Nokia Siemens Networks

3G Rel4 SCNOM

Subscriber Administration

Training Document

Legal notice

Intellectual Property Rights

All copyrights and intellectual property rights for Nokia Siemens Networks training documentation, product documentation and slide presentation material, all of which are forthwith known as Nokia Siemens Networks training material, are the exclusive property of Nokia Siemens Networks. Nokia Siemens Networks owns the rights to copying, modification, translation, adaptation or derivatives including any improvements or developments. Nokia Siemens Networks has the sole right to copy, distribute, amend, modify, develop, license, sublicense, sell, transfer and assign the Nokia Siemens Networks training material. Individuals can use the Nokia Siemens Networks training material for their own personal self-development only, those same individuals cannot subsequently pass on that same Intellectual Property to others without the prior written agreement of Nokia Siemens Networks. The Nokia Siemens Networks training material cannot be used outside of an agreed Nokia Siemens Networks training session for development of groups without the prior written agreement of Nokia Siemens Networks.

Indemnity

The information in this document is subject to change without notice and describes only the product defined in the introduction of this documentation. This document is intended for the use of Nokia Siemens Networks customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of Nokia Siemens Networks. The document has been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using it. Nokia Siemens Networks welcomes customer comments as part of the process of continuous development and improvement of the documentation.

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is” and all liability arising in connection with such hardware or software products shall be defined conclusively in a separate agreement between Nokia Siemens Networks and the customer. However, Nokia Siemens Networks has made all reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions. Nokia Siemens Networks will, if deemed necessary by Nokia Siemens Networks, explain issues which may not be covered by the document.

Nokia Siemens Networks will correct errors in the document as soon as possible. IN NO EVENT WILL NOKIA SIEMENS NETWORKS BE LIABLE FOR ERRORS IN THIS DOCUMENT OR FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY MONETARY LOSSES,SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA,THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT

This document and the product it describes are considered protected by copyrights and other intellectual property rights according to the applicable laws.

Wave logo is a trademark of Nokia Siemens Networks Oy. Nokia is a registered trademark of Nokia Corporation. Siemens is a registered trademark of Siemens AG.

Other product names mentioned in this document may be trademarks of their respective owners, and they are mentioned for identification purposes only.

Contents

1 Objectives

On completion of this module, you should be able to:

- List teleservices provided in NSN entity
- List basic supplementary services in GSM and UMTS
- Explain five locations where subscriber data is stored in the GSM and UMTS networks
- Explain best describes the authentication mechanisms used in GSM and UMTS
- Identify examples of register data
- Give the maximum capacities of the HLR, VLR, AC, and EIR
- Explain the use of NSN specific parameters in EIR, HLR and VLR

2 Introduction

This module introduces subscriber administration of the DX 200 HLR/AC/EIR and DX 200 MSS/VLR. The document covers GSM and UMTS services, the different network elements employed in subscriber administration, the concept of GSM and UMTS security, and parameter management.

The idea behind GSM/UMTS is to allow subscribers to move and change location whenever necessary, which requires the network to have a place for storing information about subscriber locations. Information about subscriber location is stored in the:

- Home Location Register (HLR), where the subscriber’s data is stored permanently
- Visitor Location Register (VLR), where subscribers’ data is stored as long as they are under the service area of the MSS/VLR in question

The GSM and UMTS networks are compatible with the Integrated Services Digital Network (ISDN). Information about subscriber services (speech, data, fax, and short messages), stored in the HLR and VLR, is interpreted in the network.

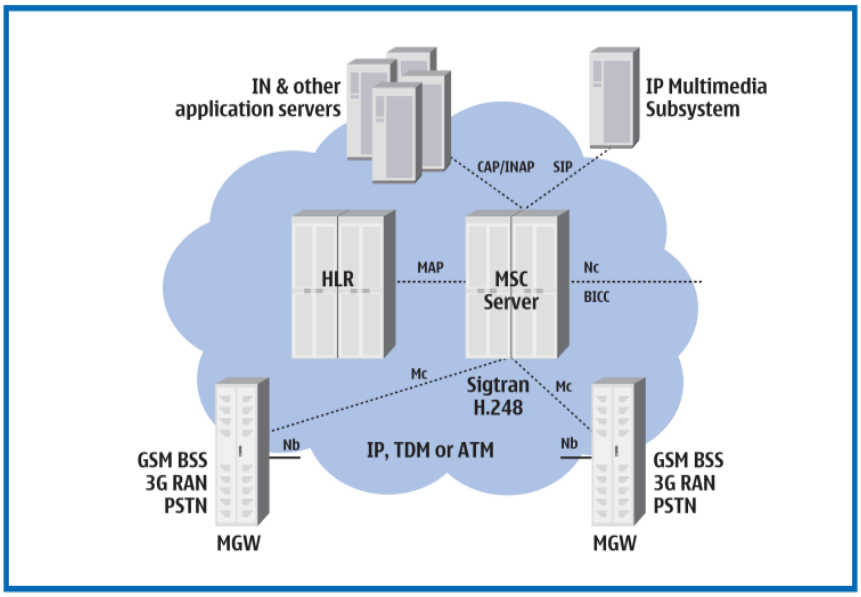


Figure 1 GSM / 3G network

3 GSM and UMTS Services

There are two kinds of services:

Basic service is the "stand-alone" service. If a subscriber needs a certain type of connection to other subscribers (for example, speech) the subscriber can buy it from the operator. In order to use another basic service (for example fax service), the subscriber needs to buy it separately.

Supplementary service is used together with a basic service in order to add functionality to the basic service, for example, forwarding a call to another number when the subscriber is not answering.

3.1 Basic Services

Basic services are divided into two categories: teleservices and bearer services.

Figure 2 illustrates the difference.

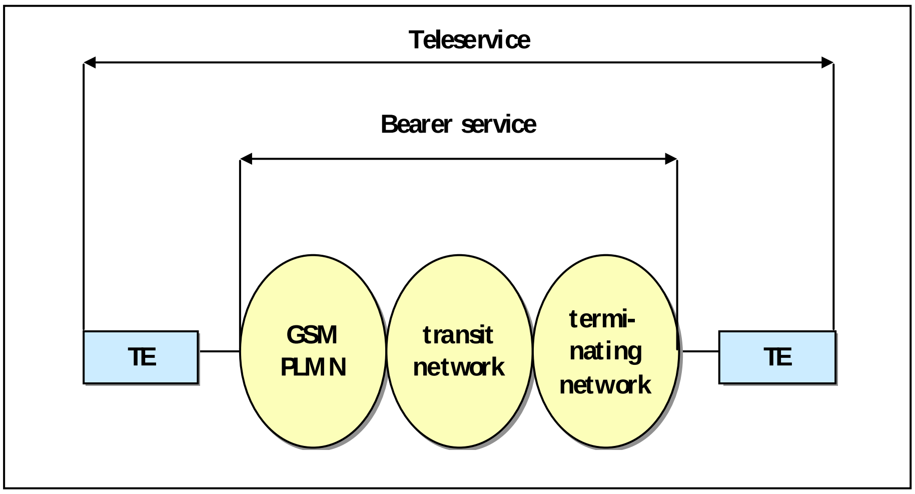


Figure 2 Teleservices and bearer services

3.2 Teleservice

Teleservices are telecommunication services that are related to the user information type (for example, short messages, fax data, or speech) or high layer capabilities. Teleservices can transfer different types of user information from one terminal to another. This service is more popular than the bearer service.

Table 1 shows the categories of teleservices and the individual teleservices.

Table 1 Teleservice categories and services

User info. type	**Teleservice category**		**Individual teleservice**		
	No.	**Name**	**No.**	**Name**	
Speech	1	Speech transmission	11 12	Telephony Emergency Calls	
Short message	2	Short message service	21 22 23	Short message MT/PP Short message MO/PP Short message cell broadcast	
Facsimile	6	Facsimile transmission	61	Alternate speech and facsimile group 3	T NT
			62	Automatic facsimile group 3	T NT

This document focuses on speech services (T11 and T12).

3.2.1 Telephony (T11)

The most popular teleservice is speech. In the GSM specification, it is known as T11 (Telephony).

3.2.2 Emergency Call (T12)

Emergency Call is a special type of speech call. The GSM system does not perform subscription checks for an emergency call. Therefore, you do not need to define the T12 service separately for the subscribers.

In the GSM system, an international emergency number, 112, is reserved for emergency calls in all PLMNs. In addition to 112, other numbers can be defined as emergency numbers.

There are several reasons to make a normal call different from an emergency call (see Table 2)

Table 2. Comparison between telephony and emergency calls

Compared cases	**Telephony**	**Emergency calls**
1. Call from MS without SIM	Not allow	Allow
2. Call from Mobile Equipment which is in black or grey list	Not allow	Allow
3. Call from a subscriber who activates call barring	Not allow	Allow
4. Priority of call	Normal	High
5. Chargeable call	Yes	No
6. Destination network	PSTN/ISDN/GSM-PLMN	PSTN/ISDN
7. Type of call	International or National	National
8. Characteristic of call	Normal	Emergency
9. Restriction analysis	Used	Not used
10. Call establishment message	SETUP	EMERGENCY_SETUP

3.3 Bearer Services

The bearer services supported by the GSM system enable the transmission of signals in a GSM network and an appropriate access point in the terminating network. Bearer services take the following low layer capabilities into account: 1.2 Kbit/s, 2.4 Kbit/s or 9.6 Kbit/s.

3.3.1 Two Main Types of Bearer Services

The DX 200 exchange supports the following bearer services:

- Asynchronous bearer services
  - Transparent and non-transparent
- Synchronous bearer services
  - Transparent

In asynchronous transmission the bit flow through the network is not continuous: the transmitting and the receiving data terminals maintain their synchronism over one single character at a time. Start and stop bits must be used so that the transmitting and receiving data terminals can operate at exactly the same speed.

In synchronous transmission the bit flow through the network is continuous, and the transmitting and receiving data terminals are bit-synchronised. Start and stop bits are not needed.

If the air interface connection is non-transparent, the GSM network can correct the detected errors with an error correction protocol such as Radio Link Protocol (RLP). The RLP takes care of error correction by resending the corrupted parts of the data. This means that the data rate used in the connection may vary.

If the air interface connection is transparent, there is no error correction in the air interface. This means that the data rate is the same throughout the connection. However, the terminals may (or may not) take care of the error detection (end-to- end error correction).

3.3.2 Bearer Service Classes

Bearer services are further divided into different classes by the type of digital data transmitted (either asynchronous or synchronous). With the General Bearer Services (GBS) concept, bearer services are combined into two classes. Class BS20 covers all asynchronous data rates, and class BS30 covers all synchronous data rates.

In a multi-numbering scheme, each data service used by a subscriber is assigned an MSISDN. The PLMN identifies the service with the Bearer Capability Information Element (BCIE).

In a single numbering scheme, the subscriber has only one MSISDN that covers all the services provisioned for him. This means that no association between the MSISDN and the provisioned data services is made in the HLR.

According to the General Bearer Services (GBS) concept, bearer services are not separated according to the user rates. Instead, there is only one asynchronous bearer service that covers all asynchronous data rates, and one synchronous bearer service that covers all synchronous data rates. The data rate is negotiated in the call set-up.

This way the GBS concept reduces the number of bearer services and telephone numbers needed by the subscriber. Certain features, such as High Speed Circuit Switched Data, require the General Bearer Services in order to function.

Table 3 Bearer services can be defined in DX 200 HLR

B11	Data c.d.a 300bps
B12	Data c.d.a 1200bps
B13	Data c.d.a 1200-75bps
B14	Data c.d.a 2400bps
B15	Data c.d.a 4800bps
B16	Data c.d.a 9600bps
B17	General Data c.d.a
B1A	Data c.d.s 1200bps
B1C	Data c.d.s 2400bps
B1D	Data c.d.s 4800bps
B1E	Data c.d.s 9600bps
B1F	General Data c.d.s

3.4 Basic Supplementary Services

Supplementary services (SS) add new functionalities to a basic service. They are not stand-alone services, but they are offered together with a basic service.

The same supplementary service can be offered for different basic services. For example, a subscriber can have Call Waiting (CW) as a supplementary service for telephony and facsimile services independently.

A supplementary service modifies or supplements a basic telecommunication service. Consequently, it cannot be offered to a user as a stand-alone service. It must be offered with a basic telecommunication service.

All supplementary services are divided into two main types: Basic SS and NSN-specific SS types. The Basic SS type stands for all the supplementary services that refer to GSM specifications. The NSN-specific SS type covers all the supplementary services that are provided by NSN and not included in GSM specification.

3.4.1 Actions and States of Supplementary Services

Before going through supplementary service examples, it is important to understand the following actions and states of supplementary services provided by the network.

Activation

This process enables a service to run a process. (Done by the service provider, subscriber, or the system)

Deactivation

This process terminates the activation process. (Done by the service provider, subscriber, or the system)

Active and operative

The status of the supplementary service when it is activated and the subscriber can operate with it.

Active and quiescent

The status of the supplementary service when it is activated, but the subscriber cannot operate with it.

The quiescent state cannot be set by MML command, but it is set automatically by interaction with some other supplementary service. For example, if one of the Call Forwarding Conditional (CFC) services is active and operative for the subscriber and the subscriber then registers to Call Forwarding Unconditional (CFU), the CFC becomes active and quiescent until the CFU is deactivated.

Examples of basic supplementary services are:

- Calling Line Identification Presentation and Restriction
- Call Waiting, Call Hold, and Multiparty Service
- Closed User Group (CUG)
- Call Barring
- Operator Determined Barring (ODB)
- Call Forwarding
- Advice of Charge (AOC)
- Explicit Call Transfer (ECT)

3.4.2 Calling Line Identification Presentation and Restriction

There are three services related to the Calling Line Identification Presentation:

- Calling Line Identification Presentation (CLIP)
- Calling Line Identification Restriction (CLIR)
- Calling Line Identity (CLI) support for roaming subscribers

Calling Line Identification Presentation (CLIP)

This service allows the subscriber to see the calling phone number in the display of the Mobile Station. The end-user sees the phone number of the caller before answering. The end user can prepare to answer or can choose to reject the call.

In case the mobile phone has a missed call logging feature, the subscriber knows which calls were not answered and can call back. This increases the number of successful calls and, thereby, the operator's revenue.

Figure 3 shows the flow of data for CLIP.

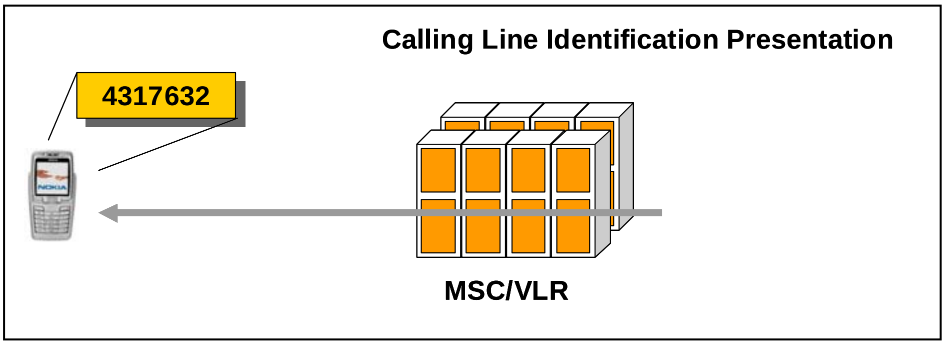


Figure 3 Calling Line Identification Presentation (CLIP)

Calling Line Identification Restriction (CLIR)

This service does not allow the network to send the MSISDN of the calling mobile subscriber to the called subscriber at the other end. With CLIR, the calling line identity is not presented to the called party although CLIP is active.

Figure 4 shows the flow of data for CLIR.

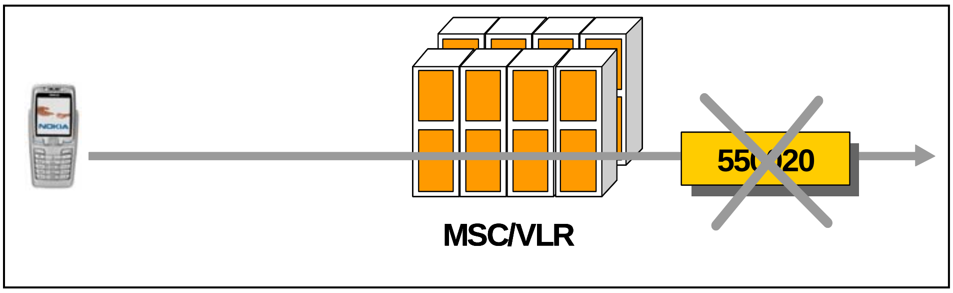


Figure 4 Calling Line Identification Restriction (CLIR)

The service provider can select whether the CLIR service is permanent or temporary. The *permanent mode* means that the calling party's number is never sent to the called party by the terminating MSS. In the *temporary mode*, subscribers can control the presentation of their numbers to the called party on a per-call basis.

As an additional feature, the called party can have an override category feature that allows CLI presentation. The Override Category is available in the CLIP service.

Calling Line Identity (CLI) support for roaming subscribers

This feature provides a second route for CLI transportation via Mobile Application Part (MAP). CLI transport via MAP is more successful and provides the CLI, if desired.

For some time, the CLI has been transported to the end-user by signalling, as with ISDN User Part (ISUP). This has not always been the case when the subscriber is roaming outside the home network, due to

- A lack of signalling level, and
- No agreement between operators.

CLI support for roaming subscribers provides a second route for the CLI transportation via Mobile Application Part (MAP).

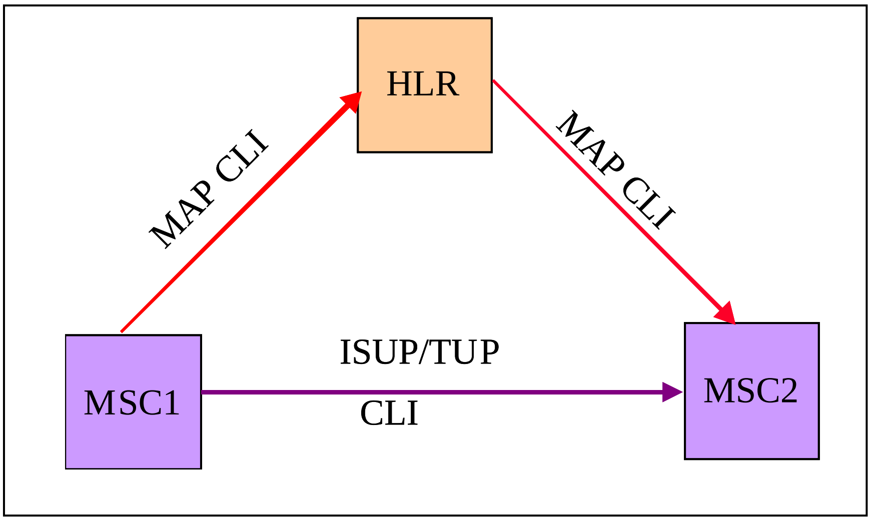


Figure 5 CLI for roaming subscriber

3.4.3 Call Waiting, Call Hold, and Multiparty Service

These three supplementary services are presented together because they are often used together.

Call Waiting is a supplementary service that enables the network to inform a busy subscriber that another call is waiting to be answered.

If the subscriber wants to answer the waiting call but does not want to release the first call, the subscriber can put the first call on hold using the supplementary service *Call Hold*.

Finally, it is also possible to combine both calls into one conversation with the *Multiparty Service*. In one conversation, there can be up to six subscribers including the mobile subscriber.

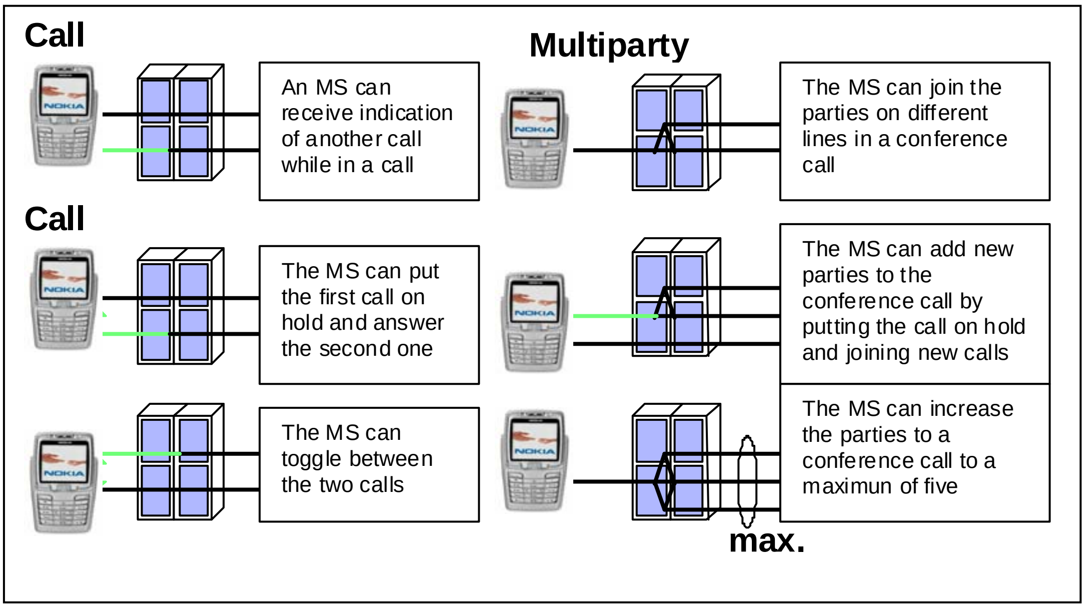

Call
An MS can receive indication of another call while in a call
Call
The MS can put the first call on hold and answer the second one
The MS can toggle between the two calls
Multiparty
The MS can join the parties on different lines in a conference call
The MS can add new parties to the conference call by putting the call on hold and joining new calls
The MS can increase the parties to a conference call to a maximun of five
max.

Figure 6 Call Waiting, Call Hold, and Multiparty Service

3.4.4 Closed User Group (CUG)

Access to CUGs can be restricted. Members of the same CUG can communicate among each other but not, in general, with users outside the group.

The service enables a closed communication environment to be set up for reasons of privacy and cost control. For example, members of a CUG can be employees of a company who are allowed to communicate only with each other.

