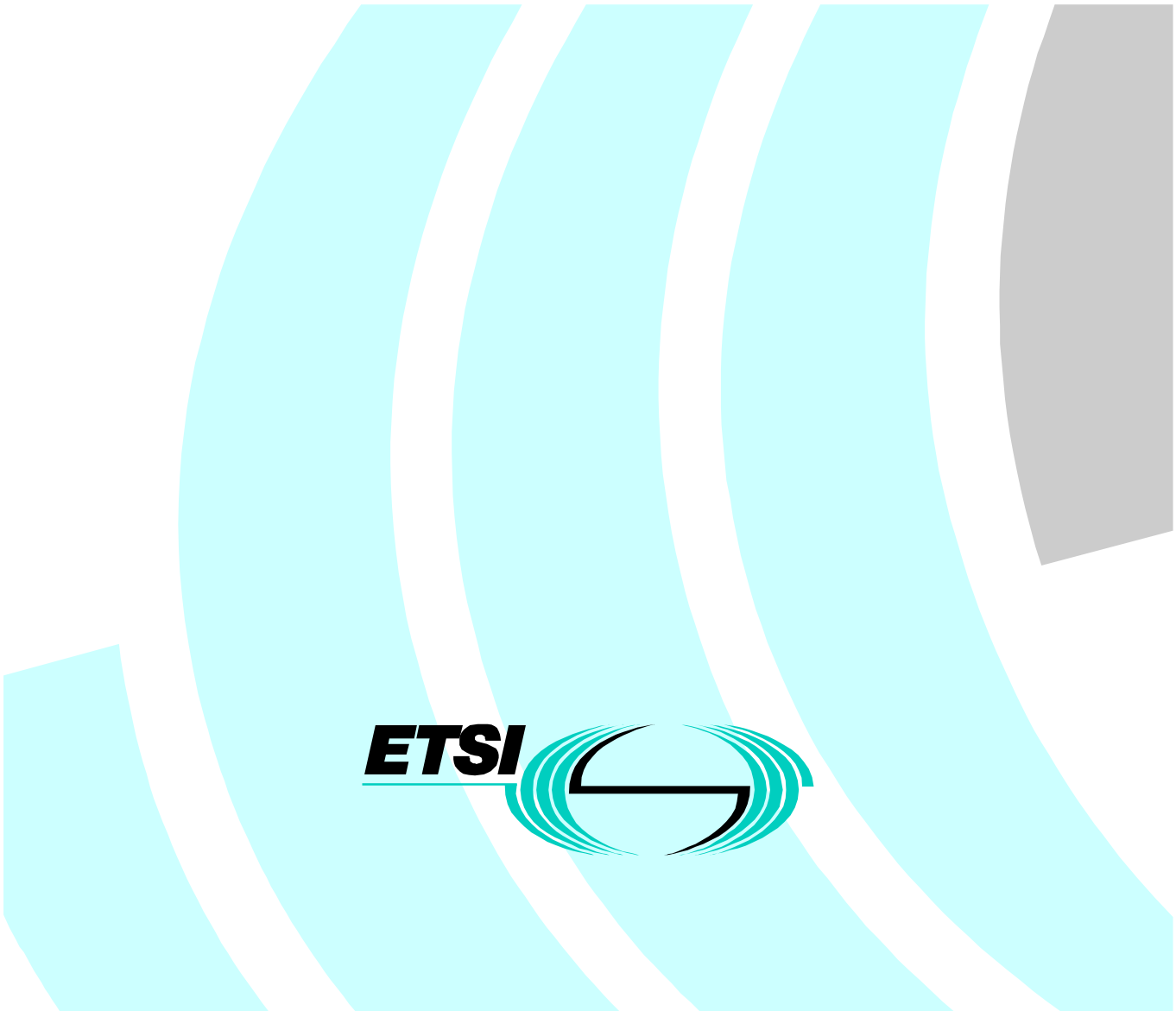
ETSI TS 101 377-3-10 V1.1.1 (2001-03)

Technical Specification

GEO-Mobile Radio Interface Specifications;
Part 3: Network specifications;
Sub-part 10: Security Related Network Functions;
GMR-2 03.020



Reference
DTS/SES-002-03020

Keywords
GMR, GSM, GSO, interface, 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

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 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,715,365	US
TS 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,754,974	US
TS 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,226,084	US
TS 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,701,390	US
TS 101 377 V1.1.1	Digital Voice Systems Inc		US	US 5,826,222	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 101 377 V1.1.1	Ericsson Mobile Communication	Improvements in, or in relation to, equalisers	GB	GB 2 215 567	GB
TS 101 377 V1.1.1	Ericsson Mobile Communication	Power Booster	GB	GB 2 251 768	GB
TS 101 377 V1.1.1	Ericsson Mobile Communication	Receiver Gain	GB	GB 2 233 846	GB
TS 101 377 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 864821

Project	Company	Title	Country of Origin	Patent n°	Countries Applicable
TS 101 377 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 101 377 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 101 377 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 101 377 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 101 377 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System	US	US 5,974,314	US
TS 101 377 V1.1.1	Lockheed Martin Global Telecommunic. Inc	Spacecraft Cellular Communication System	US	US 5,974,315	US
TS 101 377 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 101 377 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 10 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-2 03.001";

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

Sub-part 3: "Numbering, Addressing and Identification; GMR-2 03.003";

Sub-part 4: "Restoration Procedures; GMR-2 03.007";

Sub-part 5: "Organization of Subscriber Data; GMR-2 03.008";

Sub-part 6: "Handover Procedures; GMR-2 03.009";

Sub-part 7: "Technical Realization of Short Message Service (SMES) Point-to-Point; GMR-2 03.040";

Sub-part 8: "Location Registration Procedures; GMR-2 03.012";

Sub-part 9: "Discontinuous Reception (DRX) in the GMR-2 System; GMR-2 03.013";

Sub-part 10: "Security Related Network Functions; GMR-2 03.020";

Sub-part 11: "Functions Related to Mobile Earth Station (MES) in idle Mode; GMR-2 03.022";

Sub-part 12: "Technical Realization of Facsimile Group 3 Transparent; GMR-2 03.045";

Sub-part 13: "Transmission Planning Aspects of the Speech Service in the Public Satellite Mobile Network (PSMN) system; GMR-2 03.050";

Sub-part 14: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services - Stage 2; GMR-2 03.083";

Sub-part 15: "Multiparty Supplementary Services; GMR-2 03.084";

Sub-part 16: "Technical Realization of Operator Determined Barring; GMR-2 03.015";

Sub-part 17: "Call Barring (CB) Supplementary Services - Stage 2; GMR-2 03.088";

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-n 01.201.

1 Scope

The present document specifies the network functions needed to provide the security related service and functions specified in GMR-2 02.009 [2]. 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 refer 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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, subsequent revisions do apply.

[1] GMR-2 01.004 (ETSI TS 101 377-1-1): "GEO-Mobile Radio Interface Specifications; Part 1: General specifications; Sub-part 1: Abbreviations and Acronyms".

[2] GMR-2 02.009 (ETSI TS 101 377-2-3): "GEO-Mobile Radio Interface Specifications; Part 2: Service specifications; Sub-part 3: Security Aspects".

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

[4] GMR-2 04.008 (ETSI TS 101 377-4-7): "GEO-Mobile Radio Interface Specifications; Part 4: Radio interface protocol specifications; Sub-part 7: Mobile radio interface Layer 3 Specifications".

[5] GMR-2 05.001(ETSI TS 101 377-5-1): "GEO-Mobile Radio Interface Specifications; Part 5: Radio interface physical layer specifications; Sub-part 1: General description".

[6] GMR-2 05.002 (ETSI TS 101 377-5-2): "GEO-Mobile Radio Interface Specifications; Part 5: Radio interface physical layer specifications; Sub-part 2: Multiplexing and Multiple Access on the Radio Path".

[7] GMR-2 05.003 (ETSI TS 101 377-5-3): "GEO-Mobile Radio Interface Specifications; Part 5: Radio interface physical layer specifications; Sub-part 3: Channel Coding".

[8] GSM 09.02 (ETSI ETS 300 599): "European digital cellular telecommunications system (Phase 2); Mobile Application Part (MAP) specification" (V4.18.0).

3 Definitions and abbreviations

3.1 Definitions

The different security related services and functions are defined in GSM 02.09 [2].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in GMR-2 01.004 [1] and the following apply:

A3	authentication algorithm
GMR-2-A5	GMR-2 signalling data and user data encryption algorithm
A8	ciphering key generating algorithm
GSAC	GMR-2 Security Algorithm Custodian
GW	Gateway
HGW	Home Gateway
HLR	Home Location Register
IMSI	International Mobile Subscriber Identity
Kc	ciphering key
Kc[M]	message encrypted with ciphering key Kc
Ki	individual subscriber authentication key
LAI	Location Area Identity
MSC	Mobile services Switching Centre
R	Random number (RAND)
S	Signed response (SRES)
MES	Mobile Earth Station
VLR o/n	Visitor Location Register old/new

4 General

The different security related services and functions that are listed in GSM 02.09 [2] are grouped as follows:

- subscriber identity confidentiality;
- subscriber identity authentication;
- signalling information element and connectionless user data confidentiality and data confidentiality for physical connections (ciphering).

It shall be possible to introduce new authentication and ciphering algorithms during the systems lifetime. The network may support more than one authentication and ciphering algorithm.

The security procedures include mechanisms to enable recovery in event of signalling failures. These recovery procedures are designed to minimize the risk of a breach in the security of the system.

General on figures in the present document:

- signalling exchanges are referred to by functional names. The exact messages and message types are specified in GMR-2 04.008 [4] and GSM 09.02 [8];
- no assumptions are made for function splitting between MSC (Mobile Switching Centre), VLR (Visitor Location Register) and GW (Gateway). Signalling is described directly between MES and the local network (i.e. GW and VLR denoted in the figures by GW/VLR). The splitting in annex A is given only for illustrative purposes;
- addressing fields are not given; all information relates to the signalling layer;
- the term HGW is used as a general term which should be understood as HLR (Home Location Register) or AuC (Authentication Centre);
- what is put in a box is not part of the described procedure but it is relevant to the understanding of the figure.

5 Subscriber identity confidentiality

TMSI is not supported in the present version of the GMR-2 standard.

