ETSI TS 101 376-3-9 V1.1.1 (2001-03)

Technical Specification

GEO-Mobile Radio Interface Specifications;
Part 3: Network specifications;
Sub-part 9: Security related Network Functions;
GMR-1 03.020

Reference

DTS/SES-001-03020

Keywords

GMR, GSM, GSO, inetrface, MES, mobile, MSS,
network, radio, satellite, security, S-PCN

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2001.
All rights reserved.

Contents

Intellectual Property Rights

The information pertaining to essential IPRs is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

The attention of ETSI has been drawn to the Intellectual Property Rights (IPRs) listed below which are, or may be, or may become, Essential to the present document. The IPR owner has undertaken to grant irrevocable licences, on fair, reasonable and non-discriminatory terms and conditions under these IPRs pursuant to the ETSI IPR Policy. Further details pertaining to these IPRs can be obtained directly from the IPR owner.

The present IPR information has been submitted to ETSI and pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

IPRs:

Project	Company	Title	Country of Origin	Patent n°	Countries Applicable
TS 101 376 V1.1.1	Digital Voice Systems Inc		US	US 5,226,084	US
TS 101 376 V1.1.1	Digital Voice Systems Inc		US	US 5,715,365	US
TS 101 376 V1.1.1	Digital Voice Systems Inc		US	US 5,826,222	US
TS 101 376 V1.1.1	Digital Voice Systems Inc		US	US 5,754,974	US
TS 101 376 V1.1.1	Digital Voice Systems Inc		US	US 5,701,390	US

IPR Owner: Digital Voice Systems Inc
One Van de Graaff Drive Burlington,
MA 01803
USA

Contact: John C. Hardwick
Tel.: +1 781 270 1030
Fax: +1 781 270 0166

Project	Company	Title	Country of Origin	Patent n°	Countries Applicable
TS 101 376 V1.1.1	Ericsson Mobile Communication	Improvements in, or in relation to, equalisers	GB	GB 2 215 567	GB
TS 101 376 V1.1.1	Ericsson Mobile Communication	Power Booster	GB	GB 2 251 768	GB
TS 101 376 V1.1.1	Ericsson Mobile Communication	Receiver Gain	GB	GB 2 233 846	GB
TS 101 376 V1.1.1	Ericsson Mobile Communication	Transmitter Power Control for Radio Telephone System	GB	GB 2 233 517	GB

IPR Owner: Ericsson Mobile Communications (UK) Limited
The Keytech Centre, Ashwood Way
Basingstoke
Hampshire RG23 8BG
United Kingdom

Contact: John Watson
Tel.: +44 1256 864 821

Project	Company	Title	Country of Origin	Patent n°	Countries Applicable
TS 101 376 V1.1.1	Hughes Network Systems		US	Pending	US

IPR Owner: Hughes Network Systems
11717 Exploration Lane
Germantown, Maryland 20876
USA

Contact: John T. Whelan
Tel: +1 301 428 7172
Fax: +1 301 428 2802

Project	Company	Title	Country of Origin	Patent n°	Countries Applicable
TS 101 376 V1.1.1	Lockheed Martin Global Telecommunic. Inc	2.4-to-3 KBPS Rate Adaptation Apparatus for Use in Narrowband Data and Facsimile Communication Systems	US	US 6,108,348	US
TS 101 376 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Cellular Spacecraft TDMA Communications System with Call Interrupt Coding System for Maximizing Traffic ThroughputCellular Spacecraft TDMA Communications System with Call Interrupt Coding System for Maximizing Traffic Throughput	US	US 5,717,686	US
TS 101 376 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Enhanced Access Burst for Random Access Channels in TDMA Mobile Satellite System	US	US 5,875,182	
TS 101 376 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System	US	US 5,974,314	US
TS 101 376 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System	US	US 5,974,315	US
TS 101 376 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System with Mutual Offset High-argin Forward Control Signals	US	US 6,072,985	US
TS 101 376 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System with Spot Beam Pairing for Reduced Updates	US	US 6,118,998	US

IPR Owner: Lockheed Martin Global Telecommunications, Inc.
900 Forge Road
Norristown, PA. 19403
USA

Contact: R.F. Franciose
Tel.: +1 610 354 2535
Fax: +1 610 354 7244

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Satellite Earth Stations and Systems (SES).

The contents of the present document are subject to continuing work within TC-SES and may change following formal TC-SES approval. Should TC-SES modify the contents of the present document it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version 1.m.n

where:

- the third digit (n) is incremented when editorial only changes have been incorporated in the specification;
- the second digit (m) is incremented for all other types of changes, i.e. technical enhancements, corrections, updates, etc.

The present document is part 3, sub-part 9 of a multi-part deliverable covering the GEO-Mobile Radio Interface Specifications, as identified below:

Part 1: "General specifications";

Part 2: "Service specifications";

Part 3: "Network specifications";

Sub-part 1: "Network Functions; GMR-1 03.001";

Sub-part 2: "Network Architecture; GMR-1 03.002";

Sub-part 3: "Numbering, Addressing and identification; GMR-1 03.003";

Sub-part 4: "Organization of Subscriber Data; GMR-1 03.008";

Sub-part 5: "Technical realization of Supplementary Services; GMR-1 03.011";

Sub-part 6: "Location Registration and Position Identification Procedures; GMR-1 03.012";

Sub-part 7: "Discontinuous Reception (DRX); GMR-1 03.013";

Sub-part 8: "Support of Dual-Tone Multifrequency Signalling (DTMF); GMR-1 03.014";

Sub-part 9: "Security related Network Functions; GMR-1 03.020";

Sub-part 10: "Functions related to Mobile Earth station (MES) in idle mode; GMR-1 03.022";

Sub-part 11: "Technical realization of the Short Message Service (SMS) Point-to-Point (PP); GMR-1 03.040";

Sub-part 12: "Technical realization of the Short Message Service Cell Broadcast (SMSCB); GMR-1 03.041";

Sub-part 13: "Technical realization of group 3 facsimile using transparent mode of transmission; GMR-1 03.045";

Sub-part 14: Transmission Planning Aspects of the Speech Service in the GMR-1 system; GMR-1 03.050";

Sub-part 15: "Line Identification supplementary service - Stage 2; GMR-1 03.081";

Sub-part 16: "Call Barring (CB) supplementary services - Stage 2; GMR-1 03.088";

Sub-part 17: "Unstructured Supplementary Service Data (USSD) - Stage 2; GMR-1 03.290";

Sub-part 18: "Terminal-to-Terminal Call (TtT); GMR-1 03.296";

Sub-part 19: "Optimal Routing technical realization; GMR-1 03.297";

Sub-part 20: "Technical realization of High-Penetration Alerting; GMR-1 03.298";

Sub-part 21: "Position Reporting services; Stage 2 Service description; GMR-1 03.299";

Part 4: "Radio interface protocol specifications";

Part 5: "Radio interface physical layer specifications";

Part 6: "Speech coding specifications";

Part 7: "Terminal adaptor specifications".

Introduction

GMR stands for GEO (Geostationary Earth Orbit) Mobile Radio interface, which is used for mobile satellite services (MSS) utilizing geostationary satellite(s). GMR is derived from the terrestrial digital cellular standard GSM and supports access to GSM core networks.

Due to the differences between terrestrial and satellite channels, some modifications to the GSM standard are necessary. Some GSM specifications are directly applicable, whereas others are applicable with modifications. Similarly, some GSM specifications do not apply, while some GMR specifications have no corresponding GSM specification.

Since GMR is derived from GSM, the organization of the GMR specifications closely follows that of GSM. The GMR numbers have been designed to correspond to the GSM numbering system. All GMR specifications are allocated a unique GMR number as follows:

GMR-n xx.zyy

where:

- xx.0yy (z = 0) is used for GMR specifications that have a corresponding GSM specification. In this case, the numbers xx and yy correspond to the GSM numbering scheme.
- xx.2yy (z = 2) is used for GMR specifications that do not correspond to a GSM specification. In this case, only the number xx corresponds to the GSM numbering scheme and the number yy is allocated by GMR.
- N denotes the first (n = 1) or second (n = 2) family of GMR specifications.

A GMR system is defined by the combination of a family of GMR specifications and GSM specifications as follows:

- If a GMR specification exists it takes precedence over the corresponding GSM specification (if any). This precedence rule applies to any references in the corresponding GSM specifications.

NOTE: Any references to GSM specifications within the GMR specifications are not subject to this precedence rule. For example, a GMR specification may contain specific references to the corresponding GSM specification.

- If a GMR specification does not exist, the corresponding GSM specification may or may not apply. The applicability of the GSM specifications is defined in GMR-1 01.201 [2].

1 Scope

The present document specifies the network functions needed to provide the security related service and functions specified in technical specification GSM 02.09 [8].

The use of satellite communications for transmission to mobile subscribers makes public land mobile networks (PLMNs) particularly sensitive to:

- misuse of their resources by unauthorized persons using manipulated MESs, who try to impersonate authorized subscribers;

- eavesdropping on the various information that is exchanged on the satellite path.

It can be seen that PLMNs intrinsically do not provide the same level of protection to their operators and subscribers as the traditional telecommunication networks provide. This fact leads to the need to implement security features in a GMR-1 PLMN in order to protect:

- the access to the mobile services;

- any relevant item from being disclosed at the satellite path, mainly in order to ensure the privacy of user-related information.

Therefore two levels of protection are assumed:

1) where security features are provided, the level of protection at the satellite path of the corresponding items is as good as the level of protection provided in fixed networks;

2) where no special provision is made, the level of protection at the satellite path is null. All items that are not dealt with in clause 4 are considered to need no protection.

The present document draws on GSM 02.09 [8] "Security Aspect" and GSM 03.20 [10] "Security-Related Network Functions" to establish functional requirements as well as detailed procedures for GMR-1 system security.

The present document does not address the cryptological algorithms that are needed to provide different security related features. This topic is addressed in annex C. Wherever a cryptological algorithm or mechanism is needed, this is signalled with a reference to annex C. The references refers only to functionalities, and some algorithms may be identical or use common hardware.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

[1] GMR-1 01.004 (ETSI TS 101 376-1-1): "GEO-Mobile Radio Interface Specifications; Part 1: General specifications; Sub-part 1: Abbreviations and acronyms; GMR-1 01.004".

[2] GMR-1 01.201 (ETSI TS 101 376-1-2): "GEO-Mobile Radio Interface Specifications; Part 1: General specifications; Sub-part 2: Introduction to the GMR-1 Family; GMR-1 01.201".

[3] GMR-1 03.003 (ETSI TS 101 376-3-3): "GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 3: Numbering, Addressing and identification; GMR-1 03.003".

[4] GMR-1 03.296 (ETSI TS 101 376-3-18): "GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 18: Terminal-to-Terminal Call (TtT); GMR-1 03.296".

[5] GMR-1 03.297 (ETSI TS 101 376-3-19): "GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 19: Optimal Routing technical realisation; GMR-1 03.297".

[6] GMR-1 05.002 (ETSI TS 101 376-5-2): "GEO-Mobile Radio Interface Specifications; Part 5: Radio interface physical layer specifications; Sub-part 2: Multiplexing and Multiple Access; Stage 2 Service Description; GMR-1 05.002".

[7] GMR-1 05.010 (ETSI TS 101 376-5-7): "GEO-Mobile Radio Interface Specifications; Part 5: Radio interface physical layer specifications; Sub-part 7: Radio Subsystem Synchronisation; GMR-1 05.010".

[8] GSM 02.09 ETSI ETS 300 506: "Digital cellular telecommunications system (Phase 2); Security aspects (GSM 02.09 version 4.4.1)".

[9] GSM 02.17 (ETSI ETS 300 509): "European digital cellular telecommunications system (Phase 2); Subscriber Identity Module (SIM); Functional characteristics (GSM 02.17 V4.3.3)".

[10] GSM 03.20 (ETSI ETS 300 534): "Digital cellular telecommunications system (Phase 2); Security related network functions (GSM 03.20 version 4.4.1)".

3 Abbreviations

For the purposes of the present document, the abbreviations given in GMR-1 01.004 [1] and the following apply.

A3	Authentication Algorithm, used in security schemes
A5-GMR-1	Signalling data and user data encryption algorithm, used in security schemes
A8	Session key generating algorithm, used in security schemes
Block-1	Ciphering stream used in the direction from network to MES
Block-2	Ciphering stream used in the direction from MES to network
CKSN	Ciphering Key Sequence Number
GSC	GMR-1 Security Custodian, used in security schemes
HLR	Home Location Register
HPLMN	Home Public Land Mobile Network
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Station Identity
Kc	Ciphering Key, used in security schemes
Kc[M]	Message encrypted with ciphering key Kc, used in security schemes
Kc[TMSI]	TMSI encrypted with ciphering key Kc, used in security schemes
keynr	Key number associated with a session key, used in security schemes
Ki	Individual subscriber authentication key, used in security schemes
Ktt	Common ciphering key used in mobile-to-mobile calls
LAI	Location Area Identification
lsb	least significant bit
LU	Location Update
M	Clear text message, used in security schemes
MCC	Mobile County Code
MNC	Mobile Network Code
msb	most significant bit
MSC	Mobile Switching Center
MSCID	MSC/VLR Identity
n_a	Size of triplet array, used in security schemes
PLMN	Public Land Mobile Networks
RAND	Random Number
SBID	Spot beam Identity
SIM	Subscriber Identity Module
SRES	Signed Response
TMSI	Temporary Mobile Subscriber Identity

TMSI o/n	Temporary Mobile Subscriber Identity old/new, used in security schemes
triplet	Set of three numbers: RAND, SRES, and Kc, used in security schemes
VLR	Visitor Location Register
VLR o/n	Visitor Location Register old/new

4 Security features provided in a GMR-1 PLMN

4.1 General

The following security features are considered:

- Subscriber identity (IMSI) confidentiality.
- Subscriber identity (IMSI) authentication.
- User data confidentiality on physical connections.
- Signalling information element confidentiality.
- Equipment identity number (IMEI) confidentiality.