Additional capabilities and restrictions can be specified for each member of the closed user group. The additional capabilities allow the member to communicate with subscribers outside the closed user group. The additional restrictions prevent communication with other members in that closed user group. See Figure 7 for an illustration.

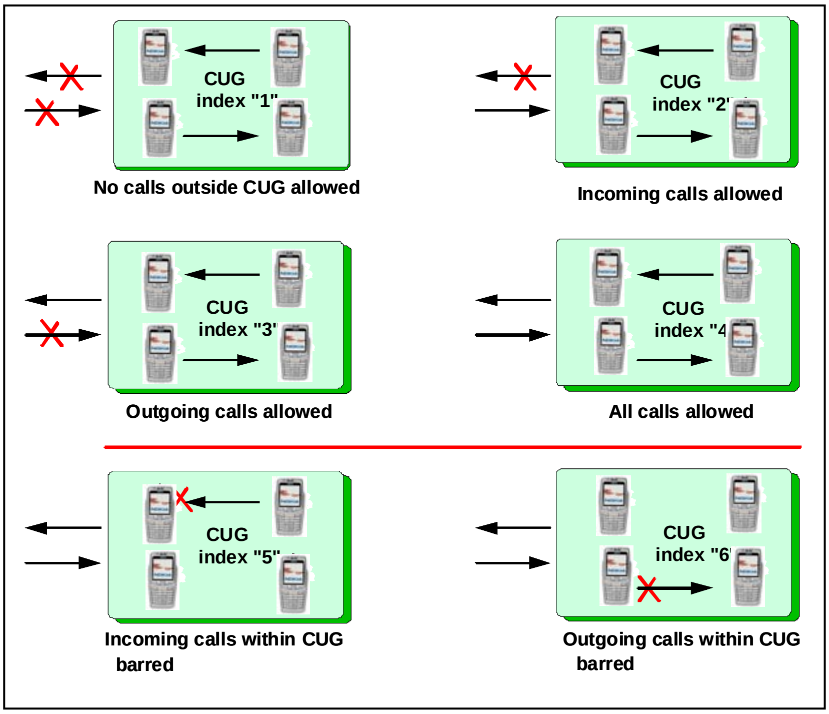


Figure 7 Closed user group

3.4.5 Call Barring

This supplementary service enables the subscriber to bar certain types of calls (such as incoming calls, outgoing calls or international calls). Call barring can be done in several ways. Examples of call barring are shown in Figure 8. It is possible to use supplementary service group codes in the deactivation of CB services (all CBs, BICs, and BOCs).

The procedures for setting Call Barring are:

1. The operator provides the subscriber Call Barring supplementary services and the password by using the ZMS command group. The subscriber can change the password later.
2. There are two ways to activate and deactivate Call Barring:
   - By subscriber: A four-digit password has to be given in order to activate/deactivate Call Barring. This password is the same for all call barring cases.
   - By you: Use the ZMS command group.

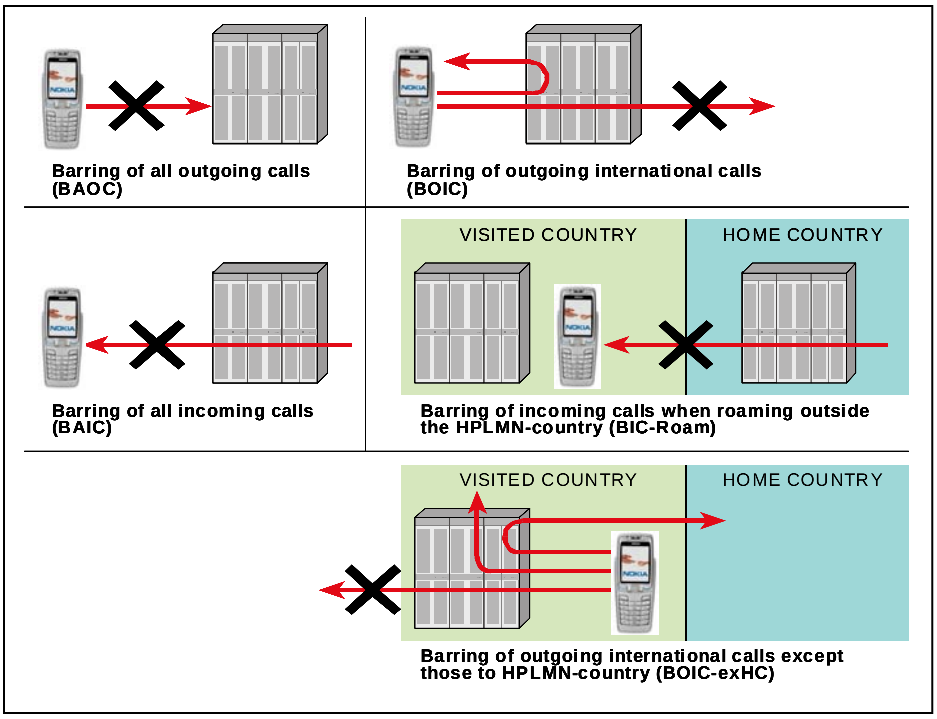

Barring of all outgoing calls
(BAOC)
Barring of outgoing international calls
(BOIC)
Barring of all incoming calls
(BAIC)
VISITED COUNTRY
HOME COUNTRY
Barring of incoming calls when roaming outside
the HPLMN-country (BIC-Roam)
VISITED COUNTRY
HOME COUNTRY
Barring of outgoing international calls except
those to HPLMN-country (BOIC-exHC)

Figure 8 Call barring situations

3.4.6 Operator Determined Barring (ODB)

You can use the ODB feature to bar incoming/outgoing calls, and subscriber roaming and service access.

This optional feature applies to the following services:

- CBO – barring of outgoing calls
- BAPR – barring of premium rate calls
- CBI – barring of incoming calls
- BOS – operator specific barring category
- BASS – barring of supplementary service management
- BREG – barring of registration of forward-to number
- BICT – barring of invocation of call transfer <option>
- BOSCF – operator specific barring of cf registration <option>
- ROAM – categories active only when roaming <option> (Possible for BICT, BASS, CBO, and BAPR.)
- BAPS – barring of all packet oriented services
- BCCF – barring of changing a call forwarding number

- BMSP – barring of mobile station initiated PDP context activation
- BPSH – barring of packet oriented services from access points in the HPLMN while the subscriber is roaming in the VPLMN
- BPSR – barring of all packet oriented services while the subscriber is roaming in the VPLMN
- BPSV – barring of packet oriented services from access points in the roamed-in VPLMN

Services affected by ODB are automatically set to inactive. For example, subscriber call forwarding services are set to inactive when you activate the barring of all outgoing calls for the subscriber. When barring is cancelled, the call forwarding service automatically becomes active again.
Figure 9 illustrates operator-determined barring.

You can set, cancel, or display ODB using the ZMG command group in the HLR. When you activate ODB with any type of outgoing call barring services, you need to define the call barring analysis of ODB in the MSSs with the ZRK command group.

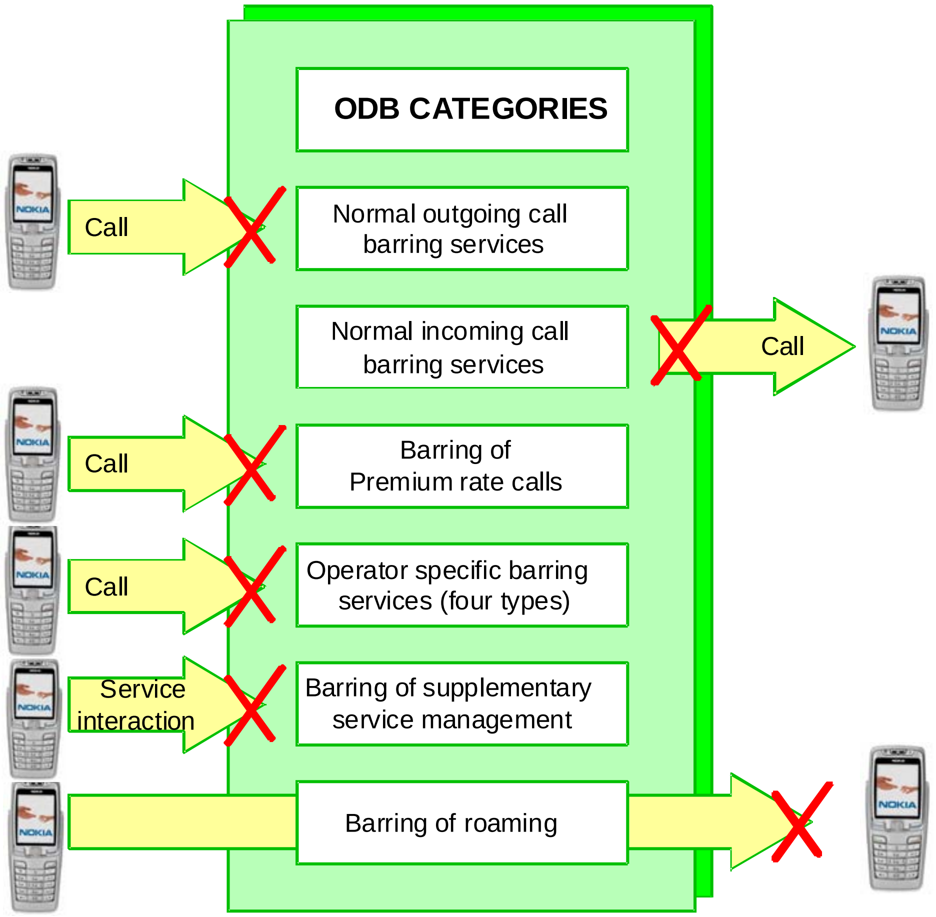

ODB CATEGORIES
Call
Normal outgoing call barring services
Normal incoming call barring services
Call
Call
Barring of Premium rate calls
Call
Operator specific barring services (four types)
Service interaction
Barring of supplementary service management
Barring of roaming

Figure 9 Operator-determined barring

3.4.7 Call Forwarding

Call forwarding is a supplementary service, which enables you to define where to forward an incoming call when an MS is busy, not reachable, or there is no answer. Call forwarding can also be unconditional.

This feature allows you to increase the amount of traffic generated in the network and the ratio of successful calls, and enables you to create operator-specific services, which increase your competitive edge.

The call forwarding package contains the following services:

- CFU - *Call Forwarding Unconditional*. All calls are forwarded to a destination pre-defined by the mobile user.

- CFC - *Call Forwarding Conditional*
- CFB – *Call Forwarding on MS Busy.* Calls are forwarded to a destination pre-defined by the mobile user if the called mobile is busy.
  - CFB-NDUB: *Call Forwarding on Busy – Network Determined, User Busy*
  - CFB-UDUB: *Call Forwarding on Busy – User Determined, User Busy*
- CFNA – *Call Forwarding on No Answer.* Calls are forwarded to a destination pre-defined by the mobile user if they are not answered within the period defined by the no reply timer. The default value of the no reply timer is 30 seconds.
- CFNR – *Call Forwarding on MS Not Reachable.* Calls are forwarded to a pre-defined destination if the called mobile is not reachable because the mobile is deregistered due to radio congestion or no paging response*.*

The subscriber can set a different forwarded-to number for each of the above services.

Calls cannot be forwarded if incoming or outgoing calls are barred, or if the number to which a call is to be forwarded is barred.

Figure 10 shows the services contained in the call-forwarding package.

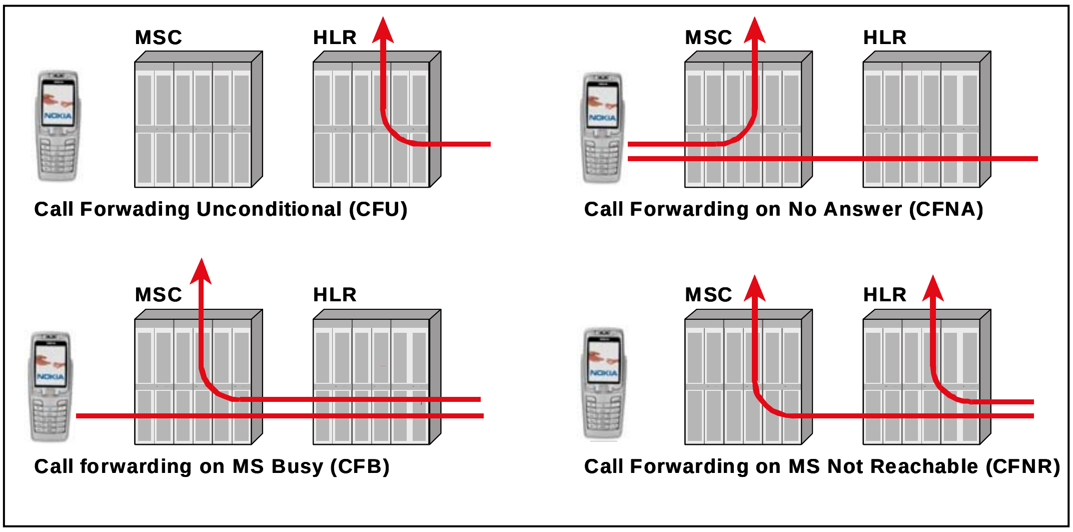

MSC
HLR
Call Forwading Unconditional (CFU)
MSC
HLR
Call Forwarding on No Answer (CFNA)
MSC
HLR
Call forwarding on MS Busy (CFB)
MSC
HLR
Call Forwarding on MS Not Reachable (CFNR)

Figure 10 Different call forwarding supplementary services

When a call is forwarded in an exchange, the call control updates a Call Forwarding Counter (CFC). The value of the CFC is always updated when the MSS receives the C-number from the VLR or the HLR. If the maximum number of call forwarding expires, the service is interrupted and an indication of a call forwarding failure is sent downwards.

The signalling network sends the number of call forwarding incidences. The maximum number of call forwarding incidences is five. However, extra call forwarding is allowed, as for example, to the VMS as shown in Figure 11. You define the maximum number of call forwarding occurrences.

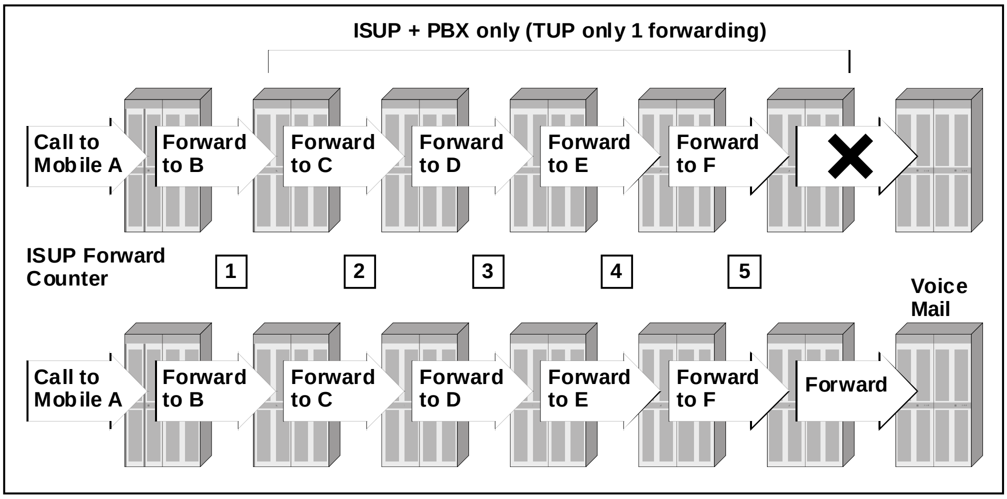


Figure 11 Prevention of call forwarding loops by forward counter

3.4.8 Advice of Charge (AOC)

The advice of charge supplementary service provides a mobile station with cost estimate for the call. At the beginning of each call (or, if necessary, during the call), the mobile station receives the AOC information from the exchange. The AOC information contains the elements (e-parameters) that define the rate at which the call is to be charged, the time dependence, and the unit increments. This is possible for mobile originating calls and for the roaming leg part in mobile-terminating calls.

AOC has two services:

- Advice of charge for information
- Advice of charge for charging

Advice of charge for information (AOCI)

This information service gives the mobile station an estimate of the cost of the call. The information is given in the subscriber's national currency. The charges are indicated for the following:

- Call in progress if the call is mobile-originated
- Roaming leg only if the call is mobile-terminated

The mobile station receives the e-parameters when the call begins or if the tariff changes during the call. If the tariff does not change, the first e-parameters are used during the whole call.

Advice of charge for charging (AOCC)

This charging service enables the mobile station to show the charge for a mobile-originated call or for the roaming leg in a mobile-terminated call to the caller. This service is intended for pay phones so that the caller knows how much the call costs and how much money is left. The e-parameters also are sent to the mobile station in this case, but the mobile sends an acknowledgement for the message before the call can be made.

3.4.9 Explicit Call Transfer (ECT)

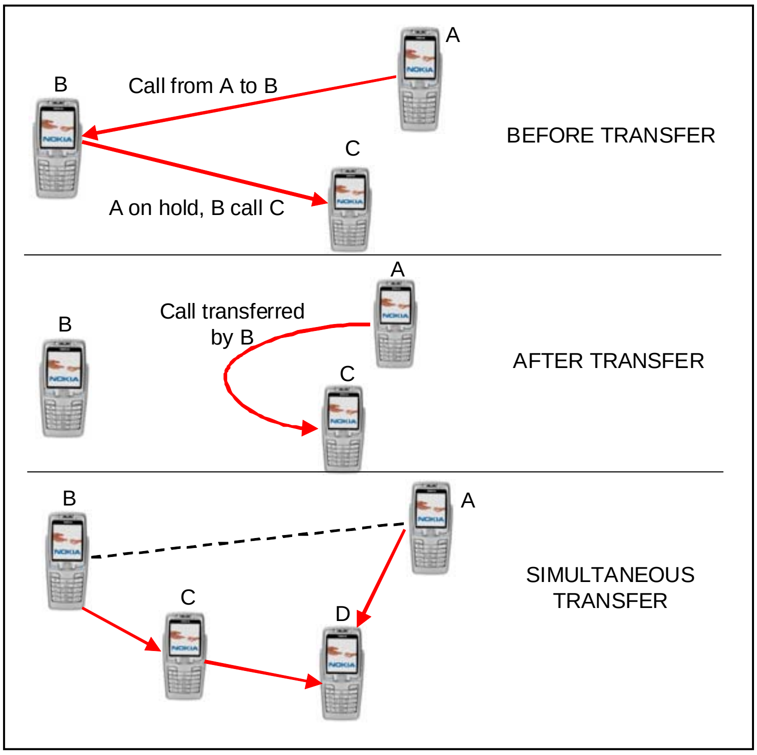


Figure 12 Explicit Call Transfer

ECT, supported in UMTS, enables a subscriber to transfer an established call to a third party without compromising ongoing activities.

ECT can be used when a subscriber is in a call and has another call on hold (both of which can be incoming or outgoing calls).

When the subscriber wants to transfer the ongoing call to the third party, who is now on hold, the subscriber connects the third party, exits the call, and resumes other mobile station connections.

If the call transfer fails, the call is connected back to the subscriber who initiated the transfer. Or the transfer party can use the call transfer recall to have the call returned if the transferred-to party does not answer the call.

The following ECT functionalities are introduced first time in the M12 release:

- Loop prevention mechanism, which prevents subscribers from transferring calls to themselves
- Notification about the transfer to parties involved in the ECT (Subscriber B and C), including the number of the other party

3.5 Additional Supplementary Services

Examples of additional supplementary services are:

- Completion of Calls to Busy Subscribers (CCBS)
- Completion of Calls on No Reply (CCNR)
- Hot Billing
- User-to-user Signalling (UUS)
- Connected Line Identification Services
- Location Services (LCS)
- Multicall

3.5.1 Completion of Calls to Busy Subscribers (CCBS)

CCBS is a supplementary service for the calling subscriber. The CCBS service allows the caller to activate call completion with a busy called user. The caller is put into a special queue to have the call go through once the person being called is available. The network monitors the destination called user to determine when the person’s mobile unit becomes idle.

Figure 13 shows the architecture for call completion supplementary services architecture.

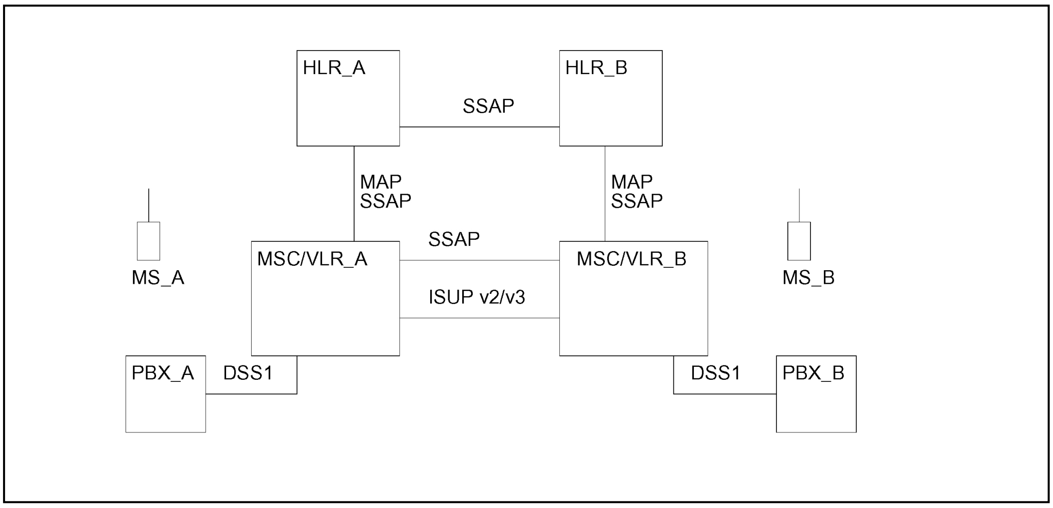


Figure 13 Elements in CCBS

Key features of the CCBS service are:

- If the called party is busy, the network offers the CCBS service to the calling subscriber.
- When the calling party activates the CCBS, the network starts monitoring the busy called party.
- When the called party becomes free again, the calling party receives an indication of this status change. If the calling party accepts the indication, the network generates a new call, a *CCBS call*, to the called user. This call has precedence over normal calls.

