TS 100 929 V6.0.1 (1998-07)

Technical Specification

Digital cellular telecommunications system (Phase 2+); Security related network functions (GSM 03.20 version 6.0.1 Release 1997)

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

ETSI

European Telecommunications Standards Institute

Reference
DTS/SMG-030320Q6 (8lo0300r.PDF)

Keywords
Digital cellular telecommunications system, Global System for Mobile communications (GSM)

ETSI Secretariat

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet
secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

Foreword

This ETSI Technical Specification has been produced by the Special Mobile Group (SMG) of the European Telecommunications Standards Institute (ETSI).
This specification defines the security related network functions within the digital cellular telecommunications system.
The contents of this specification are subject to continuing work within SMG and may change following formal SMG approval. Should SMG modify the contents of this specification it will then be re-issued with an identifying change of release date and an increase in version number as follows:

Version 6.x.y

where:

- 6 GSM Phase 2+ Release 1997;
- x the second digit is incremented for all other types of changes, i.e. technical enhancements, corrections, updates, etc.;
- y the third digit is incremented when editorial only changes have been incorporated in the specification.

Introduction

The present document includes references to features which are not part of the Phase 2+ Release 96 of the GSM Technical specifications. All subclauses which were changed as a result of these features contain a marker (see table below) relevant to the particular feature.
The following table lists all features that were introduced after Release 96.

Feature	Designator
General Packet Radio Service	$(GPRS)$

0 Scope

This GSM Technical Specification specifies the network functions needed to provide the security related service and functions specified in GSM 02.09.
This specification 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.

0.1 Normative references

This specification incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this specification only when incorporated in it by amendment or revision. For undated references, the latest edition of the publication referred to applies.

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".
[2] GSM 02.07: "Digital cellular telecommunications system (Phase 2+); Mobile Station (MS) features".
[3] GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security aspects".
[4] GSM 02.17: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM) Functional characteristics".
[5] GSM 02.60: " Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 1".
[6] GSM 03.03: "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification".
[7] GSM 03.60: " Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2"
[8] GSM 04.08: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".
[9] GSM 04.64: " Digital cellular telecommunications system (Phase 2+), General Packet Radio Service (GPRS); Logical Link Control (LLC)".
[10] GSM 05.01: "Digital cellular telecommunication system (Phase 2+); Physical layer on the radio path; General description".
[11] GSM 05.02: "Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path".
[12] GSM 05.03: "Digital cellular telecommunications system (Phase 2+); Channel coding".
[13] GSM 09.02: "Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification".

0.2 Abbreviations

Abbreviations used in this specification are listed in GSM 01.04.
Specific abbreviations used in annex A are listed in clause A.3.

1 General

The different security related services and functions that are listed in GSM 02.09 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 fixed 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 this specification:

- In the figures below, signalling exchanges are referred to by functional names. The exact messages and message types are specified in GSM 04.08 and GSM 09.02.
- No assumptions are made for function splitting between MSC (Mobile Switching Centre), VLR (Visitor Location Register) and BSS (Base Station System). Signalling is described directly between MS and the local network (i.e. BSS, MSC and VLR denoted in the figures by BSS/MSC/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 TMSI allows addressing schemes without IMSI, but the actual implementation is specified in the GSM 04-series.
- The term HPLMN in the figures below 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.

2 Subscriber identity confidentiality

2.1 Generality

The purpose of this function is to avoid the possibility for an intruder to identify which subscriber is using a given resource on the radio path (e.g. TCH (Traffic Channel) or signalling resources) by listening to the signalling exchanges on the radio path. This 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 (International Mobile Subscriber Identity), 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 radio 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 radio path; and
- the IMSI is not normally used as addressing means on the radio path (see GSM 02.09);
- when the signalling procedures permit it, signalling information elements that convey information about the mobile subscriber identity must be ciphered for transmission on the radio path.

The identifying method is specified in the following subclause. The ciphering of communication over the radio path is specified in clause 4.

2.2 Identifying method

The means used to identify a mobile subscriber on the radio path consists of a TMSI (Temporary Mobile Subscriber Identity). This TMSI is a local number, having a meaning only in a given location area; the TMSI must 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 GSM 03.03.

The network (e.g. a VLR) manages suitable data bases to keep the relation between TMSIs and IMSIs. When a TMSI is received with an LAI that does not correspond to the current VLR, the IMSI of the MS must be requested from the VLR in charge of the indicated location area if its address is known; otherwise the IMSI is requested from the MS.

A new TMSI must be allocated at least in each location updating procedure. The allocation of a new TMSI corresponds implicitly for the MS to the de-allocation of the previous one. In the fixed part of the network, the cancellation of the record for an MS in a VLR implies the de-allocation of the corresponding TMSI.

To cope with some malfunctioning, e.g. arising from a software failure, the fixed part of the network can require the identification of the MS in clear. This procedure is a breach in the provision of the service, and should be used only when necessary.

When a new TMSI is allocated to an MS, it is transmitted to the MS in a ciphered mode. This ciphered mode is the same as defined in clause 4.

The MS must store its current TMSI in a non volatile memory, together with the LAI, so that these data are not lost when the MS is switched off.

2.3 Procedures

This subclause presents the procedures, or elements of procedures, pertaining to the management of TMSIs.

2.3.1 Location updating in the same MSC area

This procedure is part of the location updating procedure which takes place when the original location area and the new location area depend on the same MSC. The part of this procedure relative to TMSI management is reduced to a TMSI re-allocation (from TMSIo with "o" for "old" to TMSIn with "n" for "new").
The MS sends TMSIo as an identifying field at the beginning of the location updating procedure.
The procedure is schematized in figure 2.1.

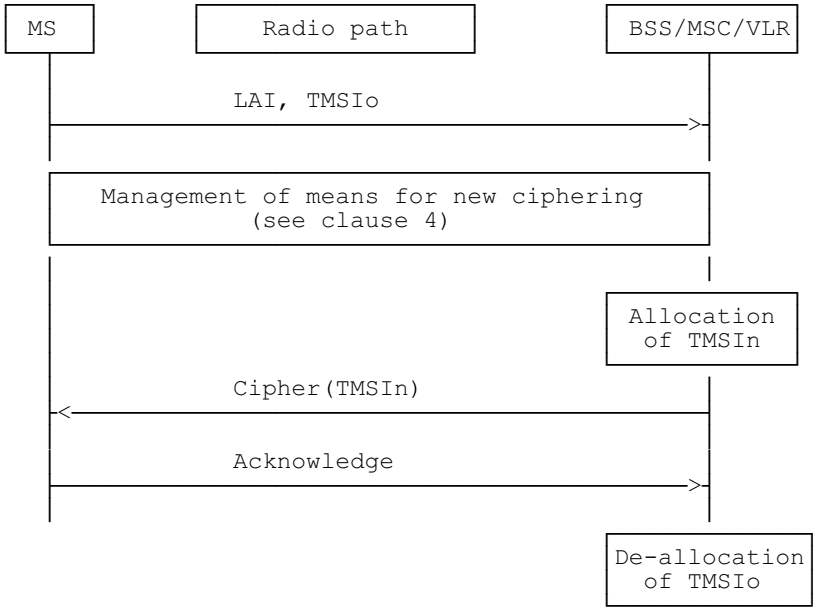


Figure 2.1: Location updating in the same MSC area

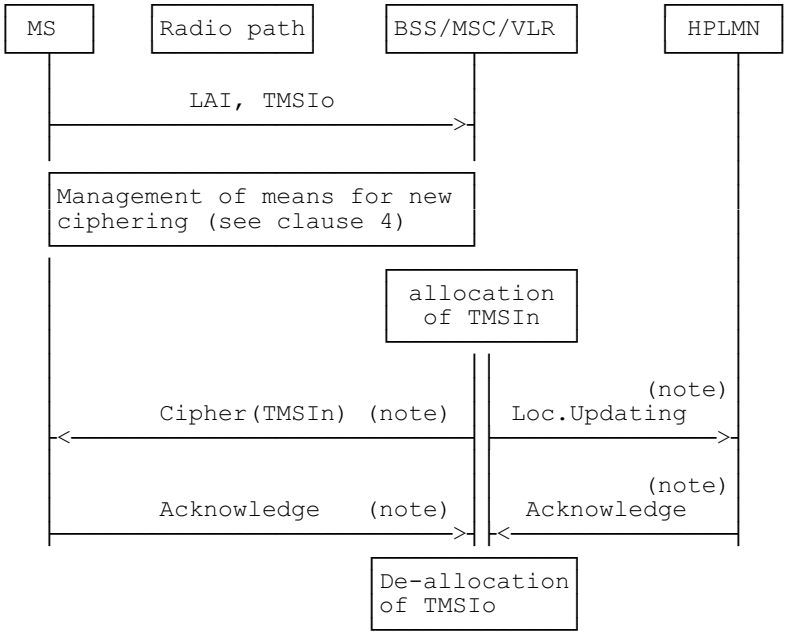
Signalling Functionalities:

Management of means for new ciphering:

The MS and BSS/MSC/VLR agree on means for ciphering signalling information elements, in particular to transmit TMSIn.