The implementation of these five security features is mandatory on both the fixed infrastructure side and the mobile earth station (MES) side. This means that all GMR-1 PLMNs and all MESs will be able to support every security feature. For all subscribers, use of these five security features is mandatory. In case of an emergency call that does not require the SIM, all security features are bypassed. Details of the authentication algorithm and the session key algorithm are left to the discretion of the local PLMN service provider.

4.2 Subscriber identity confidentiality

4.2.1 Definition

The subscriber identity confidentiality feature is the property that the IMSI is not made available or disclosed to unauthorized individuals, entities, or processes.

4.2.2 Purpose

This feature provides for the privacy of the identities of the subscribers who are using GMR-1 PLMN resources (e.g., a traffic channel or any signalling means). It allows for the improvement of all other security features (e.g., user data confidentiality) and provides for the protection against tracing the location of a mobile subscriber by listening to the signalling exchanges on the satellite path.

4.2.3 Functional requirements

This feature necessitates the confidentiality of the subscriber identity (IMSI) when it is transferred in signalling messages (see clause 4.5) together with specific measures to preclude the possibility to derive it indirectly from listening to specific information such as addresses at the satellite path.

The means used to identify a mobile subscriber on the satellite path consists of a local number called temporary mobile subscriber identity (TMSI).

When used, the subscriber identity confidentiality feature will apply for all signalling sequences on the satellite path. However, in the case of location register failure, or in case the MES has no TMSI available, use of IMSI or IMEI is allowed on the satellite path.

4.3 Subscriber identity authentication

4.3.1 Definition

IMSI authentication corroborates that the subscriber identity claimed by the user (IMSI or TMSI) is correct.

4.3.2 Purpose

The purpose of this authentication security feature is to protect the network against unauthorized use. It enables also the protection of the GMR-1 PLMN subscribers by denying the possibility for intruders to impersonate authorized users.

4.3.3 Functional requirements

The authentication of the GMR-1 PLMN subscriber identity may be triggered by the network when the subscriber applies for:

- **Access to service**: set-up of mobile-originated or terminated calls and the activation or deactivation of a supplementary service.

- **Location update**: this refers to a change of subscriber-related information element in the visitor location register (VLR) or home location register (HLR) including location updating involving change of VLR.

Confidential information contained in the SIM should never be transmitted over the satellite radio interface.

Physical security means shall be provided to preclude the possibility to obtain sufficient information to impersonate or duplicate a subscriber in a GMR-1 PLMN, in particular by deriving sensitive information from the MES equipment.

If, on an access request to the GMR-1 PLMN, the subscriber identity authentication procedure fails and this failure is not due to network malfunction, then the access to the GMR-1 PLMN will be denied to the requesting party.

4.3.3.1 Access to services

Except in the case of an emergency call, an authentication process is required for all mobile originated and mobile terminated calls.

The following list will provide an illustration of the situations requiring an authentication procedure for the originating user:

- GMR-1 MES calls PSTN user.
- GMR-1 MES calls GMR-1 MES.
- GMR-1 MES calls GSM user.
- GMR-1 MES calls GSM user roaming in GMR-1 network.
- GSM user roaming in GMR-1 network calls PSTN user.
- GSM user roaming in GMR-1 network calls GMR-1 MES.
- GSM user roaming in GMR-1 network calls GSM PLMN user.
- GSM user roaming in GMR-1 network calls another GSM user roaming in GMR-1 network.

The following list will provide an illustration of the situations requiring an authentication procedure for the terminating user:

- PSTN user calls GMR-1 MES.
- GMR-1 MES calls GMR-1 MES.
- GSM user calls GMR-1 MES.

- GSM user roaming in GMR-1 network calls GMR-1 MES.
- PSTN user calls GSM user roaming in GMR-1 network.
- GMR-1 MES calls GSM user roaming in GMR-1 network.
- GSM user calls another GSM user roaming in GMR-1 network.
- GSM user roaming in GMR-1 network calls another GSM user roaming in GMR-1 network.

Connectionless service also requires authentication, but is not now implemented.

4.3.3.2 Storage of subscriber related information

In the GMR-1 system, the subscriber related information is always stored in the VLR which provides service for the user's current roaming area. This information is passed from VLR to another VLR as the user moves around in the system. Transfer of the subscriber related information is performed by Location Update procedure, and the later is triggered whenever the MES finds a change of Location Area Identity (LAI) received from the BCCH channel.

The LAI is defined to have four different components, i.e.:

$$LAI = MCC + MNC + SBID + MSCID$$

where MCC is defined as mobile country code, MNC is defined mobile network code, SBID is defined as spot beam identity and, MSCID is defined as MSC/VLR identity. Due to a change of mobile user's location, one or more than one component in the LAI might be changed, which eventually will initiate the procedure of a location update.

Table 4.1 outlines various reasons for triggering a location update in the GMR-1 system. In the same table, the number of MSC/VLRs involved in the location update procedure is also specified.

Table 4.1: Various types of location update in the GMR-1 system

Case No.	MCC	MNC	SBID	MSCID	Number of MSC/VLRs Involved in the LU
1	-	-	-	x	2
2	-	-	x	-	1
3	-	-	x	x	2
4	x	x	-	x	2
5	x	x	x	x	2
"-": corresponding term without any change during user's motion. "x": a corresponding change takes place due to user motion.					

The relationship between location update and a mobile user's motion is summarized in figure 4.1.

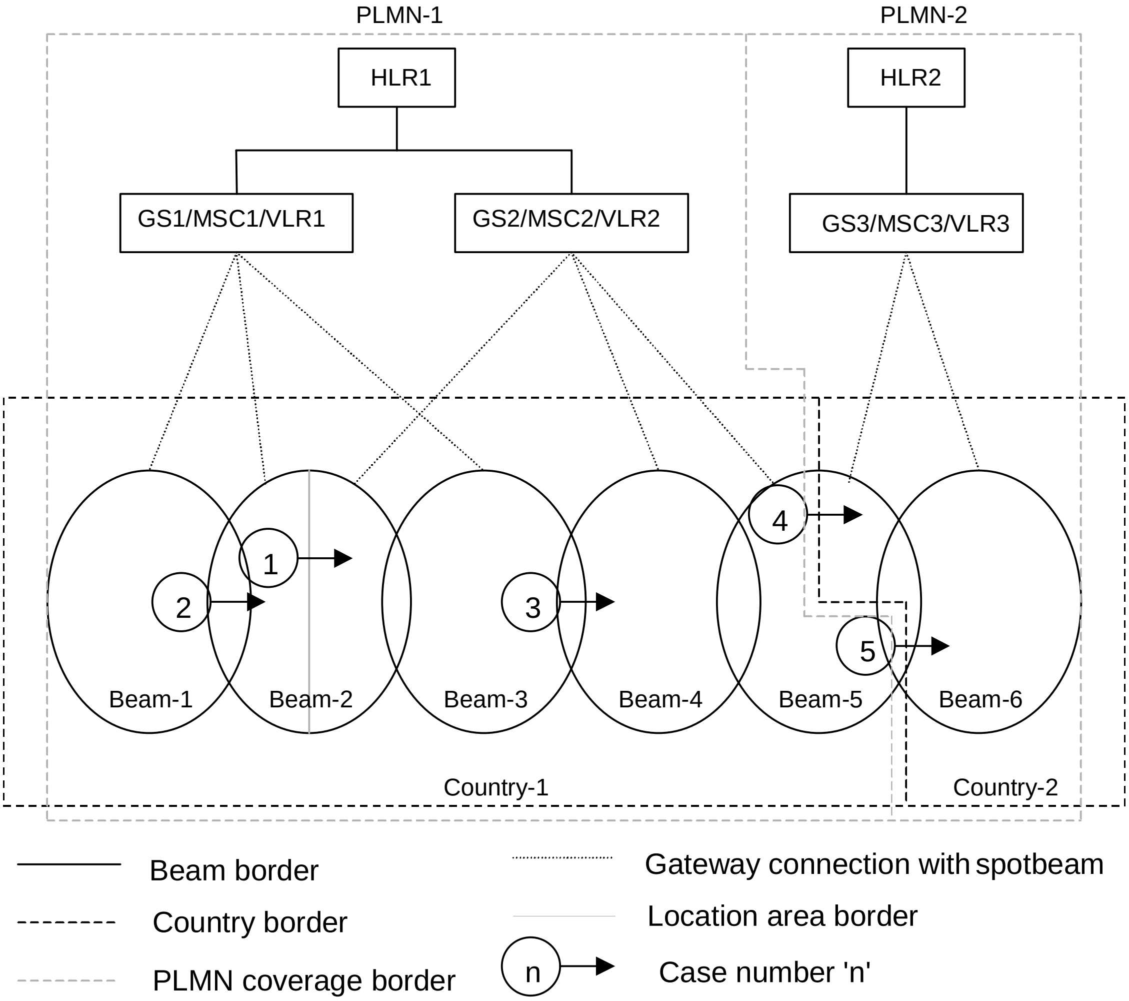


Figure 4.1: Various reasons to trigger location update due to mobile user's motion

There are five different location update cases in figure 4.1:

Case 1: In the Location Update (LU), the Gateway Station (GS) changes from GS1 to GS2, subscriber related information is passed from VLR1 to VLR2.

Case 2: In the LU, the spot beam changes from beam-1 to beam-2, subscriber related information remains in the same VLR (VLR1).

Case 3: In the LU, the GS changes from GS1 to GS2, and the spot beam changes from beam-3 to beam-4, subscriber related information is passed from VLR1 to VLR2.

Case 4: In the LU, the GS changes from GS2 to GS3, the network changes from PLMN-1 to PLMN-2, and the country changes from country-1 to country-2, subscriber related information is passed from VLR2 to VLR3.

Case 5: In the LU, the GS changes from GS2 to GS3, the spot beam changes from beam-5 to beam-6, the network changes from PLMN-1 to PLMN-2, and the country changes from country-1 to country-2, subscriber related information is passed from VLR2 to VLR3.

Apart from mobile user's motion, a location update also can be triggered by the procedure of optimal routing (OR). At the start of a mobile-originated call, if the network finds that the optimal routing GS is different from the MES's local GS, the MES is required to perform a location update from the local GS to the optimal routing GS. Upon conclusion of the mobile-originated call, the MES may register back to its original GS by performing another location update from the optimal routing GS to its original GS. See GMR-1 03.297 [5] for details. The location update procedure triggered by the OR is the same as that triggered by the mobile user's motion.

If an MES is registered and has been successfully authenticated, calls are permitted (including continuation).

If the MES is not registered or ceases to be registered, a new registration needs to be performed, and the preceding cases apply.

4.4 User data confidentiality on physical connections (voice and nonvoice)

4.4.1 Definition

The user data confidentiality feature on physical connections is the property that the user information exchanged on traffic channels is not made available or disclosed to unauthorized individuals, entities or processes.

4.4.2 Purpose

The purpose of this feature is to ensure privacy of user information on traffic channels.

4.4.3 Functional requirements

Encryption will normally be applied to all voice and nonvoice communications. See table 4.2 for a list of GMR-1 channels that are encrypted.

A standard algorithm called A5-GMR-1 will be employed throughout the system. It is permissible for the MES and/or PLMN infrastructure to support more than one algorithm. In this case, the infrastructure is responsible for deciding which algorithm to use (including the possibility not to use encryption, in which case confidentiality is not applied).

When necessary, the MES will signal to the network indicating which algorithms it supports. The serving network then selects one of these that it can support (based on an order of priority preset in the network), and signals this to the MES. The selected algorithm is then used by the MES and network.

An ON/OFF indicator for encryption is a useful feature but is not required for all situations. There should be a user option to temporarily disable or bypass this indicator if one is provided. In the case that this indicator is turned on, the MES has to check to see if user data confidentiality is switched on. If so, an indicator (e.g., a panel light) will be provided to show to the user. In the event that the MES confidentiality feature is turned off or abruptly transitions from ON to OFF, e.g., during handover, then an indication is given to the user.

This ciphering indicator feature may be disabled by the subscriber identity module (SIM).

During the establishment of a call, the trigger point for the indicator will be when the called party answers the call at the latest.

Table 4.2: GMR-1 channels which are and are not encrypted

Channel Type	Channel Name	Encryption Used?	Reasons for Use or Nonuse of Encryption
TCH Channel	TCH3	Yes	If the call set-up is performed through the TCH channel instead of the SDCCH channel, signalling messages in the TCH channel are not encrypted up to the message "Cipher Mode Command." The "Cipher Mode Acknowledge" is sent encrypted. NOTE: in order to facilitate synchronization, the cipher stream blocks are generated at both ends of the link but are discarded for DKABs.
	TCH6	Yes	Same as TCH3.
	TCH9	Yes	Same as TCH3.
BCCH Channel	BCCH	No	Common channel shared by multiple users, encryption is not applied.
	FCCH	No	Same as BCCH.
CCCH Channel	AGCH	No	Same as BCCH.
	BACH	No	Same as BCCH.
	CBCH	No	Same as BCCH.
	GBCH	No	Same as BCCH.
	PCH	No	Same as BCCH.
	RACH	No	Same as BCCH.
	TTCH	No	To avoid two bursts within the same frame using the same ciphering stream.
DCCH Channel	FACCH/3	Yes	When traffic channels are encrypted, FACCHs also use encryption. Both ends of the link generate the same size of encryption bursts suitable for TCH burst, the FACCH burst discards some bits that are not needed.
	FACCH/6	Yes	Same as FACCH/3.
	FACCH/9	Yes	Same as FACCH/3.
	SACCH	Yes	Same as FACCH/3.
	SDCCH	Yes	If the call set-up is performed through SDCCH channel instead of TCH channel, signalling messages in the SDCCH channel are not encrypted before and including the message "Cipher Mode Command," but "Cipher Mode Acknowledge" is sent encrypted.