After a successful call setup, the CCBS-specific resources are freed. When the calling party activates the service, the CCBS request is saved both in the originating queue and the target queue in the HLR. Each queue can store up to five CCBS requests.

CCBS increases operator profits by increasing number of initially successful calls. The subscriber benefits by not having to keep calling busy destination B; instead, the monitoring is left to the network. CCBS is also easy to use, since the network offers it automatically to the subscriber.

CCBS is supported all along the communication path, and that there have been no call forwardings (such as CFU , CFNRy , or CFNRe).

CCBS is not available for emergency calls.

CCBS has to be supported by both the origin and the destination PBX exchanges.

3.5.2 Completion of Calls on No Reply (CCNR)

CCNR service, which enables the subscriber A to have a call completed to a target subscriber who is currently not at home or not reachable. CCNR is not applicable to GSM, it is only applicable between PBX and PBX, or PBX and ISDN.

CCNR is not available for emergency calls.

CCNR has to be supported by both the origin and the destination PBX exchanges.

3.5.3 Hot Billing

Hot billing is a supplementary service; with it, you can provision to the subscriber in the HLR. Hot Billing is provisioned with home subscriber data handling MML programs. The subscriber data is stored to the HLR database.

With Hot Billing, detailed charging records related to a selected set of mobile subscribers can be sent immediately to the post-processing system.

The records also can be stored as follows:

- In the standard way on devices elsewhere and transferred among the other records.
- On the dedicated Virtual Data Storing Device (VDS). With the VDS device, the Hot Billing Call Detail Record (CDRs) can be stored on the disks of the Charging Unit (CHU) in the same way as the normal CDRs. They also must be transferred to the Billing Centre in the same way as normal CDRs.

Hot billing data can be transferred over:

- Connection Oriented Transport Service (COTS)
- Hot Billing Logical File (HBLOFI)
- Transmission Control Protocol/Internet Protocol (TCP/IP)

Using TCP/IP, you can achieve a higher transfer rate to the post-processing system. Also, IP links tend to be more reliable and easier to configure than, for example, COTS.

3.5.4 User-to-user Signalling (UUS)

User-to-user signalling is a supplementary service that allows a subscriber to send (or receive) a limited amount of subscriber-generated information. Two examples of subscriber-generated information are: short messages and information indicating a service is activated.

The information can be sent and received in several situations:

- During the origination of a call. When the user pushes the "off hook" button, the calling party can activate the service in the call set-up phase and send text information.
- After the calling subscriber receives an indication that the called party is being informed of the call and when the remote party's phone is alerting, the called party can send text information to the calling party. In this message, the called party can state, for example, that the phone cannot be answered because the called party is in a meeting.
- While the connection is established, all parties (calling or called) can choose to activate the service. Then, all users can, for example, send text messages to each other.

The UUS has been categorized in three services. The services indicate the call phase in which information can be sent:

- UUS 1: in call setup; call release
- UUS 2: when remote party's communication equipment is in alert phase
- UUS 3: in active call

3.5.5 Connected Line Identification Services

The Connected line identification services feature has two supplementary services:

- Connected line identification presentation (COLP)
- Connected line identification restriction (COLR)

COLP enables the calling party to view the line identity of the subscriber to whom the call was connected. This is important, for example, when the call is forwarded and the caller wants to know the true destination of the call.

COLR prevents the presentation of the line identity at call destination. Subscribers may need this for privacy or security reasons.

3.5.6 Location Services (LCS)

The Location Services (LCS) feature in MSS&HLR gives the geographic location of a specified mobile station.

The network, an external application, or a mobile station can request positioning.

Location Services is used to request the following:

- Location of emergency calls (requested by authorities)
- Surveillance of suspected criminals (requested by authorities)
- Home/office zone applications (requested by network operators)
- Network planning applications (requested by network operators)
- Electronic yellow pages (requested by third party service providers)
- Navigation (requested by mobile station)

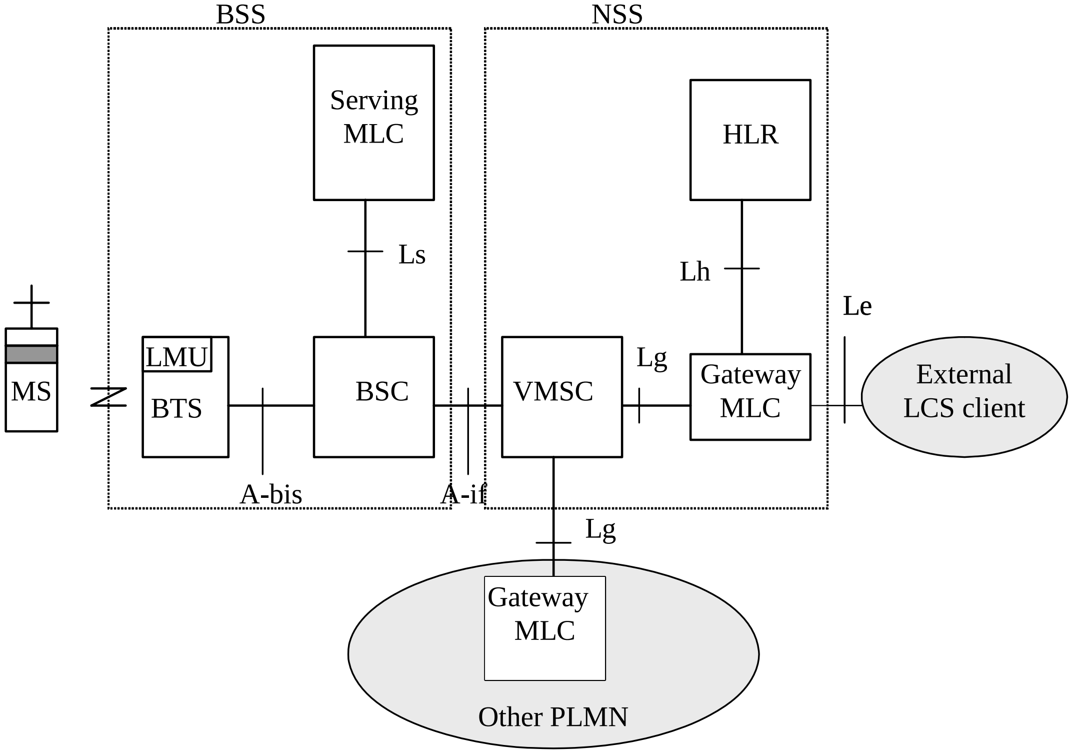


Figure 14 General logical LCS architecture

Starting from M12 the maximum number of external LCS clients is raised from 5 to 20. The HLR supports the GPRS so that location services can be handled in the SGSN.

Operators can use the feature to:

- Locate emergency calls (requested by authorities)

  It provides the subscriber’s approximate geographical location. LCS results for locating emergency calls are more accurate than other means.

- Locate the subscriber and mobile equipment (requested by a Location Services client)

  LCS gives an accurate positioning of the subscriber. The call has to be ongoing while the LCS client is positioning the mobile equipment.

- Enhance home-office zone applications (requested by network operators)

  LCS gives a more accurate positioning for applications when you want to separate home zones (private subscribers) or office zones (business subscribers) in order to offer cheaper tariffs.

3.5.7 Multicall

Multicall is a 3GPP-standardized supplementary service, supported only in UMTS access. It is applicable in the Circuit Switch (CS) domain.

It enables a mobile subscriber to have several simultaneous CS calls, made possible by using a dedicated bearer for each call.

In M12, Multicall allows up to seven simultaneous CS data calls, or six CS data calls and one CS speech call.

Maximum number of simultaneous CS bearers supported by the serving network is defined in parameter file, class 2, parameter 696:

```
WOI:2,696;
```

Whether the feature is supported in the VLR can be set with MXM command by parameter MC. MVF command can be used to filter the subscribers who have the supplementary service.

Maximum number of bearers per subscriber is to be set in HLR with MIM command by parameters NBRSB=2..7 and NBRUSER=1..NBRSB. The NBRUSER is set by user during registration. The initial value for the parameter is set by operator during service provisioning.

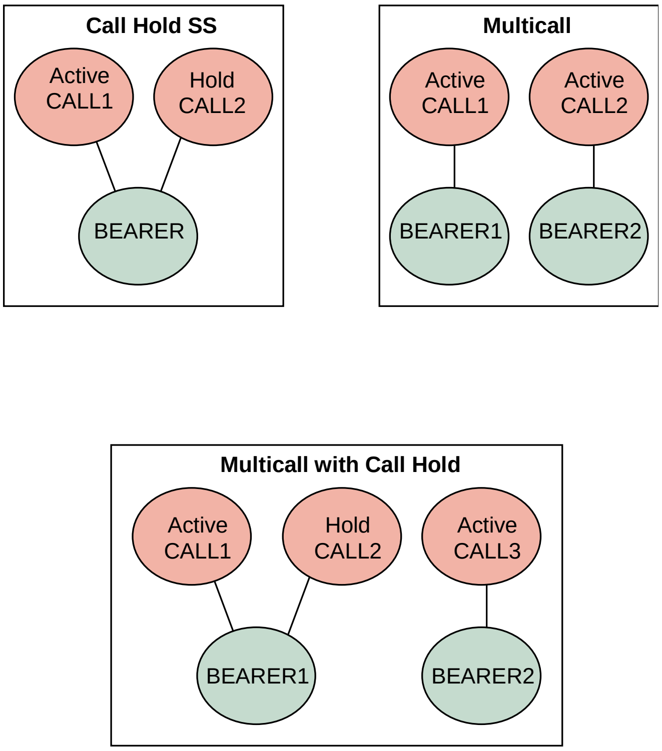


Figure 15 Bearers in Multicall, Call Hold, and Multicall with Call Hold

Limitation in circuit switch domain

The CS domain limits the subscriber to only one speech call at a time. A multimode UMTS terminal (with CS and PS capability) can have packet sessions during a CS call. However, this is not the same as a Multicall configuration, but is a new supplementary service code that VLR can receive from the HLR in the InsertSubscriberData MAP operation.

Multicall and parallel call comparison

The use of supplementary services like Call Waiting, Call Hold, and Multiparty can facilitate several parallel calls. However, all the calls share the same bearer (traffic channel) from the network to the MS. For this reason only one call can be active at a time. The Multiparty supplementary service also uses only one bearer towards the MS. A conference bridge in the network joins the calling parties.

3.6 NSN (vendor)-specific Supplementary Services

NSN develops specific supplementary services, and they cannot be found in GSM specifications. Only operators who use NSN NSS products can buy these NSN-specific supplementary services. The result for subscribers who roam into a PLMN that does not use NSN NSS products is that the subscriber may not have access to the supplementary services available in the home PLMN.

All of the NSN-specific supplementary services are optional. Operator Control Call Forwarding (OCCF), Automatic Call Redirection (RDI), and Mobile Centrex are examples of NSN-specific supplementary services.

- Operator Control Call Forwarding (OCCF)
- Automatic Call Redirection (RDI)
- Mobile Centrex and Private Numbering Plan (PNP)

3.6.1 Operator Control Call Forwarding (OCCF)

This feature enables you to set a default call forwarding with a lower priority for a mobile. If no other call forwarding is set, the default set by you is used.

For example: A subscriber does not forward calls to another number. When someone calls him and the call is not answered, the call is forwarded by using OCCF. The OCCF usually is directed to the end user’s voice mail. It means that all incoming calls end up there. When active again, the subscriber can check voice mail.

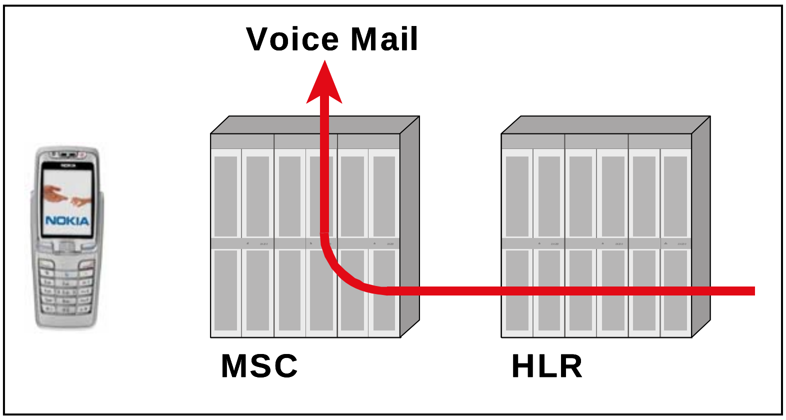


Figure 16 Operator Control Call Forwarding

This feature provides you with more successful calls, because all calls will end up somewhere (usually voice mail). Consequently, the operator receives more revenue.

3.6.2 Automatic Call Redirection (RDI)

The RDI enables you to redirect a mobile-originated call to a predefined destination (that is, a welcome announcement or the service provider's customer service). When the subscriber does not pay a bill and tries to originate a call, the call is redirected to the operator's customer service or to the announcement, "your call is barred due to unpaid phone bill." This is preferable to barring the call without informing the caller of the reason.

This feature applies to mobile originating calls. The served subscriber's ability to set up emergency calls, send short messages, and receive incoming calls remains unaffected.

If Barring of Outgoing Calls is active, the call attempt is barred and not redirected because RDI has a lower priority than ODB and Call Barring.

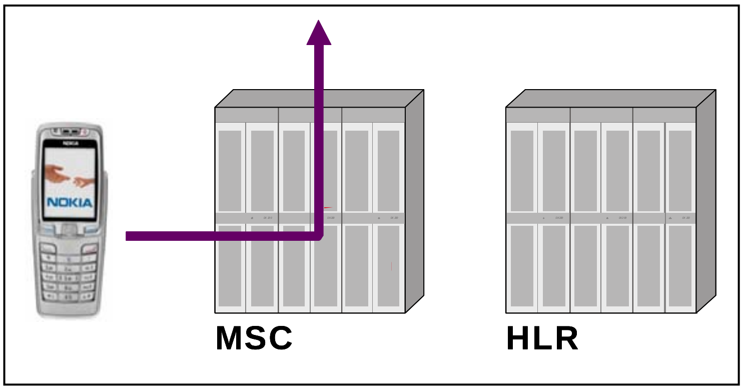


Figure 17 Automatic call redirection

3.6.3 Mobile Centrex and Private Numbering Plan (PNP)

Mobile Centrex is a private branch exchange-type application, which enables the use of abbreviated dialling inside a defined user group (usually called a Centrex group) as well as access to the supplementary services of the network.

The use of abbreviated dialling is based on the implementation of a private numbering plan (PNP). The PNP is a private numbering scheme, which allows PBX private numbers to be used in digital mobile networks.

Centrex services provide an ideal solution for an office environment by offering a capability for the subscribers to call other members of the same Centrex Group by using short private numbers. The members of the Centrex Group can use either mobiles (pure Mobile Centrex) or a mixture of mobiles and PBX subscribers (Combined Centrex).

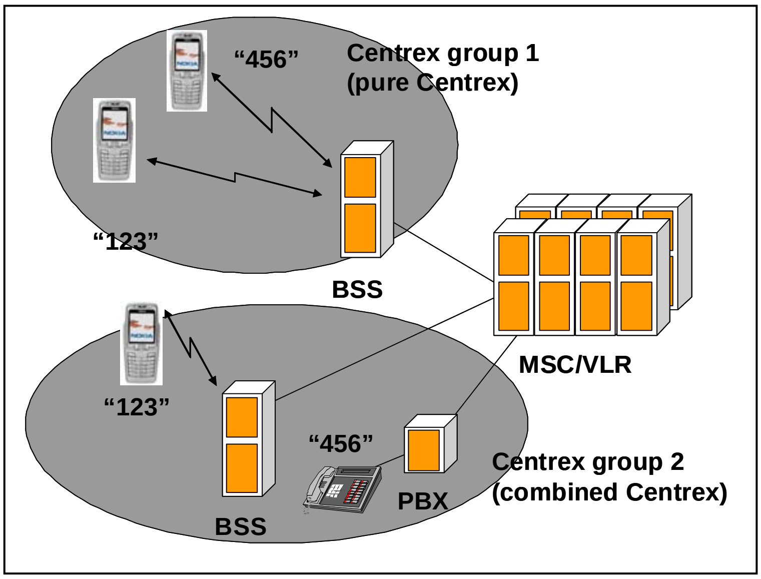


Figure 18 Mobile Centrex

4 Subscriber Information in GSM/UMTS Networks

In order to serve subscribers, networks need subscriber-related data as well as information for setting up an efficient system for subscriber management. This chapter introduces subscriber-related data and its location.

4.1 Subscriber Data Locations

Subscriber data is stored in five locations

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Authentication Centre (AC)
- Subscriber Identity Module (SIM)
- Equipment Identity Register (IMEI)

4.1.1 Home Location Register (HLR)

The Home Location Register is the static location of subscriber data in the network. A subscriber's subscription data always can be found in the HLR located in the home PLMN.

Information in the HLR can be divided into three groups according to purpose:

- Identify the subscriber
- Identify the subscriber services
- Locate the subscriber

Identify the subscriber

There are three important categories of information related to subscriber identity and collected in the HLR:

- The *International Mobile Subscriber Identity (IMSI)* is a unique number worldwide.
- The *MS Category* is used to specify the mobile station category for the subscriber: priority, ordinary, test or payphone.
- The *activation status* of a subscriber is usually activated. This means that the subscriber can use all services in the normal way. A subscriber is deactivated only in exceptional circumstances. For instance, there is a need to prevent the subscriber from using the GSM network services.

Identify the subscriber services

Both *Basic Services* and *Supplementary Services* provided for the subscriber must be stored in the HLR. In case the network operator uses Multi-Numbering, each basic service has a separate *Mobile Subscriber International ISDN Number, MSISDN.* If Single-Numbering is used, only one MSISDN is created for all basic services.

If a subscriber is allowed to use T11 and a bearer service with data rates 9600 (B16) only in the home PLMN, the network operator can implement it by setting the *Service Area of MSISDN* to its own PLMN.

Locate the subscriber

In every mobile terminated call (MTC), the originated MSS (GCS if the call originates from a PSTN) asks the HLR for routing information. This message is called “HLR_Enquiry.” The routing information in the MTC case is the Mobile Station Roaming Number, MSRN. In order to provide the MSRN, the HLR has to enquire the visited VLR. For this reason, the HLR must contain the *Visited VLR Address* of each subscriber.

This address is given in two different formats:

- *Signalling Point Code (SPC) of the VLR* can only be used if the VLR is in the same signalling network and the location of the subscriber is updated to the HLR with the SPC format.
- *VLR ISDN number* has the same structure as the MSISDN number, and is used when the location of the subscriber is updated to the HLR with the VLR ISDN format or Global Title. It can be used both when the VLR is in the same signalling network and when the VLR is in a different signalling network.

By using the VLR address (SPC or VLR ISDN number), the HLR sends the request for the MSRN to the visited VLR. This message is called “MSRN_Request.”

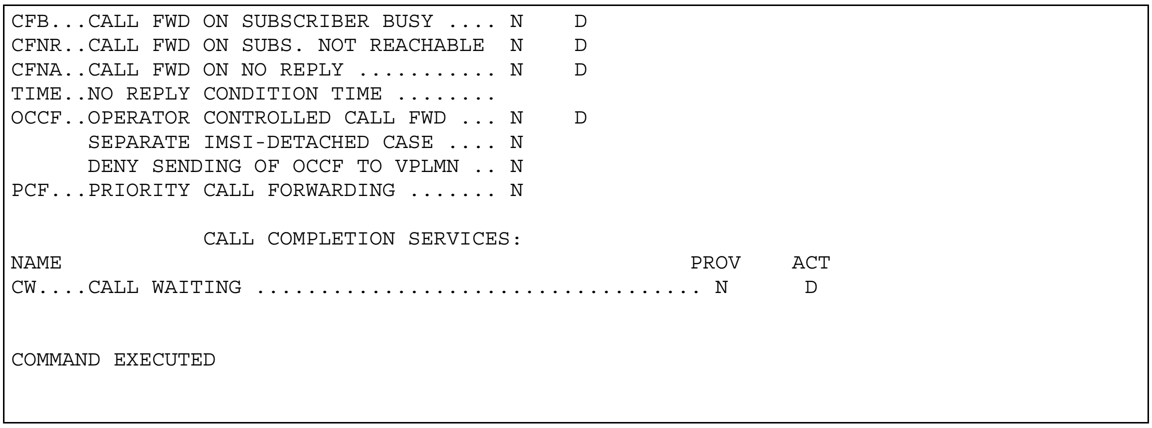
```
MIO:IMSI=460200000000105:;

DX 200    HLR02                     2009-04-17  16:41:05

                SUBSCRIBER INFORMATION:

        INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ... 460200000000105
        MOBILE STATION ISDN NUMBER ................. 8622301000105
        ATTACHED IMSI ..............................
        MOBILE STATION CATEGORY .................... OR
        ROUTING CATEGORY ........................... N
        ADDITIONAL ROUTING CATEGORY ................ N
        SERVICE AREA OF MSISDN ..................... ALL
        ACTIVATION STATUS .......................... A
        VLR-ADDRESS ................................ 8652300100
        SIGNALLING POINT CODE ...................... 00000000
        MSC-ADDRESS ................................ 8652300100
        PRIMARY BASIC SERVICE CODE ................. T11
        PRIMARY BASIC SERVICE CODE INDEX ........... 000
        ROAMING PROFILE INDEX ...................... N
        ORIGINATING CCBS ........................... N
        TERMINATING CCBS ........................... N
        FRAUD PROFILE .............................. N
        CALLING LINE IDENTIFICATION ENHANCEMENT .... N
        COMMON MSISDN NUMBER ....................... N
        OVERRIDE COMMON CLI PARAMETERS ............. N
        CMSISDN IS HUNTING GROUP NUMBER ............ N
        DENY DIRECT CALLS .......................... N
        DENY USSD WITH MEMBER NUMBER ............... N
        DENY DIRECT SMS ............................ N
MAXIMUM OF SIMULTANEOUS CS BEARERS IN MULTICALL SUBSCRIPTION:
        DEFINED BY SERVICE PROVIDER ................ N
        DEFINED BY USER ............................ N

        ZONE CODES:


        MSC AREA RESTRICTED ........................ N

        HLRU IDENTITY .............................. 0

        EMLPP MAXIMUM ENTITLED PRIORITY ............ N
        EMLPP DEFAULT PRIORITY ..................... N

        HOME COUNTRY CODE .......................... N
        NETWORK DESTINATION CODE ................... N

        ROAMING TO UTRAN RESTRICTED ................ N
        ROAMING TO GERAN RESTRICTED ................ N


COMMAND EXECUTED
```