2.3.2 Location updating in a new MSCs area, within the same VLR area

This procedure is part of the location updating procedure which takes place when the original location area and the new location area depend on different MSCs, but on the same VLR.
The procedure is schematized on figure 2.2.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 2.2: Location updating in a new MSCs area, within the same VLR area

Signalling functionalities:

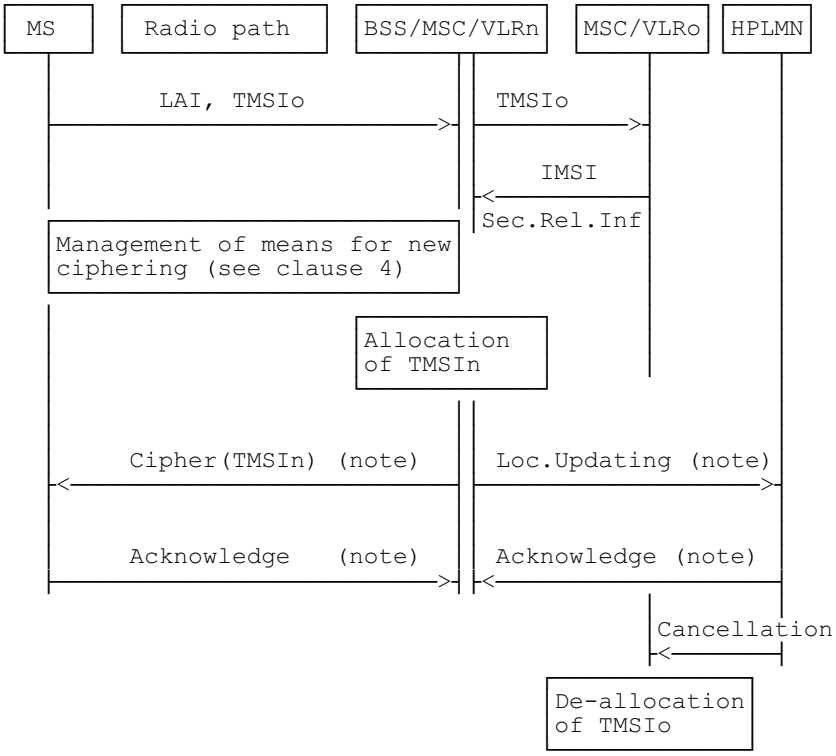
Loc.Updating:

stands for Location Updating

The BSS/MSC/VLR indicates that the location of the MS must be updated.

2.3.3 Location updating in a new VLR; old VLR reachable

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 VLRs.
The MS is still registered in VLRo ("o" for old or original) and requests registration in VLRn ("n" for new). LAI and TMSIo are sent by MS as identifying fields during the location updating procedure.
The procedure is schematized in figure 2.3.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 2.3: Location updating in a new VLR; old VLR reachable

Signalling functionalities:

Sec.Rel.Info.:

Stands for Security Related information

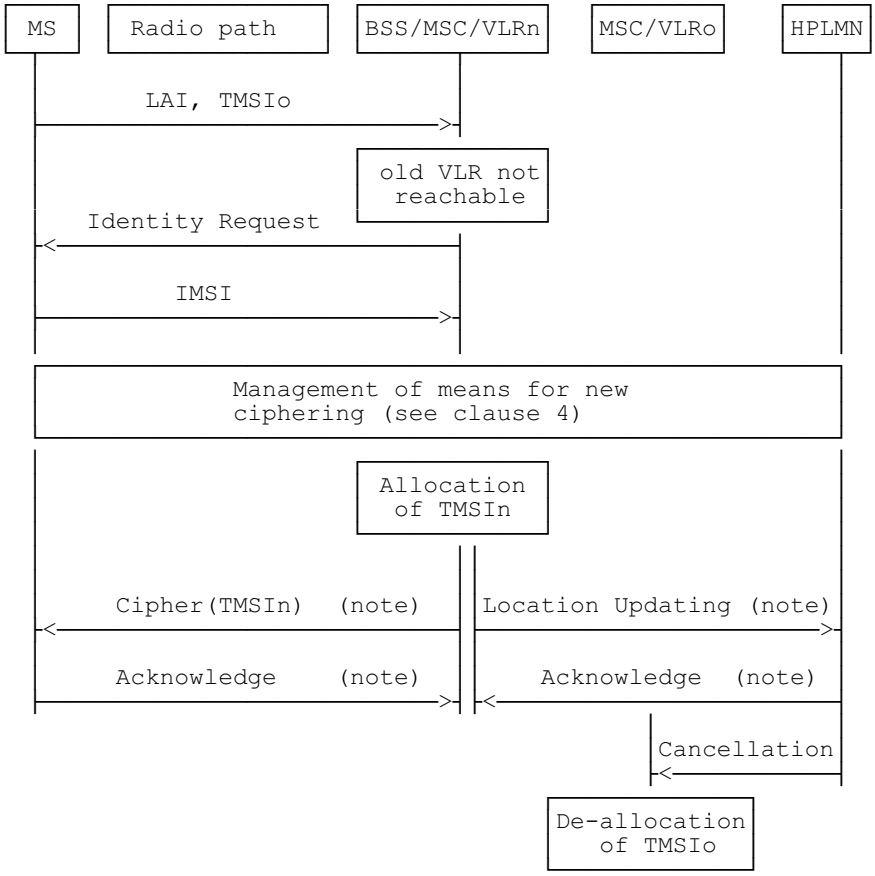
The MSC/VLRn needs some information for authentication and ciphering; this information is obtained from MSC/VLRo.

Cancellation:

The HLR indicates to VLRo that the MS is now under control of another VLR. The "old" TMSI is free for allocation.

2.3.4 Location Updating in a new VLR; old VLR not reachable

This variant of the procedure in subclause 2.3.3 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 MS in clear is necessary. The procedure is schematized in figure 2.4



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 2.4: Location Updating in a new VLR; old VLR not reachable

2.3.5 Reallocation of a new TMSI

This function can be initiated by the network whenever a radio connection exists. The procedure can be included in other procedures, e.g. through the means of optional parameters. The execution of this function is left to the network operator.
When a new TMSI is allocated to an MS the network must prevent the old TMSI from being allocated again until the MS has acknowledged the allocation of the new TMSI.
If an IMSI record is deleted in the VLR by O&M action, the network must prevent any TMSI associated with the deleted IMSI record from being allocated again until a new TMSI is successfully allocated to that IMSI.
If an IMSI record is deleted in the HLR by O&M action, it is not possible to prevent any TMSI associated with the IMSI record from being allocated again. However, if the MS whose IMSI record was deleted should attempt to access the network using the TMSI after the TMSI has been allocated to a different IMSI, then authentication or ciphering of the MS whose IMSI was deleted will almost certainly fail, which will cause the TMSI to be deleted from the MS.
The case where allocation of a new TMSI is unsuccessful is described in subclause 2.3.8.
This procedure is schematized in figure 2.5.

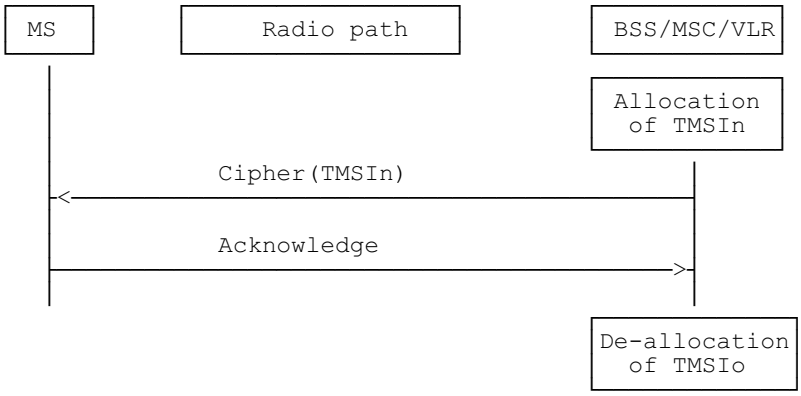
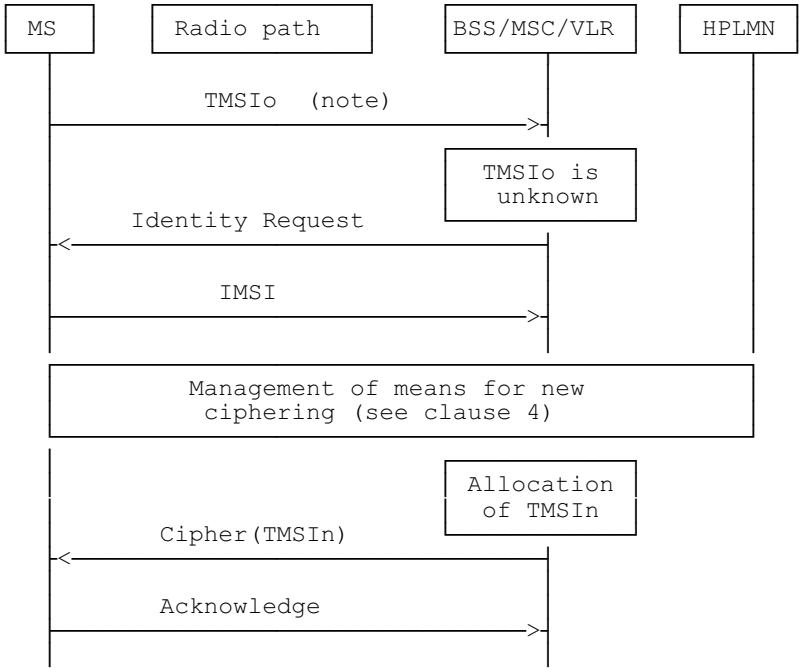


Figure 2.5: Reallocation of a new TMSI

2.3.6 Local TMSI unknown

This procedure is a variant of the procedure described in subclauses 2.3.1 and 2.3.2, and happens when a data loss has occurred in a VLR and when a MS 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 schematized in figure 2.6.