4.5 Signalling information element confidentiality

4.5.1 Definition

The signalling information element confidentiality feature is the property that a given piece of signalling information that is exchanged between MESs and Ground Stations is not made available or disclosed to unauthorized individuals, entities, or processes.

4.5.2 Purpose

The purpose of the signalling confidentiality feature is to ensure the privacy of user-related signalling elements.

4.5.3 Functional requirements

Up to a certain point in time, when the "cipher on" command is given, the call set-up procedure is not ciphered. Information transmitted during this period includes protocol discriminator, connection reference, message type, and TMSI according to the circumstance. When ciphering is turned on, then all information in the signalling channel is ciphered.

5 Subscriber identity confidentiality

5.1 Overview

The purpose of this function is to avoid the possibility for an intruder to identify which subscriber is using a given resource on the satellite path (e.g., TCH or signalling resources) by listening to the signalling exchanges on the satellite path. This function allows both a high level of confidentiality for user data and signalling and protection against the tracing of a user's location.

The provision of this function implies that the IMSI, or any information allowing a listener to derive the IMSI easily, should not normally be transmitted in clear text in any signalling message on the satellite path.

Consequently, to obtain the required level of protection, it is necessary that:

- a protected identifying method is normally used instead of the IMSI on the satellite path; and
- when the signalling procedures permit it, signalling information elements that convey information about the mobile subscriber identity shall be ciphered for transmission on the satellite path.

The identifying method is specified in the following clause. The ciphering of communication over the satellite path is specified in clause 7.

5.2 Identifying a mobile earth station

The means used to identify a mobile subscriber on the satellite path is to use TMSI. This TMSI is a local number, having a meaning only in a given location area. Therefore the TMSI shall be accompanied by the LAI (location area identification) to avoid ambiguities. The maximum length and guidance for defining the format of a TMSI are specified in GMR-1 03.003 [3].

The TMSI is always allocated by a VLR currently visited by the mobile user. The VLR manages a suitable database to keep the relationship between TMSIs and IMSIs. If the user moves to a new location area under the control of another VLR, both security related information and the user's IMSI follow the user's motion and are passed from the original VLR to the new VLR.

The allocation of a new TMSI is always associated with the procedure of location update or initial registration. Meanwhile, the allocation of a new TMSI also triggers the de-allocation of the previous one.

When a new TMSI is allocated to an MES, it is transmitted to the MES in ciphered mode. The MES shall store its current TMSI in a non-volatile memory in the SIM, together with the LAI, so that these data are not lost when the MES is switched off.

5.3 TMSI management procedures

The means of TMSI management have the following features: TMSI allocation and deallocation are always associated with mobile user's location update; the way of managing the TMSI is closely dependent on the location update procedure.

From a user identification point of view, the signalling procedure is a function of the number of MSC/VLRs involved in the location update. Two situations have been identified: location update within the same MSC/VLR and location update between different MSC/VLRs, as shown in table 4.1. In the following clauses the TMSI management procedures will be described in terms of these two different situations.

5.3.1 User identification during location update within the same GS/MSC/VLR coverage area

This procedure is part of the location updating procedure that takes place when the original location area and the new location area depend on the same GS/MSC/VLR. The procedure relative to TMSI management is reduced to a TMSI reallocation (from TMSIo with "o" for "old" to TMSIn with "n" for "new"). Note that the location area identity (LAI) is always associated with a TMSI. Thus, a new LAI will require a new TMSI. However, the designators "o" and "n" are applied to the TMSI, by convention, and not to the LAI in the following figures.

The MES sends TMSIo as an identifying field at the beginning of the location updating procedure. The procedure is summarized in figure 5.1.

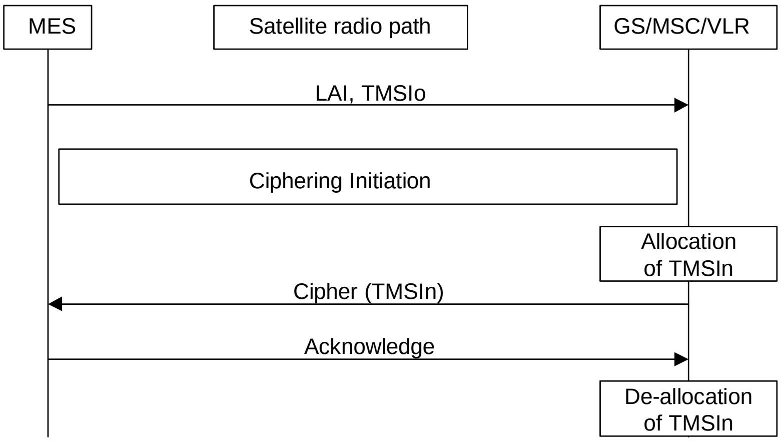


Figure 5.1: User identification during location update in the same GS/MSC/VLR area

Signalling functionality:

- MES initiates location update procedure, both LAI and TMSIo are transmitted over the satellite link in clear text.
- Ciphering Initiation (clause 6). The MES and GS/MSC/VLR agree on means for ciphering signalling information elements, in particular for transmission of TMSIn.
- A new TMSI is assigned by the VLR. It is passed to the MES in ciphered mode.

5.3.2 User identification during location update between different GS/MSC/VLRs

This procedure is part of the normal location updating procedure, using TMSI and LAI, when the original location area and the new location area depend on different GS/MSC/VLRs.

The MES is still registered in VLRo ("o" for old or original) and requests registration in VLRn ("n" for new). LAI and TMSIo are sent by MES as identifying fields during the location updating procedure. Note, that in this normal procedure, the new VLR obtains Location Update information directly from the old VLR. It will be noted later that in some cases, the VLRn shall go directly to the HLR in order to obtain the subscriber related information.

The procedure is shown figure 5.2.

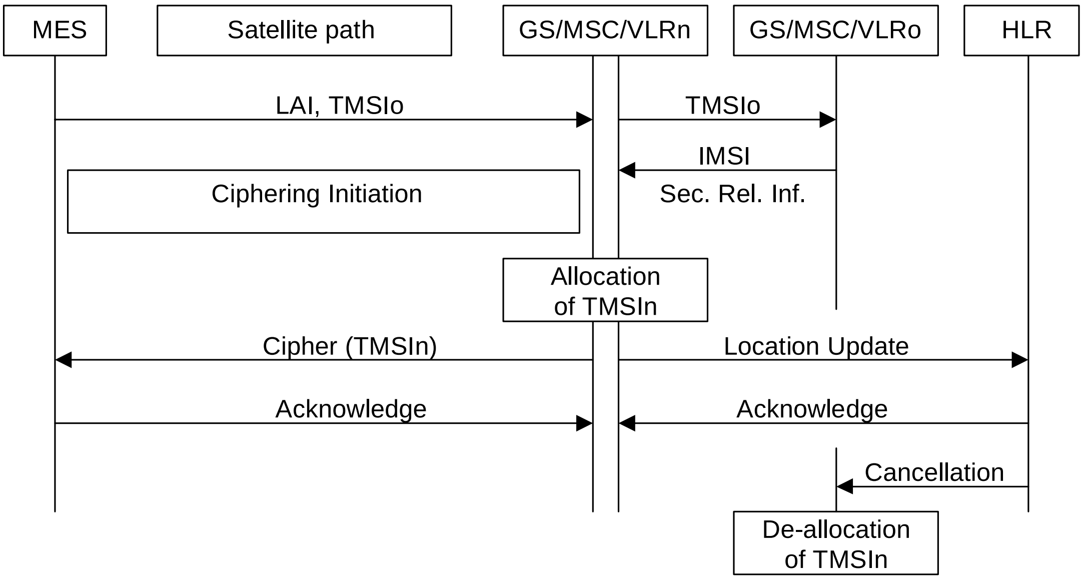


Figure 5.2: User identification during location update in different GS/MSC/VLR areas

Signalling functionality:

- MES initiates location update procedure; both LAI and TMSIo are transmitted over the satellite link in clear text.
- The MSC/VLRn needs some information for authentication and ciphering; this information is obtained from MSC/VLRo.
- Ciphering initiation. The MES and GS/MSC/VLR agree on means for ciphering signalling information elements, in particular for transmission of TMSIn.
- A new TMSI is assigned by the VLRn. It is passed to the MES in ciphered mode.
- The VLRn informs the MES's HLR about this location update.
- The HLR indicates to VLRo that the MES is now under control of another VLR. The "old" TMSI is free for allocation.

5.3.3 User identification during location registration

This situation occurs where an MES requests first time registration, but there is no TMSI available. In this case, the IMSI is used for identification. The IMSI is sent in clear text via the satellite path as part of the registration process.

This procedure is shown in figure 5.3.

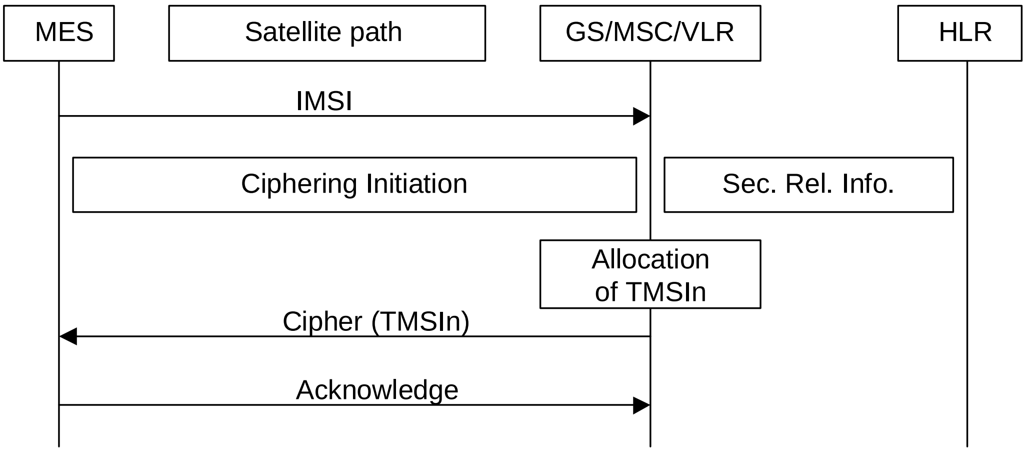


Figure 5.3: User identification during MES registration for the first time

Signalling functionality:

- The MES initiates the registration procedure. The mobile user's IMSI is transmitted over the satellite path in clear text.
- Ciphering initiation. The VLR asks for security-related information from its HLR. The MES and GS/MSC/VLR agree on the means for ciphering signalling information elements, in particular for transmission of TMSIn.
- A new TMSI is assigned by the VLR. It is passed to the MES in ciphered mode.

5.3.4 User identification with a system malfunction

To cope with malfunctioning situations, e.g., arising from a software failure or loss of database, the fixed part of the network can require the user's IMSI without encryption. This procedure is a breach in the provision of the service and should be used only when necessary.

When a TMSI is received with an LAI that does not correspond to the current VLR, the IMSI of the MES shall be requested by the VLR in charge of the indicated location area.

5.3.4.1 Location update, TMSI lost

This situation occurs where an MES asks for location update but its TMSI is lost. In this case, the IMSI is used for identification. The IMSI is sent in clear text via the satellite path as part of the location update.

The same signalling procedure shown in figure 5.3 can be reused in this case.

5.3.4.2 Location update between different GS/MSC/VLR coverage areas, old VLR not reachable

This situation arises when the VLR receiving the LAI and TMSIo cannot identify the VLRo. In that case the relation between TMSIo and IMSI is lost, and the identification of the MES in clear is necessary.

The procedure is shown in figure 5.4.