6 Subscriber identity authentication

6.1 Generality

The definition and operational requirements of subscriber identity authentication are given in GMR-2 02.009 [2]. The authentication procedure will be used to set the ciphering key (see clause 7). Therefore, it is performed after the subscriber identity (IMSI) is known by the network and before the channel is encrypted.

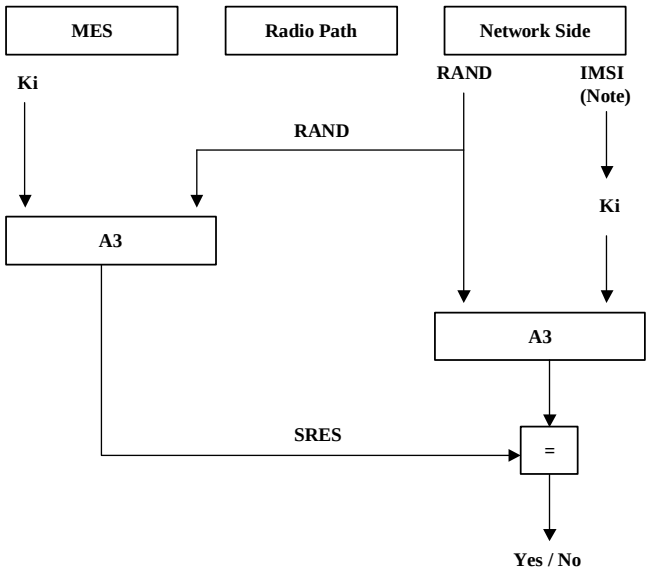
Two network functions are necessary: the authentication procedure itself, and the key management inside the network.

6.2 The authentication procedure

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

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

The general procedure is schematized in figure 6.2-1.



NOTE: IMSI is used to retrieve Ki in the network.

Figure 6.2-1: 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.

Ki is stored on the network side in the Home Gateway (HGW), in an Authentication Centre (AuC). An AuC can be physically integrated with other functions, e.g. in a Home Location Register (HLR).

6.3.1 General authentication procedure

When needed for each MES, the GW/VLR requests security related information from the HLR/AuC corresponding to the MES. This includes an array of pairs of corresponding RAND and SRES. These pairs are obtained by applying Algorithm A3 to each RAND and the key Ki as shown in figure 6.2-1. The pairs are stored in the VLR as part of the security related information.

The procedure used for updating the vectors RAND/SRES is schematized in figure 6.3.1-1.

NOTE: The Authentication Vector Response contains also Kc(1..n) which is not shown in this and the following figures. For discussion of Kc see clause 7.

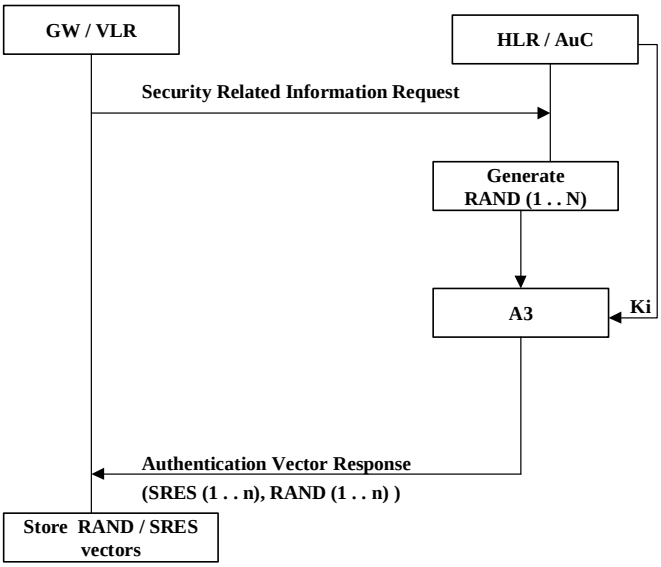


Figure 6.3.1-1: Procedure for updating the vectors RAND/SRES

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 schematized in figure 6.3.1-2.

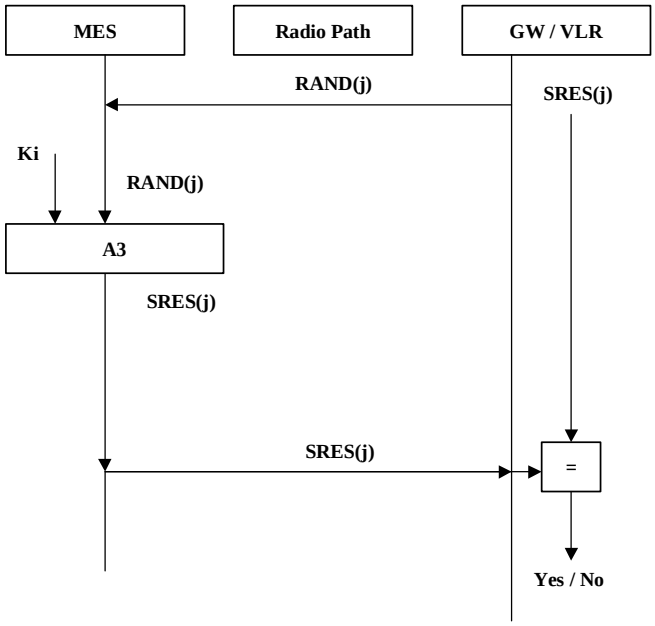


Figure 6.3.1-2: General authentication procedure

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

TMSI is not supported in the present version of the GMR-2 standard.

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

During location updating in a new VLR, pairs of RAND/SRES contained in the security related information are requested directly from the HGW.

The procedure is schematized in figure 6.3.3-1.

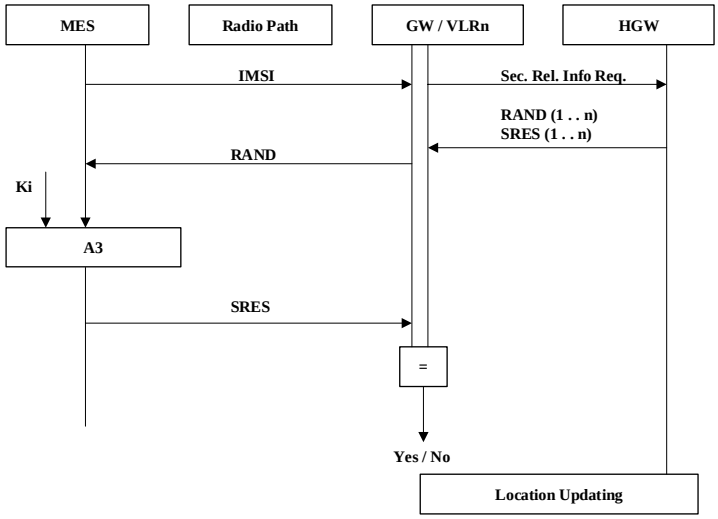


Figure 6.3.3-1: Authentication at location updating in a new VLR

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

TMSI is not supported in the present version of the GMR-2 standard.

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

TMSI is not supported in the present version of the GMR-2 standard.

6.3.6 Authentication with IMSI if authentication with TMSI fails

TMSI is not supported in the present version of the GMR-2 standard.

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

If a VLR successfully requests security related information from the HLR, it shall discard any security related information which is marked as used in the VLR.

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

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

7 Confidentiality of signalling information elements, connectionless data and user information elements on physical connections

7.1 Generality

In GMR-2 02.009 [2], some signalling information elements are considered sensitive and must be protected. The confidentiality of connectionless user data requires at least the protection of the message part pertaining to OSI layers 4 and above.

The user information confidentiality of user information on physical connections concerns the information transmitted on a traffic channel on the MES - GW 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 where the confidentiality function is an OSI layer 1 function. The scheme described below assumes that the main part of the signalling information elements is transmitted on S-SDCCH (Satellite Stand-alone Dedicated Control Channel), and that the Common Control Channels are only used for the allocation of an S-SDCCH.

Four points have to be specified:

- the ciphering method;
- the key setting;
- the starting of the enciphering and deciphering processes;
- the synchronization.

7.2 The ciphering method

The layer 1 data flow (transmitted on S-SDCCH or S-TCH) is ciphered by a bit per bit or stream cipher, i.e. the data flow on the radio path is obtained by the bit per bit binary addition of the user data flow and a ciphering bit stream, generated by algorithm GMR-2-A5 using a key determined as specified in clause 7.3. The key is denoted below by Kc, and is called "Ciphering Key". Deciphering is performed by exactly the same method.

The external specification for the GMR-2-A5 Algorithm is provided in annex C.

7.3 Key settings

Mutual key setting is the procedure that allows the mobile station and the network to agree on the key Kc to use in the ciphering and deciphering algorithms GMR-2-A5.

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 must occur on a S-SDCCH not yet encrypted and as soon as the identity of the mobile subscriber (i.e. 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 6.3.

The values Kc are computed together with the SRES values. The security related information (see clause 6.3.1) consists of RAND, SRES and Kc.

The key Kc is stored by the mobile station until it is updated at the next authentication.

Key setting is schematized in figure 7.3-1

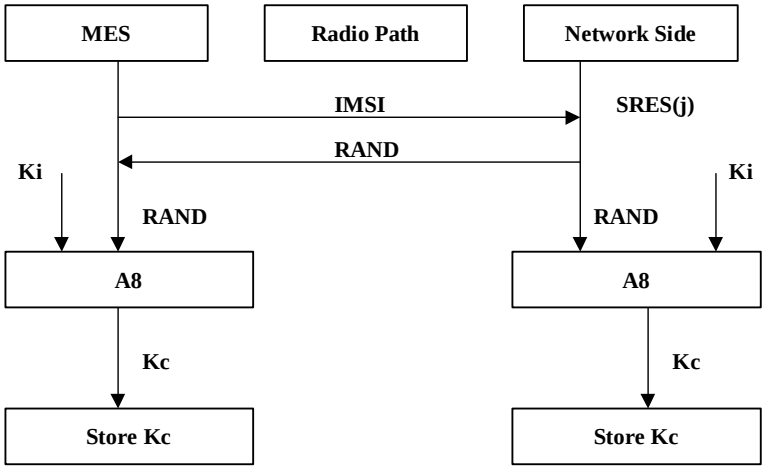


Figure 7.3-1: Key setting

7.4 Ciphering key sequence number

The ciphering key sequence number is a number which is associated with the ciphering key Kc and they are stored together in the mobile station and in the network.