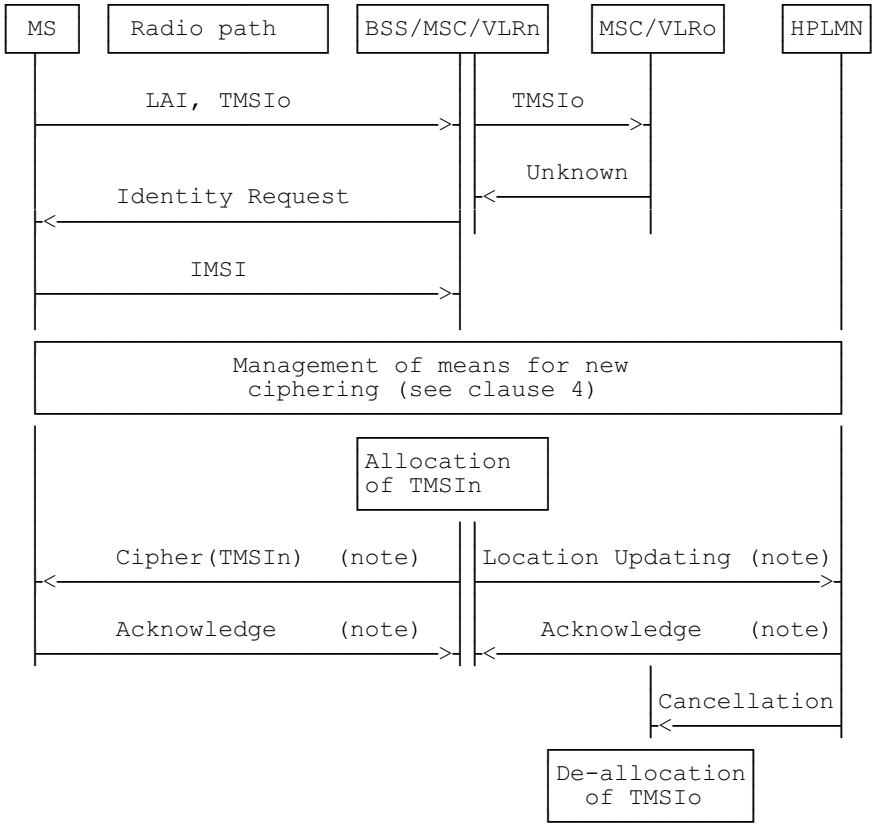


NOTE: Any message in which TMSIo is used as an identifying means in a location area managed by the same VLR.

Figure 2.6: Location updating in the same MSC area; local TMSI unknown

2.3.7 Location updating in a new VLR in case of a loss of information

This variant of the procedure described in 2.3.3 arises when the VLR in charge of the MS has suffered a loss of data. In that case the relation between TMSIo and IMSI is lost, and the identification of the MS in clear is necessary.
The procedure is schematized in figure 2.7.



NOTE: From a security point of view, the order of the procedures is irrelevant.

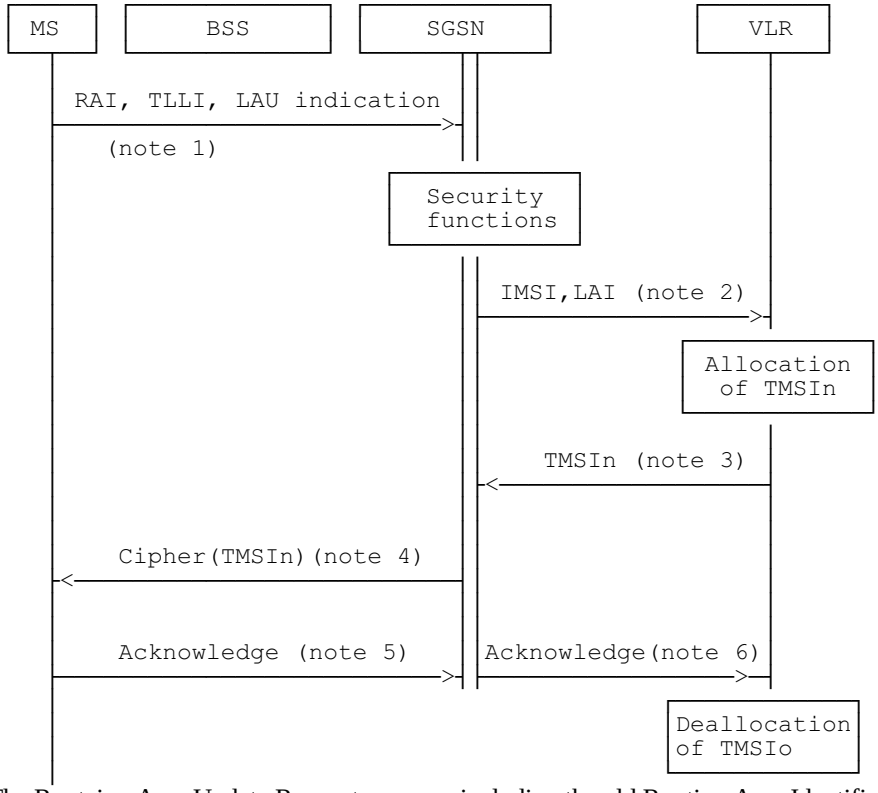
Figure 2.7: Location updating in a new VLR in case of a loss of information

2.3.8 Unsuccessful TMSI allocation

If the MS does not acknowledge the allocation of a new TMSI, the network shall maintain the association between the old TMSI and the IMSI and between the new TMSI and the IMSI.
For an MS-originated transaction, the network shall allow the MS to identify itself by either the old TMSI or the new TMSI. This will allow the network to determine the TMSI stored in the MS; the association between the other TMSI and the IMSI shall then be deleted, to allow the unused TMSI to be allocated to another MS.
For a network-originated transaction, the network shall identify the MS by its IMSI. When radio contact has been established, the network shall instruct the MS to delete any stored TMSI. When the MS has acknowledged this instruction, the network shall delete the association between the IMSI of the MS and any TMSI; this will allow the released TMSIs to be allocated to another MS.
In either of the cases above, the network may initiate the normal TMSI reallocation procedure.
Repeated failure of TMSI reallocation (passing a limit set by the operator) may be reported for O&M action.

2.3.9 Combined location area updating with the routing area updating $(GPRS)$

This subclause is only applicable if GPRS is supported.
This procedure is part of the location updating of a General Packet Radio Service (GPRS) class A or B mobile when the Gs-interface (SGSN MSC/VLR signalling interface) is implemented. This procedure is not relevant if the Gs-interface is not implemented.
The location area updating procedure and the routing area updating procedure are combined to one MS Serving GPRS Support Node (SGSN) procedure. The MS includes a Location Area Update (LAU) indication in the Routing Area Update Request message. The SGSN performs the location updating towards the VLR on behalf of the MS.
The procedure described in figure 2.8 shows only the interaction between the SGSN and the VLR. The full procedure including the update to other network element (e.g. HLR, old MSC/VLR) is described in GSM 03.60 .



NOTE 1: The Routeing Area Update Request message including the old Routing Area Identifier (RAI), the Temporary Logical Link Identifier (TLLI), and an indication that a combined Location Area Update (LAU) is performed.
NOTE 2: Location Updating message.
NOTE 3: Location Updating Accept message including the new TMSI.
NOTE 4: Routing Area Update Accept message including the new TMSI and the new TLLI (if any).
NOTE 5: Routing Area Update Complete message including the TLLI and TMSI.
NOTE 6: TMSI Reallocation Complete message including the TMSI.

Figure 2.8: Combined routing area and location updating in the same VLR

When the VLR does not change the TMSI, the old TMSI will stay in use and there is no need to send any TMSI to the MS.
In case of combined routing area update and inter-VLR location area updating procedure, the old TMSI will be cancelled and the HLR is updated as described in GSM 03.60.
If the Location Updating message indicates a reject (if for example the MS try to enter a forbidden location area), then this should be indicated to the MS and the MS shall not access non-GPRS service until a successful Location Update is performed.
For the combined location and routing area update and the combined GPRS Attach and IMSI Attach for GPRS class A and B mobiles, the authentication is performed by the SGSN. The authentication procedure for GPRS is described in annex D. The MSC/VLR relies on the SGSN authentication. This authentication procedure generates no ciphering key for circuit switched ciphering.
The ciphering key for circuit switched operation is allocated through an authentication by MSC/VLR when the circuit switched service is requested. Also, the MSC/VLR may use the old ciphering key if existing.

3 Subscriber identity authentication

3.1 Generality

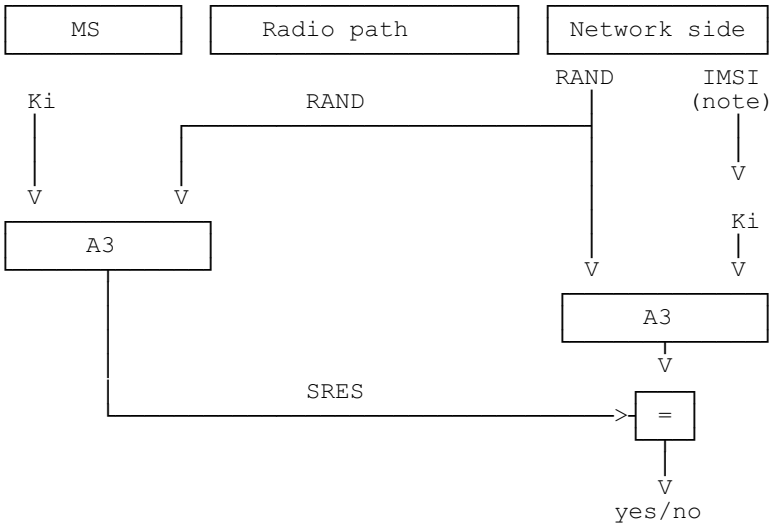
The definition and operational requirements of subscriber identity authentication are given in GSM 02.09.
The authentication procedure will also be used to set the ciphering key (see clause 4). Therefore, it is performed after the subscriber identity (TMSI/IMSI) is known by the network and before the channel is encrypted.
Two network functions are necessary: the authentication procedure itself, and the key management inside the fixed subsystem.

3.2 The authentication procedure

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

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

The general procedure is schematized in figure 3.1.



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

Figure 3.1: The authentication procedure

Authentication algorithm A3 is specified in annex C.