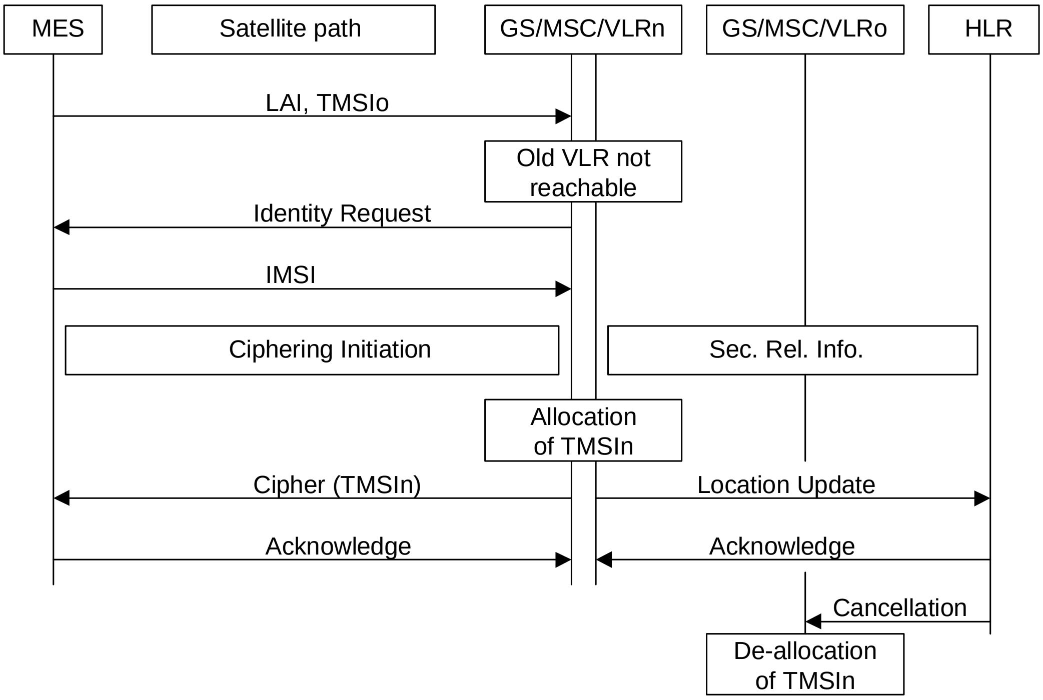


Figure 5.4: User identification during location update, different MSC/VLRs, old VLR not reachable

Signalling functionality:

- MES initiates location update procedure, both LAI and TMSIo are transmitted over the satellite link in clear text.
- By analysing the LAI contained in the location update request, the MSC/VLRn realizes the VLRo is not reachable. The GS/MSC/VLRn asks the MES to submit its identity.
- The mobile user's IMSI is passed to the VLRn over the satellite path in clear text.
- Ciphering initiation. The VLRn asks for security related information from its HLR. The MES and GS/MSC/VLRn agree on means for ciphering signalling information elements, in particular for transmission of TMSIn.
- A new TMSI is assigned by the VLRn. It is passed to the MES in ciphered mode.
- The VLRn informs the MES's HLR about this location update.
- The HLR indicates to VLRo that the MES is now under control of another VLR. The "old" TMSI is free for allocation.

5.3.4.3 Location update in the same GS/MSC/VLR coverage area, local TMSI unknown

This situation arises when a data loss has occurred in a VLR and when an MES uses an unknown TMSI, e.g., for a communication request or for a location updating request in a location area managed by the same VLR.

This procedure is shown in figure 5.5.

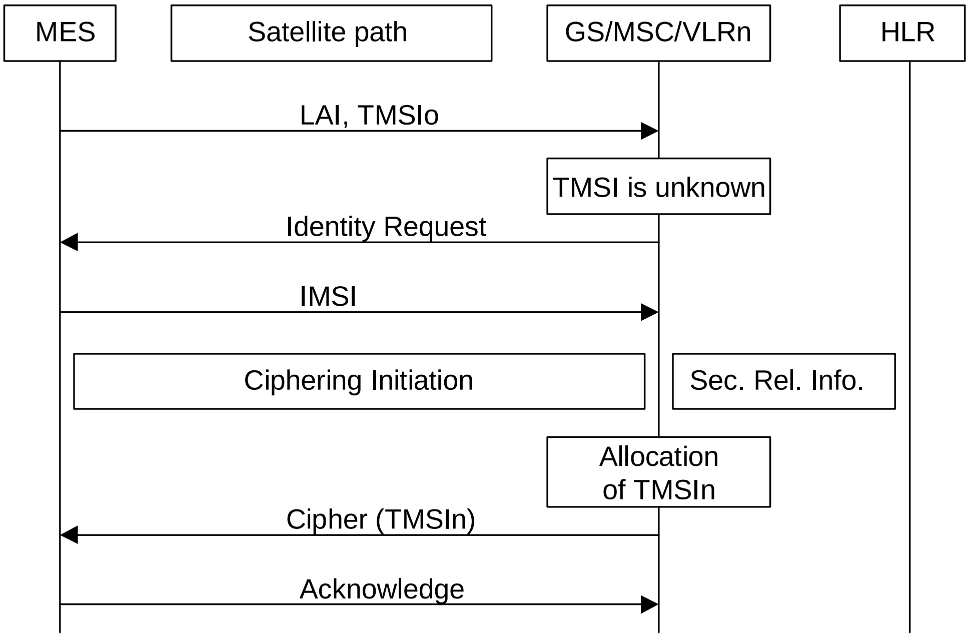


Figure 5.5: User identification during location update, same MSC/VLR, local TMSI unknown

Signalling functionality:

- MES initiates location update procedure, both LAI and TMSIo are transmitted over the satellite link in clear text.
- By analysing the LAI, it is decided that the MES has already registered in this VLR, but the VLR cannot find a corresponding record in its database matching the TMSIo. The GS/MSC/VLR asks the MES to submit its identity.
- The mobile user's IMSI is passed to the VLR over the satellite path in clear text.
- Ciphering initiation. The VLR asks for security related information from its HLR. The MES and GS/MSC/VLR agree on means for ciphering signalling information elements, in particular for transmission of TMSIn.
- A new TMSI is assigned by the VLR. It is passed to the MES in ciphered mode.

5.3.4.4 Location update between different GS/MSC/VLR coverage areas, loss of information

This situation arises when the VLR in charge of the MES has suffered a loss of data. In that case the relationship between TMSIo and IMSI is lost, and the identification of the MES without encryption is necessary.

The procedure is summarized figure 5.6.

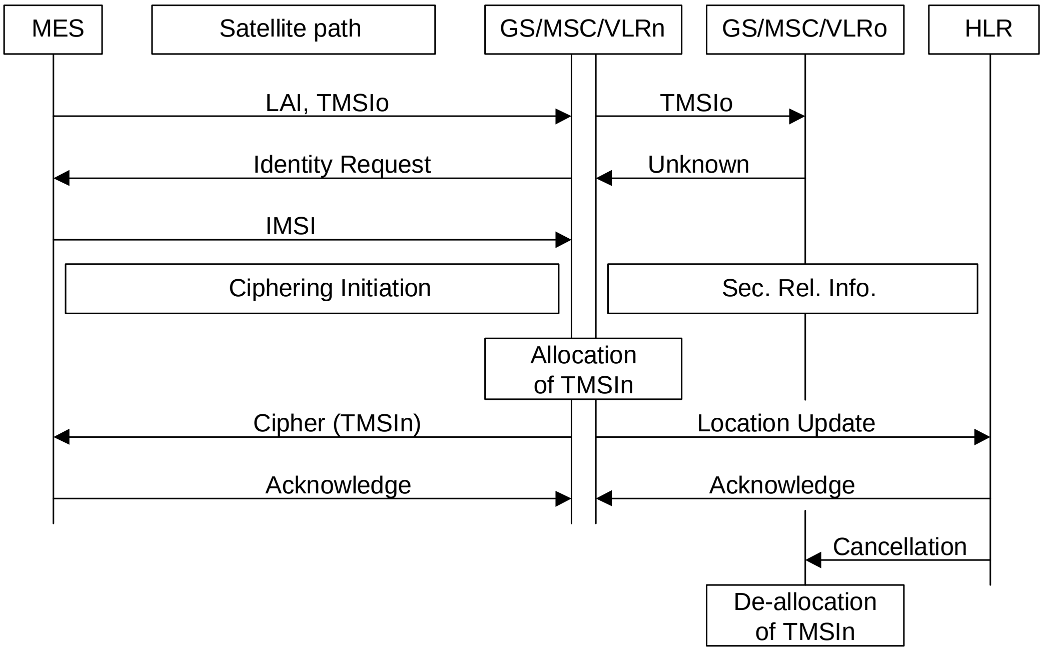


Figure 5.6: User identification during location update, different MSC/VLRs, loss of information

Signalling functionality:

- MES initiates location update procedure, both LAI and TMSIo are transmitted over the satellite link in clear text.
- Based on the received LAI, the VLRn interrogates the VLRo in order to obtain all security related information and the user's IMSI. But the VLRo cannot recognize this user due to a loss of information. In this case, the GS/MSC/VLRn shall ask the MES to submit its identity.
- The mobile user's IMSI is passed to the VLRn over the satellite path in clear text.
- Ciphering initiation. The VLRn asks for security related information from its HLR. The MES and GS/MSC/VLRn agree on means for ciphering signalling information elements, in particular for transmission of TMSIn.
- A new TMSI is assigned by the VLRn. It is passed to the MES in ciphered mode.
- The VLRn informs the MES's HLR about this location update.
- The HLR indicates to the VLRo that the MES is now under the control of another VLR. The "old" TMSI is free for allocation.

6 Subscriber identity authentication

6.1 General

The definition and operational requirements of subscriber identity authentication were described in clause 4.

The authentication procedure will also be used to set the ciphering key (see clause 6). Therefore, it is performed after the subscriber identity (TMSI/IMSI) is known by the network and before the channel is encrypted. It is possible that a call can begin in cipher mode as soon as a traffic channel is allocated. Currently this feature is not supported in the GMR-1.

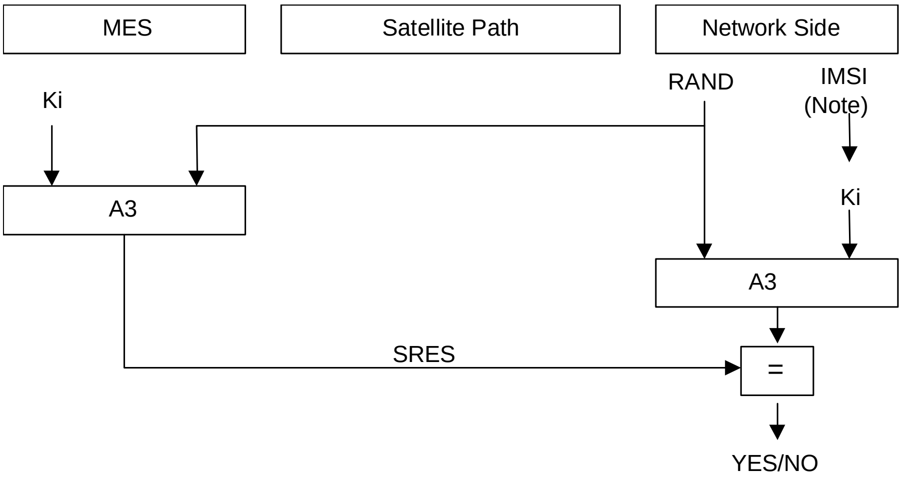
Two network functions are necessary: the authentication procedure itself and the key management within the ground subsystem.

6.2 The authentication procedure

The authentication procedure consists of the following exchange between the fixed subsystem and the MES.

- The fixed subsystem transmits a non-predictable number RAND to the MES.
- The MES computes the signature of RAND, say SRES, using algorithm A3 stored in the SIM and some secret information: the Individual Subscriber Authentication Key, denoted below by Ki also stored in the SIM.
- The MES transmits the signature SRES to the fixed subsystem.
- The fixed subsystem tests SRES for validity.

The general procedure is shown in figure 6.1.



NOTE: IMSI is used to retrieve Ki.

Figure 6.1: The authentication procedure

Authentication algorithm A3 is specified in annex C.

6.3 Subscriber authentication key management

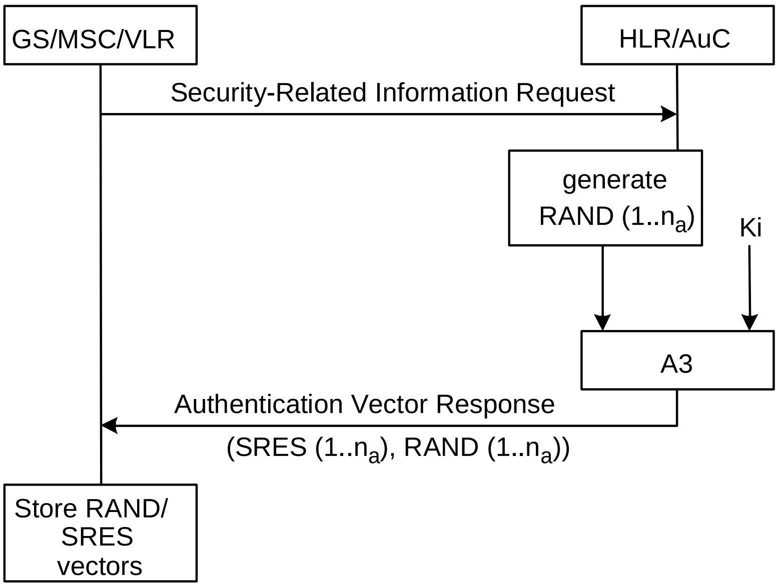
The subscriber authentication key Ki is allocated, together with the IMSI, at subscription time and both are contained on the SIM in non-readable form.

Ki is stored on the network side in the HLR, in an authentication center (AuC). A PLMN may contain one or more AuCs. An AuC can be physically integrated with other functions, e.g., in an HLR.

6.3.1 General authentication procedure

When needed for each MES, the GS/MSC/VLR requests security-related information from the HLR/AuC corresponding to the MES. This information includes an array of "triplets" of corresponding RAND, SRES, and session key, called Kc, to be described in clause 7. The first two numbers in each triplet, RAND and SRES, are obtained by applying algorithm A3 to each RAND and the key Ki, as shown in figure 6.1. The pairs are stored in the VLR as part of the security-related information.

The procedure used for updating the vectors RAND/SRES is shown in figure 6.2.


GS/MSC/VLR
HLR/AuC
Security-Related Information Request
generate RAND (1..n_a)
Ki
A3
Authentication Vector Response
(SRES (1..n_a), RAND (1..n_a))
Store RAND/ SRES vectors

NOTE: The Authentication Vector Response also contains Kc(1..n_a). For clarity, the Kc vector is not shown in figure 6.2 and the remaining figures in clause 6. For discussion of Kc, see clause 7.