However since it is not directly involved in any security mechanism, it is not addressed in the present document but in GMR-2 04.008 [4] instead.

7.5 Starting of the ciphering and deciphering process

The MES and the GW must co-ordinate the instants at which the enciphering and deciphering processes start on S-SDCCH and S-TCH.

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

No information elements for which protection is needed must be sent before the ciphering and deciphering processes are operating.

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

The starting of enciphering and deciphering processes is schematized in figure 7.5-1.

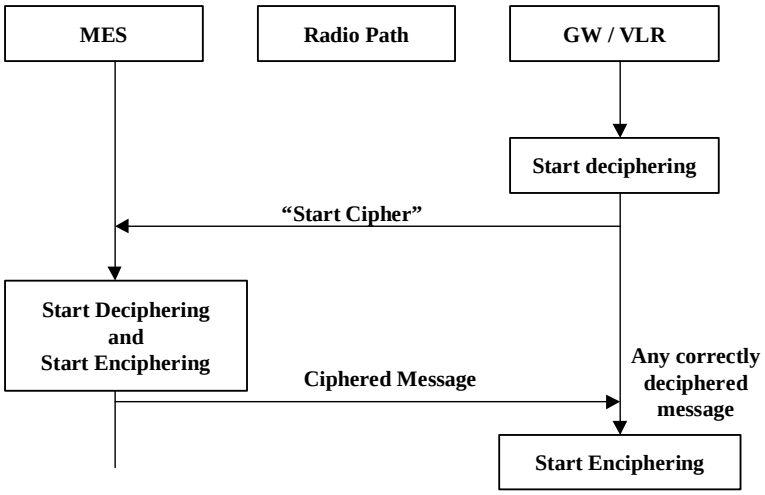


Figure 7.5-1: Starting of the enciphering and deciphering processes

When a S-TCH is allocated for user data transmission, the key used is the one set during the preceding S-SDCCH session (Call Set-up). The enciphering and deciphering processes start immediately.

7.6 Synchronization

The enciphering stream at one end and the deciphering stream at the other end must be synchronized, for the enciphering bit stream and the deciphering bit streams to coincide. The underlying Synchronization scheme is described in annex C.

7.7 Handover

Inter-beam, inter-GWS and inter-MSC handovers are not required in GMR-2. However, intra-beam handovers are supported. When an in-call handover due to poor channel quality occurs, the message cipher/decipher capability shall be maintained and the key, Kc, remains unchanged.

7.8 Negotiation of the GMR-2-A5 algorithm

Not more than seven versions of the GMR-2-A5 Algorithm will be defined.

When an MES wishes to establish a connection with the network, the MES shall indicate to the network which of the seven versions of the GMR-2-A5 Algorithm it supports.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the ME, 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 GMR-2-A5 Algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released;

2) if the MES and the network have at least one version of the GMR-2-A5 Algorithm in common, then the network shall select one of the mutually acceptable versions of the GMR-2-A5 Algorithm for use on that connection;

3) if the MES and the network have no versions of the GMR-2-A5 Algorithm in common and the network is willing to use an unciphered connection, then an unciphered connection shall be used.

7.9 Ciphering of single-hop mobile-to-mobile connections

Encryption over a single hop mobile-to-mobile link is not supported.

8 Synthetic summary

Figure 8-1 shows in a synopsis a normal location updating procedure with all elements pertaining to security functions, i.e., authentication and Kc management.

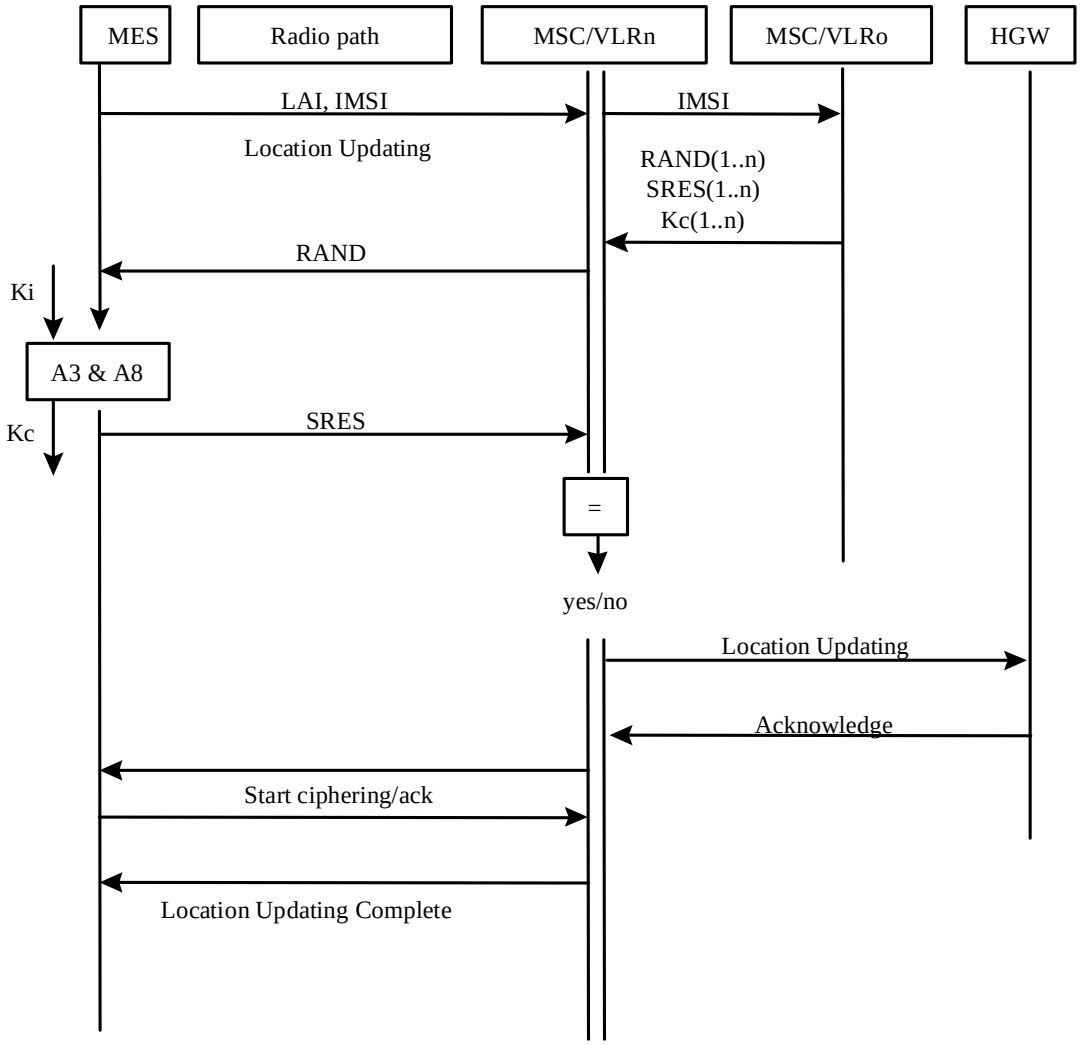


Figure 8-1: Normal location updating procedure

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

A.1 Introduction

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

A.2 Short description of the schemes

Scheme 1: Location registration:

- Using IMSI Identification.

The situation occurs where an MES requests registration. The IMSI is sent in clear text via the radio path as part of the location updating.

Scheme 2: Location updating:

- MES registered in VLR.

The mobile station stays within the area controlled by the VLR. The mobile station is already registered in this VLR. All information belonging to the mobile station is stored in the VLR, so no connection with the HLR is necessary. Identification is done by the CKSN, LAI and IMSI. For authentication a new set of RAND, SRES and Kc is already available in the VLR.

Scheme 3a: Location updating:

- MES not yet registered in VLR and MES transitioning from GSM PLMN to GMR-2.

The VLR requests authentication information from the MES HLR.

Scheme 3b: Location updating:

- MES not yet registered in VLR and MES transitioning from GMR-2 to GSM PLMN.

The VLR requests authentication information from the MES HLR.

Scheme 4: Call set-up:

- mobile originated;
- to Home Gateway.

The user of the registered MES wants to set-up a call. Identification is done by using the IMSI. All signalling information elements in all messages on the radio path are encrypted with ciphering key Kc.

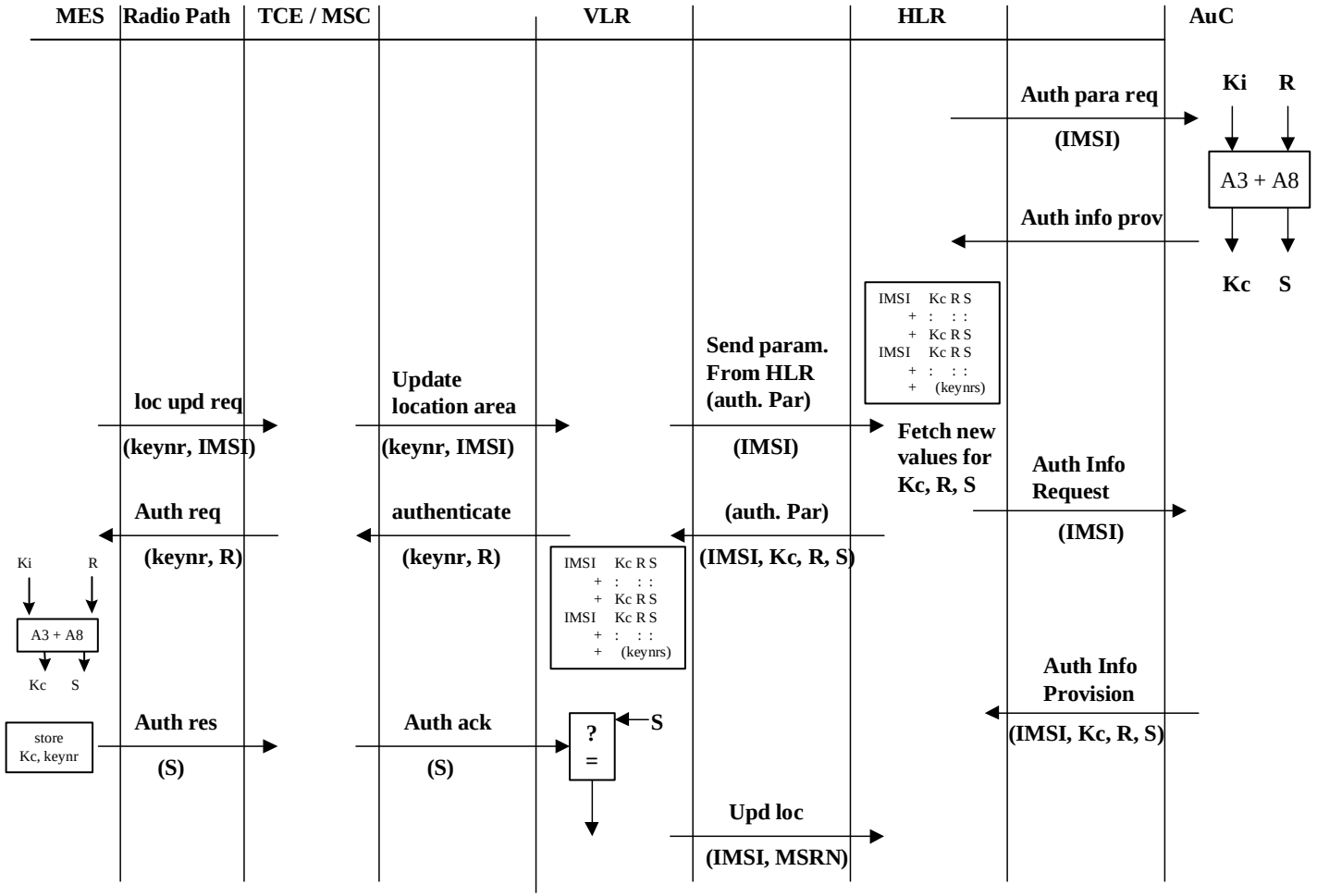
Scheme 5: Call set-up:

- mobile terminated;
- early assignment.

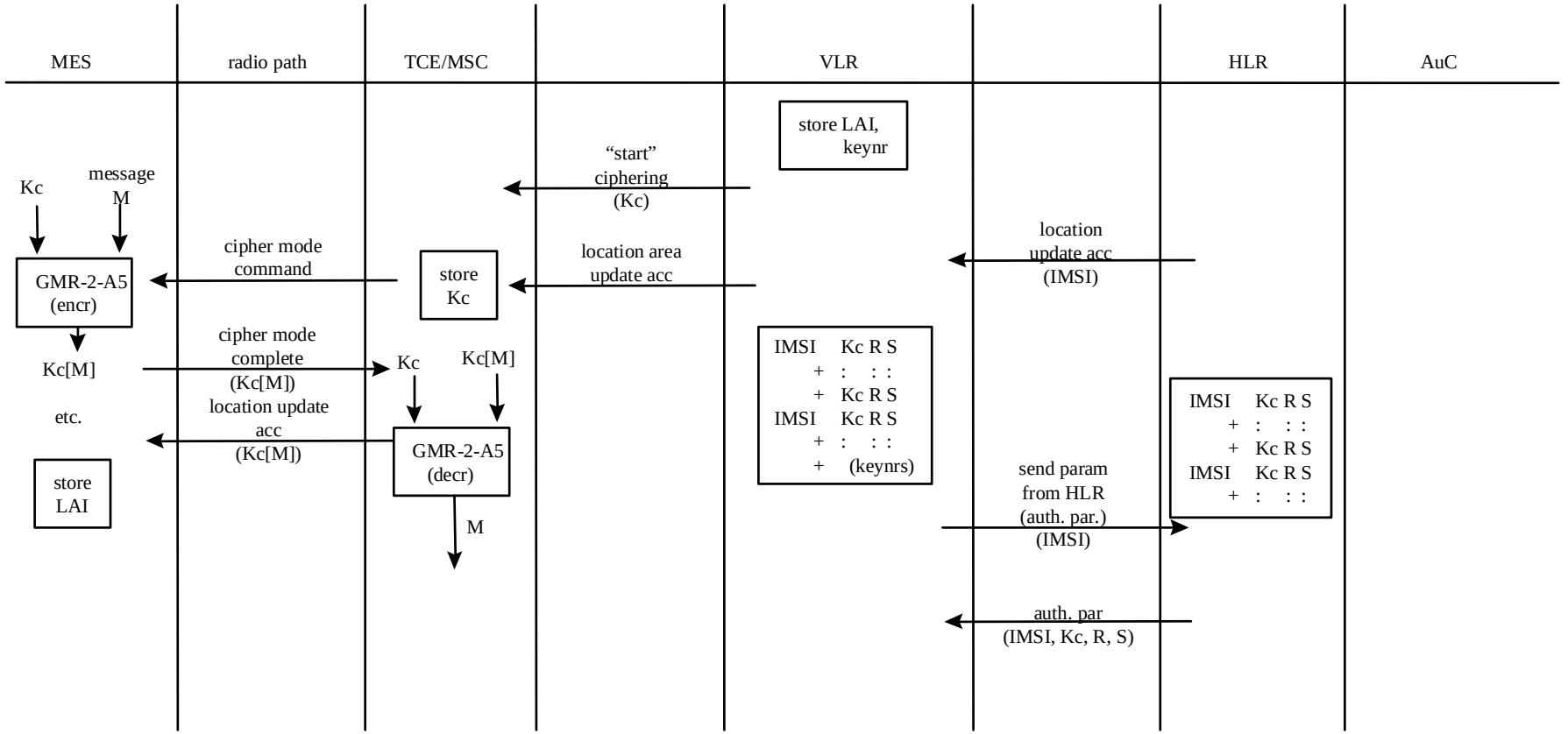
A paging request is sent to the registered MES, addressed by the IMSI. All signalling information elements in all messages on the radio path are encrypted with ciphering key Kc after the cipher mode command message. The GW is setting up calls with "early assignment".

Scheme 6: Longhaul Call set-up:

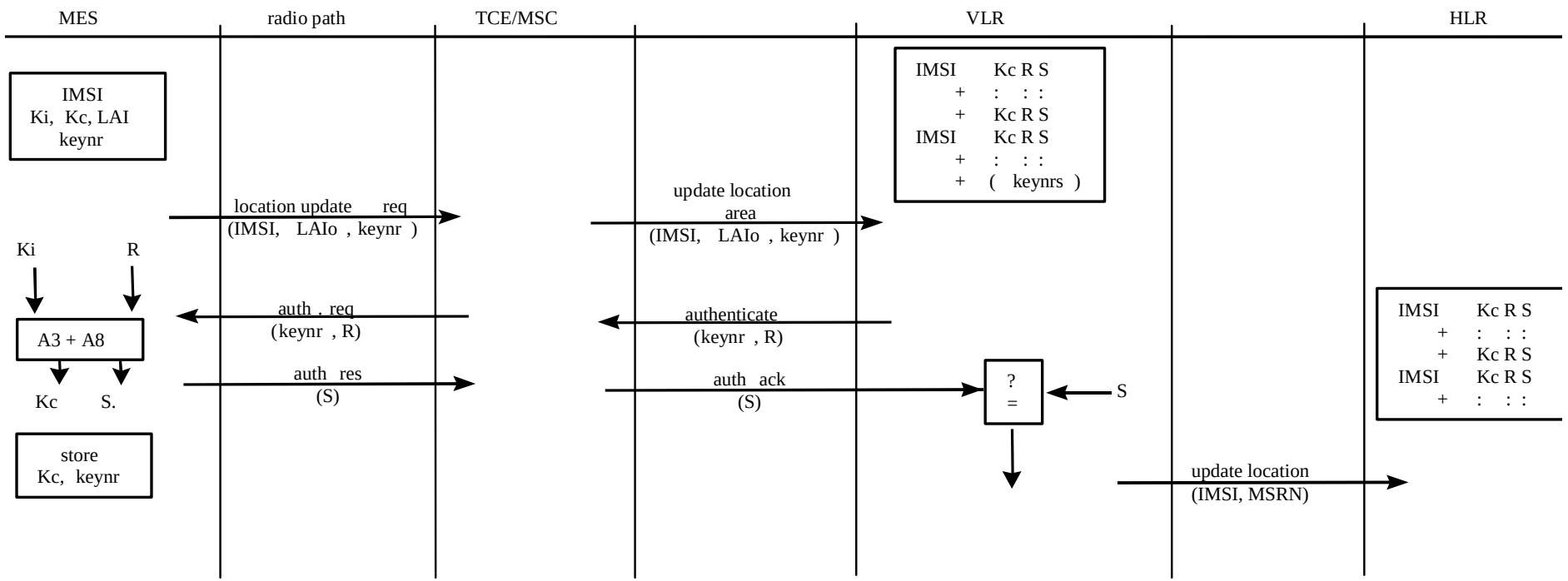
- mobile originated;
- early assignment.