3.3 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 Public Land Mobile Network (HPLMN), in an Authentication Centre (AuC). A PLMN may contain one or more AuC. An AuC can be physically integrated with other functions, e.g. in a Home Location Register (HLR).

3.3.1 General authentication procedure

When needed for each MS, the BSS/MSC/VLR requests security related information from the HLR/AuC corresponding to the MS. 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 3.1. 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 3.2.

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 4.

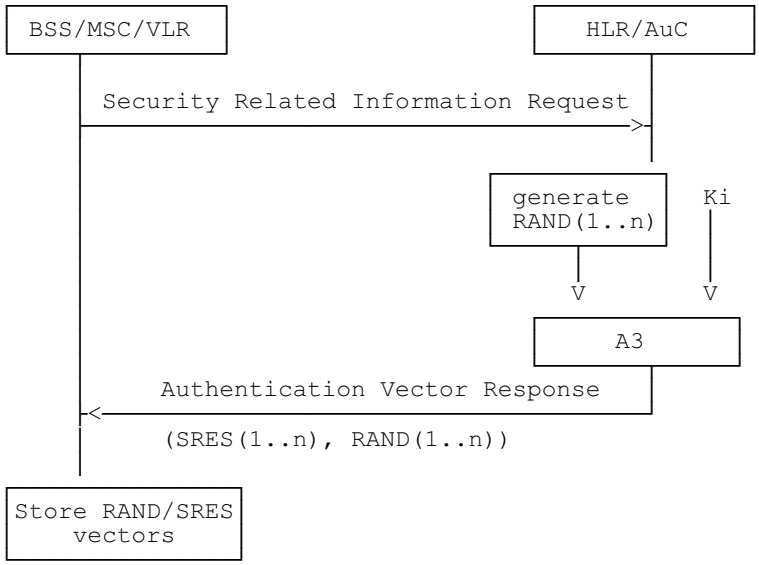


Figure 3.2: Procedure for updating the vectors RAND/SRES

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 MS. It then tests the answer from the MS by comparing it with the corresponding SRES, as schematized in figure 3.3.

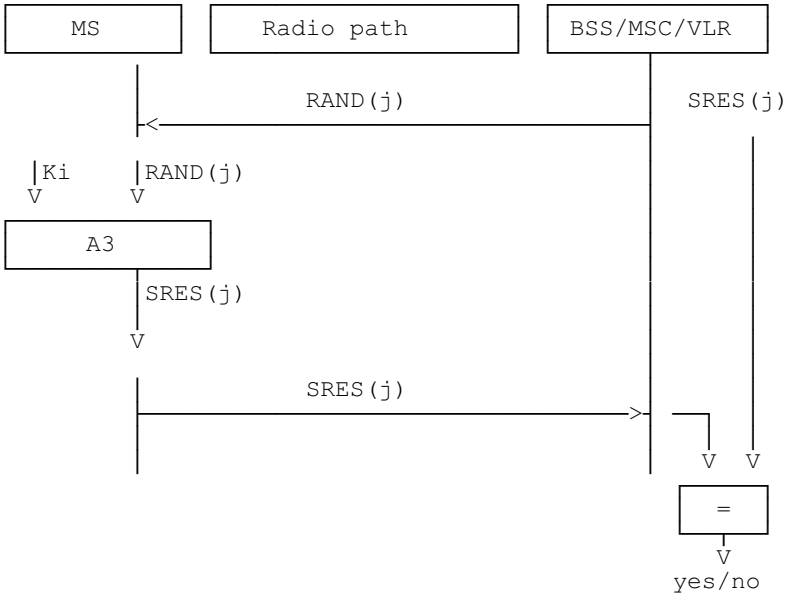


Figure 3.3: General authentication procedure

3.3.2 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 subclause. In the case when identification is done using TMSI, pairs for authentication as part of security related information are given by the old VLR (VLRo). The old VLR shall send to the new VLR only those pairs which have not been used.
The procedure is schematized in figure 3.4.

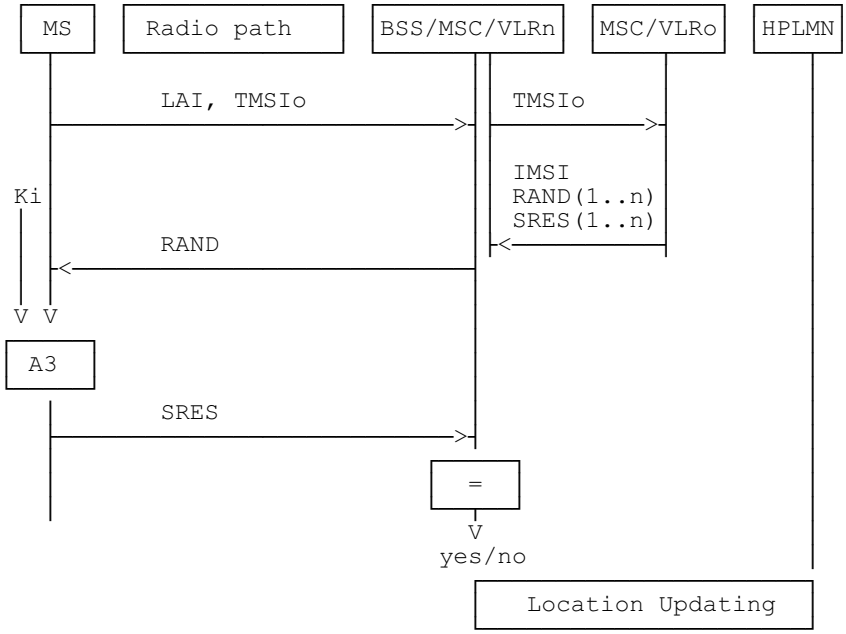


Figure 3.4: Authentication at location updating in a new VLR, using TMSI

3.3.3 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 subclause 3.3.2 cannot be used. Instead, pairs of RAND/SRES contained in the security related information are requested directly from the HPLMN.
The procedure is schematized in figure 3.5.

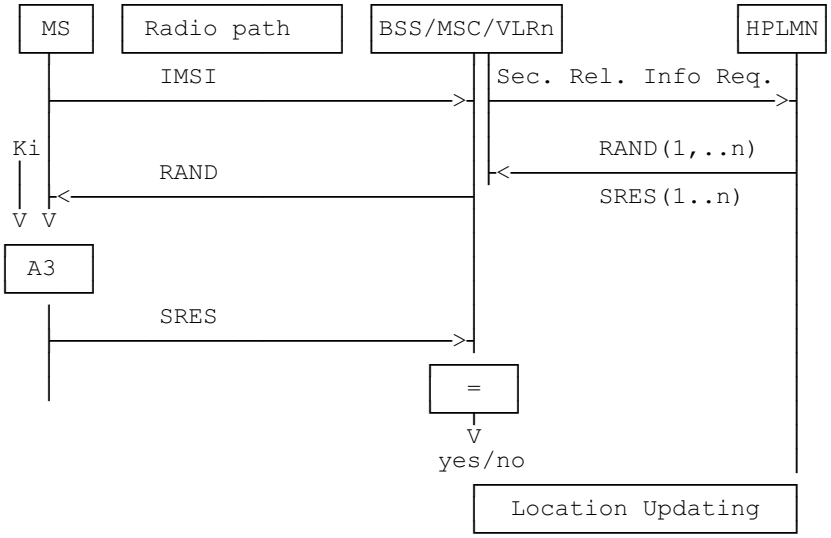


Figure 3.5: Authentication at location updating in a new VLR, using IMSI

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

This case is an abnormal one, when a data loss has occurred in the "old" VLR.
The procedure is schematized in figure 3.6.

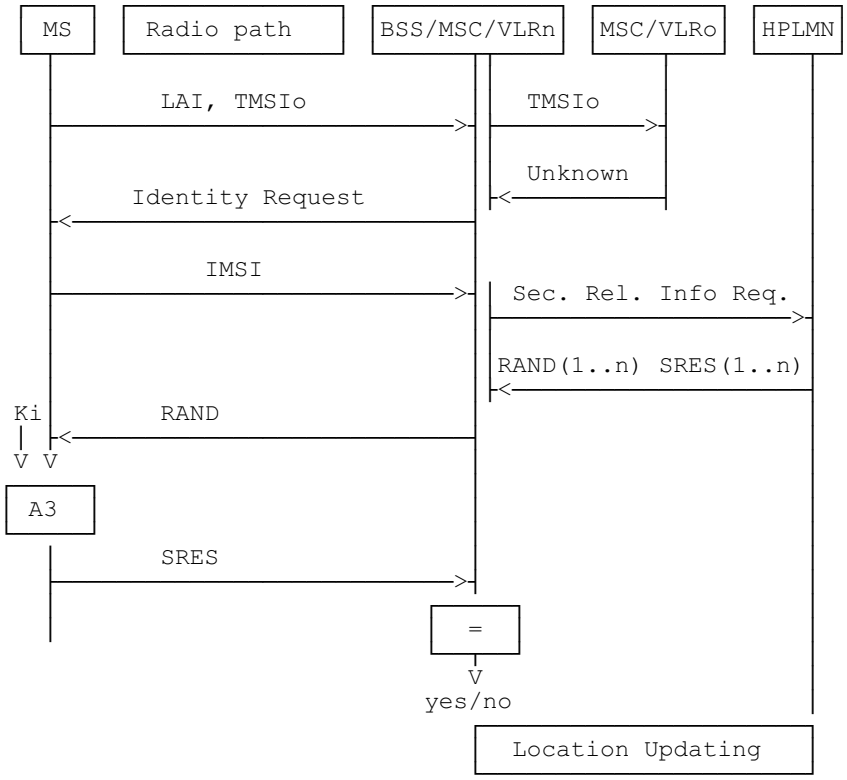


Figure 3.6: Authentication at location updating in a new VLR, using TMSI, TMSI unknown in "old" VLR