Figure 6.2: Procedure for updating the vectors RAND/SRES

When an MSC/VLR performs an authentication, including the case of a location updating within the same VLR area, it chooses a RAND value in the array corresponding to the MES. It then tests the answer from the MES by comparing it with the corresponding SRES, as shown in figure 6.3.

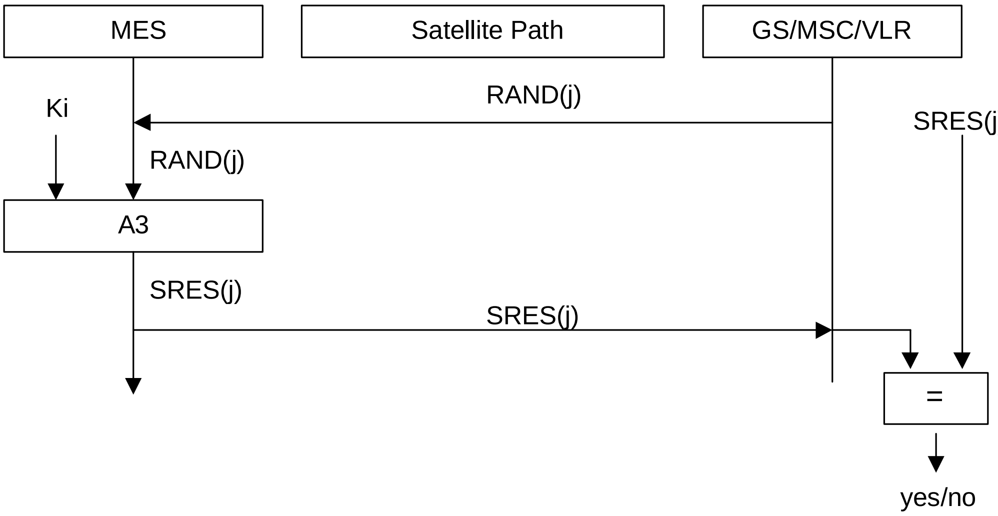


Figure 6.3: General authentication procedure

6.3.2 Authentication at location updating in a new VLR, using TMSI

During location updating in a new VLR (VLRn), the procedure to get pairs for subsequent authentication may differ from that described in the previous clause. In the case where identification is done using TMSI, pairs for authentication as part of security related information are given by the old VLR (VLRo). The old VLR will send only those pairs that have not been used to the new VLR.

The procedure is shown in figure 6.4.

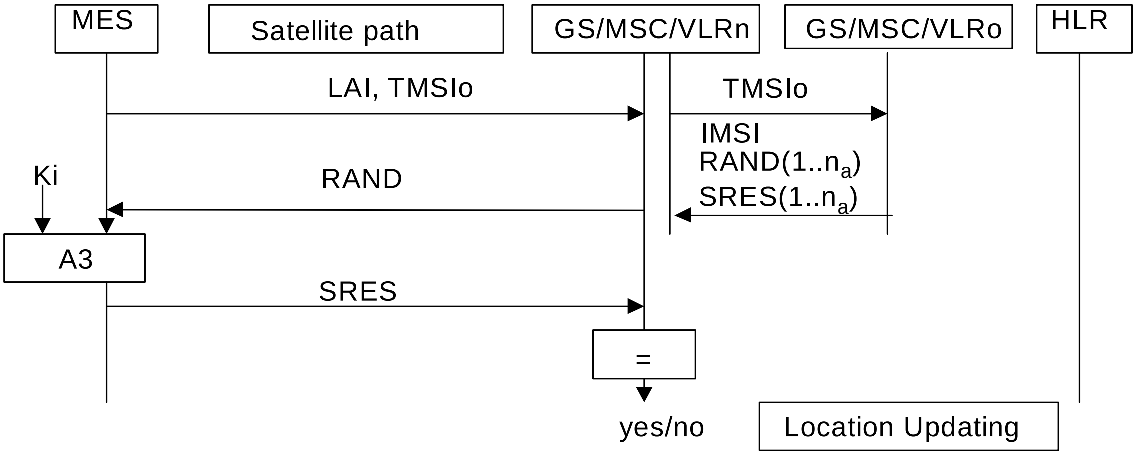


Figure 6.4: Authentication during location updating in a new VLR, using TMSI

6.3.3 Authentication at location updating in a new VLR, using IMSI

When the IMSI is used for identification, or more generally when the old VLR is not reachable, the procedure described in clause 6.3.2 cannot be used. Instead, pairs of RAND/SRES contained in the security related information are requested directly from the HLR.

The procedure is shown in figure 6.5.

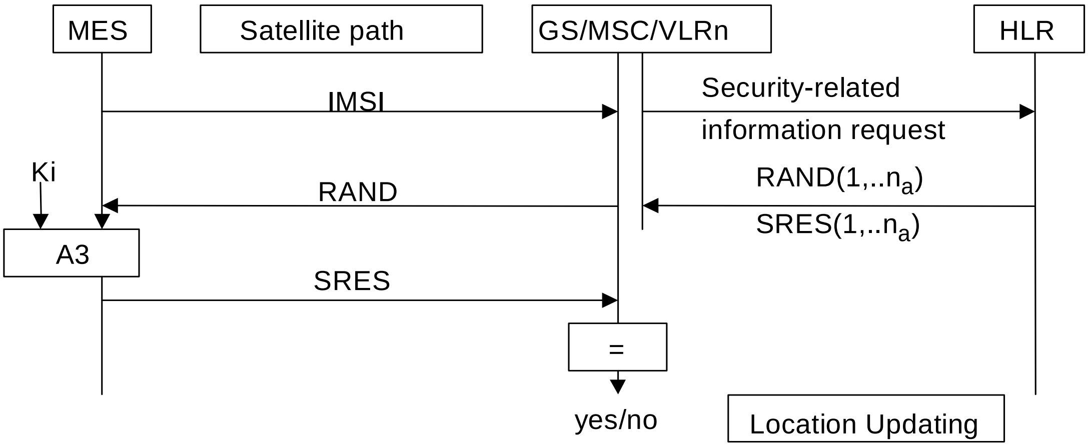


Figure 6.5: Authentication at location updating in a new VLR, using IMSI

6.3.4 Authentication at location updating in a new VLR, using TMSI, TMSI unknown in "old" VLR

This case, where a data loss has occurred in the "old" VLR, is an abnormal one.

The procedure is shown in figure 6.6.

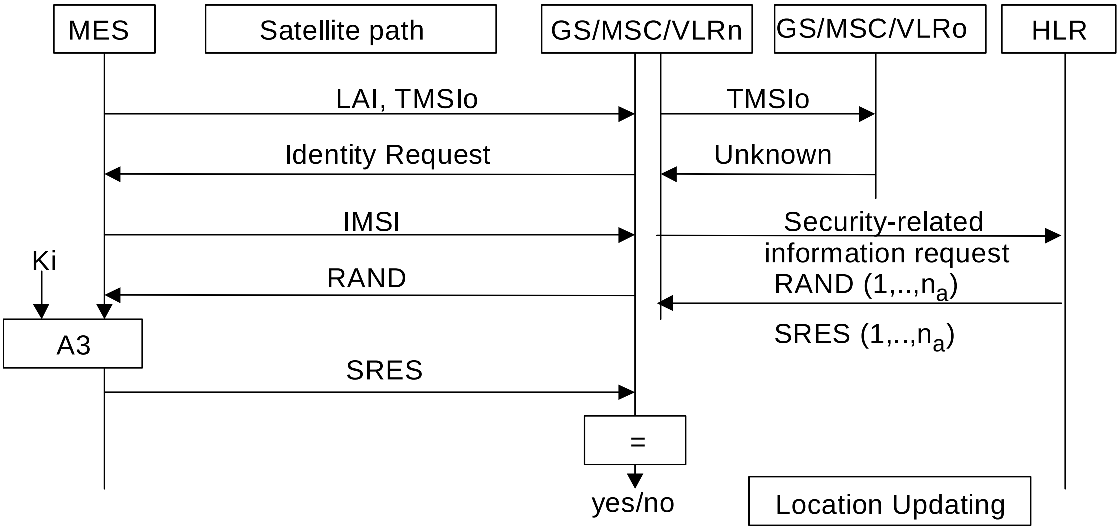


Figure 6.6: Authentication at location updating in a new VLR, using TMSI, TMSI unknown in "old" VLR

6.3.5 Authentication at location updating in a new VLR, using TMSI, old VLR not reachable

This case occurs when an old VLR cannot be reached by the new VLR.

The procedure is shown in figure 6.7.

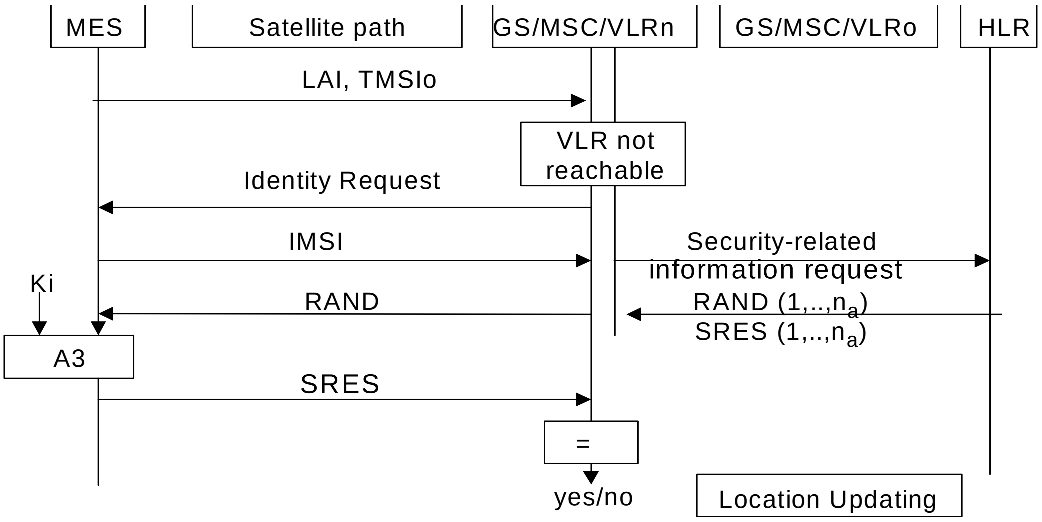


Figure 6.7: Authentication at location updating in a new VLR, using TMSI, old VLR not reachable

6.3.6 Authentication with IMSI if authentication with TMSI fails

If authentication of an MES that identifies itself with a TMSI is unsuccessful, the network requests the IMSI from the MES and repeats the authentication using the IMSI. Optionally, if authentication using the TMSI fails, the network may reject the access request or location registration request that triggered the authentication.

6.3.7 Reuse of security-related information in failure situations

Security-related information consisting of sets of RAND, SRES, and Kc is stored in the VLR and in the HLR.

When a VLR has used a set of security-related information to authenticate an MES, it will delete the set of security-related information or mark it as used. When a VLR needs to use security-related information, it will use a set that is not marked as used in preference to a set that is marked as used; if there are no sets that are not marked as used, then the VLR may use a set that is marked as used. It is an operator option to define how many times a set of security-related information may be reused in the VLR; when a set of security-related information has been reused as many times as is permitted by the operator, it will be deleted.

If a VLR successfully obtains security-related information from the HLR, it will discard any security-related information that is marked as used in the VLR.

If a VLR receives a request from another VLR for security-related information, it will send only the sets that are not marked as used.

If an HLR receives a request for security-related information, it will send any sets that are not marked as used; those sets will then be deleted or marked as used. If there are no sets that are not marked as used, the HLR may, as an operator option, send sets that are marked as used. It is an operator option to define how many times a set of security-related information may be resent by the HLR; when a set of security-related information has been sent as many times as is permitted by the operator, it will be deleted.

7 Confidentiality of signalling information and user information on physical connections

7.1 General

As noted in clause 4, some signalling information elements are considered sensitive and shall be protected.

To ensure identity confidentiality, the temporary subscriber identity shall be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it.

Confidentiality of user information on physical connections concerns the information transmitted on a traffic channel on the MES-GS interface (e.g., for speech). It is not an end-to-end confidentiality service.

These needs for a protected mode of transmission are fulfilled with the same mechanism as where the confidentiality function is an Open Systems Interconnection (OSI) layer 1 function. The scheme description that follows assumes that the main part of the signalling information elements is transmitted on DCCH and that the CCCH is only used for the allocation of a DCCH.

This clause does not treat the subject of confidentiality in terminal-to-terminal (TtT) connections. See clause 8 for TtT encryption.

Four points have to be specified:

1) Ciphering.

2) Setting the session key.

3) Initiation and acknowledgement of start of cipher.

4) Synchronization of the cipher streams at both ends of the link.

7.2 Ciphering

Layer 1 data flow (transmitted on DCCH or TCH) is ciphered on a bit-per-bit basis, i.e., the data flow on the satellite path is obtained by the bit-per-bit binary addition of the user data flow and a ciphering bit stream, generated by algorithm A5-GMR-1 using a session key determined as specified in clause 7.3. The session key is denoted below by Kc and is called "Ciphering Key." As its name suggests, the session key is used for the duration of the cipher-ON mode at both ends of the link.

Deciphering is performed by exactly the same method.

Algorithm A5-GMR-1 is specified in annex C.

7.3 Setting the session key

Mutual key setting is the procedure that allows the MES and the network to agree on the key Kc to use in the ciphering and deciphering algorithms A5-GMR-1.

A key setting is triggered by the authentication procedure. Key setting may be initiated by the network as often as the network operator wishes.