Figure 19   Output of subscriber data in the HLR

```
MBO:IMSI=460200000000105;

DX 200    HLR02                     2009-04-17  16:50:07

                BASIC SERVICE DATA:

        INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ... 460200000000105


        MOBILE STATION ISDN NUMBER ................ 8622301000105
        BASIC SERVICE ............................. T11,000
        SERVICE AREA OF MSISDN .................... ALL

        MOBILE STATION ISDN NUMBER ................
        BASIC SERVICE ............................. T21,000
        SERVICE AREA OF MSISDN .................... ALL

        MOBILE STATION ISDN NUMBER ................
        BASIC SERVICE ............................. T22,000
        SERVICE AREA OF MSISDN .................... ALL

COMMAND EXECUTED
```

Figure 20   Information on subscriber’s basic services in the HLR

```
MSO:IMSI=460200000000105,BSERV=T11;

DX 200    HLR02                     2009-04-17  16:52:02

                SUPPLEMENTARY SERVICES:

    INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ... 460200000000105
    AOC....ADVICE OF CHARGE .................... N
    HOLD...CALL HOLD ........................... N
    CLIP...CALLING LINE ID PRESENTATION ........ N
    CLIR...CALLING LINE ID RESTRICTION ......... N
    COLP...CONNECTED LINE ID PRESENTATION ...... N
    COLR...CONNECTED LINE ID RESTRICTION ....... N
    CT.....CALL TRANSFER ....................... N
    RDI....REDIRECTION DESTINATION INDEX ....... N
    MPTY...MULTI PARTY SERVICE ................. N
    CHC....CHARGING CLASS ...................... N
    CA.....CHARGING AREA .......................
    HB.....HOT BILLING ......................... N
    CSARP..CS ALLOCATION/RETENTION PRIORITY..... N
    USSDB..USSD BARRING......................... N

MOBILE STATION ISDN NUMBER .......................... 8622301000105
BASIC SERVICE CODE .................................. T11
CALL RESTRICTION SERVICES:
NAME                                                 PROV    ACT
BAIC..BARRING OF ALL MTC ............................  N      D
BIRO..BARRING OF MTC WHEN ROAMING IN VPLMN COUNTRY ..  N      D
BAOC..BARRING OF ALL MOC ............................  N      D
BOIC..BARRING OF INTERNATIONAL MOC ..................  N      D
BOIH..BARRING OF INT. MOC EXCEPT TO HPLMN COUNTRY ...  N      D
BORO..BARRING OF MOC WHEN ROAMING IN VPLMN COUNTRY ..  N      D
PSW...PASSWORD ......................................

                CALL FORWARDING SERVICES:
NAME                                 PROV  ACT  C-NUMBER          OPTIONS
CFU...CALL FWD UNCONDITIONAL ......... N    D
```



```
CFB...CALL FWD ON SUBSCRIBER BUSY .... N    D
CFNR..CALL FWD ON SUBS. NOT REACHABLE  N    D
CFNA..CALL FWD ON NO REPLY ........... N    D
TIME..NO REPLY CONDITION TIME ........
OCCF..OPERATOR CONTROLLED CALL FWD ... N    D
      SEPARATE IMSI-DETACHED CASE .... N
      DENY SENDING OF OCCF TO VPLMN .. N
PCF...PRIORITY CALL FORWARDING ....... N

               CALL COMPLETION SERVICES:
NAME                                                PROV    ACT
CW....CALL WAITING ...................................  N      D


COMMAND EXECUTED
```

Figure 21   Supplementary services in the HLR

Table 4   Subscriber information summary in the HLR

Subscriber data	Identify subscriber	Identify services	Locate subscriber
1. IMSI	✓		
2. MSISDN		✓	
3. Service area of MSISDN		✓	
4. MS Category	✓		
5. Activation Status	✓		
6. VLR Address			✓
7. Teleservices		✓	
8. Bearer Services		✓	
9. Supplementary Services		✓	

4.1.2 Visitor Location Register (VLR)

The VLR stores the *dynamic* subscriber data in the network. When roaming in the VLR's service area, a subscriber's subscription data can be found in the VLR of the area in question.

The information in the VLR is almost the same as in the HLR. It can be divided into five groups according to purpose:

- Identifying the subscriber
- Identifying subscriber services

- Locating the subscriber
- Authenticating the subscriber
- Identifying the equipment

Identifying the subscriber

When the HLR sends the request for routing information to the VLR in a mobile terminated call, the message contains the identity of the subscriber in the **IMSI** format. IMSI is also used in the VLR to identify the subscriber.

The result of the routing information request is that the VLR assigns a temporary number, which defines both the location of the VLR in the international network and the identity of the subscriber. This number is called *Mobile Station Roaming Number (MSRN).* Each VLR has a range of numbers reserved for this purpose (typically 800 – MSRN Pool).

The VLR sends the MSRN to the HLR, which forwards it to the originated MSS. The originated MSS can use the MSRN for routing the call to the visited MSS. When the call is connected to the visited MSS, the visited MSS sends the MSRN (which identifies the subscriber according to the latter part of the MSRN) back to the VLR. After that, the MSRN can be re-used for another call set-up.

In the VLR, the subscriber can be identified with another number, the *Temporary Mobile Subscriber Identity (TMSI).* It can be used between the VLR and the MS in order to hide the real identity of the subscriber. TMSI is reallocated after each (or n^{th}) successful authentication between the MS and the network. Nevertheless, using TMSI is optional.

The MS category and the activation status of a subscriber are also used in the VLR the same way as in the HLR.

Identifying subscriber services

Information about the basic and supplementary services is also stored in the VLR and can be interrogated with MML.

Locating the subscriber

There are two types of subscriber information:

- **VLR level**

  The MS's location on a VLR level is the *Location Area (LA)*. The identity of the location area is called *Location Area Identity (LAI).* When TMSI is used for identifying the subscriber, it is always used with LAI. This is necessary in order to be able to make an inter-VLR location update without a need to send IMSI in the air interface.

- **PLMN level**

  Since there can be more than one HLR in a PLMN, the VLR contains the MS's HLR address to point to the correct HLR.

Authenticating the subscriber

The authentication of the subscriber is optional. The authentication data is needed only if the network operator activates the authentication checking. For GSM subscribers, the VLR stores the Authentication Triplet (K_c, SRES, and RAND) for each subscriber. Since more than one triplet is usually requested from the AC at a time, many triplets can be kept in the VLR with the maximum number of triplets being seven.

This information cannot be found by using an MML command.

The Universal Mobile Telecommunication System (UMTS) security covers two main functionalities in MSS and VLR: authentication and key agreement between the mobile station and the network as well as ciphering and integrity protection of radio access links.

Authentication and key agreement is based on a similar challenge-response method as that in the GSM system. In UMTS the authentication is mutual, meaning that the mobile station can also check the authenticity of the network. The current security system does not provide enough protection against malicious attacks due to the available processing power and the already discovered holes.

As the evolution approaches to the 3G systems (UMTS), the phrases like "user confidentiality", "data integrity" become more and more important. After implementing this feature the MSS/VLR will be able to provide 3G level security to UMTS subscribers, and it will be able to handle the "old" GSM subscribers as well. Depending on the connecting network elements it will also be able to make conversions between GSM and UMTS security context.

Instead of GSM Authentication Triplet, UMTS use Authentication quintet, which is a concatenate on of RAND, XRES, CK, IK, and AUTN.

For more information, see Authentication.

Identifying the equipment

Whenever the MSS requests the Equipment Identification Register (EIR) to perform IMEI checking, and the EIR sends the IMEI and the colour list of the mobile equipment back to the MSS, the IMEI and the colour list are stored or updated in the VLR (see "Equipment Identity Register (EIR)").

```
MVO:IMSI=460200000000105:;
MSCi      MSS04                    2009-04-17  16:55:06
                SUBSCRIBER INFORMATION:

        INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ...... 460200000000105
        TEMPORARY MOBILE SUBSCRIBER IDENTITY .......... N
        ACTIVATION STATUS ............................. A
        MOBILE STATION CATEGORY ....................... OR
        EXACT MOBILE STATION CATEGORY ................. UNK
        ROUTING CATEGORY .............................. N
        ADDITIONAL ROUTING CATEGORY ................... N
        MOBILE COUNTRY CODE ........................... 0460H
        MOBILE NETWORK CODE ........................... 0030H
        LOCATION AREA CODE OF IMSI .................... 012CH/00300D
        RADIO ACCESS INFO ............................. GSM
        MOBILE NOT REACHABLE FLAG ..................... N
        HLR FAILURE FLAG .............................. N
        SUPPLEMENTARY SERVICE CHECK FLAG .............. N
        IMSI DETACH FLAG .............................. N
        DETACH CAUSE ..................................
        LAST ACTIVATE DATE ............................ 04-17 16:42
        LAST USED CELL ID ............................. 012DH/00301D
        HLR-ADDRESS ................................... 8622301000
        SECURITY CONTEXT TYPE.......................... GSM

        INTELLIGENT NETWORK MOBILITY MANAGEMENT:
        SCP ADDRESS ................................... N
        DETECTION POINT NAME .......................... N
        SERVICE KEY ................................... N
        TRANSACTION TYPE .............................. N
              INTELLIGENT NETWORK SHORT MESSAGE SERVICE:
        SCP ADDRESS ................................... N
        DETECTION POINT NAME .......................... N
        SERVICE KEY ................................... N
        TRIGGERING ALL MULTIPLE MESSAGES .............. N

        COMPLETION OF CALL TO BUSY SUBSCRIBER:
        ORIGINATING CCBS .............................. N
        TERMINATING CCBS .............................. N
        CCBS MONITORED ................................ N

        SUBSCRIBER FRAUD OBSERVATION:
        NUMBER OF CALL TRANSFERS ...................... 0
        NUMBER OF OBSERVATION ACTIVATIONS ............. 0
        NUMBER OF SAMPLING PERIOD ..................... 0

        SIMULTANEOUS CALL TRANSFER IN PROGRESS ........ 0

        FRAUD DETECTION AND LIMITATION:
        TIME LIMIT OF MO CALLS ........................ DEF
        ACTION PARAMETER FOR MO CALLS ................. DEF
        TIME LIMIT OF CF CALLS ........................ DEF
        ACTION PARAMETER FOR CF CALLS ................. DEF
        TIME LIMIT OF CT CALLS ........................ DEF
        ACTION PARAMETER FOR CT CALLS ................. DEF
        MAX. NUMBER OF CT INVOCATIONS ................. DEF
        ACTION PARAMETER FOR CT INVOCATIONS ........... DEF
        ZONE CODES:

        EMLPP PRIORITY INFORMATION:
        EMLPP MAXIMUM ENTITLED PRIORITY................ N
        EMLPP DEFAULT PRIORITY......................... N
        SGSN ADDRESS .................................. N
        CONFIRMED RADIO CONTACT VIA SGSN .............. N
        VLRU IDENTITY ................................. 0
        MOBILE SUBSCRIBER INTERNATIONAL ISDN NUMBER ... 8622301000105
        MOBILE SUBSCRIBER ALTERNATE LINE SERVICE MSISDN
        BASIC SERVICES:
        T11 T21 T22
        MULTISIM INFO:
        OWN MSISDN ................................... N
COMMAND EXECUTED
```

Figure 22   Subscriber information in the VLR

```
MVS:IMSI=460200000000105:BSERV=T11;

MSCi      MSS04                     2009-04-17  17:46:12

        INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ...... 460200000000105
        BASIC SERVICE CODE ............................ T11
        AOC...ADVICE OF CHARGE ........................ N
        HOLD..CALL HOLD ............................... N
        CLIP..CALLING LINE ID PRESENTATION ............ N
        CLIR..CALLING LINE ID RESTRICTION ............. N
        COLP..CONNECTED LINE ID PRESENTATION .......... N
        COLR..CONNECTED LINE ID RESTRICTION ........... N
        CT....CALL TRANSFER ........................... N
        RDI...REDIRECTION DESTINATION INDEX ........... N
        MPTY..MULTI PARTY SERVICE ..................... N
        SSET..SERVICE SET INDEX ....................... N
        CHC...CHARGING CLASS .......................... N
        CA....CHARGING AREAS ..........................
        HB....HOT BILLING ............................. N
        USSDB.USSD BARRING ............................ N
        PIC...PREFERRED INTEREXCHANGE CARRIER .........
        PLOCK.PREFERRED INTEREXCHANGE CARRIER LOCK .... CAC ALLOWED

                CALL RESTRICTION SERVICES:
    NAME                                                PROV   ACT
    BAOC..BARRING OF ALL MOC ..........................   N     D
    BOIC..BARRING OF INTERNATIONAL MOC ................   N     D
    BOIH..BARRING OF INT. MOC EXCEPT TO HPLMN COUNTRY ..   N     D

                CALL FORWARDING SERVICES:
    NAME                                PROV ACT C-NUMBER           OPTIONS
    CFU...CALL FWD UNCONDITIONAL ........ N    D
    CFB...CALL FWD ON SUBSCRIBER BUSY ... N    D
    CFNR..CALL FWD ON SUBS. NOT REACHABLE N    D
    CFNA..CALL FWD ON NO REPLY .......... N    D
    TIME..NO REPLY CONDITION TIME .......

                CALL COMPLETION SERVICES:
    NAME                                                PROV   ACT
    CW....CALL WAITING ................................   N      D

COMMAND EXECUTED
```

Figure 23   Supplementary services information in the VLR

Table 5 Summary of subscriber information in the VLR

Subscriber Data	Identify subscriber	Identify services	Locate subscriber	Authenticate subscriber	Identify equipment
1. IMSI	✓				
2. MSISDN		✓			
3. MS Category	✓				
4. Activation Status	✓				
5. Teleservices		✓			
6. Bearer Services		✓			
7. Supplementary Services		✓			
8. MSRN	✓				
9. TMSI	✓				
10. LAI			✓		
11. HLR Address			✓		
12. Authentication Triplets/ Quintet				✓	
13. IMEI					✓
14 colour list					✓

4.1.3 Authentication Centre (AC)

The Authentication Centre (AC) is the network element that contains subscriber data for authentication, or checking the subscriber's true identity during call setup.

For GSM Subscribers

Each of them receives a unique IMSI number, authentication key (Ki), and a version of algorithms A3 and A8. All of this data is stored in the AC. The AC uses the IMSI, Ki, and A3 algorithm for generating the authentication triplets (RAND, SRES, Kc) for user authentication and speech encryption security features.

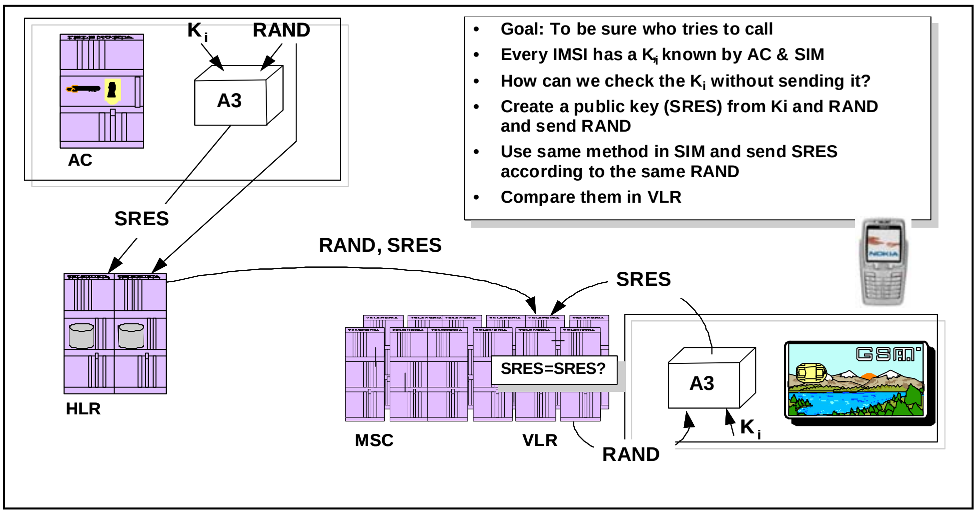
Permanent subscriber data stored in the AC includes:

- IMSI
- Authentication Key (K_i)
- Versions of Algorithms A3 and A8

For security reasons, the authentication key K_i cannot be displayed after being inserted in the AC database.

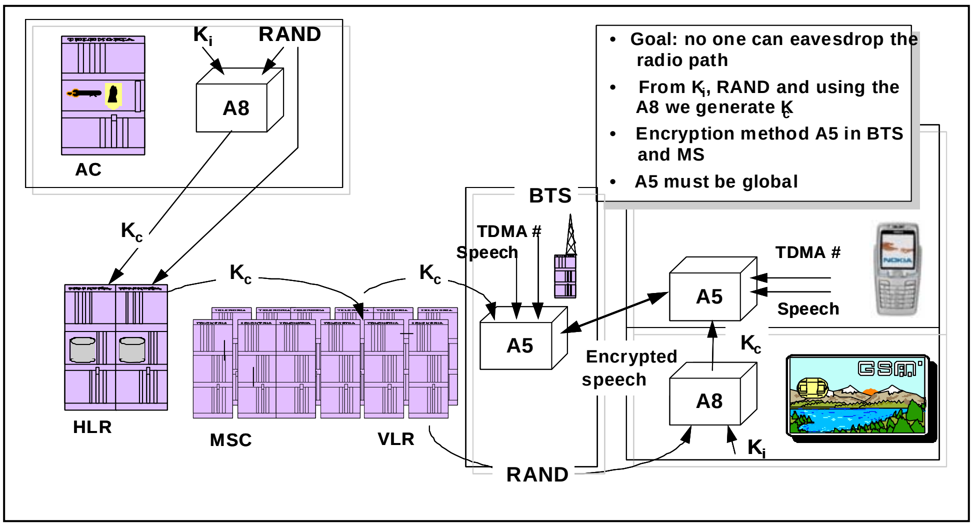
Different A3 and A8 algorithms can be used in different PLMNs.

When the authentication check is started, the visited VLR asks for the authentication triplets from the HLR. The HLR passes this request to the AC. The authentication triplets are then sent by request from the AC to the HLR, which forwards them to the visited VLR. Several triplets at the same time are transferred to the VLR when needed.



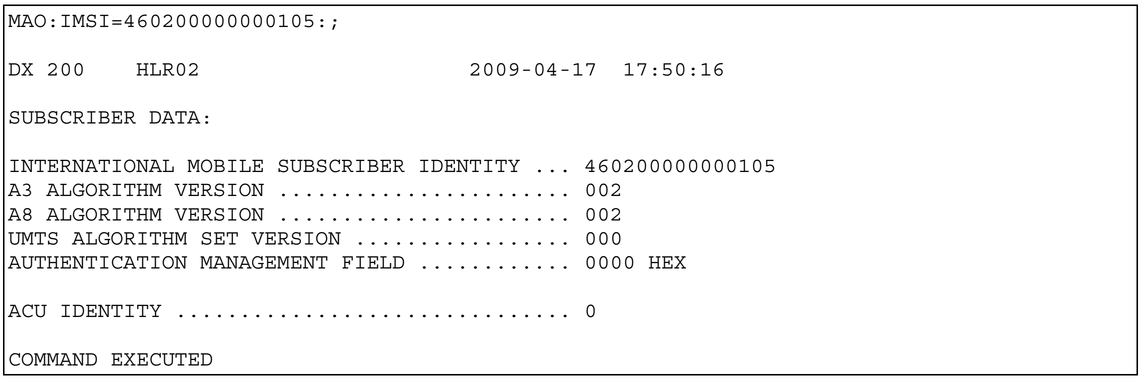
- Goal: To be sure who tries to call
- Every IMSI has a K_i known by AC & SIM
- How can we check the K_i without sending it?
- Create a public key (SRES) from Ki and RAND and send RAND
- Use same method in SIM and send SRES according to the same RAND
- Compare them in VLR

Figure 24 Use of RAND and SRES for user authentication



- Goal: no one can eavesdrop the radio path
- From K_i, RAND and using the A8 we generate K_c
- Encryption method A5 in BTS and MS
- A5 must be global

Figure 25 Use of RAND and K_c for speech encryption in air interface



```
MAO:IMSI=460200000000105:;

DX 200    HLR02                    2009-04-17  17:50:16

SUBSCRIBER DATA:

INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ... 460200000000105
A3 ALGORITHM VERSION ....................... 002
A8 ALGORITHM VERSION ....................... 002
UMTS ALGORITHM SET VERSION ................. 000
AUTHENTICATION MANAGEMENT FIELD ............ 0000 HEX

ACU IDENTITY ............................... 0

COMMAND EXECUTED
```

Figure 26   Information for a GSM subscriber in the AC

For UMTS Subscribers

For UMTS, the AUC uses the IMSI, K and UV algorithms for generating the authentication quintets, which it distributes to the VLR or SGSN for storage and use.

Authentication quintet is generated in AC.