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

The case occurs when an old VLR cannot be reached by the new VLR.
The procedure is schematized in figure 3.7

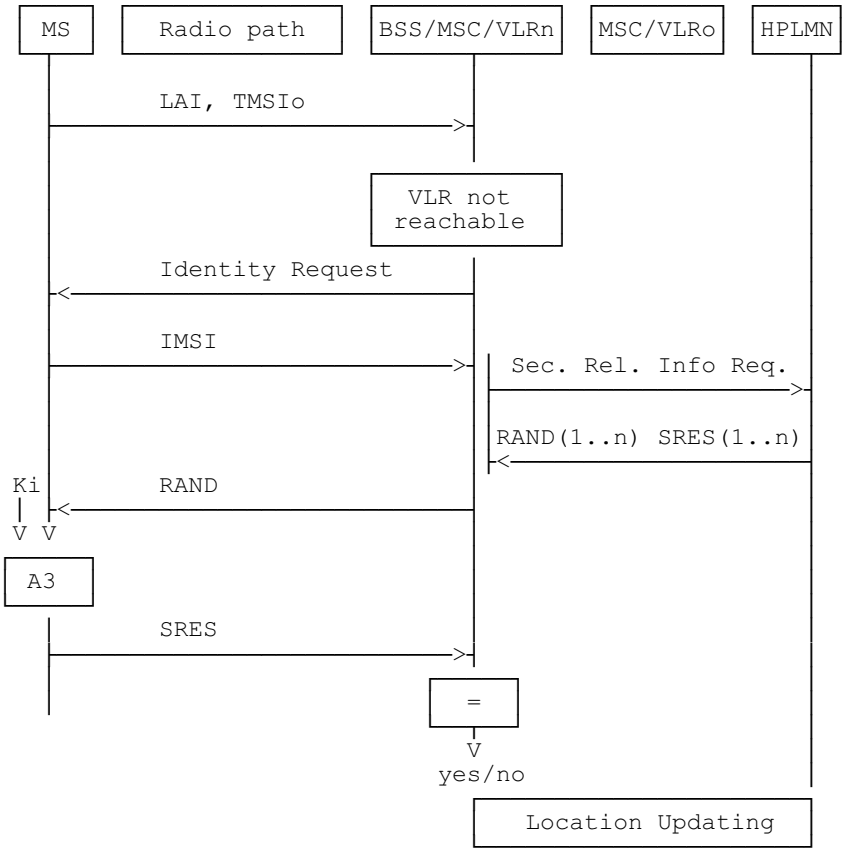


Figure 3.7: Authentication at location updating in a new VLR, using TMSI, old VLR not reachable

3.3.6 Authentication with IMSI if authentication with TMSI fails

If authentication of an MS which identifies itself with a TMSI is unsuccessful, the network requests the IMSI from the MS, 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 which triggered the authentication.

3.3.7 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 MS, 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 send 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.

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

4.1 Generality

In GSM 02.09, some signalling information elements are considered sensitive and must be protected.
To ensure identity confidentiality (see clause 2), the Temporary Subscriber Identity must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it.
The confidentiality of connection less 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 MS-BSS 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 a OSI layer 1 function. The scheme described below assumes that the main part of the signalling information elements is transmitted on DCCH (Dedicated Control Channel), and that the CCCH (Common Control Channel) is only used for the allocation of a DCCH.
Four points have to be specified:

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

4.2 The ciphering method

The layer 1 data flow (transmitted on DCCH or 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 A5 using a key determined as specified in subclause 4.3. The key is denoted below by Kc, and is called "Ciphering Key".
For multislot configurations (e.g. HSCSD) different ciphering bit streams are used on the different timeslots. On timeslot "n" a ciphering bit stream, generated by algorithm A5, using a key Kcn is used. Kcn is derived from Kc as follows:

> Let BN denote a binary encoding onto 64 bits of the timeslot number "n" (range 0-7). Bit "i" of Kcn, Kcn(i), is then calculated as Kc(i) xor (BN<<32(i)) ("xor" indicates: "bit per bit binary addition" and "<<32" indicates: "32 bit circular shift"), the number convention being such that the lsb of Kc is xored with the lsb of the shifted BN.

Deciphering is performed by exactly the same method.
Algorithm A5 is specified in annex C.

4.3 Key setting

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 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 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 MS 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 subclause 3.3.
The values Kc are computed together with the SRES values. The security related information (see subclause 3.3.1) 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 4.1.

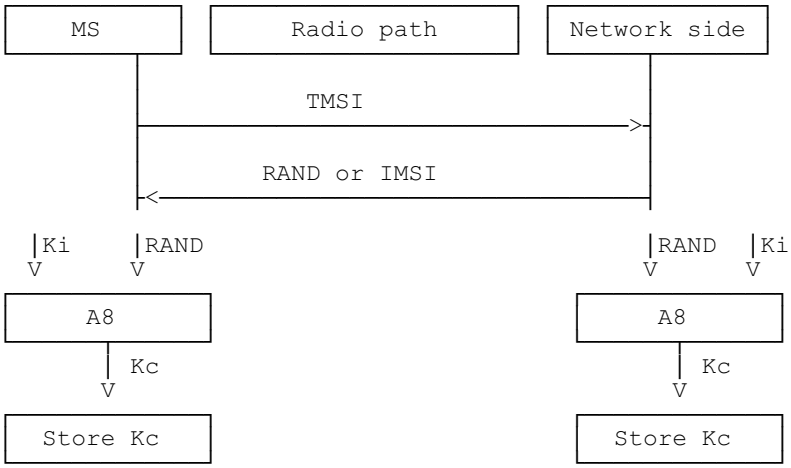


Figure 4.1: Key setting

4.4 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 this specification but in GSM 04.08 instead.

4.5 Starting of the ciphering and deciphering processes

The MS and the BSS must co-ordinate the instants at which the enciphering 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 the key Kc has been made available at the BSS.
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 BSS, which sends in clear text to the MS a specific message, here called "Start cipher". Both the enciphering and deciphering start on the MS side after the message "Start cipher" has been correctly received by the MS. Finally, enciphering on the BSS side starts as soon as a frame or a message from the MS has been correctly deciphered at the BSS.
The starting of enciphering and deciphering processes is schematized in figure 4.2.

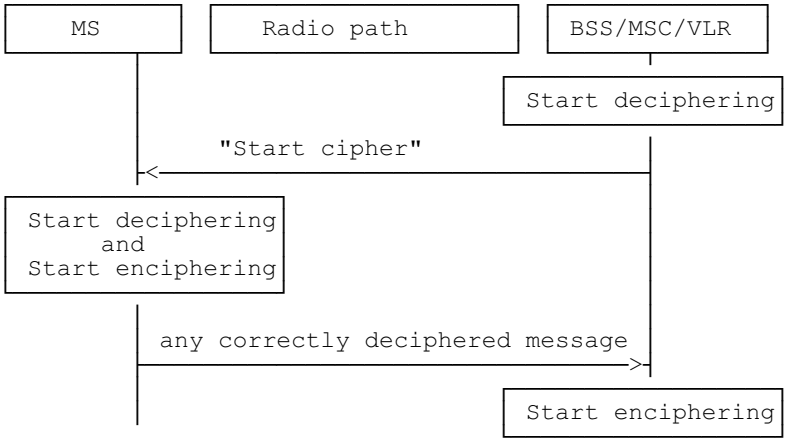


Figure 4.2: Starting of the enciphering and deciphering processes

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

4.6 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.

4.7 Handover

When a handover occurs, the necessary information (e.g. key Kc, initialization data) is transmitted within the system infrastructure to enable the communication to proceed from the old BSS to the new one, and the Synchronization procedure is resumed. The key Kc remains unchanged at handover.

4.8 Negotiation of A5 algorithm

Not more then seven versions of the A5 algorithm will be defined.
When an MS wishes to establish a connection with the network, the MS shall indicate to the network which of the seven versions of the A5 algorithm it supports. The network shall not provide service to an MS which indicates that it does not support the ciphering algorithm(s) required by GSM 02.07.
The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the A5 algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.
2) If the MS and the network have at least one version of the A5 algorithm in common, then the network shall select one of the mutually acceptable versions of the A5 algorithm for use on that connection.
3) If the MS and the network have no versions of the A5 algorithm in common and the network is willing to use an unciphered connection, then an unciphered connection shall be used.

5 Synthetic summary

Figure 5.1 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.