Key setting shall occur on a DCCH not yet encrypted and as soon as the identity of the mobile subscriber (i.e., TMSI or IMSI) is known by the network.

The transmission of Kc to the MES is indirect and uses the authentication RAND value; Kc is derived from RAND by using algorithm A8 and the Subscriber Authentication key Ki, as defined in annex C.

As a consequence, the procedures for the management of Kc are the authentication procedures described in clause 6.

Just as with RAND and SRES (clause 6), there is an array of session keys, Kc (1…n_a) that are sent out to GSs as the MES changes its location. The Kc values are computed together with the SRES values. The security-related information known as a "triplet," (see clause 6.3.1) consists of RAND, SRES, and Kc. The ciphering key sequence number, keynr, is simply an accounting variable which enables the GS and the MES to cite a specific triplet in the array. All numbers in the array are stored together in the MES and in the network.

Kc is stored by the MES until it is updated at the next authentication. It is possible to begin a call using the stored session key from a previous call. In this case, it is not necessary to give the "cipher on" command. This feature is not currently supported in the GMR-1.

Session key setting is shown in figure 7.1.

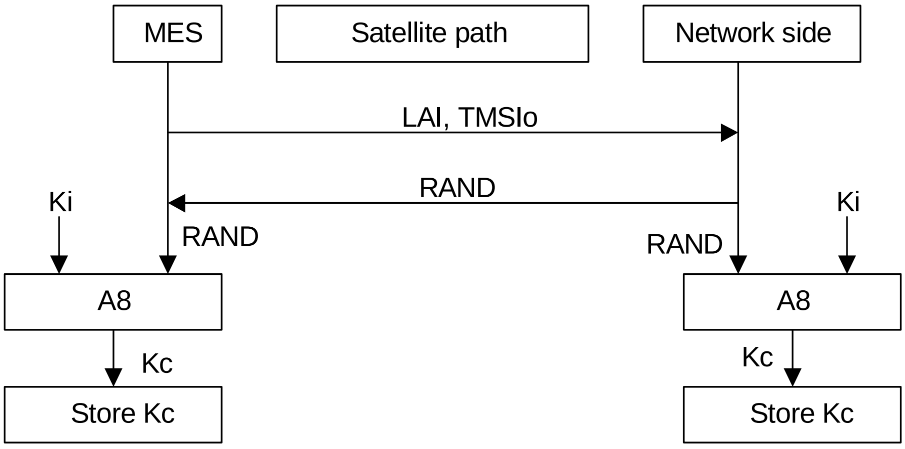


Figure 7.1: Key Setting

7.4 Start of ciphering and deciphering

The MES and the GS shall coordinate the frame number (FN) in which the ciphering and deciphering processes start on DCCH and TCH.

On DCCH, this procedure takes place under the control of the network some time after the completion of the authentication procedure (if any) or after Kc has been made available at the GS.

The transition from clear text mode to ciphered mode proceeds as shown in figure 7.2. Deciphering starts in the GS, which sends in clear text to the MES a specific message, here called "Start cipher." Both the ciphering and deciphering start on the MES side after the message "Start cipher" has been correctly received by the MES. Finally, ciphering on the GS side starts as soon as a frame or a message from the MES has been correctly deciphered at the GS.

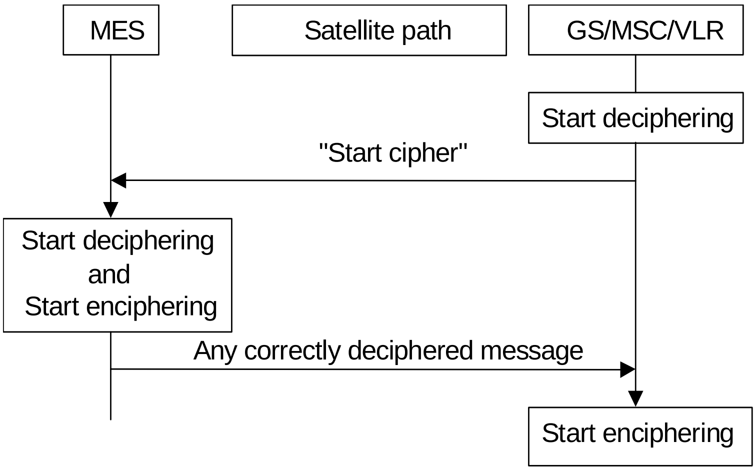


Figure 7.2: Starting of the ciphering and deciphering processes

When a TCH is allocated for user data transmission, the key used is the one set during the preceding DCCH session (Call Set-up). Ciphering and deciphering will start immediately on the first frame of a TCH.

7.5 Frame number tag

GMR-1 will use the FN to ensure that the cipher streams appear statistically independent from one frame to the next and that cipher streams do not repeat within a hyperframe. The combination of session key Kc and FN will create a unique internal initialization variable to the A5-GMR-1 algorithm (annex C) that is guaranteed not to repeat within a hyperframe.

7.6 Negotiation of A5-GMR-1

When an MES wishes to establish a connection with the network, the MES will indicate to the network which versions of the A5-GMR-1 algorithm it supports. The network will not provide service to an MES which indicates that it does not support the minimum ciphering algorithm(s) required by GMR-1.

The network will compare its ciphering capabilities and preferences, and any special requirements, with those indicated by the MES and act according to the following rules:

1) If the MES and the network have no versions of the A5-GMR-1 algorithm in common and the network is not prepared to use an unciphered connection, then the connection will be released.

2) If the MES and the network have at least one version of the A5-GMR-1 algorithm in common, then the network will select one of the mutually acceptable versions of the A5-GMR-1 algorithm for use on that connection.

3) If the MES and the network have no versions of the A5-GMR-1 algorithm in common and the network is willing to use an unciphered connection, then an unciphered connection will be used.

7.7 Implementation of bidirectional ciphering

For implementation purposes, two ciphering streams will be generated on each side of the communication link, one for ciphering and the other for deciphering. As shown in figure 7.3, S1 is the ciphering stream used in the direction from network to MES and S2 is the ciphering stream used in the direction from MES to network.

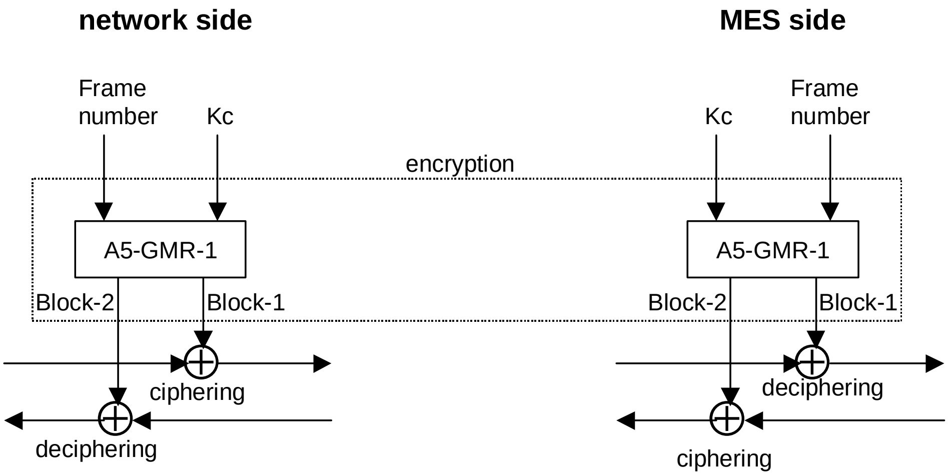


Figure 7.3: Implementation of bidirectional ciphering

Both ciphering and deciphering are performed by applying an "XOR" operation between the coded bits of the information stream and a ciphering sequence generated by the A5-GMR-1 algorithm. The forward link and return link directions use two different ciphering sequences: one sequence is used for ciphering in the mobile and deciphering in the GS, denoted as "S2" in figure 7.3; and another one is used for deciphering in the mobile and ciphering in the GS, denoted as "S1" in figure 7.3.

8 Terminal-to-terminal call privacy

8.1 Ciphering requirement

The GMR-1 network will be able to support a single–hop call in the ciphering mode. In this mode there are two MESs and the network involved at the same time. It is required that both MESs will be able to communicate directly in the ciphered mode in a single satellite hop, that is without having to work in double hop through the network. In the GMR-1 network, the ciphering in a single-hop terminal-to-terminal call is carried out by modifying existing ciphering technique between MES/network and by establishing a ciphering between MESs. The additional requirements to carry out ciphering in a single-hop call in a GMR-1 network are as follows:

1) Both MESs as well as the network will use the common ciphering algorithm and a common ciphering key during a TtT call.

2) In the GMR-1 single-hop call the HLR and MESs are not involved in the generation of the common ciphering key (Ktt).

3) The common ciphering key (Ktt) will be generated by the network (TCS) and will be transferred to both MESs in normal cipher mode between the network and each MES, using separate session Key Kc. After switching to L-to-L link, one of the MES's functions as "network" for purpose of the definition of S1 and S2, as shown in figure 7.3.

4) The network will be able to transfer the following parameters to each MES during the subsequent TtT channel assignment procedure:

   - the common ciphering key Ktt (64 bits);
   - mobile/network designation for the use of S1 and S2 (1 bit);
   - the frame number correction indication (1 bit).

a) In the single-hop call, the ciphering mode of operation begins first with both MESs talking to the GS in normal cipher mode, each with a separate Kc. Then, after the common key (Ktt) is transferred to both MESs, the mode is changed from the ciphered mode with Kc to the ciphered mode with the common key Ktt, but the ciphering algorithm remains unchanged. It remains in this ciphered mode until the end of the call.

b) During a TtT call, a direct L-to-L link is established through the satellite to enable the call to take place. The original L-C links are maintained to enable the GS to monitor both sides of the TtT call.

8.2 Generation of the common key (Ktt) and start of ciphering and deciphering

Each MES and the network perform the security procedures such as authentication, TMSI allocation and ciphering in the same way as in a normal TtG/GtT call. The network (TCS) will generate sets of common ciphering keys (Ktt) to be employed during calls, as described in annex D. The Ktt generation does not involve the HLR and Ats as in a normal TtG/GtT call. During the subsequent TtT channel assignment procedure, the network will deliver the common ciphering key (Ktt), mobile/network designation for the use of S1 and S2 (see GMR-1 03.296 [4]), and the frame number correction indication. The parameters are transferred to each MES in the ciphered mode with the Ats using separate cipher keys.

8.2.1 The use of S1 and S2

The MES instructed to act as a mobile shall use S1 on its receive side. The MES instructed to act as a network shall use S2 on its receive side. After the call gets transferred to an L-to-L link, the GS will continue to monitor both sides of a TtT call by way of the L-C connections of the satellite. Both L-L and L-C links will exist on the satellite simultaneously to permit TtT calls. Since the role of S1 and S2 reverses in the MES designated as "network," the monitoring function of the GS also reverses the role of S1 and S2 for that terminal. There is no ciphering on the TTCH from GSs to MESs.

8.2.2 Frame number correction

Due to the timeslot mapping delay at the satellite L-L switch, the timeslots at which the satellite receives and those at which the satellite transmits may not be in the same frame. The frame number of the receive (RX) timeslots and that of the transmit (TX) timeslots for TtT connection at the satellite may differ, at most, by one. If the RX timeslots are in frame N, the TX timeslots are either in frame N or frame N+1. This frame number slip information is known at the timeslot assignment for a TtT call, and it is sent to both MESs as frame number offset IE (1 bit, whether the current frame number will be decrement or not) in the ASSIGNMENT COMMAND 2 message.

The receiving side of both MESs will implement frame number correction based on the frame number offset IE, starting from the SABM/UA exchange with SAPI 2.

There is no change in frame number slip issue in the L-C links from MES(o) to GS(t1) and from MES(t) to GS(t2).

8.2.3 Change of cipher mode with Kc to cipher mode with Ktt

The change of cipher mode to start the enciphering and deciphering process is schematized in figure 8.1. The cipher mode with key Kc(o) between MES(o) and the network is changed into the cipher mode with key Ktt first. Deciphering with Ktt starts in the GS, which sends in ciphered text with key Kc(o) to the MES(o) a specific message, here called "Start cipher with Ktt." Both the ciphering and deciphering start on the MES(o) side after the message "Start cipher with Ktt" has been correctly received by the MES(o). Ciphering synchronization between MES(o) and the GS is confirmed when a frame or a message from the MES(o) has been correctly deciphered at the GS.

After the cipher mode with key Ktt between MES(o) and the GS has been established successfully, the same procedure used between MES(o) and the GS is performed between MES(t) and the GS. At the same time, an L-to-L link on the satellite is established. When a frame or a message from the MES(t) has been correctly deciphered at the GS, ciphering synchronization between MES(t) and the GS is confirmed.

At this stage, both MESs have already "turned on" the cipher operation with key Ktt, both at the transmitters and the receivers. The MES(t) will initiate the verification of ciphering synchronization with MES(o) by sending a message in cipher mode with key Ktt. If the message is correctly received and deciphered by MES(o), MES(o) will respond to MES(t) by sending a message in cipher mode with key Ktt. Ciphering synchronization with Ktt between MES(o) and MES(t) is confirmed when MES(t) successfully deciphers the response message in cipher mode with Ktt from MES(o).