Scheme 1: Location registration

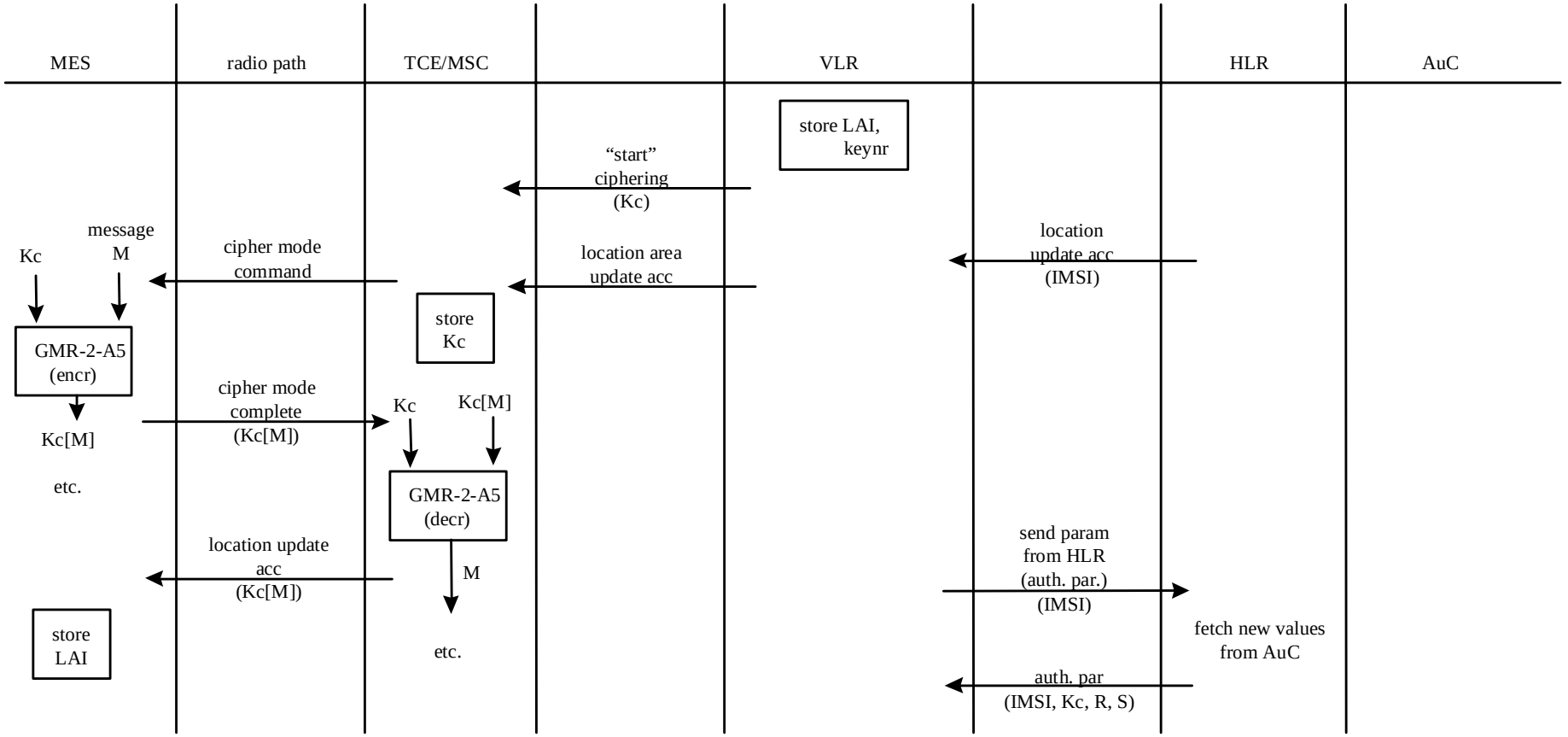


Scheme 1 (concluded)

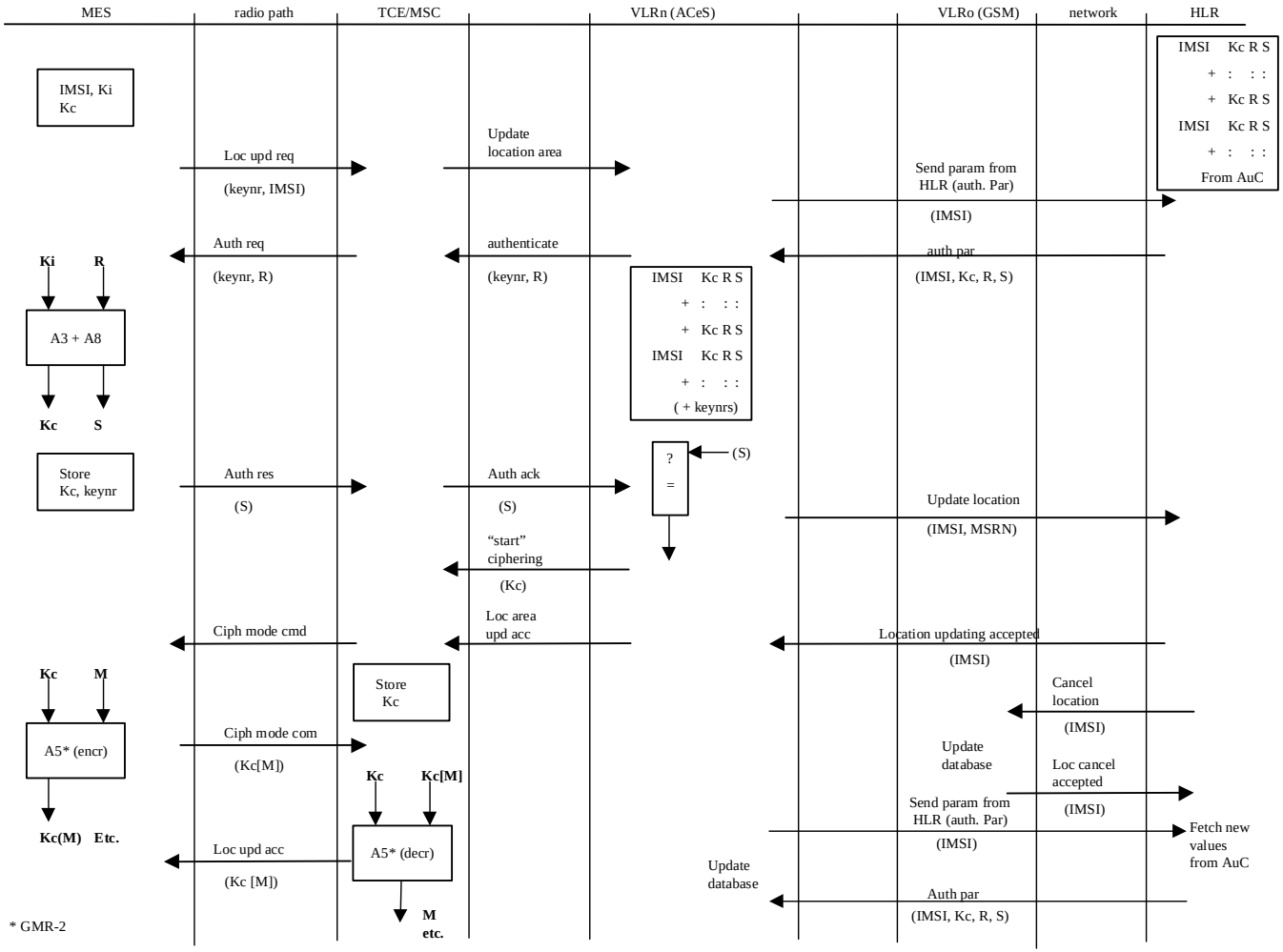


Scheme 2: Location updating

- MES registered in VLR

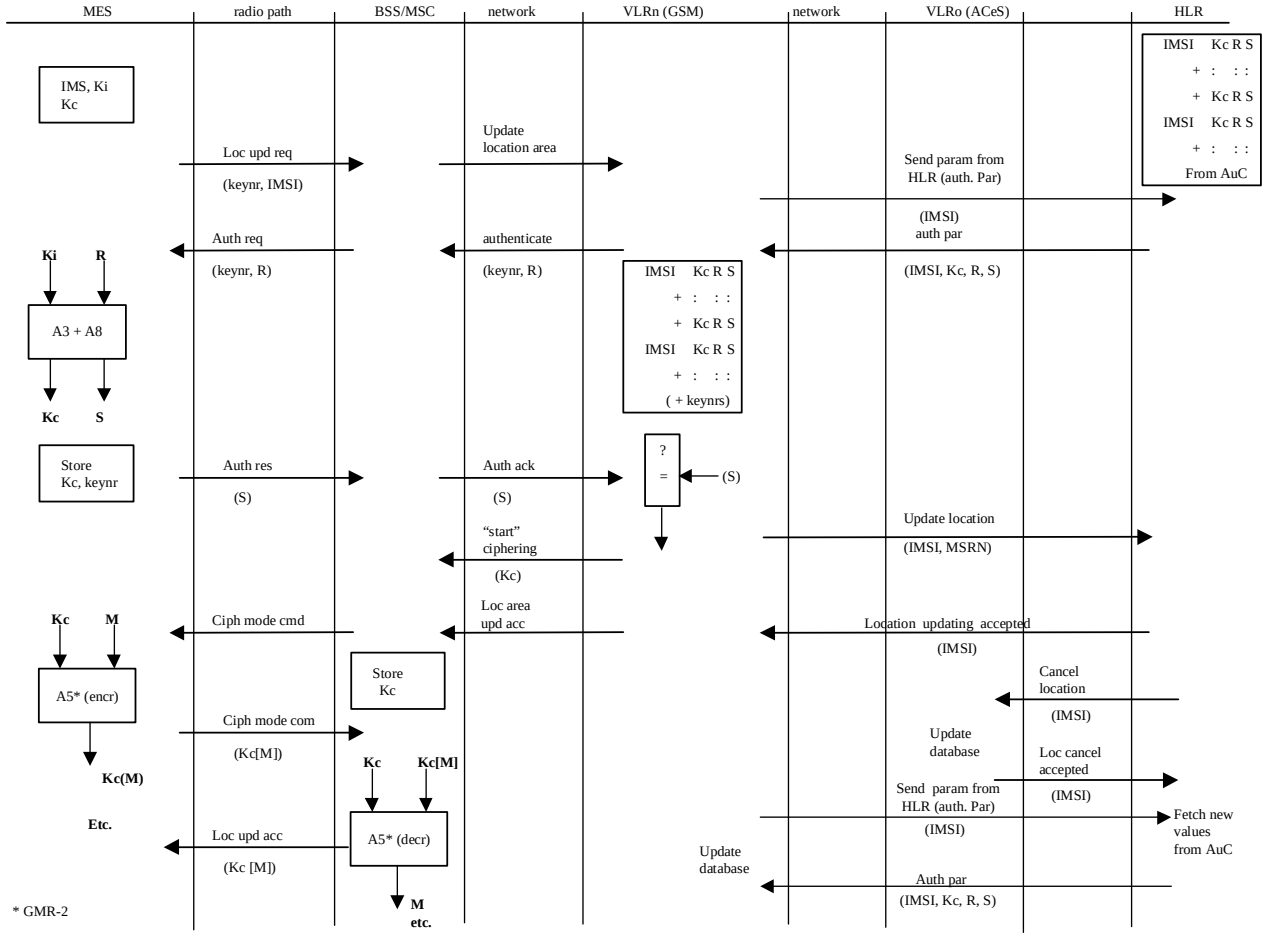


Scheme 2 (continued)