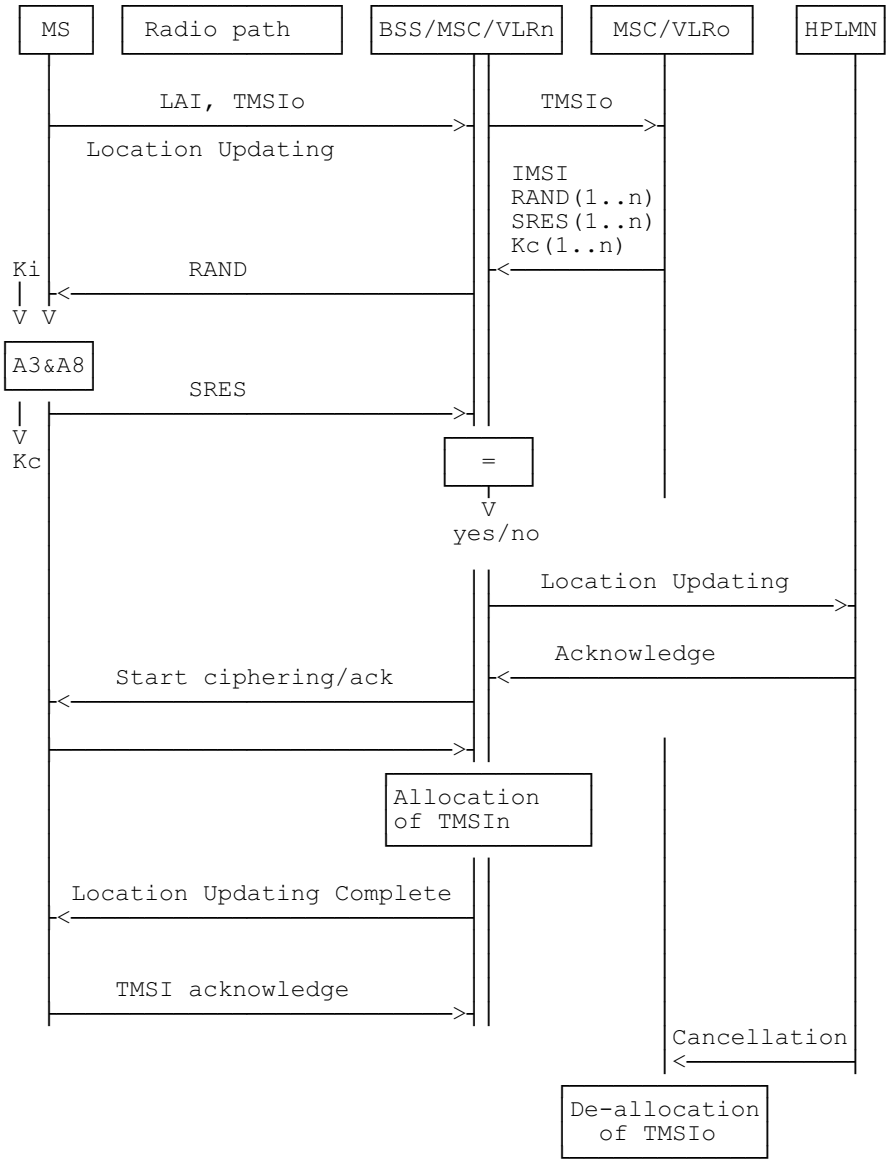


Figure 5.1: Normal location updating procedure

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 BSS/MSC.

A.2 Short description of the schemes

Scheme 1: Location registration
- no TMSI available.
  The situation occurs where an MS requests registration and for some reason e.g. TMSI is lost or this is the first registration, there is no TMSI available. In this case the IMSI is used for identification. The IMSI is sent in clear text via the radio path as part of the location updating.

Scheme 2: Location updating
- MS registered in VLR;
- TMSI is still available.
  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 TMSI. For authentication a new set of RAND, SRES and Kc is already available in the VLR.

Scheme 3: Location updating
- MS not yet registered in VLR;
- TMSI is still available.
  The MS has roamed to an area controlled by another VLR. The LAI is used to address the "old" VLR. The TMSI is used for identification. The "old" VLR informs the "new" VLR about this MS. The security related information is sent by the "old" VLR to the "new" VLR.

Scheme 4: Location updating
- MS not yet registered in VLR and no old LAI.
  The VLR cannot identify the VLR where the MS was last registered. Identification is therefore done by using the IMSI. The VLR cannot request authentication information from the previous VLR (LAI not available), so the HLR has to send the authentication information to the VLR.

Scheme 5: Call set-up
- mobile originated;
- early assignment.
  The users of the registered MS wants to set-up a call. Identification is done by using the TMSI. All signalling information elements in all messages on the radio path are encrypted with ciphering key Kc. The PLMN is setting up calls with "early assignment".

Scheme 6: Call set-up
- mobile originated;
- off air call set-up.
  As in scheme 5 the user of the registered MS wants to set-up a call. Identification is done by using the TMSI. All signalling information elements in all messages on the radio path are encrypted with ciphering key Kc after the cipher mode command message. The PLMN is setting up calls with "off air call set-up"

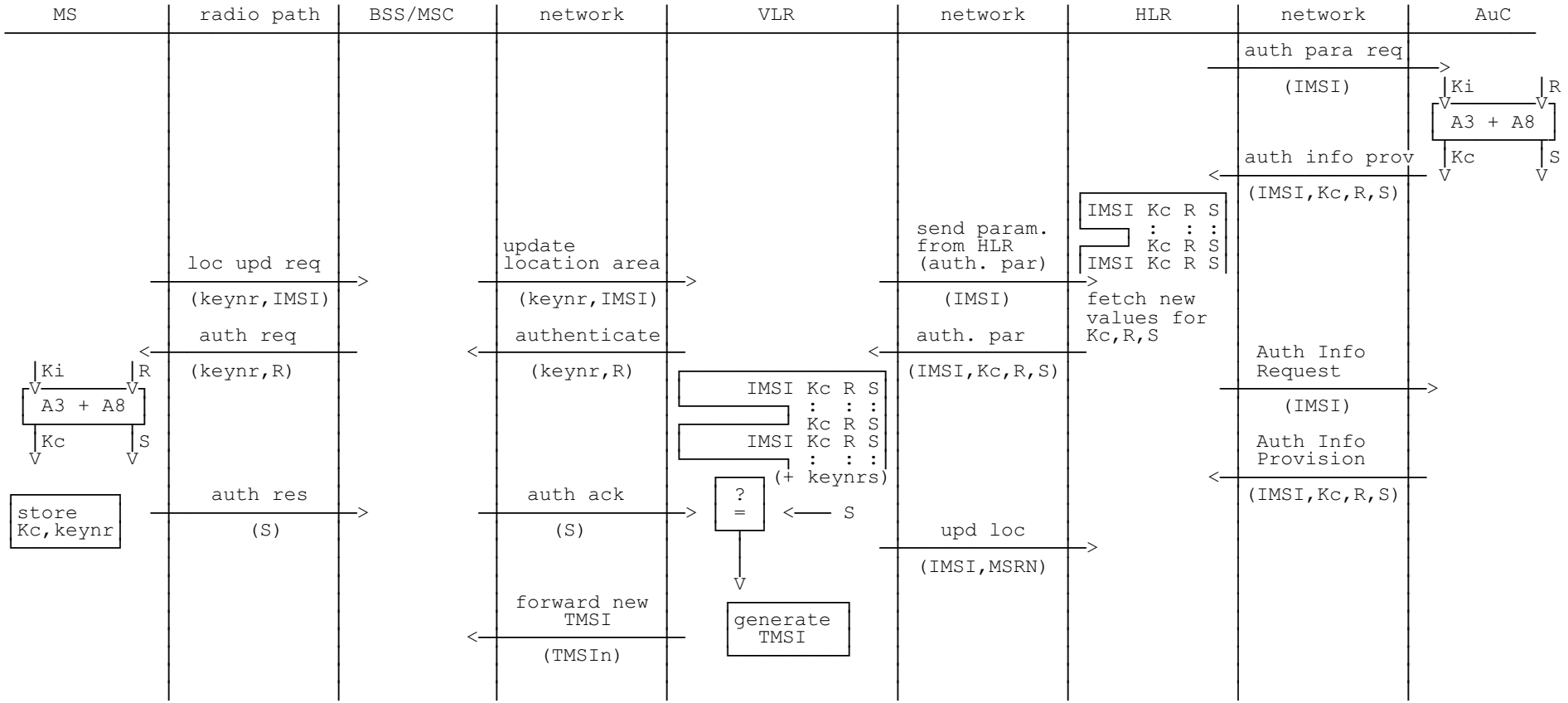
Scheme 7: Call set-up
- mobile terminated;
- early assignment.
  A paging request is sent to the registered MS, addressed by the TMSI. All signalling information elements in all messages on the radio path are encrypted with ciphering key Kc after the cipher mode command message. The PLMN is setting up calls with "early assignment".

A.3 List of abbreviations

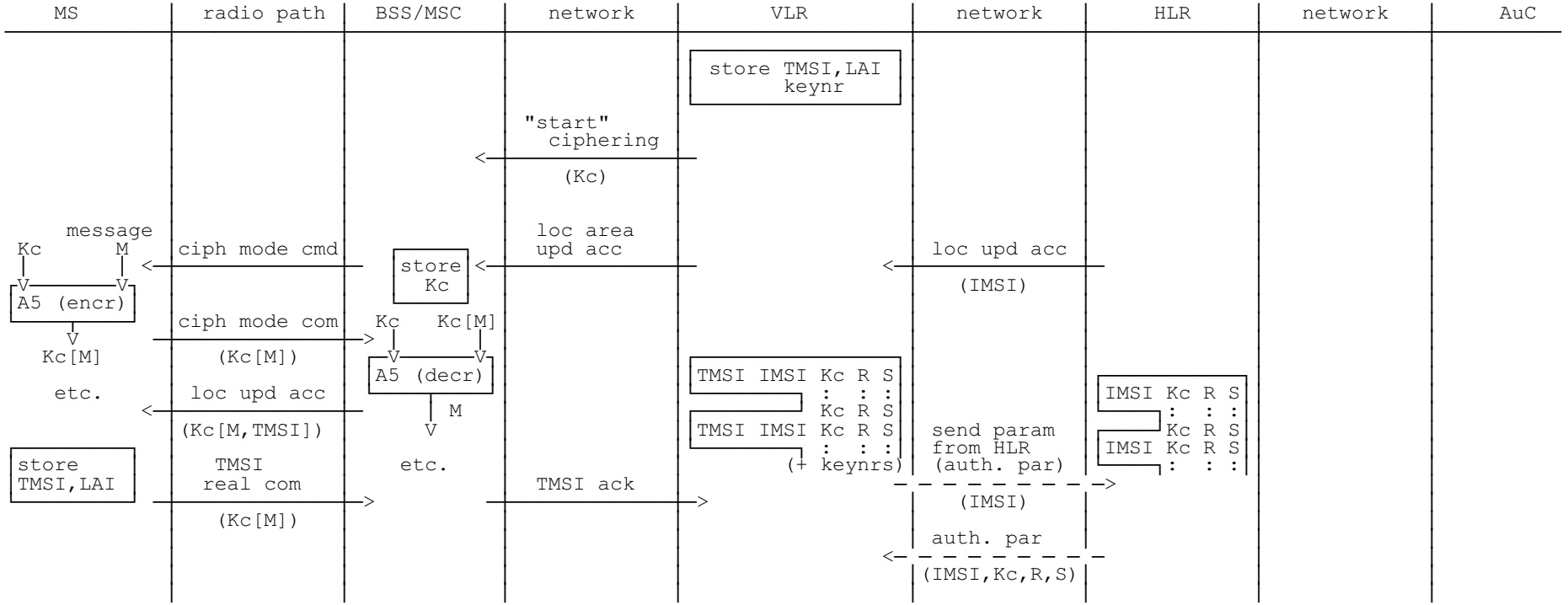
In addition to the abbreviations listed in GSM 01.04, the following abbreviations are used in the schemes:

A3	authentication algorithm
A5	signalling data and user data encryption algorithm
A8	ciphering key generating algorithm
BSS	Base Station System
HLR	Home Location Register
IMSI	International Mobile Subscriber Identity
Kc	ciphering key
Kc[M]	message encrypted with ciphering key Kc
Kc[TMSI]	TMSI encrypted with ciphering key Kc
Ki	individual subscriber authentication key
LAI	Location Area Identity
MS	Mobile Station
MSC	Mobile services Switching Centre
R	Random number (RAND)
S	Signed response (SRES)
TMSI o/n	Temporary Mobile Subscriber Identity old/new
VLR o/n	Visitor Location Register old/new

Scheme 1 Location registration
- no TMSI available



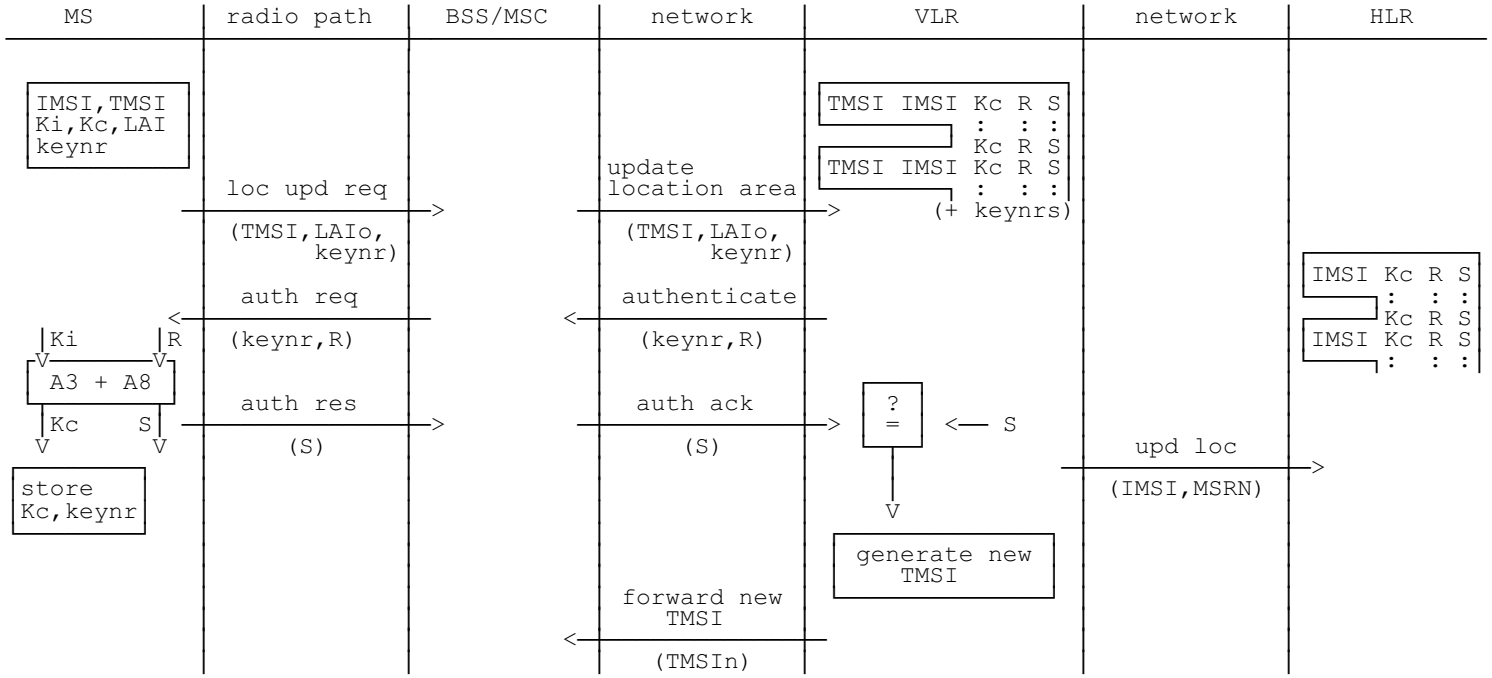
Scheme 1 (concluded)