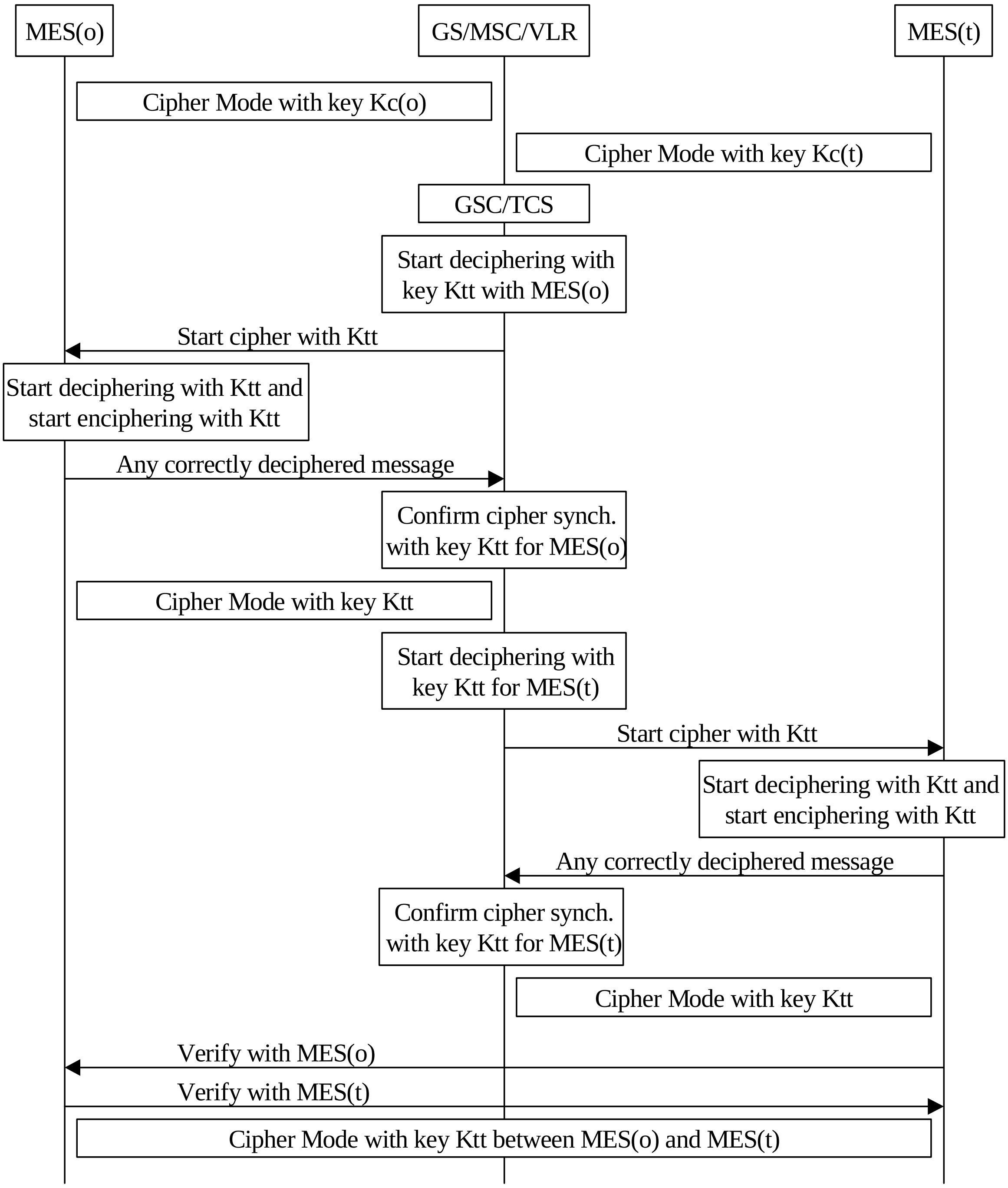
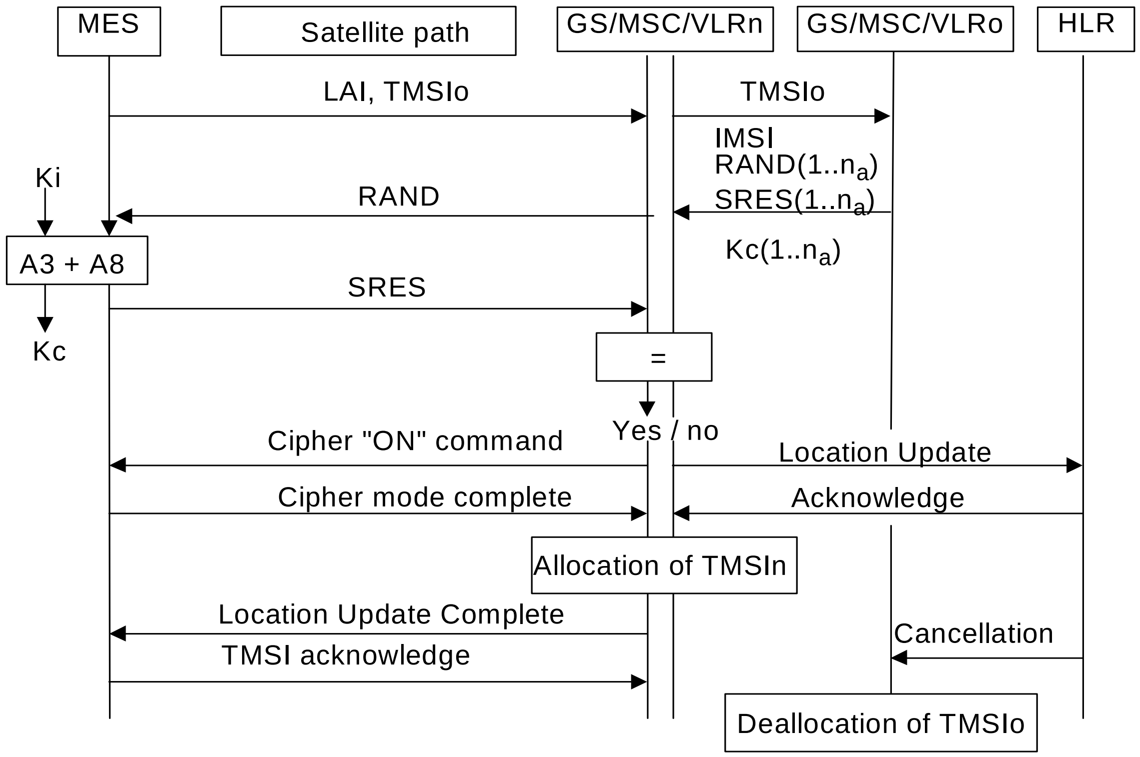

MES(o)
GS/MSC/VLR
MES(t)
Cipher Mode with key Kc(o)
Cipher Mode with key Kc(t)
GSC/TCS
Start deciphering with key Ktt with MES(o)
Start cipher with Ktt
Start deciphering with Ktt and start enciphering with Ktt
Any correctly deciphered message
Confirm cipher synch. with key Ktt for MES(o)
Cipher Mode with key Ktt
Start deciphering with key Ktt for MES(t)
Start cipher with Ktt
Start deciphering with Ktt and start enciphering with Ktt
Any correctly deciphered message
Confirm cipher synch. with key Ktt for MES(t)
Cipher Mode with key Ktt
Verify with MES(o)
Verify with MES(t)
Cipher Mode with key Ktt between MES(o) and MES(t)

Figure 8.1: Starting of the enciphering and deciphering process with key ktt

9 Summary

Figure 9.1 shows in a synopsis a normal location updating procedure with all elements pertaining to security functions, i.e., to TMSI management, authentication, and Kc management.



NOTE: n_a is the size of the array

Figure 9.1: Normal location updating procedure

Annex A (informative): Security issues related to signalling schemes and key management

A.1 Introduction

The diagram in this annex indicates the security items related to signalling functions and to some of the key management functions. The purpose of the diagram is to give a general overview of signalling, both on the satellite path and in the fixed network. The diagram indicates how and where keys are generated, distributed, stored, and used. The security functions are split between VLR and GS/MSC.

A.2 Short description of the scheme

In order to provide an illustrative example of an MES performing a location update in the same VLR, the following will show the steps involved.

Figure A.1 shows the exchange of security information for this scenario. The MES stays within the area controlled by the VLR. The MES is already registered in this VLR. All information belonging to the MES is stored in the VLR, so no connection with the HLR is necessary. Identification is done by the ciphering key sequence number (CKSN), LAI, and TMSI. For authentication, a new set of RAND, SRES, and Kc is already available in the VLR.

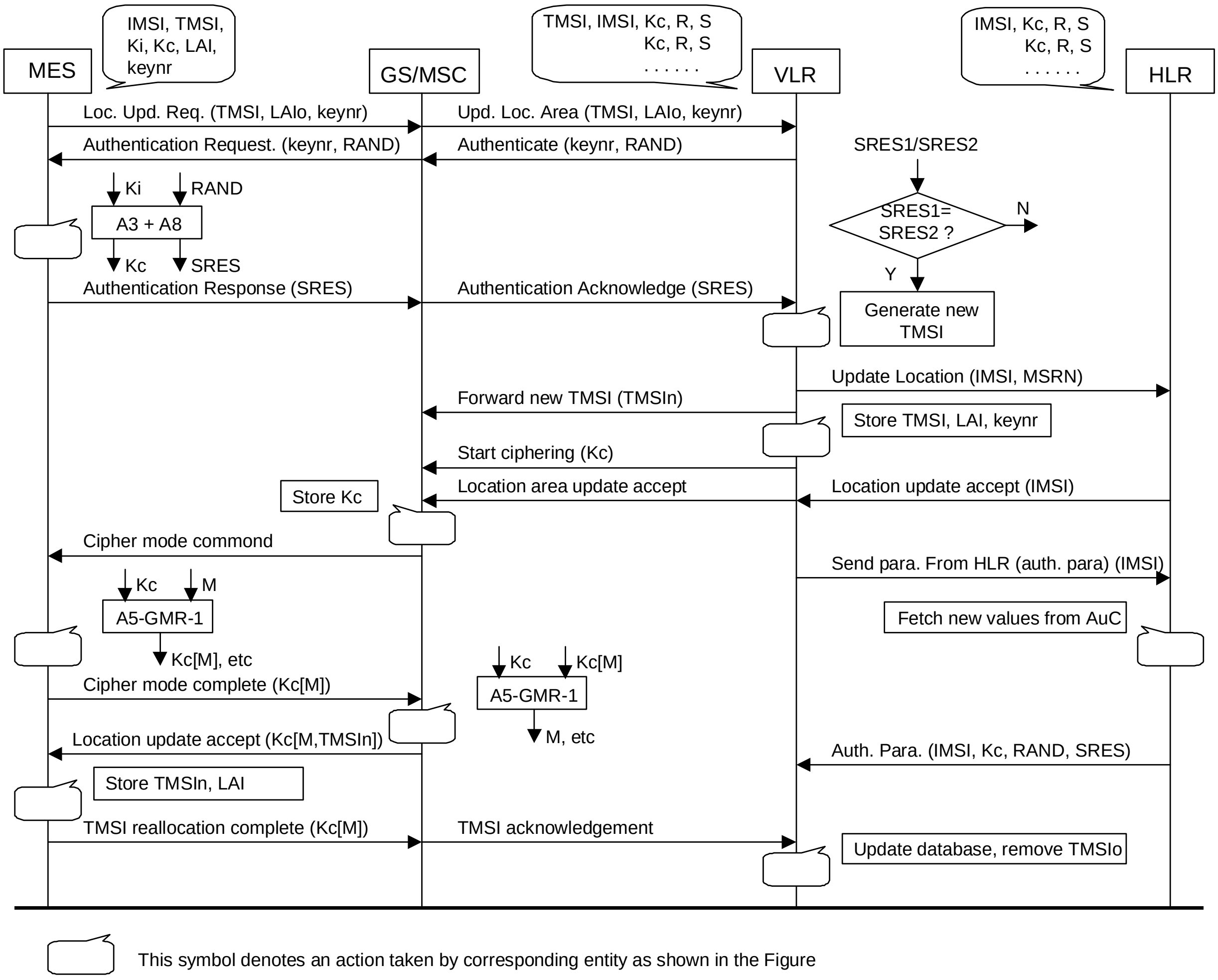

MES
IMSI, TMSI, Ki, Kc, LAI, keynr
GS/MSC
TMSI, IMSI, Kc, R, S Kc, R, S . . . . . .
VLR
IMSI, Kc, R, S Kc, R, S . . . . . .
HLR
Loc. Upd. Req. (TMSI, LAIo, keynr)
Upd. Loc. Area (TMSI, LAIo, keynr)
Authentication Request. (keynr, RAND)
Authenticate (keynr, RAND)
SRES1/SRES2
Ki
RAND
A3 + A8
SRES1= SRES2 ?
N
Y
Kc
SRES
Authentication Response (SRES)
Authentication Acknowledge (SRES)
Generate new TMSI
Update Location (IMSI, MSRN)
Forward new TMSI (TMSIn)
Store TMSI, LAI, keynr
Start ciphering (Kc)
Store Kc
Location area update accept
Location update accept (IMSI)
Cipher mode commond
Send para. From HLR (auth. para) (IMSI)
Kc
M
A5-GMR-1
Fetch new values from AuC
Kc[M], etc
Kc
Kc[M]
Cipher mode complete (Kc[M])
A5-GMR-1
M, etc
Location update accept (Kc[M,TMSIn])
Auth. Para. (IMSI, Kc, RAND, SRES)
Store TMSIn, LAI
TMSI reallocation complete (Kc[M])
TMSI acknowledgement
Update database, remove TMSIo
This symbol denotes an action taken by corresponding entity as shown in the Figure

Figure A.1: Location updating in the same VLR

Annex B (informative): Security information to be stored in the GMR-1 system

B.1 Introduction

This annex gives an overview of the security related information and the places where this information is stored in the GMR-1 network.

