation in the radio path.
- **HSCSD:** this version of High Speed Circuit Switched Data (HSCSD) allows the connection of 2, 3, or 4 time slots on one radio channel each carrying 9.6 kbits/s. The DTI handles rate conversion to PSTN or ISDN as appropriate.

DTI IMPLEMENTATION

The DTI is integrated within an MSC/VLR. The DTI is managed by the Data Transmission Subsystem (DTS).

The DTI sub-rack contains eight plug-in units, each one supporting four data channels. Therefore, each DTI sub-rack can support a total of 32 simultaneous data calls.

MESSAGE CENTER (MC)

MC FUNCTIONS

An MC may be added to a GSM network to provide one or more of the following messaging services:

- Voice mail
- Fax mail
- Short Message Service (SMS) text messages
- SMS Cell Broadcast (SMSCB) text messages

These services can generate considerable revenue for a network operator, as they are becoming increasingly popular.

Voice Mail

Voice mail ensures that all calls to a person can be completed, even when a person does not answer calls. A calling party can record a voice message for the subscriber they are calling.

A subscriber can use their MS to select diversion to voice mail based on a particular event or status (e.g. busy, unreachable).

The subscriber is informed that they have voice messages in their mailbox by means of either a short text message or phone call from the network at regular intervals. If their MS is detached, this indication is sent when the subscriber next attaches to the network.

The subscriber can then retrieve their voice mail messages at a later stage. Functions for storing voice messages over a long period also exist.

Fax Mail

Fax mail operates similarly to voice mail. For MS's that support fax, a subscriber can set diversion for all or some fax calls to a fax mailbox. When the MS is next attached to the network, the network will deliver the fax message to a fax machine identified by the MS.

SMS

A short text message consists of up 160 alphanumeric characters, entered at a Short Message Entity (SME) such as an MS (using the keypad) or computer terminal.

A short message always originates or terminates in a GSM network, meaning that a short message can not be sent between two SMEs residing outside a GSM network.

The short message originator knows if the message delivery is successful or unsuccessful via notification. When a message is submitted, the deferred delivery option can be requested. This option makes it possible to specify the time the message is to be delivered.

An MC, which handles SMS messages is often referred to as an SMS Center (SMS-C). When a message is to be forwarded to an MS, the system must first determine where the MS is situated. As in ordinary voice traffic, a gateway requests the routing information. The gateway is called the SMS GMSC.

Each short message is time stamped by the SMS-Center when it is submitted. A message is deleted once the delivery is successful or once the time specified in deferred delivery expires.

When a message is buffered, the SMS-C regularly attempts to deliver the message, at intervals defined by the operator.

SMSCB

The SMSCB service enables a message of up to 93 alphanumeric characters to be delivered to all attached MS's in one cell. This may be useful for identifying key phone numbers in the cell's area such as that of a hospital or police station. Alternatively, it may be used for advertising services within the cell (e.g. "Superfood Restaurant in this area at the junction of M8 and I33").

MC IMPLEMENTATION

One MC node may handle one or more messaging service. For example, depending on the amount of SMS traffic, it may be more efficient to have one MC acting as an SMS-C only, with other messaging services handled by another separate MC.

It is also possible to integrate SMS-C functions on an MSC, leading to the term SMS InterWorking MSC (SMS-IWMSC). Additionally, the SMS GMSC functions may reside in the same node as the GMSC functions used for voice calls.

In Ericsson's GSM systems the MC is implemented by Ericsson's MXE product. The most important component of MXE is the message kernel. The message kernel is the central message store and forward nucleus responsible for safe storage of messages, routing and retry attempts.

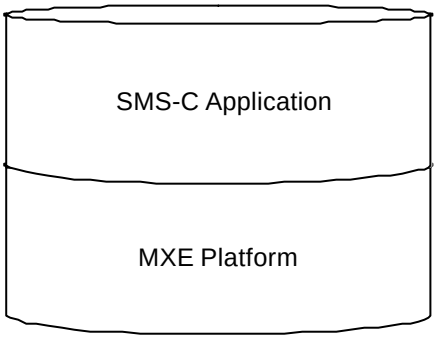


Figure 6-11 SMS-C on an MXE

SERVICE SWITCHING FUNCTION (SSF), SERVICE CONTROL FUNCTION (SCF) AND SERVICE DATA POINT (SDP)

This section gives a brief introduction to the Mobile Intelligent Network (MIN) handling capabilities of Ericsson's GSM systems. For a more detailed survey of such functions, please refer to the appendix titled "Mobile Intelligent Network Services".

Mobile Intelligent Network (MIN) nodes can be added to a basic GSM network to provide value-added services such as Freephone and Personal Number to subscribers.

Ericsson's MIN nodes include:

- **Service Switching Function (SSF):** an SSP acts as an interface between the call control functions of the mobile network and the service control functions of a Service Control Point (SCP). Ericsson's SSP is an AXE-based AM (SSFAM) and may be integrated within an MSC/VLR (recommended) or stand-alone.
- **Service Control Function (SCF):** a SCP contains the intelligence of a MIN service or services. This intelligence is realized in software programs and data. Ericsson's SCP is also an AXE-based AM (SCFAM) and the recommended configuration is as a stand-alone node, accessible by all MSC/SSPs.
- **Service Data Point (SDP):** an SDP manages the data which is used by a MIN service. Ericsson's SDP is a stand-alone node based on Unix.