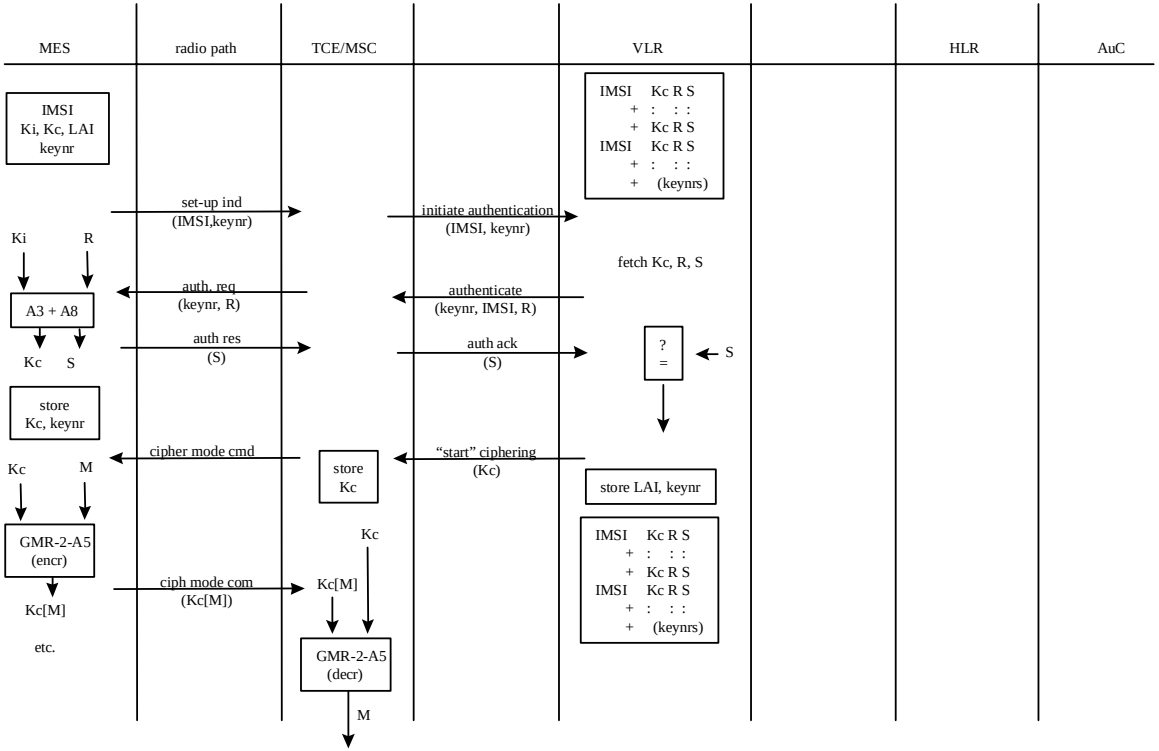
Scheme 3a: Location updating

- MES not yet registered in VLR
- MES transitioning from GSM PLMN to GMR-2



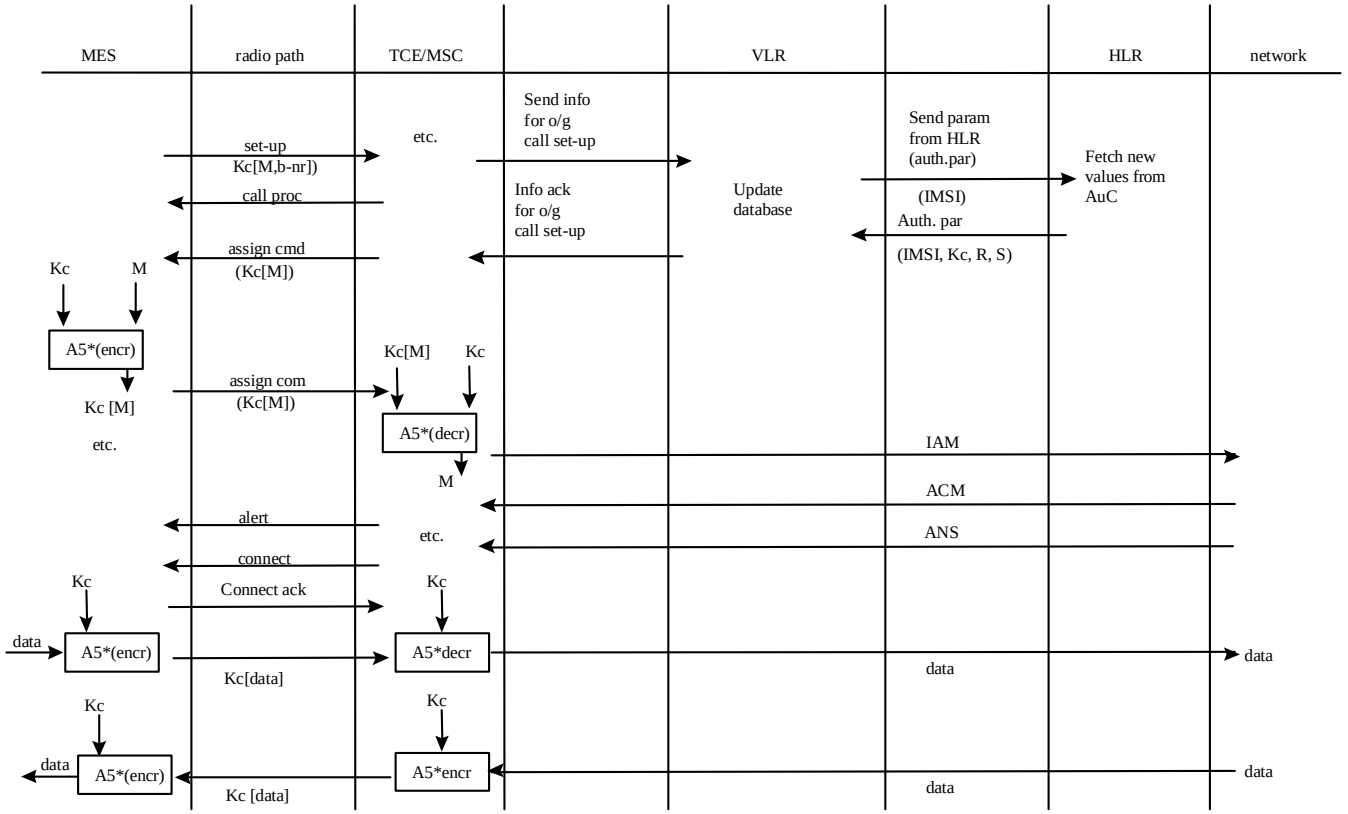
Scheme 3b: Location updating

- MES not yet registered in VLR
- MES transitioning from GMR-2 to GSM PLMN



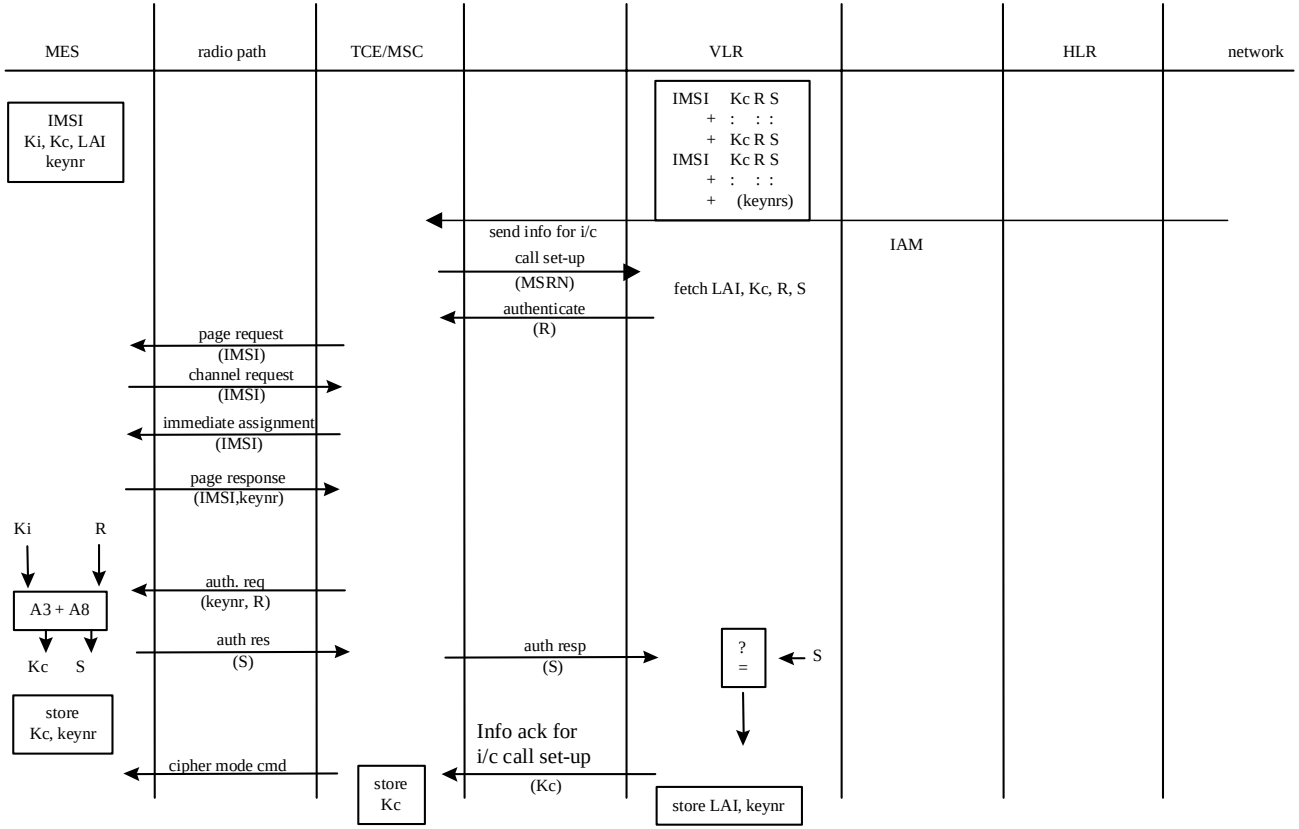
Scheme 4: Call set-up

- Mobile originated
- MES to Home Gateway



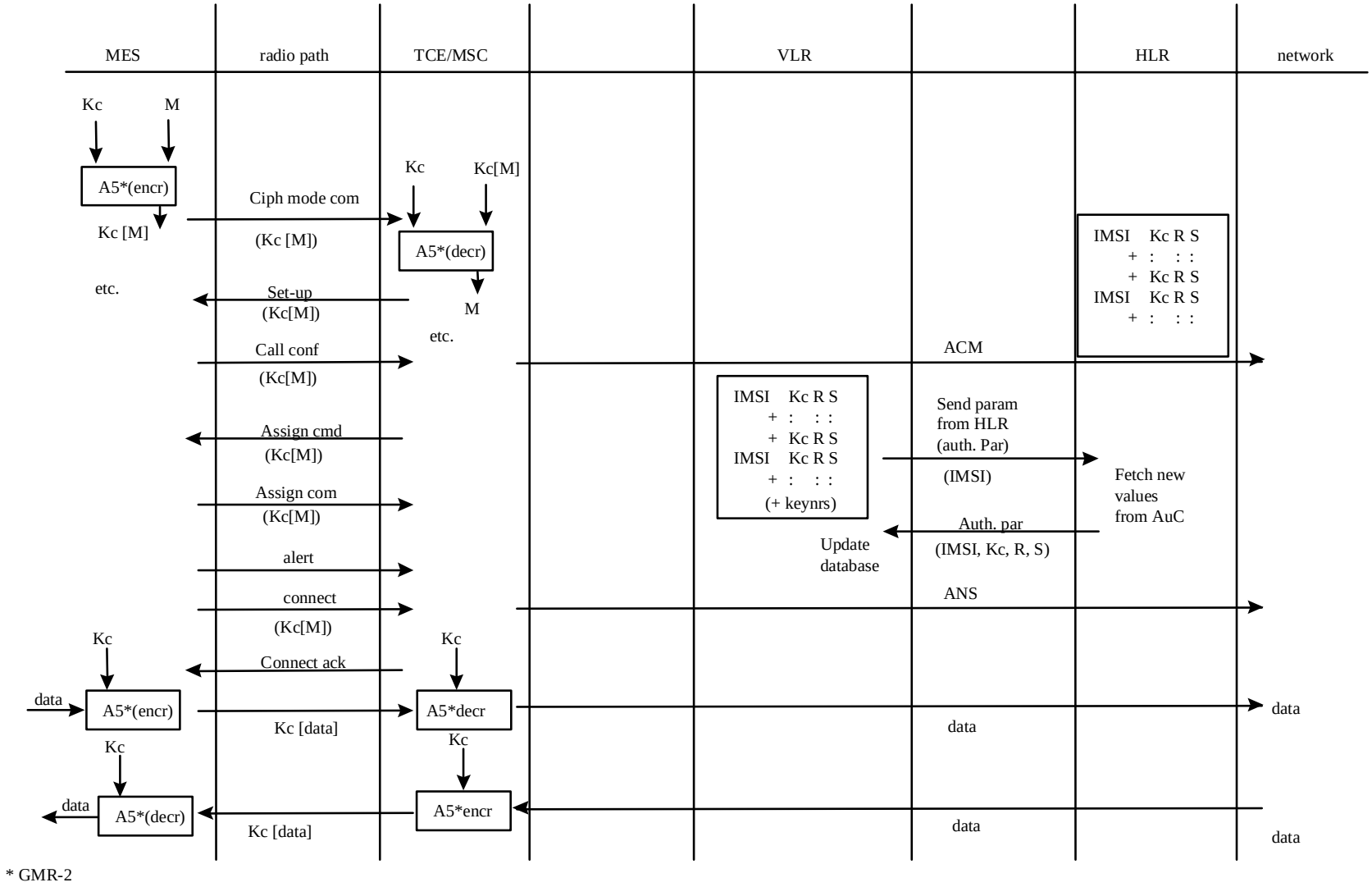