The entities of the GMR-1 network where security information is stored are:

- HLR
- VLR
- MSC
- GS
- MES
- AUC

B.2 Entities and security information

B.2.1 Home location register

If required, sets of Kc, RAND, and SRES coupled to each IMSI are stored in the HLR.

B.2.2 Visitor location register

Sets of Kc, RAND, and SRES coupled to each IMSI are stored in the VLR. In addition the CKSN, LAI, and TMSI are stored together with the presumed valid Kc.

After a new TMSI is generated, both the old and the new TMSI are stored. When the old TMSI is no longer valid, it is removed from the database.

B.2.3 Mobile services switching center/gateway station

Encryption algorithm A5-GMR-1 is stored in the MSC/GS.

Call related information stored in the MSC includes the ciphering key Kc and CKSN associated with the identity of the mobile engaged in this call.

After a new TMSI is generated, both the old and the new TMSI are stored. When the old TMSI is no longer valid, it is removed from the database.

B.2.4 Mobile earth station

The MES permanently stores these variables in the SIM:

- Authentication algorithm A3.
- Encryption algorithm A5-GMR-1.
- Ciphering key generating algorithm A8.
- Individual subscriber authentication key Ki.

The MES generates and stores:

- Ciphering key Kc.

The MES receives and stores:

- Ciphering key sequence number.
- TMSI.
- LAI.

The last four variables are stored in the SIM.

B.2.5 Authentication center (AuC)

The AuC are implements:

- Authentication algorithm(s) A3;
- Ciphering key generating algorithm(s) A8.

The secret individual authentication keys Ki of each subscriber are stored in an AuC

Annex C (normative): External specifications of security related algorithms

C.1 Scope

This annex specifies the cryptological algorithms that are needed to provide the various security features and mechanisms.

The following three algorithms are considered in the present document.

• Algorithm A3:	Authentication algorithm.
• Algorithm A5-GMR-1:	Ciphering/deciphering algorithm.
• Algorithm A8:	Ciphering key generator.

Algorithm A5-GMR-1 shall be common to all GMR-1 PLMNs and all MESs (in particular, to allow roaming). The external specifications of A5-GMR-1 are defined in clause C.2.3. The internal specifications of algorithm A5-GMR-1 are managed under the responsibility of GMR-1 Security Custodian (GSC); they will be made available in response to an appropriate request.

Algorithms A3 and A8 are at each PLMN operator discretion. Only the formats of their inputs and outputs shall be specified. It is also desirable that the processing times of these algorithms remain below a maximum value. Proposals for algorithms A3 and A8 are managed by GSC and available in response to an appropriate request for those PLMN operators who wish to use them.

C.2 Specifications for algorithm A5-GMR-1

C.2.1 Purpose

Algorithm A5-GMR-1 is used for both data and signalling information elements at the physical layer on the dedicated channels (TCH or DCCH).

C.2.2 Implementation indications

Algorithm A5-GMR-1 is implemented into both the MES and the GS. The GS side description assumes that one algorithm, A5-GMR-1, is implemented for each physical channel (TCH or DCCH).

The ciphering takes place before modulation and after interleaving the deciphering takes place after demodulation symmetrically. Both ciphering and deciphering need algorithm A5-GMR-1 and start at different times.

As an indication, recall that, due to the TDMA techniques used in the system, the useful data (also called the plain text) are organized into bursts NT3, NT6, and NT9. See table C.1.

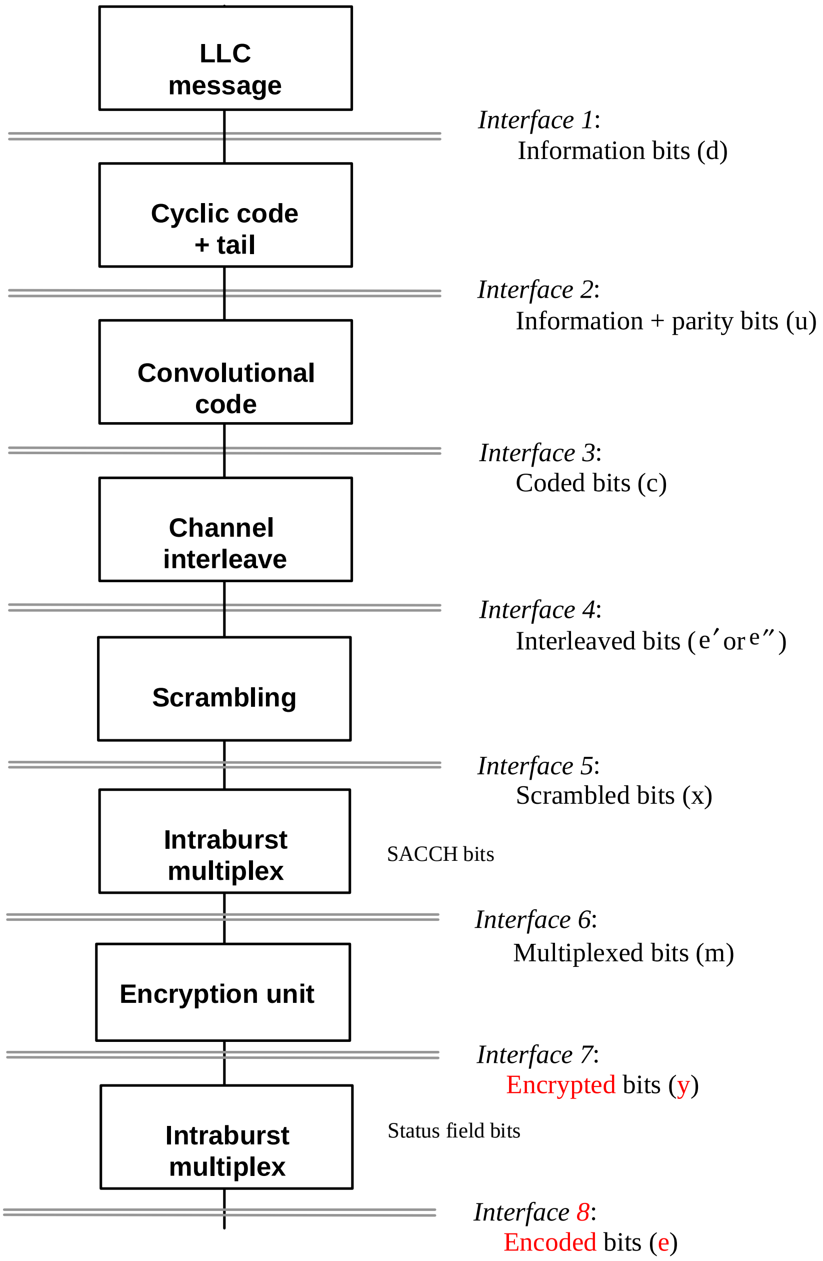


Figure C.1: Channel coding and interleaving organization

Note, that 4 status bits, which are part of a 24-bit status field, are multiplexed with the coded bits and become encrypted. The unique word is never encrypted. (Numbers come from GMR-1 05.002 [6])

Table C.1: Cipher stream block sizes for encrypted bursts in GMR-1

GMR-1 Burst Size	Number of Coded Bits	Number of status bits	Size of Cipher Stream Block Needed To Encrypt Traffic Burst
TCH3	208	4	208
TCH6/FACCH6	430	4	430
SDCCH	208	0	208
TCH9/FACCH9	658	4	658
NT3 for FACCH	96	8	96

For ciphering TCH3 bursts, for example, algorithm A5-GMR-1 produces a sequence of 208 encipher/decipher bits (here called Block) in each frame, which are combined by a bit-wise modulo 2 addition with the 208-bit plain text block. The first encipher/decipher bit produced by A5-GMR-1 is added to the intraburst multiplexer output as shown in figure C.1.

For each slot deciphering is performed on the MES side with the first block (Block-1) of 208 bits produced by A5-GMR-1, and ciphering is performed with the second block (Block-2). As a consequence, on the network side, Block-1 is used for ciphering and Block-2 for deciphering. Therefore algorithm A5-GMR-1 shall produce two blocks of 208 bits (i.e., Block-1 and Block-2).

One of the inputs to the A5-GMR-1 is the 19-bit frame number. Use of the frame number ensures no repetition of a cipher block within a hyperframe, which lasts 3 hours and 28 minutes in GMR-1. For details on frame numbering synchronization, see GMR-1 05.010 [7] "Radio Subsystem Synchronization".

Figure C.2 summarizes the implementation described above, with only one ciphering/ deciphering procedure represented (the second one for deciphering/ciphering is symmetrical).

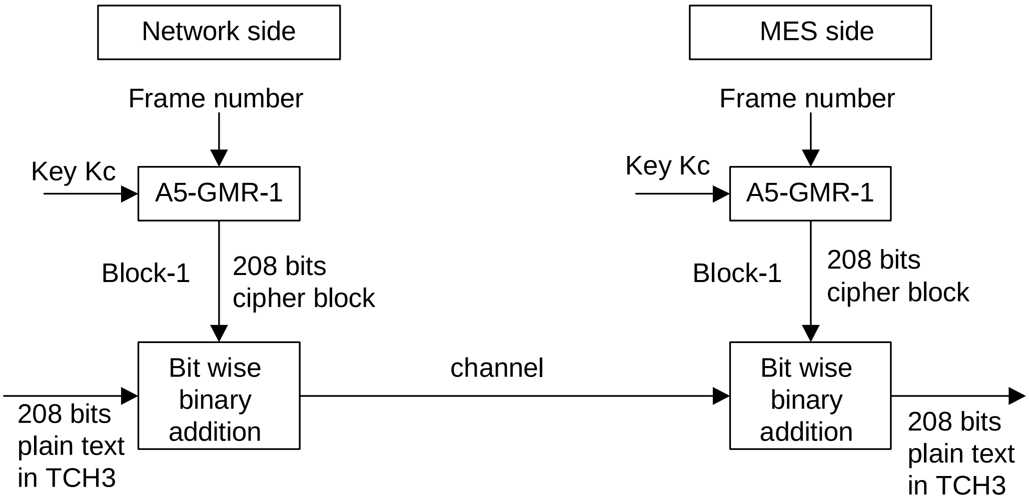


Figure C.2: Deciphering on the MES side

C.2.3 External specifications of algorithm A5-GMR-1

The two input parameters (COUNT and Kc) and the output parameters (BLOCK1 and BLOCK2) of algorithm A5-GMR-1 will use the following formats:

Length of Kc:	64 bits
Length of FN:	19 bits
Length of BLOCK1:	See table C.1
Length of BLOCK2:	See table C.1
Length of Ktt:	64 bits

Algorithm A5-GMR-1 will produce BLOCK1 and BLOCK2 in less than a TDMA frame duration.

NOTE: If the actual length of the ciphering key is less than 64 bits, then it is assumed that the actual ciphering key corresponds to the most significant bits of Kc and that the remaining and less significant bits are set to zero. For signalling and testing purposes, the ciphering key Kc is considered to be 64 unstructured bits.

C.2.4 Internal specification of algorithm A5-GMR-1

The internal specification of algorithm A5-GMR-1 is managed under the responsibility of the GSC; it will be made available in response to an appropriate request.

C.3 Algorithm A3

Algorithm A3 is considered as a matter for GMR-1 PLMN operators. Therefore, only external specifications are given. However a proposal for a possible algorithm A3 is managed by the GSC and available upon appropriate request.

C.3.1 Purpose

As defined here, the purpose of algorithm A3 is to allow authentication of a mobile subscriber's identity.

To this end, algorithm A3 shall compute an expected response SRES from a random challenge RAND sent by the network. For this computation, algorithm A3 makes use of the secret authentication key Ki.

C.3.2 Implementation and operational requirements

On the MES side, algorithm A3 is contained in a SIM.

On the network side, it is implemented in the HLR or the AuC. The two input parameters (RAND and Ki) and the output parameter (SRES) of algorithm A3 will use the following formats:

- Length of Ki: 128 bits
- Length of RAND: 128 bits
- Length of SRES: 32 bits
- Length of Ktt: 64 bits

The runtime of algorithm A3 will be less than 200 msec.

C.4 Algorithm A8

Algorithm A8 is considered as a matter for GMR-1 PLMN operators as is algorithm A3.

A proposal for a possible algorithm A8 is available upon appropriate request.

C.4.1 Purpose

Algorithm A8 shall compute the ciphering key Kc from the random challenge RAND sent during the authentication procedure, using the authentication key Ki.

C.4.2 Implementation and operational requirements

On the MES side, algorithm A8 is contained in the SIM, as specified in GSM 02.17 [9].

On the network side, algorithm A8 is colocated with algorithm A3.

The two input parameters (RAND and Ki) and the output parameter (Kc) of algorithm A8 will follow the following formats:

- Length of Ki: 128 bits
- Length of RAND: 128 bits
- Length of Kc: 64 bits
- Length of Ktt: 64 bits

Because the maximum length of the actual ciphering key is fixed by the GSC algorithm A8 will produce this actual ciphering key and extend it (if necessary) into a 64-bit word where the non-significant bits are forced to zero. It is assumed that any non-significant bits are the lsbs and that the actual ciphering key is contained in the msbs. For signalling and testing purposes, the ciphering key Kc will be 64 unstructured bits.

Annex D (informative): Generation of session keys for direct terminal-to-terminal calls

The GS setting up the TtT call will generate a 64 bit session key, Ktt, using a random number generator. It will keep and number up to 10 session keys at a time for use by MESs wishing to make TtT calls. Session keys for TtT calls will be transferred in encrypted mode only. Storage of session keys Ktt for archival purposes will be possible following guidelines for storage of Kc.

History

Document history		
V1.1.1	March 2001	Publication