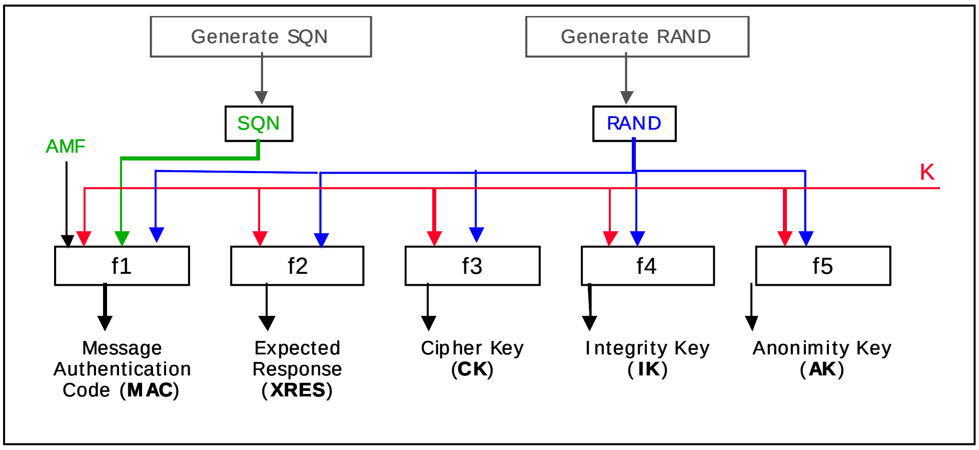


Figure 27   UMTS authentication vector generation in AUC

The generation of quintets starts with the generation of a sequence number (SQN) and a random number (RAND). The subscriber's individual secret authentication key (K) is used as a parameter in every algorithm. The algorithms f1, f2, f3, f4 and f5 are used to calculate the following values:

- a message authentication code MAC= f1K (SQN, RAND, AMF), where f1 is a message authentication function

- an expected response XRES=f2K (RAND), where f2 is a message authentication function
- a cipher key CK=f3K (RAND), where f3 is a key generating function
- an integrity key IK=f4K (RAND), where f4 is a key generating function
- an anonymity key AK=f5K (RAND), where f5 is a key generating function, or if AK is not needed, f5=0

After the algorithms are calculated the authentication token (AUTN=SQN + AK|| AMF || MAC, where + denotes xor) is constructed. The actual quintet is a concatenation of RAND, XRES, CK, IK, and AUTN.

```
MAO:IMSI=460100000000006:;
HLRi      HLR01                    2009-04-17  17:47:55

SUBSCRIBER DATA:
INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ... 460100000000006
A3 ALGORITHM VERSION ...................... 000
A8 ALGORITHM VERSION ...................... 000
UMTS ALGORITHM SET VERSION ................ 050
AUTHENTICATION MANAGEMENT FIELD ........... 0000 HEX

ACU IDENTITY .............................. 0

COMMAND EXECUTED
```

Figure 28 Information for a UMTS subscriber in the AC

Table 6 Summary of subscriber information in the AC

Subscriber data	Identify subscriber	Authenticate subscriber
1. IMSI	✓	
2. K_I ,A3 and A8, f1~f5, c2, c3		✓

4.1.4 Equipment Identity Register (EIR)

The main task of the EIR is to trace users of mobile equipment in order to limit equipment malfunction and misuse in the network.

```
MEO:IMEI=27181672274951;
DX 220     DX220-HLR                  2007-04-12  15:19:24

IMEI    =  27181672274951
DATE    =  2005-02-10
LIST    =  BLACK
CLASS.  =  LOCAL
REASON  =  DUPLICATED IMEI
VISIB.  =  EIR & IMEI DB

IMEI    =  27181672200000  ---   27181672299999
DATE    =  2003-01-18
LIST    =  WHITE
CLASS.  =  GLOBAL

COMMAND EXECUTED
```

Figure 29   Listing information in the EIR

And If the IMEI is part of an IMEI series, the following data on that series are displayed as well.

User equipment listing is stored in the EIR, according to the following criteria:

- **White List** contains identity series of type-approved mobiles. This list allows user equipment to operate normally in the network.
- **Grey List** contains identities of mobile stations that are under suspicion. The MSS monitors them.
- **Black List** contains identities of equipment that is stolen or otherwise not allowed to operate in the network. The MSS disconnects black-listed call.

You can then find out from the EIR how the mobile equipment is listed.

```
MVP:IMSI=244051234;
DX 200      DX 200-MSC                  2007-01-01     03:03:23

        SUBSCRIBER EQUIPMENT IDENTITY DATA:

        IMSI             2440512345

        IMEI (VLR)       123456789911110     WHITE LIST
          SV OF IMEI                  98

        IMEI (MOBILE)    123456789911110
          SV OF IMEI                  98


COMMAND EXECUTED
```

Figure 290   Interactive IMEI Query

4.1.5 Subscriber Identity Module (SIM)/ Universal Subscriber Identity Module (USIM)

The MS (Mobile Station)/ UE (User Equipment) consists of a Subscriber Identity Module (SIM)/ USIM (Universal Subscriber Identity Module), and an ME (Mobile Equipment) / UT (User Terminal).

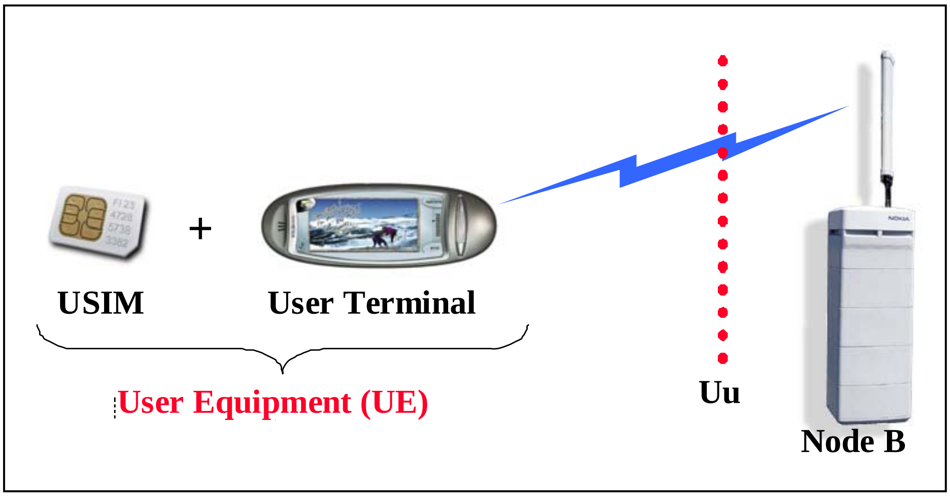


Figure 31 Elements and interfaces of the mobile equipment

The SIM/USIM is a smart card of the size of a credit card or a smaller plug-in card, which contains subscription details. The significance of the SIM is that the GSM/ UMTS enable the subscriber to carry his subscription information on a plastic card no bigger than a credit card. This removable module contains all the information required to allow the GSM/ UMTS PLMN to identify the subscription to which charges must be directed. By inserting the SIM into any equipment, it becomes the subscriber’s phone.

Without the SIM card, it is only possible to make emergency calls. You can, however, also deny that.

The information in a SIM/USIM can be separated into four groups by its purpose:

- Identify the subscriber
- Authenticate the subscriber to the network
- Authenticate the subscriber to the SIM card
- Register data

Identify the subscriber

To identify the subscriber, the **IMSI** has to be stored on a SIM/USIM. This data is permanent data (you cannot modify the IMSI).

The **TMSI** can be used as the subscriber identity data.

Authenticate the subscriber to the network

When the subscriber purchases a SIM/USIM, it is personalised electrically. This data is also permanent data.

For GSM:

- K_I
- Algorithm A3/ A8

For UMTS:

- K
- f1: a message authentication function for network authentication;
- f2: a message authentication function for user authentication;
- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;
- f5: a key generating function to derive the anonymity key for normal operation;
- c2: Conversion function for interoperation with GSM from XRES (UMTS) to SRES (GSM);
- c3: Conversion function for interoperation with GSM from Ck and IK (UMTS) to Kc (GSM).

Table 7 USIM – Authentication and key agreement – Cryptographic functions

Symbol	**Description**	**Lifetime**	**Standardised / Proprietary**	**Mandatory / Optional**
f1	Network authentication function	Permanent	Proprietary	Mandatory
f2	User authentication function	Permanent	Proprietary	Mandatory
f3	Cipher key generating function	Permanent	Proprietary	Mandatory
f4	Integrity key generating function	Permanent	Proprietary	Mandatory
f5	Anonymity key generating function (for normal operation)	Permanent	Proprietary	Optional
c2 and c3	Conversion functions for interoperation with GSM	Permanent	Standard	Optional

Authenticate the subscriber to the SIM/USIM card

You also can authenticate the use of a subscription, which is SIM/USIM, locally. Each SIM/USIM card has a *Personal Identification Number (PIN).* The PIN is a security function that prevents the use of a stolen MS/UE or SIM/USIM. The PIN has to be given before the mobile can be used. The user can disable the use of a PIN and/or change the code.

When a PIN is given incorrectly three consecutive times, the SIM/USIM is blocked. To unblock the SIM, a *Personal Unblocking Key (PUK)* is required. PUK is also in the SIM. If a PUK is given incorrectly ten consecutive times, the SIM/USIM is destroyed.

Register data

Register data is the data that the MS/UE gets from the network. It is defined only if the MS/UE is registered in the network. Register data can, for example, be:

- LAI
- TMSI
- Periodic Location Updating Time
- PLMN Identity Numbers

Furthermore, the SIM/USIM has information about different networks. The card can have the eight most desirable PLMN identity numbers stored in the memory. The user can add and remove data from the PLMN list. There also is a list of forbidden networks; it is created when the mobile has tried to get in a network, but the Visitor Location Register has not accepted the registration.

Table 8 Summary of subscriber information in the SIM/USIM

Subscriber data	Identify subscriber	Authenticate subscriber to network	Authenticate subscriber to SIM card	Register data
1. IMSI	✓			
2. TMSI	✓			✓
3. SIM: K_I ,A3 and A8, USIM: K, f1~f5, c2, c3		✓		
4. LAI				✓
5. Periodic LU Time				✓
6. PLMN Info				✓
7. PIN			✓	
8. PUK			✓	

4.2 Implementing the HLR, VLR, AC, and EIR

Subscriber data is stored in the databases of the VLR Unit (VLRU) in the DX 200 MSS/VLR, and in the databases of the HLR, AC, and EIR units (HLRU, ACU, and EIRU) in the DX 200 HLR/AC/EIR. Subscriber data is distributed to them according to a distribution algorithm handled by the Central Memory (CM) to keep the load constant between different unit pairs.

4.2.1 Implementing the HLR

The HLR subscriber database is located in the HLRUs and the backup copies are on the HLRU's WDUs.

If a new HLRU pair is added, the new subscribers are added into it until the amount of subscribers is the same in every pair. The CM is responsible for the distribution.

4.2.2 Implementing the VLR

The VLR database is located in the VLRU's RAM. Hence, the data is lost in a restart and has to be fetched from the HLR.

Subscribers are distributed to different VLRU pairs so that the load is constant between different pairs. The CM is responsible for the distribution by converting TMSI to IMSI and checking which VLRU is the emptiest. This means that if a new VLRU pair is added, the new subscribers are added into it until the amount of subscribers is the same in every pair.

4.2.3 Implementing the AC

The AC database is located in the ACUs and the backup copies are on the ACU's WDUs.

The AC is divided into two parts: Authentication Data Manager and Authentication Triplet/Quintet Generator.

The structure of the authentication data is similar to the HLR, including distributed authentication databases and a centralised distributor. New subscribers are directed to the emptiest ACU.

4.2.4 Implementing the EIR

The Equipment Identification Register (EIR) database resides in the RAM of the EIRU. Each EIRU contains a remote copy of the main EIR database. In subrack, the main database of the EIR is located in the CM, but the disk copies of the database files are stored in the OMU's hard disk. In a cartridge, the main database of the EIR is in the RAM of EMU and the disk copies are in the disk of EMU.

All EIRUs have the same data; several units share the processing load. The equipment data will be on white, grey, or black lists.

Note

An IMEI entry in an MML command can be a single IMEI or an IMEI range. In the white list, one entry can consist of up to 1 million single IMEIs. In black and grey lists, one entry can consist of up to 1,000 single IMEIs.

Table 9 Capacity of HLR/AC/EIR (i-series with forced ventilation) and VLR

Database	Maximum capacity	Maximum unit	Maximum capacity
HLR	500,000 sub. Per pair	10 pairs	5,000,000
AC	200,000 sub. Per pair	5 pairs	10,000,000
VLR	200,000 sub. Per pair	8 pairs	1,600,000
EIR		7 units	*White list:* 200,000 IMEI entries (1…1,000,000 IMEIs/entry) *Grey list:* 4 million IMEI entries (1…1,000 IMEIs/entry) *Black list:* 10 million IMEI entries (1…1,000 IMEIs/entry)

Regarding the capacity for signaling transmission can be remarkably improved with highly efficient signaling features, SIGTRAN and 2Mbit/s signaling links between two signaling points. The HLRi can support 31 x 2Mbit/sec signaling capacity.

The HLRi without forced ventilation can provide 2 400 000 subscribers and 800 000 telemetric subscribers.

5 Telemetric Subscriber (Optional)

A new type of subscriber is the *telemetric subscriber*. Telemetric subscribers have the same identifiers—IMSI and MSISDN—as normal subscribers. However, telemetric subscribers have a more limited service profile.

The categorization of telemetric subscribers is not standardized. NSN uses these categories:

- Category Telemetric-1 (TmS-1)
- Category Telemetric-2 (TmS-2)
- Category Telemetric-3 (TmS-3)

The maximum number of telemetric subscribers:

- 1 250 000 in HLRi

5.1.1 Category Telemetric-1 (TmS-1)

TmS-1 subscribers can be companies, which require individual subscriber registrations, but not from the point of view of charging.

With this category

- T21 and T22 for SMS are the basic set
- ODB, TRACE and OLCM are handled
- USSD and emergency calls are possible by default.

Practically only periodic location updates are generated as traffic during busy hours.

5.1.2 Category Telemetric-2 (TmS-2)

TmS-2 subscribers are individual subscribers. This category can be used with house alarms, remote switches, vending machines, and so forth.

With this category of telemetric subscribers

- T21 and T22 for SMS are the basic set
- ODB, TRACE and OLCM are handled
- USSD and emergency calls are possible by default.

SMS, USSD and periodic location updates are generated as traffic during busy hours.

5.1.3 Category Telemetric-3 (TmS-3)

TmS-3 subscribers are individual subscribers. With this category

- T21 and T22 for SMS and data calls (one data service) are the basic set
- ODB, TRACE and OLCM are handled
- USSD and emergency calls are possible by default.

SMS, USSD and data calls, also normal/periodic location updates are generated as traffic during busy hours.

6 GSM and UMTS Security

6.1 Authentication

Authentication is a common GSM and UMTS security function that validates the mobile user. The purpose of authentication is twofold. On the one hand, it aims to prevent unauthorized use of the network, and on the other hand, it establishes an agreement between the mobile and the network on a security key set that is used later in ciphering and integrity protection.

The VLR initiates GSM authentication and key agreement independently of the radio access network) when the MS is a GSM subscriber using a SIM card or in case when the MS is a UMTS subscriber using a USIM card but the release of the mobile equipment is not R99+.

The VLR initiates UMTS authentication and key agreement independently of the radio access network) if the MS is a UMTS subscriber with a USIM with R99+ mobile equipment.

6.1.1 GSM Network Elements Involved in Authentication

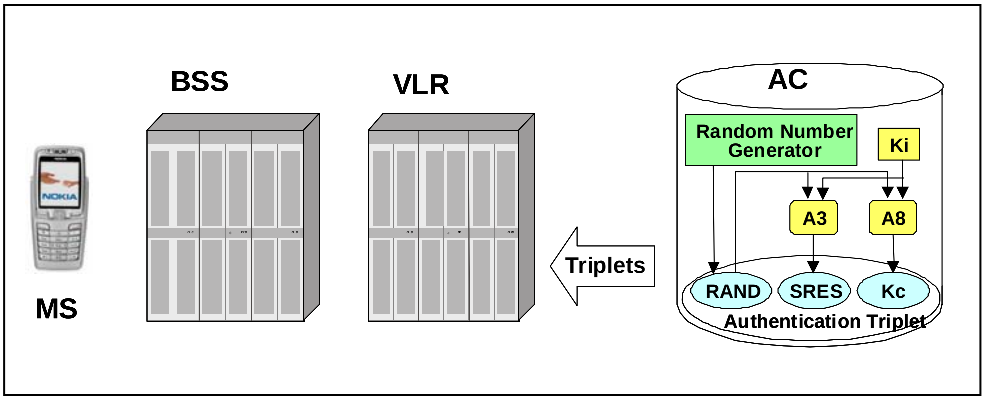


Figure 32 Network elements involved in authentication

Authentication occurs when a mobile sets up an event and the VLR starts the procedure according to the authentication parameters that specify the situations when authentication is performed. The VLR sends the mobile a RAND and a ciphering key sequence number (CKSN) to be used for later encryption.

Figure 33 shows the path of information in a VLR authentication request.

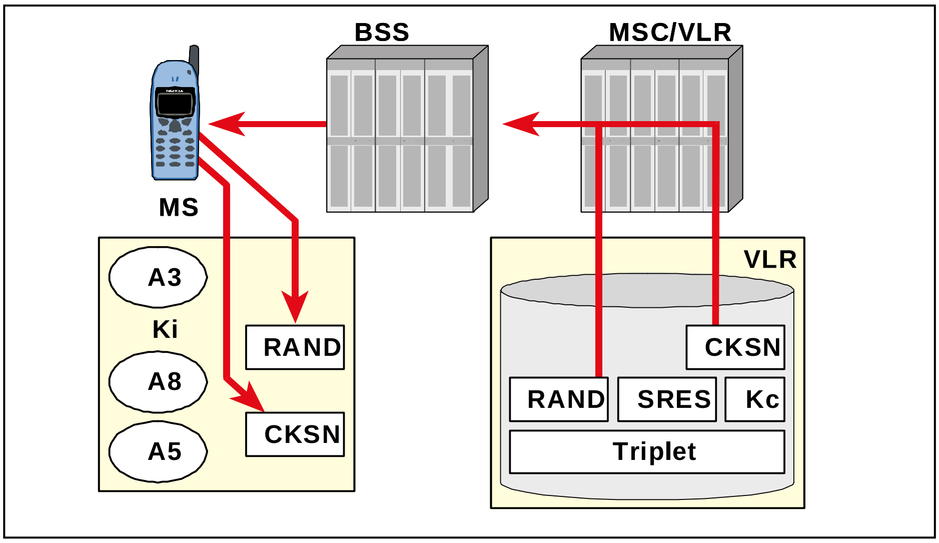


Figure 33 VLR authentication request

The mobile uses the RAND, its authentication key (K_i), and the A3 algorithm stored in the SIM to calculate an SRES. It then sends the SRES to the VLR. The VLR compares the SRES to the SRES that has been calculated and sent from the AC. If they match, the event can continue.

Figure 34 shows the flow of information when the mobile station responds to a VLR authentication request.

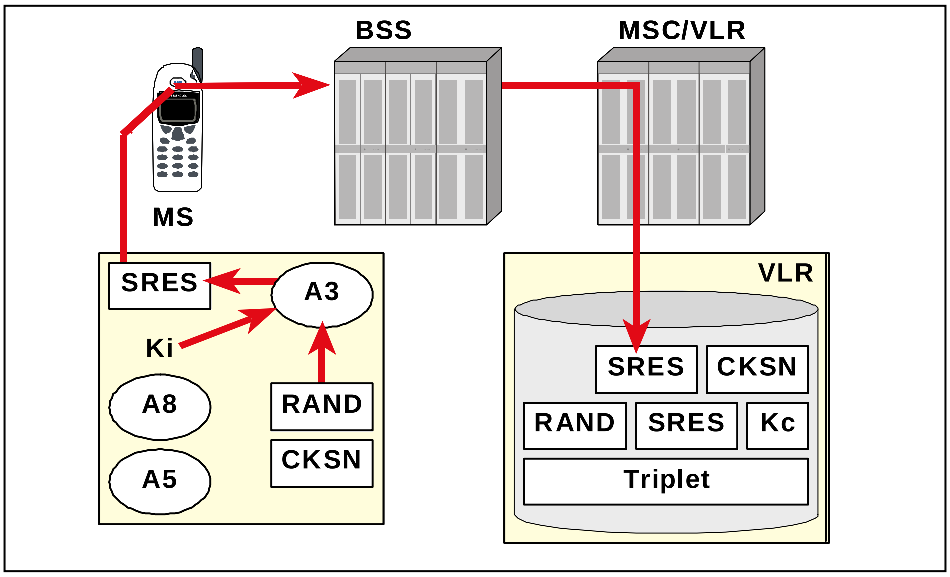


Figure 34 MS response to the VLR authentication request

6.1.2 UMTS Network Elements Involved in Authentication

The UMTS security provides authentication and key agreement between the mobile station and the network as well as ciphering and integrity protection of radio access links.

The VLR initiates UMTS authentication and key agreement (independently of the radio access network) if the MS is a UMTS subscriber with a UMTS-capable mobile equipment.

Authentication and key agreement is based on a similar challenge-response method as that in the GSM system. In UMTS the authentication is mutual, meaning that the mobile station can also check the authenticity of the network.

The UMTS authentication procedure is performed between the VLR and the mobile station through the RAN. Note that the UMTS parameters, RAND, AUTN and RES are sent transparently through the UTRAN or GSM BSS. The role of the AUC is to store the authentication data and to generate the quintets needed in the authentication procedure and to send the quintets to the VLR.

If the VLR does not have enough unused authentication vectors (quintets) it requests new ones from the AUC.

The network elements that are involved in the UMTS authentication procedure are shown in the figure below.

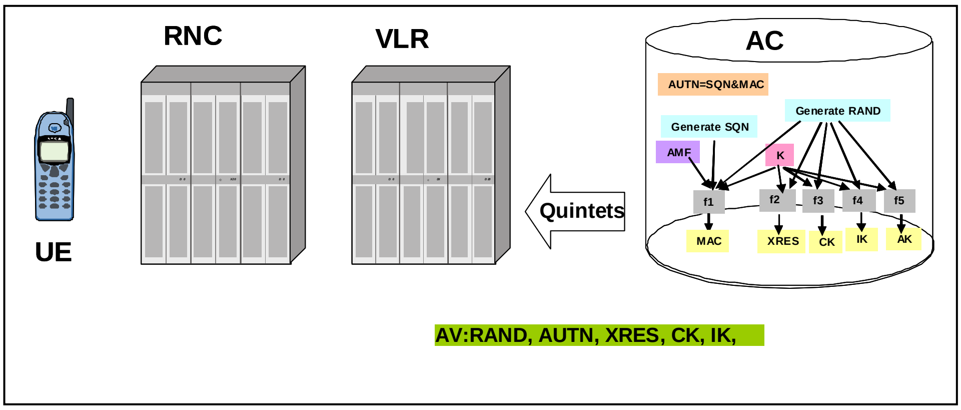


Figure 35 The network elements involved in UMTS authentication

AUC generates quintets for UMTS subscribers and sends them to the VLR. If the requested amount of quintets cannot fit into a single response, and segmentation is supported in both sides, AUC sends only one segment at a time, and waits for subsequent requests from the VLR.