* GMR-2

Scheme 4 (continued)



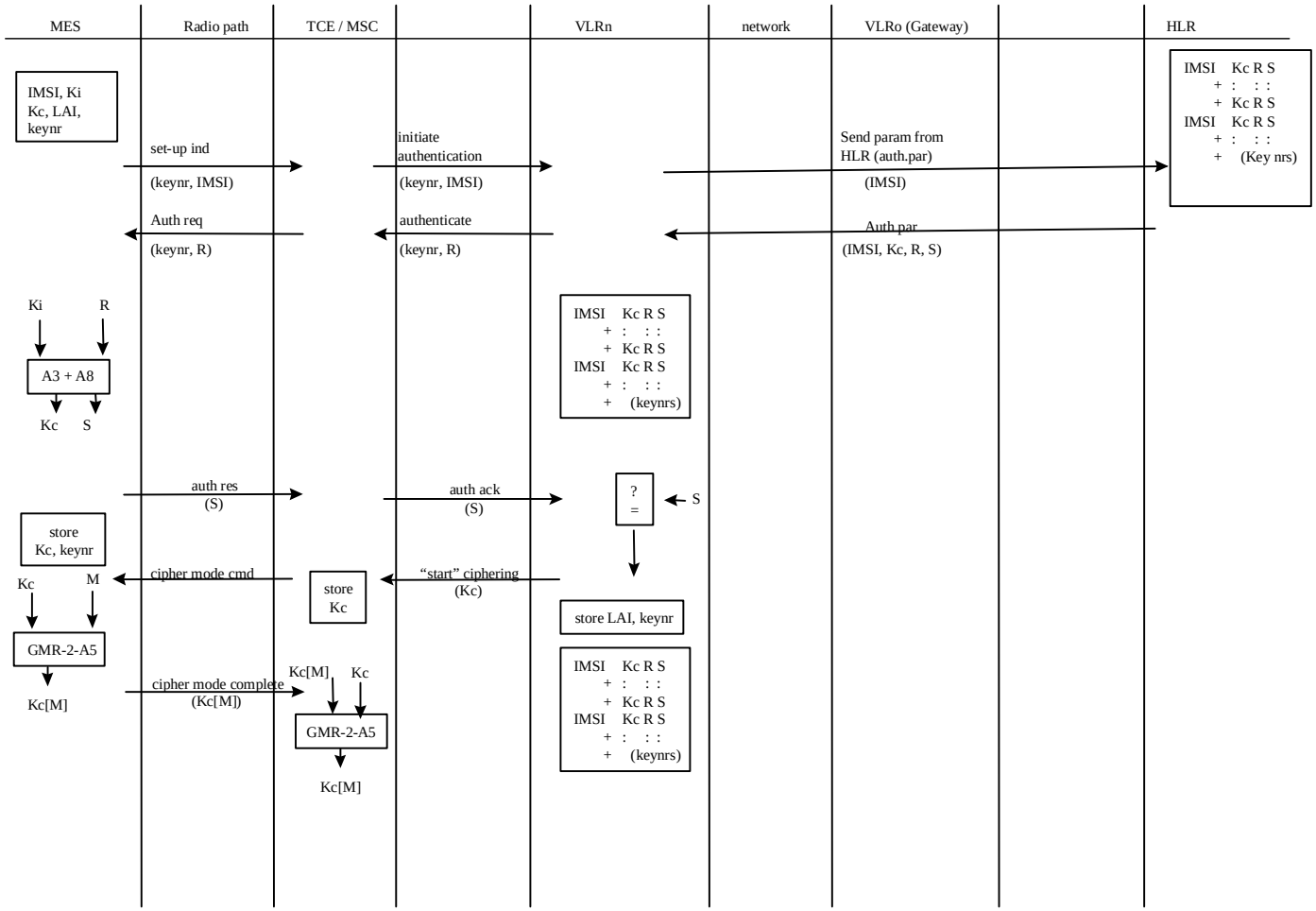
Scheme 5: Call set-up

- Mobile terminated
- Early assignment

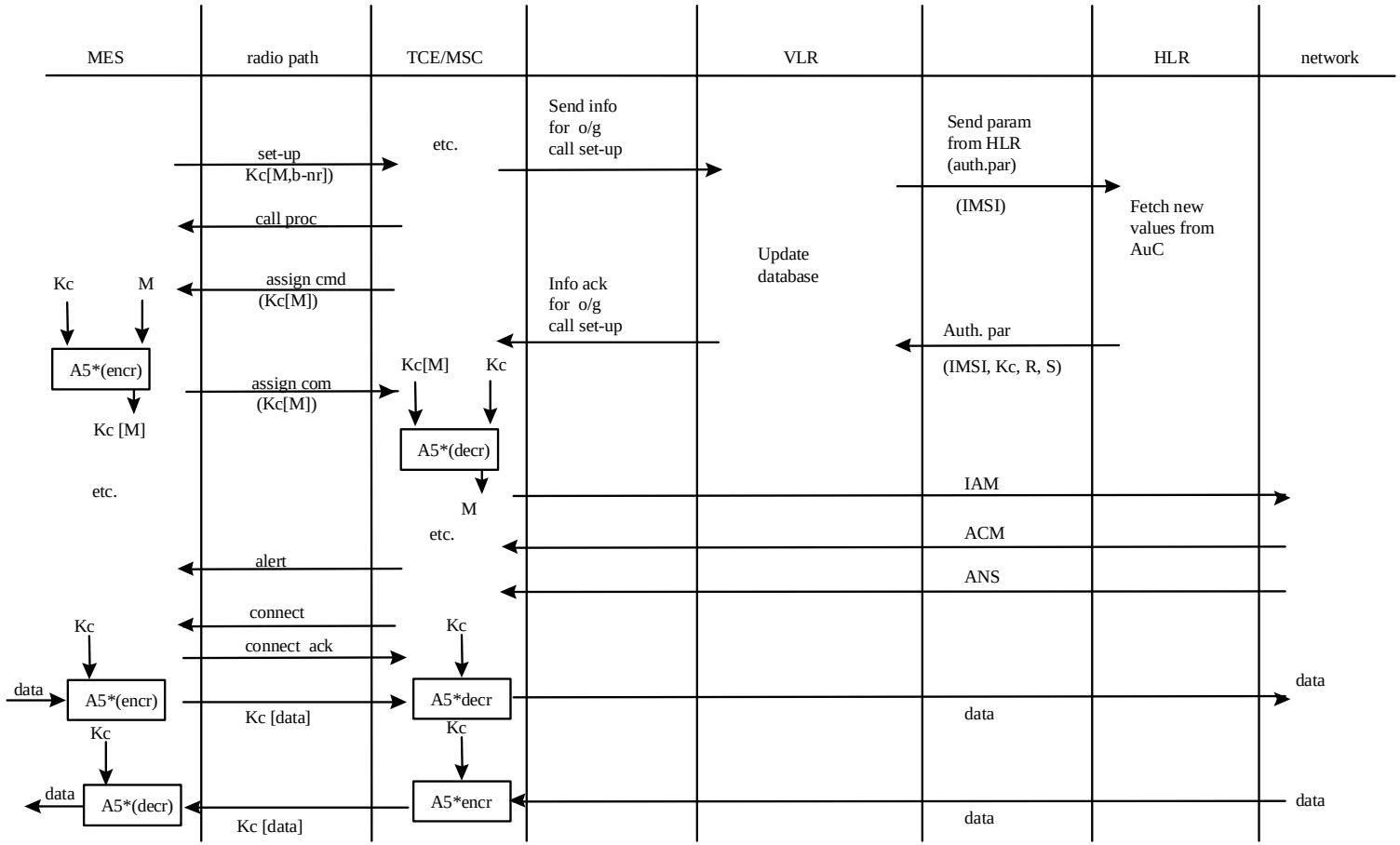


* GMR-2

Scheme 5 (continued)



Scheme 6: Long Haul Call Setup



* GMR-2

Scheme 6 (continued)

Annex B (informative): Security information to be stored in the entities of the GMR-2 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-2 network.