At the end of the operation the VLR stores the received vectors to its database. The authentication procedure is initiated by the VLR and is shown in Figure 36.

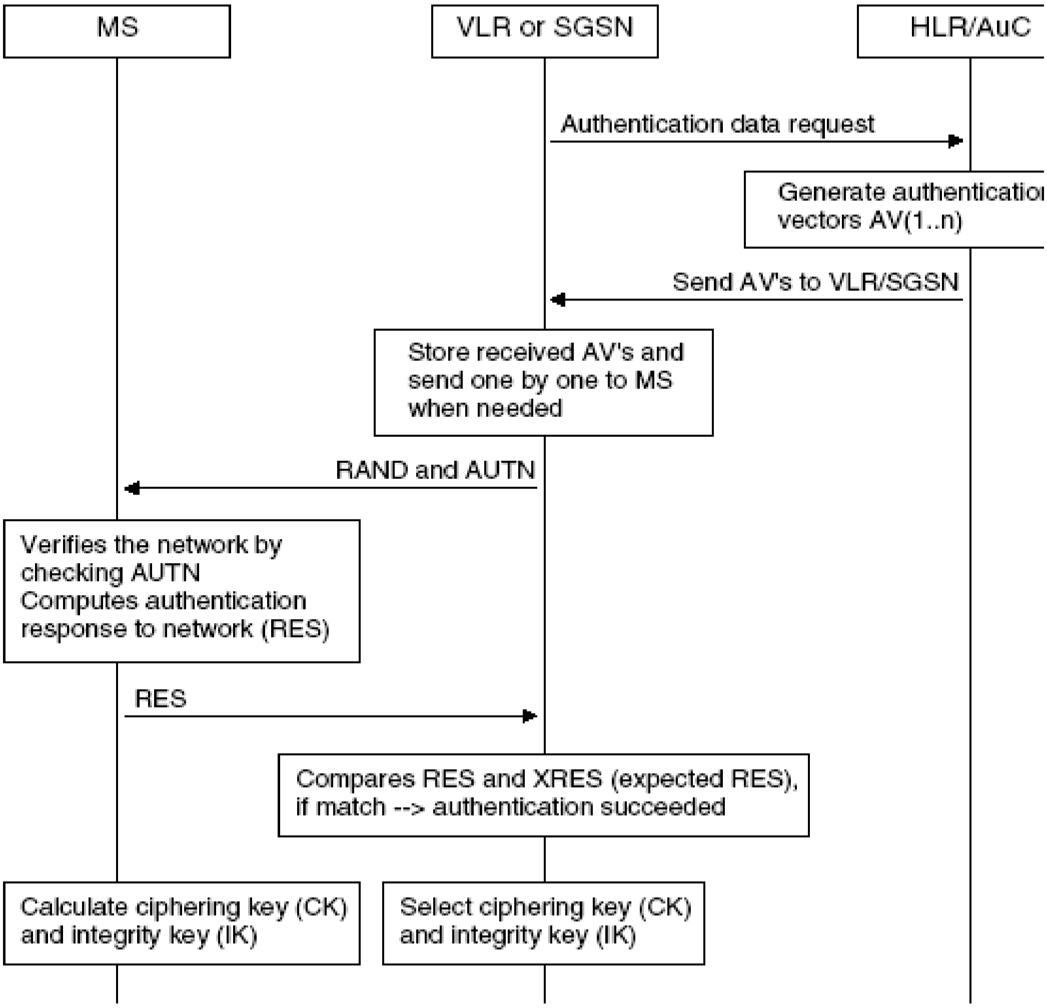

MS
VLR or SGSN
HLR/AuC
Authentication data request
Generate authenticatio
vectors AV(1..n)
Send AV's to VLR/SGSN
Store received AV's and send one by one to MS when needed
RAND and AUTN
Verifies the network by checking AUTN
Computes authentication response to network (RES)
RES
Compares RES and XRES (expected RES), if match --> authentication succeeded
Calculate ciphering key (CK) and integrity key (IK)
Select ciphering key (CK) and integrity key (IK)

Figure 36 UMTS authentication and key agreement

The VLR selects an authentication vector and sends its RAND, the AUTN component and the KSI to the mobile station.

The mobile station checks the MAC in the network token (AUTN) and may reject it by sending an authentication reject message to the VLR. The authentication failure report is generated towards the HLR. When the HLR receives an authentication failure report, it can decide to cancel the location of the user. If the mobile station accepts the MAC, it checks the sequence number included in the AUTN to verify the freshness of the authentication vector.

If the mobile station finds the sequence number out of range, it sends a synchronisation failure message to the VLR including authentication synchronisation information (AUTS).

If the VLR receives a synchronisation failure message, it initiates a re-synchronisation procedure to the AUC including RAND and AUTS. As a response the AUC is forced to correct its counter and to generate fresh authentication vectors.

If the authentication (both the MAC and the SQN) succeeds in the mobile station, it computes a response (RES) and sends it to the VLR. The VLR compares this response to the expected response and if they are different, it rejects the transaction and sends an authentication failure report to the HLR.

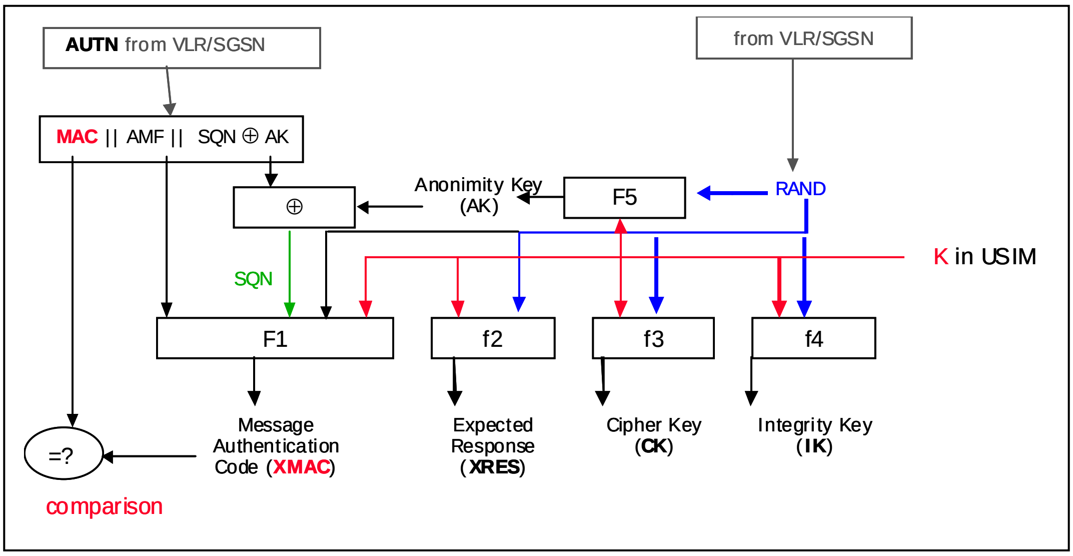


Figure 37 Authentication Vector Generation and Check in USIM

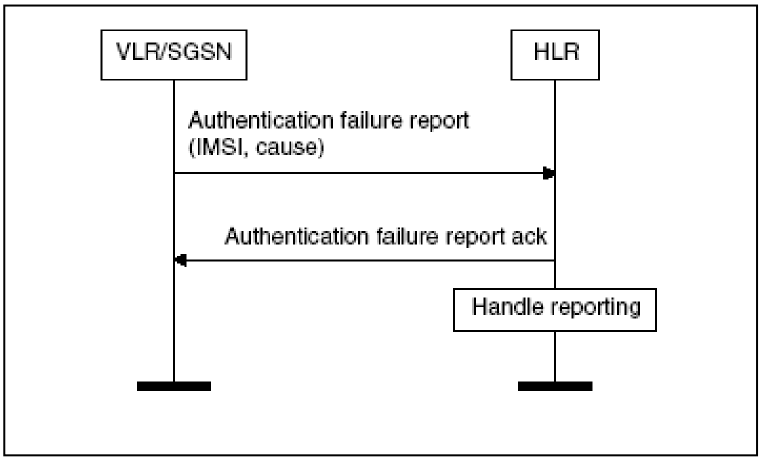

VLR/SGSN
HLR
Authentication failure report
(IMSI, cause)
Authentication failure report ack
Handle reporting

Figure 38 Authentication Failure Report

Due to synchronisation the same quintet cannot be used twice for authentication. Consequently, the VLR can repeat authentication only in case the mobile station does not respond to the challenge at all. Moreover, authentication retry is controlled with the same RAUT and TRAUT parameters as in the GSM authentication.

If the RES differs from the XRES stored in the VLR or the mobile station rejects authentication because of MAC failure, the VLR reviews authentication by requesting the IMSI from the mobile station (if TRAUT=Y), however this procedure occurs only if the IMSI-TMSI association is correct. In case it turns out that the association is wrong, a new location update or call setup is initiated.

The authentication can be repeated once in case the procedure cannot succeed because of synchronisation failure, however, recurring synchronisation failures will entail the rejection of the transaction.

If the subscriber makes an inter-VLR location update within the same PLMN and it identifies itself with a TMSI, the new VLR sends an identification request to the previous VLR. The previous VLR returns the IMSI and the unused authentication vectors if the subscriber in question has any of them. The Current Security Context (CSC) is also transferred in the acknowledgement message.

The VLR requests up to 4 quintets. If the requested number of quintets cannot fit into a single response, segmentation is performed. The IMSI is present only in one segment and the CSC is present in all segments.

6.1.3 GSM and UMTS Authentication Differences

Authentication mechanisms in GSM and UMTS differ.

- In GSM, it is a challenge and response situation. The network sends a random challenge to a mobile station. The mobile station in turn calculates a response using a special A3 authentication algorithm. In the Authentication Centre, the response is compared in the network to the corresponding value.
- In UMTS, the authentication and key agreement algorithm is based on the challenge and response method in the GSM system. In the UMTS system, the authentication is mutual between the network and the subscriber: The network authenticates the subscriber, and the subscriber authenticates the network.

6.1.4 SECMO Hardware (Optional)

The new security module, SECMO-B, ensures reliable performance for both UMTS and GSM authentication. The SECMO-B plug-in unit is also extremely well protected against unauthorised attempts to access its contents.

The SECMO-B plug-in units enable the handling of the increased performance requirements set for the AUC Encryption by, for example, UMTS authentication.

The SECMO plug-in unit contains a HW random number generator needed in the encryption and authentication calculations.

The security of SECMO-B is ensured with several precautions against attempts to obtain sensitive subscriber data in the SECMO-B. The entire plug-in unit is covered with an opaque mechanical cover which cannot be removed without removing the plug-in unit from the cartridge. An alarm is set if any attempt to break the protection is detected. All sensitive data, such as cryptographic keys, is handled in clear form only inside a specially protected environment. Reading the data memory of the SECMO from outside or getting a service terminal connection to the SECMO-B is not possible. In addition, the SECMO-B is equipped with intrusion detection circuitry that is able to detect attempts to remove, break or drill through the cover of the areas where keys or sensitive data is handled. If the plug-in unit is removed from the cartridge, all sensitive data in it is destroyed.

SECMO is located in the ACU and DBDU which are backed up with the 2n redundancy principle.

For more information on SECMO-B, see **Feature 1207: New SECMO HW, Feature Description**.

6.2 Ciphering and Integrity Protection

Ciphering means the transformation of plaintext to ciphertext by cryptographic techniques. In other words, the signal (meaning speech or data) is deliberately distorted. The aim is to provide signalling confidentiality in the GSM and the UMTS network by encrypting the radio path. This way eavesdropping on the radio path can be prevented. Besides ciphering, integrity protection is supported and performed exclusively in the UMTS network.

The VLR initiates GSM ciphering if the GSM subscriber uses the GSM RAN or the UMTS subscriber is attached to the BSS. Note that in the latter case the CK and IK are converted to Kc.

The VLR initiates UMTS ciphering and integrity protection if a UMTS subscriber uses the UMTS radio access network or a GSM subscriber is attached to the UMTS radio access network. Note that in the latter case the Kc is converted to CK and IK.

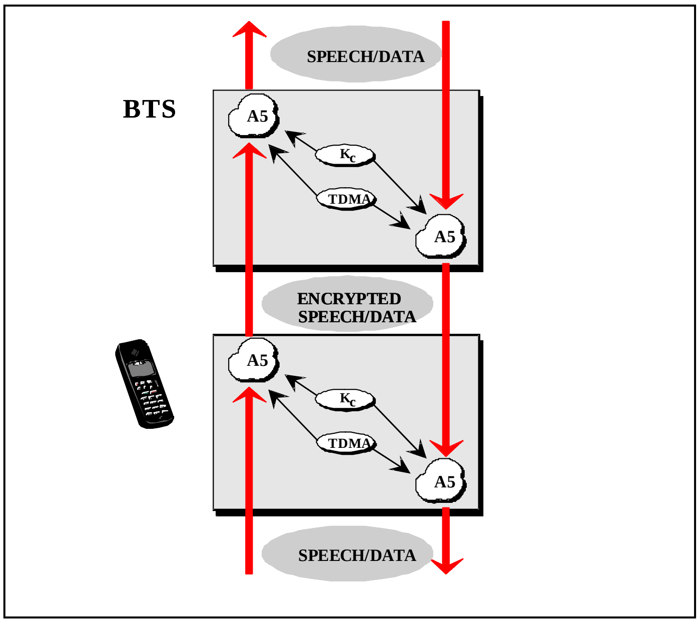


Figure 39 Ciphering or Speech Encryption in GSM Network

The ciphering and integrity protection are performed between the UE and the RNC (UMTS) or the MS and BTS (GSM), and they can be used once the subscriber has been authenticated in the VLR area. They can be performed in two ways: either in connection with authentication, or without being preceded by authentication in the same transaction. The idea of ciphering and integrity protection without authentication is that the mobile has saved the KSI or CKSN received in the last authentication. This saved KSI or CKSN is compared to the one saved in the VLR in the last authentication. If the two KSIs or CKSNs are identical, authentication is not needed. If the two KSIs or CKSNs are not identical, authentication is performed. The basic element in both actions is a key set identifier (CKSN in GSM and KSI in UMTS). It is used to check that the mobile and the VLR use the same set of security keys for ciphering and integrity protection.

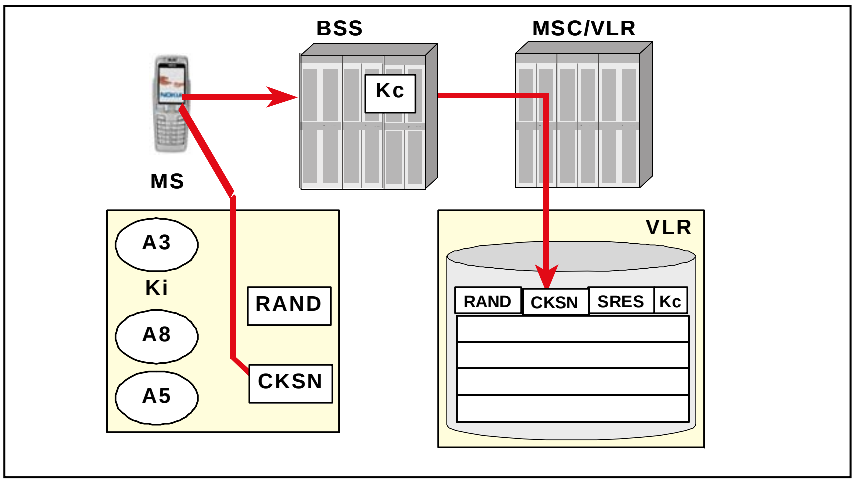


Figure 40 CKSN Comparison

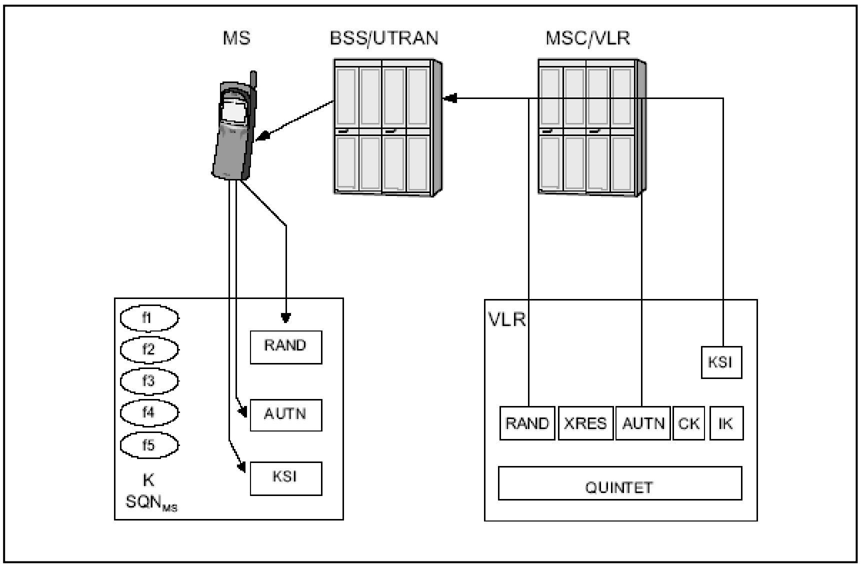


Figure 41 KSI Comparison

The authentication of subscribers attached via UTRAN cannot be completely turned off. The reason is that a UMTS transaction cannot be made without integrity protection except for emergency calls and periodic location updates without TMSI reallocation. On the other hand, integrity protection cannot be started without a valid integrity key that is agreed on throughout authentication. In case of UMTS security the ciphering key length is increased to protect the network against brute force attacks.

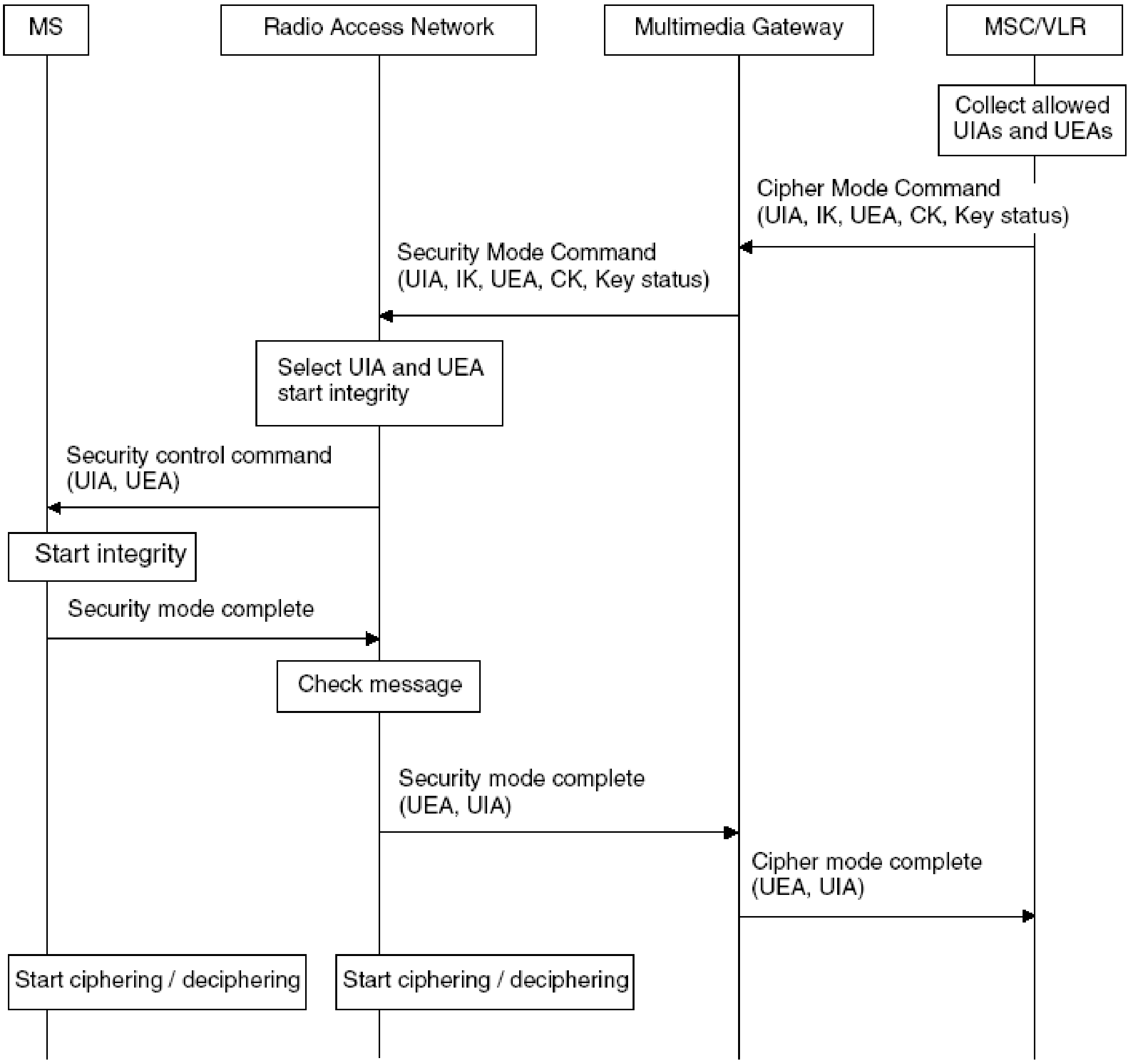

MS
Radio Access Network
Multimedia Gateway
MSC/VLR
Collect allowed UIAs and UEAs
Cipher Mode Command (UIA, IK, UEA, CK, Key status)
Security Mode Command (UIA, IK, UEA, CK, Key status)
Select UIA and UEA start integrity
Security control command (UIA, UEA)
Start integrity
Security mode complete
Check message
Security mode complete (UEA, UIA)
Cipher mode complete (UEA, UIA)
Start ciphering / deciphering
Start ciphering / deciphering

Figure 42 UMTS security mode setup

When the MS and the VLR agreed about a key set in a successful authentication the MSS/VLR sends the selected ciphering and integrity keys and the supported ciphering algorithms and integrity algorithms to the RAN. The MSS/VLR indicates whether the sent keys are new or old ones. If the keys are new it earns that they are the result of a preceding authentication and key agreement within the current transaction. The RAN knows the supported algorithms on the MS side, so it can select an appropriate algorithm for both ciphering and integrity protection. At the same time on the RAN side the integrity protection is started.

When the MS receives the algorithms it starts integrity protection and sends a security mode complete message to the RAN. The radio access network checks whether or not the integrity of the message is correct and it also sends a security mode complete message to the MGW. Finally ciphering and deciphering starts in both the MS and the RAN side.

Using the MML commands connected to handling ciphering and integrity protection, you can

- set the ciphering ON or OFF (separately for GSM and UMTS)
- disable or enable non-ciphered connection (separately for GSM and UMTS)
- set the ciphering and integrity (A5 or UEA and UIA) algorithms to be used

6.3 IMEI Checking

You can use IMEI checking, an equipment security function, to verify the identity of a mobile equipment. This means that you can detect stolen or suspicious equipment. Once you detect such equipment, you can bar it from using the network, or you can monitor its use. IMEI numbers are stored in the EIR database, which has three equipment lists: white, grey, or black.

The MSS controls IMEI checking and checking requests. Transfer of an IMEI is necessary when a user equipment has an event, such as location update, mobile terminated call, or IMSI attach, defined by IMEI checking parameters (with the ZMX command group). First the system asks the mobile equipment to send its IMEI. After receiving it, the MSS sends the IMEI check request to the EIR. The EIR searches its databases to determine on which list the mobile's IMEI is located, and then returns information to the MSS whether the mobile equipment is on the black, grey, white, or unknown list. The MSS acts on the information accordingly (for example, the MSS may terminate the call if the mobile's IMEI is found to be on the black list).

There are two kinds of IMEI checking:

- IMEI checking inside the VLR
- IMEI status checking from the EIR coloured lists

You can define the parameter values of these actions with a ZMXN command.

The IMEI checking procedure can be executed in the following situations:

- Location update of a new subscriber in the VLR
- IMSI attach procedure
- Any other radio contact procedure you order.

You can set the IMEI checking frequency and define different IMEI check for own and roaming subscribers.

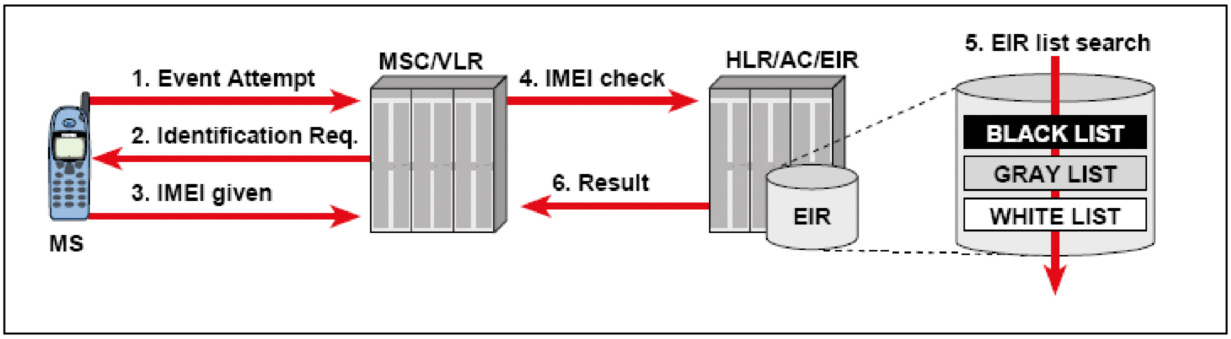


Figure 43 IMEI status checking from the EIR

6.3.1 Central Equipment Identity Register (CEIR)

CEIR is a central database or central point for updating data to the EIR, which is maintained locally on each PLMN. The CEIR is responsible for collecting, processing, and making local data from individual PLMN available as part of the common data for PLMNs worldwide.

In order to benefit from the establishment of the CEIR, it is therefore necessary to have an interface between the CEIR and the EIR. The interface has two basic functions:

- to read the common data from the CEIR and update it to the EIR
- to collect the data input to the EIR and send it to the CEIR so that the common data can be updated.

With CEIR, stolen mobile phones can also be barred in countries that are connected to the CEIR. Connecting an EIR to the CEIR requires an X.25 FTAM interface.

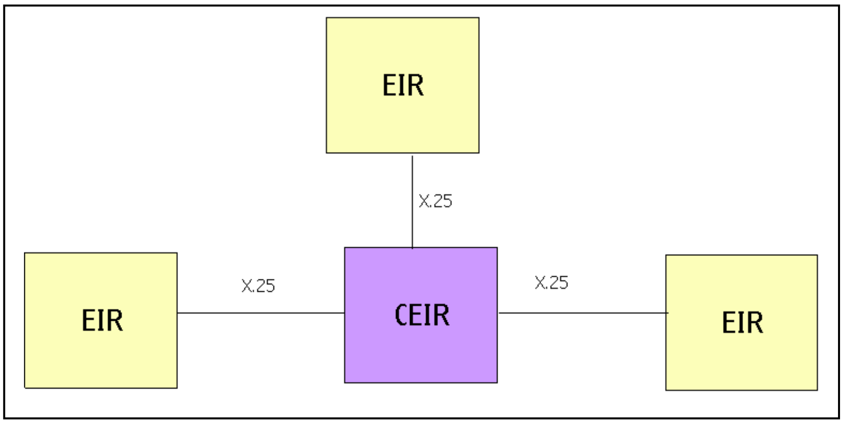


Figure 44 CEIR-EIR Interface

6.4 TMSI Reallocation

The purpose of TMSI is to provide better subscriber confidentiality in the radio path. Instead of using the IMSI (International Mobile Subscriber Identity) for identification, the mobile can use TMSI whenever possible.

You can handle the use of TMSI in two ways:

- Set the use of TMSI ON or OFF.
- Define the frequency of the TMSI reallocation in various situations.

6.4.1 Setting the TMSI ON or OFF

To set the use of TMSI ON/OFF means that you can allow or block the use of TMSI in the VLR. To set the use of TMSI ON/OFF requires a VLR-specific parameter.

Note

If the parameter is set to OFF, the TMSI is not in use and other TMSI-specific parameters have no effect

With the MXM command, you can disable or enable the use of the TMSI in the VLR.

6.4.2 Defining the TMSI Reallocation Frequency

TMSI reallocation means changing the mobile’s TMSI. The TMSI reallocation frequency is PLMN-specific. PLMN-specific parameters control VLR functions, which depend on the subscriber’s home PLMN. Defining the TMSI reallocation frequency enables you to differentiate roaming subscribers from each other. This means, for example, that you can use TMSI allocation more frequently with your home subscribers than with visitors.

Examples of TMSI-specific parameters are:

- TMSI allocation on location update with a new visitor
- TMSI allocation on IMSI attach
- TMSI allocation on Mobile Originated Call

Generally, TMSI reallocation should be ON with location update, IMSI attach, and location update with a new visitor. According to GSM specifications, TMSI is location-area-specific. With the MXN command, you can define the TMSI allocation scheme on the basis of the subscribers’ home PLMN.

7 Parameter Management in EIR, HLR and VLR

This section presents the parameter management possibilities in three network elements of the GSM network: Equipment Identity Register (EIR), Home Location Register (HLR), and Visitor Location Register (VLR).

You can define how the network performs for subscribers, such as home and roaming subscribers, and also define the methods for putting subscribers IMEIs on colour lists.

7.1 EIR Parameter Management

EIR parameter management involves handling of EIR-specific parameters that define the correlation between the three EIR lists and interact with VLR-specific parameters.

In practice, EIR parameter handling involves:

- Defining the colour of unknown equipment or an equipment identity that is not found on any EIR list during IMEI checking
- Defining the correlation between the EIR lists

The following defines what is meant by white list status and the correlation between black and grey lists:

  - The white list status defines if an equipment identity can be added to another EIR list if it is not on a white list. The white list can be defined as obligatory or optional. When the white list is set to obligatory, the equipment identity cannot be entered to any other list without first being on the white list.
  - The correlation between black and grey lists defines if an equipment identity can be added to the black/grey list when it already exists on the one or the other list.

By default, the same equipment identity can be entered on the black and grey lists even if it already exists on the one or the other list, and that the white list is optional.

Correlation checking is done only when entering an IMEI on a list. This means that the restrictions are valid after you have set the correlations. The coloured lists are not automatically compared in order to find out if a restricted IMEI entry is on two lists simultaneously.

With the command MEP, you can display and change the values of the EIR parameters.

```
MEP:;

EIR PARAMETERS DATA:

        UNKNOWN EQUIPMENT …........ W
        BLACK/GREY CORRELATION ….. N
        WHITE OBLIGATORY …........ Y

COMMAND EXECUTED
```

Figure 45   EIR parameters

In the NSN solution, the IMEI consists of 14 digits. If, for example, the system refers to the “three last digits”, this means that you take the last three digits of the 14 digits. The 15th digit is always 0.

7.2 HLR Parameter Management

HLR parameter management involves handling parameters that affect the entire HLR function. Using HLR parameters, you can control certain functionalities in the HLR and affect all HLR subscribers. The parameters are divided into HLR-specific and PLMN-specific parameters. The MJ command group is used to manage the parameters.

*HLR-specific par*ameters, as the name implies, are general HLR parameters that do not depend on the PLMN. These parameters define HLR actions and affect all subscribers in the HLR.

PLMN-specific parameters control those HLR functions that depend on the PLMN where the subscriber is roaming. These parameters control how the HLR operates with other networks.

PLMN-specific parameters are used to handle the following operations:

- Transfer subscriber data when the updating of subscriber data fails
- Define denied services and roaming limitations (that is, restricted basic or supplementary services, and restricted roaming for subscribers with certain services)

Figure 46 & 47 show HLR-specific parameters and PLMN-specific parameters respectively.

```
MJO:;
DX 200    HLR02                     2009-04-17  17:56:12
                     HLR PARAMETERS:

    NCF    = CHECK NUMBER OF CALL FORWARDINGS ............. Y
    OMCF   = OVERRIDE OF MULTIPLE CALL FORWARDINGS ......... N
    MCF    = MAXIMUM NUMBER OF CALL FORWARDINGS ............ 5
    TIME   = DEFAULT VALUE FOR NO_REPLY_CONDITION_TIMER .... 10
    INSN   = NUMBER OF INSERT ATTEMPTS ..................... 2
    INSI   = INTERVAL BETWEEN INSERT ATTEMPTS .............. 1
    DELN   = NUMBER OF DELETION ATTEMPTS ................... 2
    DELI   = INTERVAL BETWEEN DELETION ATTEMPTS ............ 0
    ALERT  = DELAY OF SENDING ALERTSC ...................... 0
    SCPUA  = ALLOW LOCATION UPDATE WHILE SCP UNAVAILABLE ... Y
    MMGAP  = ALLOW GAPPING ................................. N
    SCPSS  = ALLOW SS MANAGEMENT WHILE SCP UNAVAILABLE ..... Y
    ATI    = ALLOW ANY TIME INTERROGATION .................. N
    CIW    = CAMEL - CORE INAP INTERWORKING ................ BOTH
    DAUC   = ALLOW DELETE SUBSCRIBER IN AUC ................ N
    ACFR   = ACTION IN CF REGISTRATION ..................... RP
    AIAFR  = ACTION IN AUTHENTICATION FAILURE REPORT........ NA
    CPCF   = C SUBSCRIBER NUMBER FOR PRIORITY CF ...........
    CLIR   = CLIR IS SENT INSTEAD OF COMMON MSISDN ......... N
    SHCU   = SKIP HPLMN COUNTER UPDATES .................... N
    CSRI   = CHECK PLMN PARAMETERS IN SRI .................. Y
    HOMEP  = HOME NETWORK DEFINITION ....................... 0
    ARP    = ALLOCATION CLASS .............................. 0

    HOMING PREFIXES:
    NOT DEFINED
COMMAND EXECUTED
```

Figure 46   HLR-specific parameters in the HLR

```
MJP:NAME=HPLMN:;
HLRi      HLR01                     2009-04-17  17:55:10
                 PLMN PARAMETERS

 PLMN NAME ................................. HPLMN
 PLMN ADDRESS .............................. 86123
 INDEX ..................................... 1
 TYPE ...................................... HPLMN
 SUBSCRIBER REMOVED FROM VLR IF UPDATE FAILS. N
 ROAMING NOT ALLOWED WITH CERTAIN SERVICES .. N
 SUPPORTED CAMEL PHASE ..................... D

 NOT ALLOWED BASIC SERVICES:
 NOT ALLOWED SUPPLEMENTARY SERVICES:
COMMAND EXECUTED
```

Figure 47   PLMN-specific parameters in the HLR

7.3 VLR Parameter Management

VLR parameter management allows you to control VLR functionalities using VLR parameters.

VLR parameters are divided into PLMN-specific and VLR-specific parameters. This means that you can differentiate home and visitor subscribers, as for example, if you want to use authentication more often with visiting subscribers than with home subscribers.

7.3.1 VLR-specific Parameters

VLR-specific parameters are parameters used for controlling VLR functions that do not depend on the subscriber’s HPLMN (Home PLMN). Home and visiting subscribers are handled with the same VLR-specific parameters.

With VLR-specific parameters you can handle:

- General VLR operations (for example, VLR cleaning, triplet record, deregistration)
- Security operations (for example, use of authentication and IMEI checking)
- Use of TMSI paging and searching
- Support of supplementary services, teleservices, and bearer services.

7.3.2 PLMN-specific Parameters

PLMN-specific parameters control VLR functions that depend on the subscriber’s HPLMN. With PLMN-specific parameters you can handle:

- Roaming status
- IMEI checking parameters
- TMSI allocation parameters
- Authentication and ciphering parameters
- Advice of Charge parameters
- Equal Access parameters
- Intelligent network mobility management

Figure 48 & 49 show VLR-specific parameters and PLMN-specific parameters respectively.

Note

Some information in the VLR and PLMN parameters printout relates to cellular radio network management.

```
< ZMXO;
LOADING PROGRAM VERSION 19.9-0
MSCi      MSS04                     2009-04-17  18:01:08
                                VLR PARAMETERS

TMSI:                         USED
IMPLICIT IMSI DETACH:         NOT USED
AUTHENTICATION:               NOT USED
AUTHENT RETRY:                NOT USED
TMSI AUTHENT RETRY:           NOT USED
AUTH RETRY WITH NEW TRIPLET:  NOT USED
EMERGENCY CALL:       AUTHENT NOT USED          IMEI CHECKING NOT USED
ALLOW CCBS WHEN UDUB:       NO
ALLOW CCBS WHEN CFB ACTIVE: NO
ALLOW LOCATION UPDATE WHILE SCP UNAVAILABLE:        YES
ALLOW GAPPING IN IN-MM:                             NO
ALLOW SHORT MESSAGE TRANSFER WHILE SCP UNAVAILABLE: YES
ALLOW GAPPING IN IN-SMS:                            NO
NUMBER OF SIMULTANEOUS CALL TRANSFERS:
ALLOW CALL TRANSFER WHEN MAX EXCEEDED:              NO
TRAFFIC TERMINATION ON TERM REQUEST:                NOT USED
DEFAULT ACTION FOR CALL TRANSFER INVOCATIONS:       REPORT
--------------------------------------------------------------------------------
TIME LIMITS
  LOITERING:                            001 DAYS 00 HRS.
  IMPLICIT DEREGISTRATION:              012 HRS. 00 MIN.
  CALL WAITING:                         00 MIN. 50 SEC.
  INCOMING CALL COMPLETION RESPONSE:    04 MIN. 20 SEC.
  TMSI FREEZING                         NOT USED
--------------------------------------------------------------------------------
VLR CLEANING START TIME:        04:12
TRIPLETS:                       MIN=0
QUINTETS:                       MIN=2
CDR ON LOCATION UPDATE:         DISABLED
--------------------------------------------------------------------------------
VLR TRAFFIC CONTROL PRIORITIES
MOBILE ORIGINATED CALL             70
MOBILE TERMINATED CALL             55
MOBILE ORIGINATED SHORT MESSAGE    70
MOBILE TERMINATED SHORT MESSAGE    55
INTRA VLR LOCATION UPDATE          40
INTER VLR LOCATION UPDATE          30
PRIORITY MODE CPU LEVEL            85%
--------------------------------------------------------------------------------
SUPPORTED SUPPLEMENTARY SERVICES
  CALL FORWARDING:        CFU CFB CFNA CFNR
  CALL COMPLETION:        CW HOLD
  MULTIPARTY:             MPTY
  CHARGING:               AOCI AOCC
  CALL RESTRICTION:       BAOC BOIC BOIH
  NOKIA SPECIFIC SERV:    SSET
--------------------------------------------------------------------------------
SUPPORTED TELESERVICES
  SPEECH TRANSMISSION:    T11
  SHORT MESSAGE:          T21 T22
  FACSIMILE TRANSMISSION: T61 T62
--------------------------------------------------------------------------------
SUPPORTED BEARER SERVICES
  DATA C.D.A:             B11 B12 B13 B14 B15 B16
  DATA C.D.S:             B1A B1C B1D B1E B1F
--------------------------------------------------------------------------------
PAGE AND SEARCH
  LIMIT FOR SIMULTANEOUS SEARCHES:  SEARCHES ARE NOT LIMITED
  NUMBER OF SEARCH REPETITIONS:     2
  SEARCH RESPONSE WAITING TIME:     3000 MSEC.
  TMSI PAGE REPETITION IN MT CALL:  NOT USED
  TMSI PAGE REPETITION IN MT SMS:   NOT USED
  TMSI PAGE REPETITION IN MT USSD:  NOT USED
  TMSI PAGE REPETITION IN MT LR:    NOT USED
--------------------------------------------------------------------------------
DEFAULT REJECT CAUSE CODES

                        TO GSM   TO UMTS
GSM SUBSCRIBER          NO       NO
UMTS SUBSCRIBER (USIM)  NO       NO
--------------------------------------------------------------------------------
IMSI ANALYSIS FAILURE REJECT CAUSE CODE IN GSM NETWORK  : PLMN
IMSI ANALYSIS FAILURE REJECT CAUSE CODE IN UMTS NETWORK : PLMN

COMMAND EXECUTED
```

Figure 48   VLR-specific parameters in the VLR

```

MXP:IND=1;

MSCi      MSS04                     2009-04-17  18:05:00
                               PLMN PARAMETERS

VISITOR PLMN CHINA1 IN FOREIGN COUNTRY
INDEX:          1
CIPHERING:      NOT USED
TRIPLET RE-USE: USED
EMLPP DEFAULT PRIORITY LEVEL: 4        SUPPORT OF EMLPP: YES
COUNTRY CODE LENGTH:    2
MSRN GROUP:                   00        BLACK LIST EFFECT:      ALLOW
MSRN LIFE TIME:               90 SEC.   GREY LIST EFFECT:       ALLOW
PNS TIME LIMIT:               20 SEC.   UNKNOWN IMEI EFFECT:    ALLOW
TRAFFIC TERMINATION ON CANCEL LOCATION: NOT USED
SUPPORTED CAMEL PHASE:                  NOT SUPPORTED
FRAUD OBSERVATION AND LIMITATION:       NOT USED
REGIONAL ROAMING:                       NOT ALLOWED
ZONE CODES:
ZONE CODES FROM HLR:                    USED
EXACT MS CATEGORY USAGE:                NOT ALLOWED
REJECT CAUSE FOR UDL REJECTION:         ROAM
USAGE OF PLMN SPECIFIC SS 253:          NOT SUPPORTED
--------------------------------------------------------------------------------
ADVICE OF CHARGE PARAMETERS

  E1:    0,0           E2:    0,0            E3:     0,00
  E4:    0,0
  E7:    0,0
--------------------------------------------------------------------------------
A5 ALGORITHM PARAMETERS

  NONCIPHERED CONNECTION: ALLOWED
  A5/1: NOT ALLOWED     A5/2: NOT ALLOWED     A5/3: NOT ALLOWED
  A5/4: NOT ALLOWED     A5/5: NOT ALLOWED     A5/6: NOT ALLOWED
  A5/7: NOT ALLOWED
--------------------------------------------------------------------------------
IMEI STATUS CHECK FROM EIR IN CASE OF...
```

```
  LOC UP:     NOT USED     PER UP:  NOT USED    IMSI ATTACH:  NOT USED
  MO CALL:    NOT USED     MO SMS:  NOT USED    SS OPER:      NOT USED
  MT CALL:    NOT USED     MT SMS:  NOT USED    MT USSD:      NOT USED
  MT LOC REQ: NOT USED
--------------------------------------------------------------------------------
USAGE FREQUENCY COUNTERS  (0 = NOT USED)

  TMSI ALLOCATION
    LOC UP NEW VIS:    1          LOC UP:     1           PER UP:        1
    IMSI ATTACH:       1          MO CALL:    0           MO SMS:        0
    MT CALL:           0          MT SMS:     0           MT LOC REQ:    0
    MT USSD:           0          SS OPER:    0

  AUTHENTICATION
    LOC UP NEW VIS:    0          LOC UP:     0           PER UP:        0
    IMSI ATTACH:       0          MO CALL:    0           MO SMS:        0
    MT CALL:           0          MT SMS:     0           MT LOC REQ:    0
    MT USSD:           0          SS OPER:    0

  IMEI CHECKING
    LOC UP NEW VIS:    0          LOC UP:     0           PER UP:        0
    IMSI ATTACH:       0          MO CALL:    0           MO SMS:        0
    MT CALL:           0          MT SMS:     0           MT LOC REQ:    0
    MT USSD:           0          SS OPER:    0
--------------------------------------------------------------------------------
INTELLIGENT NETWORK MOBILITY MANAGEMENT

  SCP ADDRESS:
  SERVICE KEY: N

--------------------------------------------------------------------------------
INTER-PLMN HANDOVER AGREEMENTS
  MOBILE COUNTRY CODE   MOBILE NETWORK CODE

--------------------------------------------------------------------------------
EQUIVALENT PLMNS
  MOBILE COUNTRY CODE   MOBILE NETWORK CODE

UMTS CIPHERING: NOT USED
--------------------------------------------------------------------------------
UMTS ENCRYPTION PARAMETERS

NONCIPHERED CONNECTION: ALLOWED

SUPPORTED ALGORITHMS: UEA1

--------------------------------------------------------------------------------
UMTS SECURITY PARAMETERS

SUPPORTED ALGORITHMS: UIA1

--------------------------------------------------------------------------------
NETWORK ACCESS RIGHTS

                          TO GSM    REJECT CODE      TO UMTS   REJECT CODE
 GSM SUBSCRIBERS          YES                        YES
UMTS SUBSCRIBERS (USIM)   YES                        YES

--------------------------------------------------------------------------------
TRACE ACTIVATION PARAMETER

  TRACE ACTIVATION FROM THIS PLMN: NOT ALLOWED

COMMAND EXECUTED
```

Figure 49   PLMN-specific parameters in the VLR

8 Appendix A - Creating Subscriber in HLR

1. Normal subscriber is created by using command ZMIC

   e.g. Create a mobile subscriber in the HLR whose IMSI number is 244051112345 and MSISDN number is 358501154321. The rest of the parameters have default values.