The entities of the GMR-2 network where security information is stored are:

- home location register;
- visitor location register;
- TCE;
- mobile earth station;
- authentication centre.

B.2 Entities and security information

B.2.1 Home location register (HLR)

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

B.2.2 Visitor location register (VLR)

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

B.2.3 Traffic channel equipment (TCE)

Encryption algorithm GMR-2-A5 is stored in the TCE.

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

B.2.4 Mobile Earth Station (MES)

The MES stores permanently:

- authentication algorithm A3;
- encryption algorithm GMR-2-A5;
- ciphering key generating algorithm A8;
- individual subscriber authentication key Ki;
- ciphering key Kc;

- ciphering key sequence number;
- IMSI.

The MES generates and stores:

- ciphering key Kc.

The MES receives and stores:

- ciphering key sequence number;
- LAI.

B.2.5 Authentication centre (AuC)

In the authentication centre are implemented:

- authentication algorithm(s) A3;
- ciphering key generating algorithm(s) A8.

The secret individual authentication keys Ki and the IMSI of each subscriber are stored in an authentication centre.

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

This annex specifies the cryptological algorithms which are needed to provide the various security features and mechanisms defined in, respectively, GMR-2 02.009 [2] and the present document.

The following three algorithms are considered:

- algorithm A3: Authentication algorithm;
- algorithm GMR-2-A5: Ciphering/deciphering algorithm;
- algorithm A8: Ciphering key generator.

Algorithm GMR-2-A5 must be common to all GMR-2 GWs and all mobile stations (in particular, to allow roaming). The external specifications of Algorithm GMR-2-A5 are defined in clause C.1.3. The internal specifications of Algorithm GMR-2-A5 are managed under the responsibility of the GSAC; they will be made available in response to an appropriate request.

Algorithms A3 and A8 are at each GW operator discretion. Only the formats of their inputs and outputs are specified. Candidates for Algorithm A3 and A8 are managed by the GSAC and available, for those GW operators who wish to use them, in response to an appropriate request.

C.1 Specification for algorithm GMR-2-A5

C.1.1 Purpose

Algorithm GMR-2-A5 realizes the protection of both user data and signalling information elements at the physical layer on the dedicated channels (S-TCH or S-DCCH).

Synchronization of both the enciphering and deciphering must be guarantied.

C.1.2 Implementation indications

Algorithm GMR-2-A5 is implemented into both the MES and the GW. On the GW side, the description below assumes that one algorithm GMR-2-A5 is implemented for each physical channel (S-TCH or S-DCCH).

The ciphering takes place before modulation and after interleaving (see GMR-2 05.001 [5]); the deciphering takes place after demodulation symmetrically. Both enciphering and deciphering need algorithm GMR-2-A5 and start at different times (see clause 4).

As an indication, recall that, due to the TDMA techniques used in the system, the useful data (also called the plain text in the sequel) are organized into blocks of 120 bits. Then, each block is incorporated into a normal burst (see GMR-2 05.002 [6]) and transmitted during a time slot. According to GMR-2 05.003 [7], the useful information bits into a block are numbered e0 to e59 and e60 to e119. Successive slots, for a given physical channel are separated at least by a frame duration, approximately 4,615 ms (see GMR-2 05.001 [5]).

For ciphering/deciphering, algorithm GMR-2-A5 produces, for each transmit and receive burst, a sequence of 120 encipher/decipher bits (here called BLOCK) which is combined by a bit-wise modulo 2 addition with the 120-bit plain text block. The first encipher/decipher bit produced by GMR-2-A5 is added to e0, the second to e1 and so on. As an indication, the resulting 120-bit block is then applied to the burst builder (see GMR-2 05.001 [5]).

For each slot, deciphering is performed on the MES side with the first block (BLOCK1) of 120 bits produced by GMR-2-A5, and enciphering is performed with the second block (BLOCK2). As a consequence, on the network side BLOCK1 is used for enciphering and BLOCK2 for deciphering. Therefore algorithm GMR-2-A5 must produce two blocks of 120 bits (i.e. BLOCK1 and BLOCK2) each 4,615 ms.

Synchronization is guarantied, by driving algorithm GMR-2-A5 by an explicit time variable, COUNT, derived from the TDMA frame number. COUNT is expressed in 22 bits as the concatenation of the binary representation of T1, T3 and T2. It is an input parameter of algorithm GMR-2-A5. The coding of COUNT is shown in figure C-1.

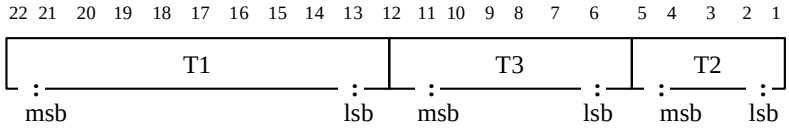


Figure C-1: The coding of COUNT

In the binary representation of COUNT, Bit 22 is the most significant bit (msb) and bit 1 the least significant bit (lsb) of COUNT. T1, T3 and T2 are represented in binary. (For definition of T1, T3 and T2, see GMR-2 05.002 [6]).

The GMR-2-A5 algorithm is also driven by an input called “Direction Bit", which is defined as follows:

- Direction Bit for Ciphering and Deciphering in the Mobile-to-PSTN direction = binary 0;
- Direction Bit for Ciphering and Deciphering in the PSTN-to-Mobile direction = binary 1.

Figure C-2 summarizes the implementation indications listed above, with only one enciphering/deciphering procedure in the PSTN-to-Mobile direction represented (the second one for deciphering/enciphering is symmetrical).

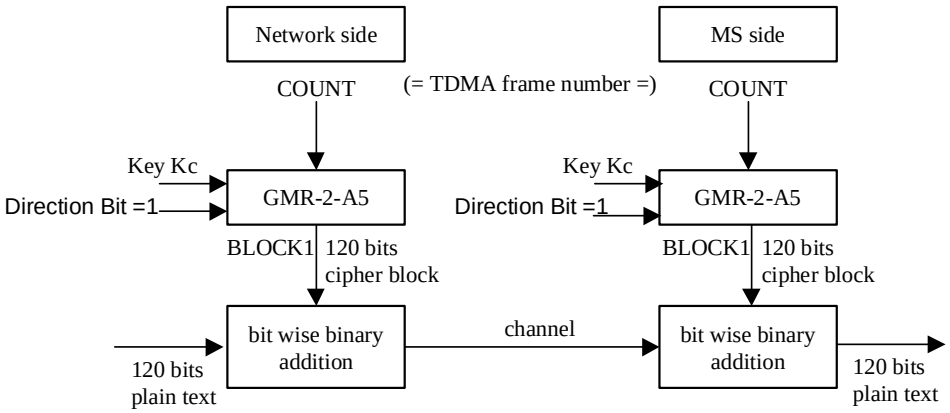


Figure C-2: Deciphering on the MES side

C.1.3 External specifications of algorithm GMR-2-A5

The two input parameters (COUNT and Kc) and the output parameters (BLOCK1 and BLOCK2) of algorithm GMR-2-A5 shall use the following formats:

- length of Kc: 64 bits;
- length of COUNT: 22 bits;
- length of BLOCK 1: 120 bits;
- length of BLOCK 2: 120 bits.

Algorithm GMR-2-A5 shall produce BLOCK 1 and BLOCK 2 in less than a TDMA, frame duration, i.e. 4,615 ms.

BLOCK 1 and BLOCK 2 are defined in C.1.2.

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. It must be clear that for signalling and testing purposes the ciphering key Kc is considered to be 64 unstructured bits.

C.1.4 Internal specification of algorithm GMR-2-A5

The internal specification of algorithm GMR-2-A5 is managed under the responsibility of the GSAC; it will be made available in response to an appropriate request.

C.2 Algorithm A3

Algorithm A3 is considered as a matter for GMR-2 GW operators. Therefore, only external specifications are given. However a proposal for a possible algorithm A3 is managed by the GSAC. Candidate algorithms will be made available upon appropriate request.

C.2.1 Purpose

The purpose of algorithm A3 is to allow authentication of a mobile subscriber's identity.

To this end, algorithm A3 must 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.2.2 Implementation and operational requirements

On the MES side, algorithm A3 is contained in a Subscriber Identity Module, as specified in GSM 02.17 [3].

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 shall use the following formats:

- length of Ki: 128 bits;
- length of RAND: 128 bits;
- length of SRES: 32 bits.

The run-time of algorithm A3 shall be less than 500 ms.

C.3 Algorithm A8

Algorithm A8 is considered as a matter for GMR-2 GW operators as is Algorithm A3.

A proposal for a possible algorithm A8, is managed by the GSAC. Candidate algorithms will be made available upon appropriate request.

C.3.1 Purpose

As previously described algorithm A8 must compute the ciphering key Kc from the random challenge, RAND, sent during the authentication procedure, using the authentication key Ki.

C.3.2 Implementation and operational requirements

On the MES side, algorithm A8 is contained in the SIM, as specified in GSM 02.17 [3].

On the network side, algorithm A8 is co-located with algorithm A3.

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

- length of Ki: 128 bits;
- length of RAND: 128 bits;
- length of Kc: 64 bits.

If the output length of the actual ciphering key is less than 64 bits, algorithm A8 shall 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 least significant bits and that, the actual ciphering key is contained in the most significant bits. For signalling and testing purposes, the ciphering key Kc is considered to be 64 unstructured bits.

History

Document history		
V1.1.1	March 2001	Publication