   ```
   ZMIC:IMSI=244051112345,MSISDN=358501154321;
   ```

2. Telemetric subscriber

   e.g. Create a telemetric subscriber of category 1 in the HLR whose IMSI number is 244053430008 and MSISDN number is 358505430008. The primary basic service of the subscriber is short message MT/PP.

   ```
   ZMIC:IMSI=244053430008,MSISDN=358505430008,CAT=TMS1,PBS=T21;
   ```

3. GPRS subscriber is created by using command ZMNC

   E.g. Create a PDP context for the 23455555535433 subscriber. The identity of the PDP is 1, the type of the PDP context is X.25, and the address of the PDP is 35812345678. The visitor PLMN address is not allowed, the allocation class is normal priority, the index of the quality of services profile parameter is 1, and the access point name is CORPORATE.COM.

   ```
   ZMNC:IMSI=23455555535433:PDPID=1,PDPTYPE=F000,PDPADDR=531832
   5476F8,VPLMN=N,ALLOC=2,QOSP=1,APN="CORPORATE.COM";
   ```

4. Intelligent Network (IN) subscriber is created under command group ZMQG

   E.g. set the intelligent network category key 250, full intelligent network service profile, and service set index 1200 for the subscriber whose IMSI is 244051112345.

   ```
   ZMQG:IMSI=244051112345:ICK=250,INSP=FULL, SSET=1200;
   ```

9 Appendix B - Defining Basic Services and Supplementary Services in HLR

1. Defining Basic Service

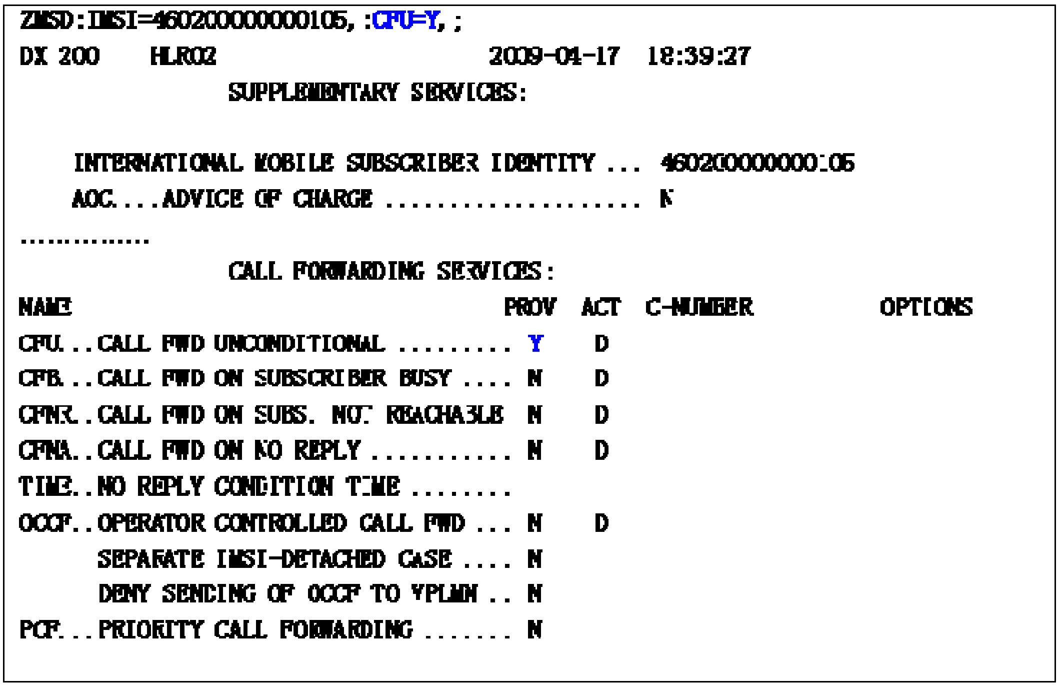
   Creating the subscriber in HLR using the command ZMIC, it means we are already having *primary basic service* which is T11. In order to add or modify basic services, we additionally create another basic service for that particular subscriber with the command ZMBC, and we can use different MSISDN for each basic service.

2. Defining Supplementary Services

   In providing the supplementary services in HLR DX200, there are two things, first: some supplementary services can be put into use just by providing the services, e.g. Calling Line ID Presentation (CLIP) or we need to do more steps in activation and bringing those services into use, for example: Call Waiting.

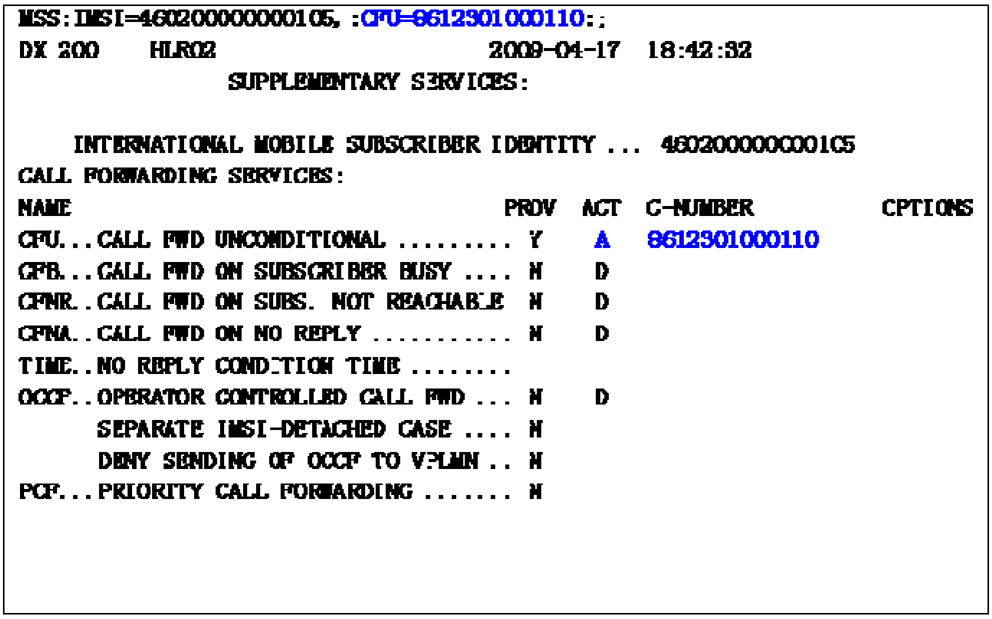
   In order to be able to do defining, activating and deactivating supplementary services, one needs to do following steps:

   - Defining the Supplementary Service : ZMSD



```
ZMSD:IMSI=460200000000105, :CFU=Y,;
DX 200     HLR02                        2009-04-17   18:39:27
                SUPPLEMENTARY SERVICES:

    INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ...  460200000000105
    AOC....ADVICE OF CHARGE ....................  N
..............
                CALL FORWARDING SERVICES:
NAME                                  PROV  ACT  C-NUMBER          OPTIONS
CFU...CALL FWD UNCONDITIONAL ......... Y     D
CFB...CALL FWD ON SUBSCRIBER BUSY .... N     D
CFNR..CALL FWD ON SUBS. NOT REACHABLE  N     D
CFNA..CALL FWD ON NO REPLY ........... N     D
TIME..NO REPLY CONDITION TIME ........
OCCF..OPERATOR CONTROLLED CALL FWD ... N     D
      SEPARATE IMSI-DETACHED CASE .... N
      DENY SENDING OF OCCF TO VPLMN .. N
PCF...PRIORITY CALL FORWARDING ....... N
```

– Activating Supplementary Services (applied for e.g. CFU etc.) ZMSS



```
MSS:IMSI=460200000000105, :CFU=8612301000110:;
DX 200     HLR02                        2009-04-17   18:42:32
                SUPPLEMENTARY SERVICES:

    INTERNATIONAL MOBILE SUBSCRIBER IDENTITY ...  460200000000105
CALL FORWARDING SERVICES:
NAME                                  PROV  ACT  C-NUMBER          CPTIONS
CFU...CALL FWD UNCONDITIONAL ......... Y     A   8612301000110
CFB...CALL FWD ON SUBSCRIBER BUSY .... N     D
CFNR..CALL FWD ON SUBS. NOT REACHABLE  N     D
CFNA..CALL FWD ON NO REPLY ........... N     D
TIME..NO REPLY CONDITION TIME ........
OCCF..OPERATOR CONTROLLED CALL FWD ... N     D
      SEPARATE IMSI-DETACHED CASE .... N
      DENY SENDING OF OCCF TO VPLMN .. N
PCF...PRIORITY CALL FORWARDING ....... N
```

– Deactivation Supplementary Services ZMSS by keying in the parameter “D” for deactivation.

10 Appendix C

10.1 GSM Phases 1, 2, and 2+

GSM Phase 1

GSM Standardisation was started by CEPT in Groupe Spécial Mobile. GSM held its first meeting in December 1982, in Stockholm. In 1988, ETSI was founded and GSM was reorganised under it as SMG (Special Mobile System). In 990, GSM modifications for the 1800 MHz frequency band were started. The system was renamed to DCS 1800. The DCS specifications were delta specifications to GSM in Phase 1. The first goal was to finish all specifications so that the first networks could start during 1991. Around 1988 the idea of Phase 2 as a functional enhancement of Phase 1 gradually crystallised. Thus, Phase 1 contains only the most important services.

GSM Phase 2 and Phase 2+

Phase 2 was created at the same time as Phase 1, since it became known that specifications for the planned services would not be on time. During Phase 2, the services that were not completed in Phase 1 were specified, and the GSM and DCS 1800 specifications merged. The general optimisation of Phase 1 and signalling improvements were also completed. At first, new ideas such as Phase 2+ were added to Phase 2 specifications. The SMG #16 decided not to add new functionalities to Phase 2, as a result of which the Phase 2+ series (5.x.y) emerged.

10.2 GSM numbering

GSM numbering covered in this section includes MSISDN, IMSI, TMSI, LAI, MSRN, and IMEI.

1. MSISDN (Mobile Station International ISDN Number) (E.164)

Purpose

The MSISDN (E.164) is the number dialled to reach the called party. It is used to identify the mobile subscriber’s service. One mobile subscriber can have several MSISDNs, depending on the number of services subscribed to (such as, telephony, facsimile, and data). The MSISDN is a unique number globally.

Structure

The MSISDN follows the same format as a normal telephone number in the PSTN:

MSISDN: CC + NDC + SN

(Digits: 1-3 1-3 *)

* The MSISDN length cannot exceed 15 digits.

Table 10 summarises the field IDs in the MSISDN structure.

Table 10 MSISDN structure

Field ID	Field name	Length (digits)	Meaning
CC	Country Code	1-3	Identifies the country
NDC	National Destination Code	1-3	Identifies the PLMN inside a country
SN	Subscriber Number	*)	Identifies the mobile subscriber’s service inside a PLMN.

Table 11 CC examples

Country	CC
Finland	358
Germany	49
Thailand	66

Country	CC
China	86

Table 12   MSISDN examples

	CC	NDC	SN
Finland	358	50	220020
China	86	139	00100

2. IMSI (International Mobile Subscriber Identity) (E.212)

Purpose

The IMSI (E.212) is used to identify the mobile subscriber. It is a unique number globally for each mobile subscriber. Each mobile subscriber has only one IMSI, but can have several MSISDNs depending on the number of services subscribed to.

Structure

IMSI: MCC + MNC + MSIN

(Digits: 3   2   max. 10)

Table 13   IMSI structure

Field ID	Field name	Length (digits)	Meaning
MCC	Mobile Country Code	3	Identifies the country
MNC	Mobile Network Code	2	Identifies the PLMN inside a country
MSIN	Mobile Subscriber Identity Number	Max. 10	Identifies the mobile subscriber inside a PLMN

Table 14   MCC examples

Country	MCC
Finland	244
Germany	262
China	460
Thailand	520

Table 15 IMSI examples

	MCC	MNC	MSIN
Finland	244	06	0000000020
China	460	00	0000000003

3. TMSI (Temporary Mobile Subscriber Identity)

Purpose

The mobile subscriber can be identified with the TMSI instead of the IMSI. The advantages of using TMSI are:

- Increased security because you do not send the IMSI over the air interface
- Increased paging capacity on the radio path because the TMSI size is smaller than the IMSI size

TMSI use is optional, but most operators use it for the above stated reasons. TMSI is always used with Location Area Identity (LAI) in order to identify which area the mobile subscriber is visiting. TMSI is generated by the VLR and can be identified only by the generating VLR. For example, if there are five VLRs in a PLMN and you visit VLR-2 first and then move to VLR-4, the previous TMSI generated by VLR-2 cannot be identified by VLR-4.

Structure

TMSI is an operator-specific number, which means that it is impossible to provide a standard structure for the TMSI. However, the TMSI number length is fixed to 32 bits (4 bytes/8 hexadecimal digits).

Examples

Table 16 TMSI examples

	Hex
TMSI –1	00045A0B
TMSI-2	00045D0B

4. LAI (Location Area Identity)

Purpose

The LAI is used to identify a location area in a GSM network.

Structure

The structure of the LAI is:

LAI: MCC + MNC + LAC

(Digits: 3 2 4 (hex))

Table 17 summarises field ID information for LAI.

Table 17 LAI structure

Field ID	Field name	Length (digits)	Meaning
MCC	Mobile Country Code	3	Identifies the country
MNC	Mobile Network Code	2	Identifies the PLMN inside a country
LAC	Location Area Code	4 hex digits	Identifies the Location Area inside a PLMN

Examples

Table 18 LAI examples

	MCC	MNC	LAC
Finland	244	06	00FE
China	460	00	01A7

5. MSRN (Mobile Station Roaming Number)

Purpose

The MSRN is a routing number used in mobile terminated calls. It is unique globally and consists of two parts. The first part is used to identify the visited VLR. The latter is used to identify the mobile subscriber visiting the VLR area.

Structure

The MSRN has the same structure as the MSISDN. But the MSRN number range is different from the MSISDN range:

MSRN: CC + NDC + SN

(Digits: 1-3   1-3   *)

* The MSRN cannot exceed 15 digits.

Table 19 summarises field ID information for the MSRN structure.

Table 19   MSRN structure

Field ID	Field name	Length (digits)	Meaning
CC	Country Code	1-3	Identifies the country
NDC	National Destination Code	1-3	Identifies the PLMN inside a country
SN	Subscriber Number	*)	Identifies the visited VLR (first 1-3 digits) and the mobile subscriber (the rest of the number)

Examples

Table 20   MSRN examples

	CC	NDC	SN
Finland	358	50	7700000123
China	86	139	00100123

6. IMEI (International Mobile station Equipment Identity)

Purpose

The IMEI identifies the mobile equipment globally.

Structure

IMEI: TAC + FAC + SNR + SP

(Digits: 6   2   6   1)

Table 21 IMEI structure

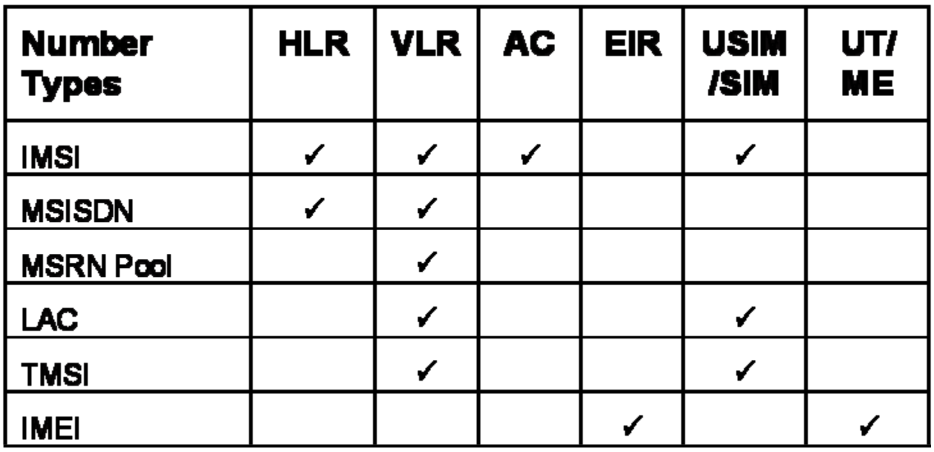
Field ID	Field name	Length (digits)	Meaning
TAC	Type Approval Code	6	Identifies the mobile equipment model, for example, Nokia 6110
FAC	Final Assembly Code	2	Identifies to which assembly series the mobile belongs
SNR	Serial Number	6	Identifies the mobile in an assembly series
SP	Spare	1	For future use

Examples

Table 22 IMEI examples

	TAC	FAC	SNR	SP
Mobile 1	490109	10	091624	0
Mobile 2	490526	10	544192	8

7. Summary of Number Locations



Number Types	HLR	VLR	AC	EIR	USIM /SIM	UT/ ME
IMSI	✓	✓	✓		✓	
MSISDN	✓	✓				
MSRN Pool		✓				
LAC		✓			✓	
TMSI		✓			✓	
IMEI				✓		✓

11 Glossary

Abbreviation	Term
AC	Authentication Centre
AES	Advanced Encryption Standard
AoC	Advice of Charge
AoCC	Advice of Charge (Charging)
AoCI	Advice of Charge (Information)
AUTN	Authentication Token
AV	Authentication Vector
BAIC	Barring of All Incoming Calls
BAOC	Barring of All Outgoing Calls
BAPR	Barring of premium rate calls
BAPS	Barring of All Packet Oriented Services
BASS	Barring of supplementary service management
BCCF	Barring of changing a call forwarding number
BCCH	Broadcast Control Channel
BIC	Barring of Incoming Calls
BIC-Roam	Barring of Incoming Calls when roaming Outside the Home PLMN Country
BICT	Barring of invocation of call transfer <option>
BIRO	Barring of All Incoming Calls when roaming Outside Home PLMN
BMSP	Barring of mobile station initiated PDP context activation
BOIC	Barring of Outgoing International Calls
BOIC-exHC	Barring of Outgoing International Calls except those directed to the Home PLMN Country
BOS	Operator specific barring category
BOSCF	Operator specific barring of CF registration <option>
BREG	Barring of registration of forwarded-to number
BPSH	Barring of packet oriented services from access points in the HPLMN while the subscriber is roaming in a VPLMN

Abbreviation	Term
BPSR	Barring of all packet oriented services while the subscriber is roaming in a VPLMN
BPSV	Barring of packet oriented services from access points in the roamed-to VPLMN
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CBI	Barring of incoming calls
CBO	Barring of outgoing calls
CCBS	Completion of Calls to Busy Subscribers
CCNR	Completion of Calls on No Reply
CD	Call Deflection
CDR	Call Detail Record
CFB	Call Forwarding on Mobile Subscriber Busy
CFB-NDUB	Call Forwarding on Busy – Network Determined, User Busy
CFB-UDUB	Call Forwarding on Busy – User Determined, User Busy
CFC	Call Forwarding Counter
CFNA	Call Forwarding on No Answer
CFNR	Call Forwarding on Not Reachable
CFNRc	Call Forwarding on Mobile Subscriber Not Reachable
CFNRy	Call Forwarding on No Reply
CFU	Call Forwarding Unconditional
CGI	Cell Global Identity
CI	Cell Identity
CKSN	Ciphering key sequence number
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CNAP	Calling Name Presentation
COLP	Connected line identification presentation

Abbreviation	Term
COLR	Connected line identification restriction
COTS	Connection Oriented Transport Service
CUG	Closed User Group
CW	Call Waiting
DES	Data Encryption Standard
DPK	Data Protection Key
ECT	Explicit Call Transfer
EIR	Equipment Identification Register
eMLPP	Enhanced Multi-Level Precedence and Pre-emption
FPGA	Field Programmable Gate Array
GCS	Gateway MSS
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HBLOFI	Hot Billing Logical File
HOLD	Call Hold
HON	Handover Number
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISDN	Integrated Services Digital Network
LA	Location Area
LAC	Location Area Code
LAI	Location Area Identity
LCS	Location Services
MAC	Message Authentication Code
MSISDN	MSS ISDN number
MMI	Man Machine Interface
MML	Man Machine Language
MPC	Modem Pool

Abbreviation	Term
MPTY	Multi Party Service
MS	Mobile Station
MSISDN	Mobile Station Subscriber ISDN Number
MSP	Multiple Subscriber Profile
MSRN	Mobile Station Roaming Number
OCCF	Operator Controlled Call Forwarding
PLMN	Public Land Mobile Network
PNP	Private Numbering Plan
PNS	Personal Number Service
ROAM	Categories active only when roaming <option> (for BICT, BASS, CBO, and BAPR)
SACCH	Slow Associated Control Channel
SDCCH	Standalone Dedicated Control Channel
SIM	Subscriber Identity Module
SMS	Short Message Service
SMSS	Short Message Service Centre
SOR	Support of Optimal Routing for Late Call Forwarding
SPNP	Support of Private Numbering Plan
TCH	Traffic Channel
TCP/IP	Transmission Control Protocol/Internet Protocol (TCP/IP)
TMSI	Temporary Mobile Station Identity
UMTS	Universal Mobile Telecommunications System
USSD	Unrestricted Supplementary Service Data
UUS	User -to-user signalling
VISDN	VLR ISDN number