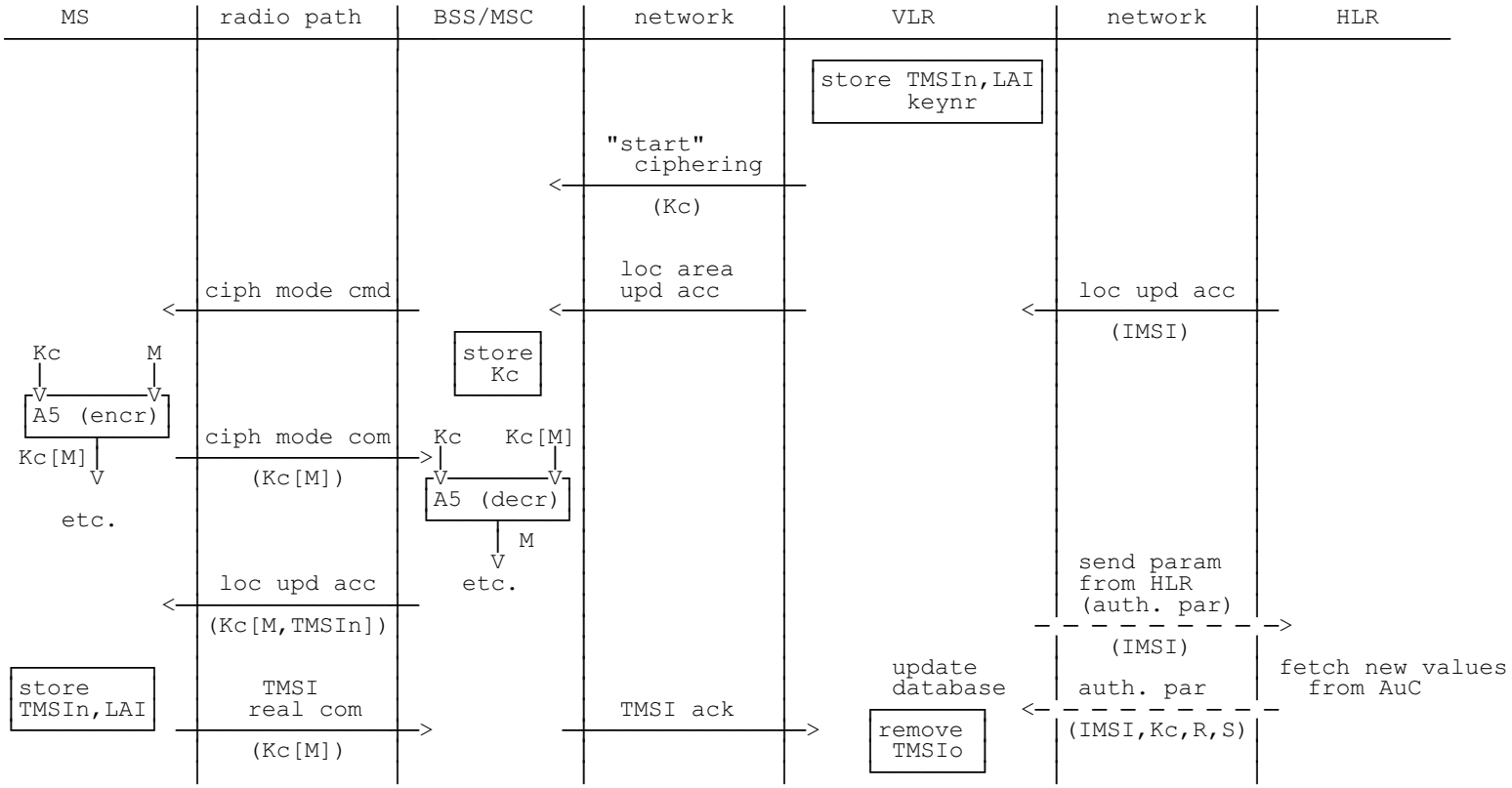
Scheme 2 Location updating

- MS registered in VLR

- TMSI is still available



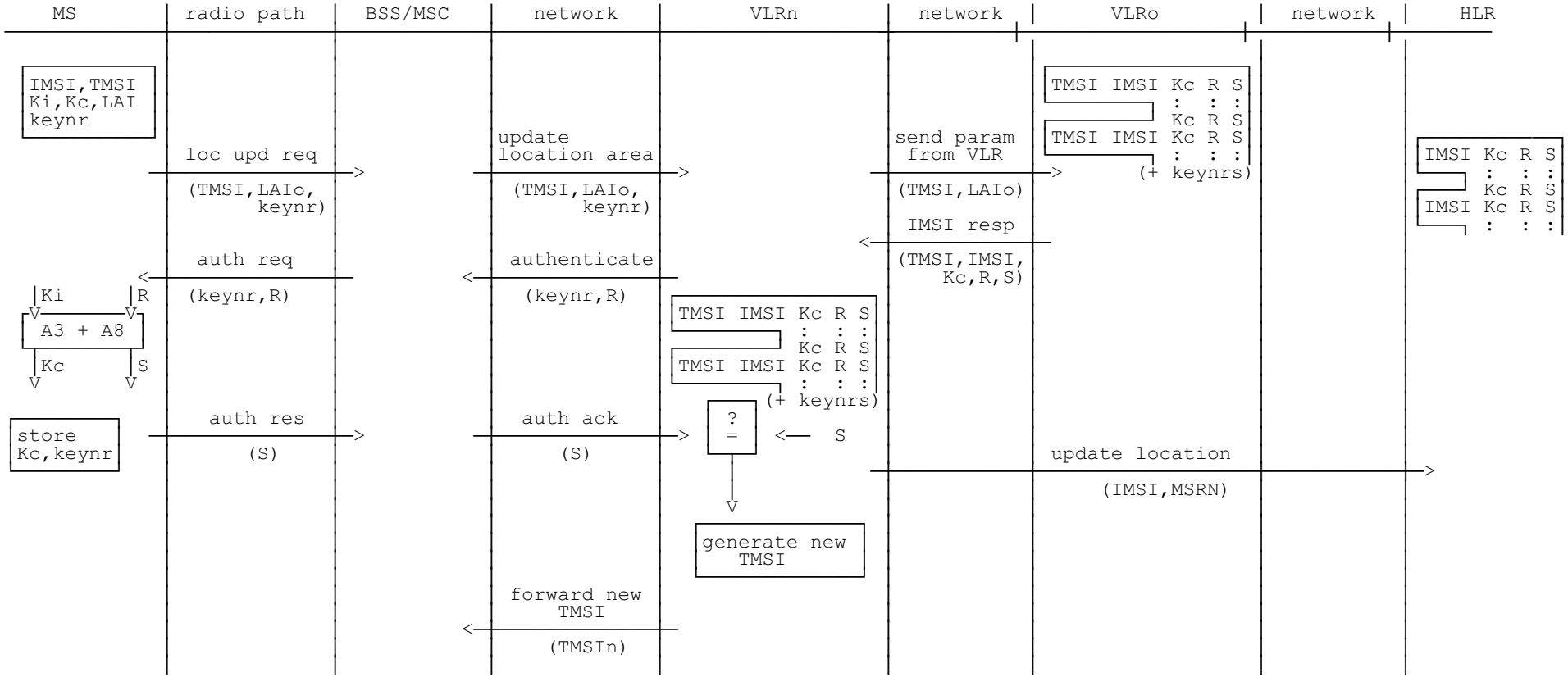
Scheme 2 (concluded)



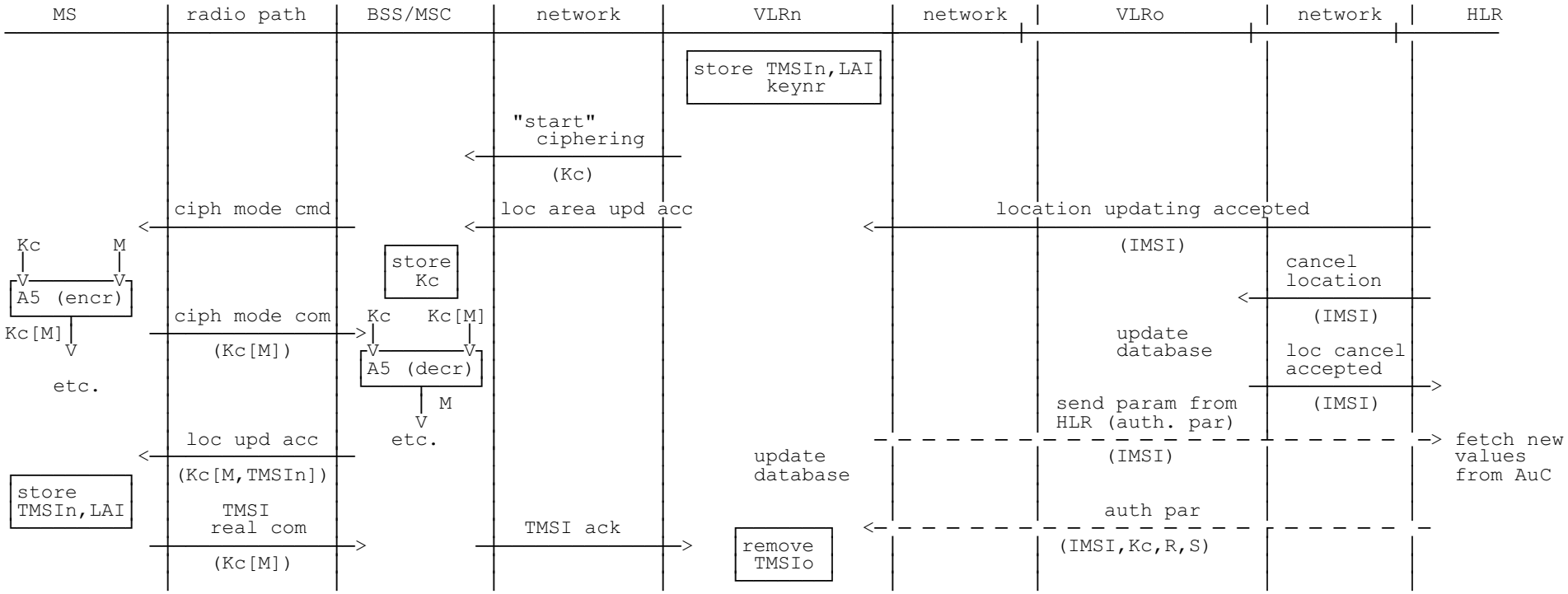
Scheme 3 Location updating

- MS not yet registered in VLR

- TMSI is still available

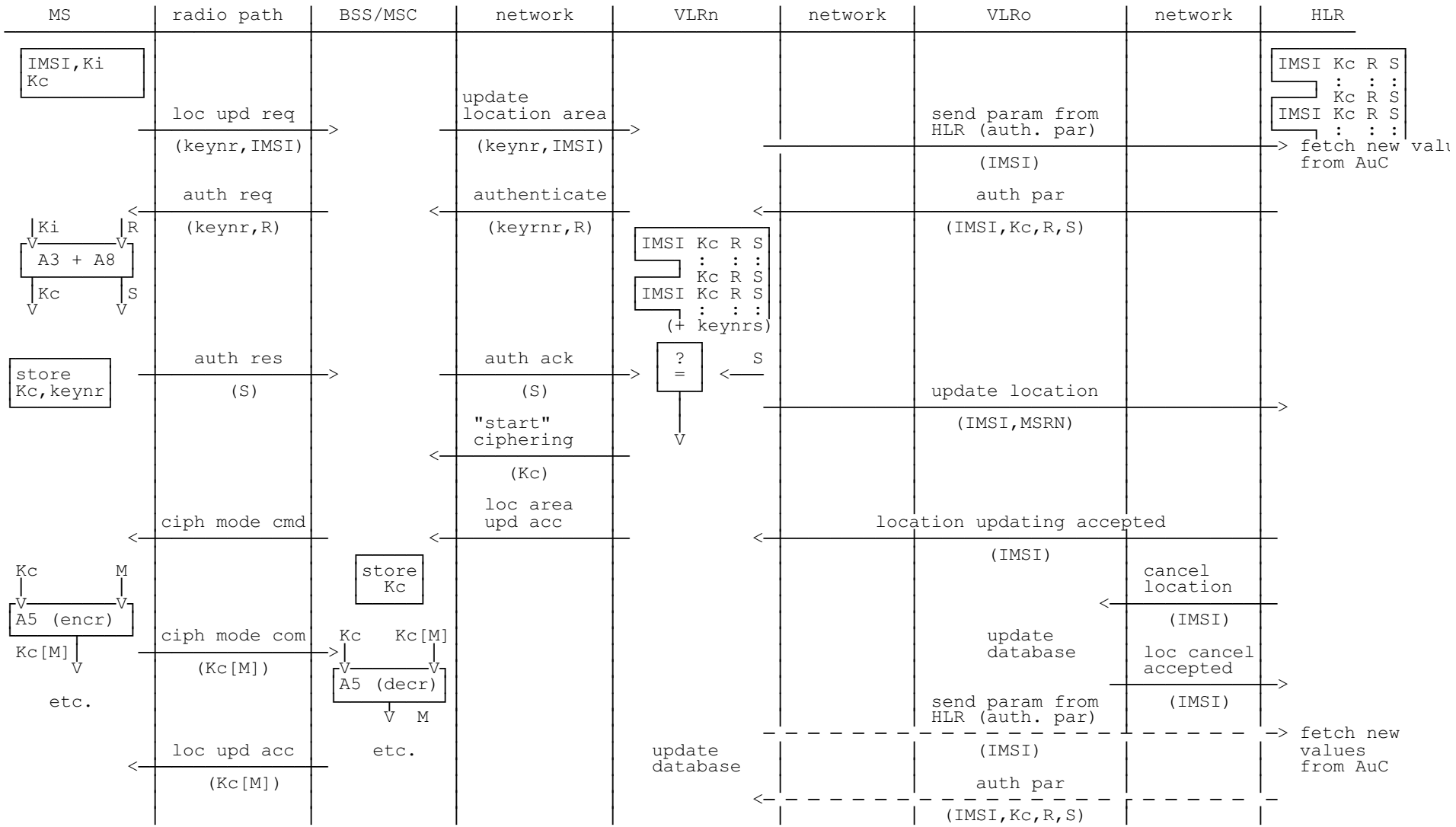


Scheme 3 (concluded)



Scheme 4 Location updating

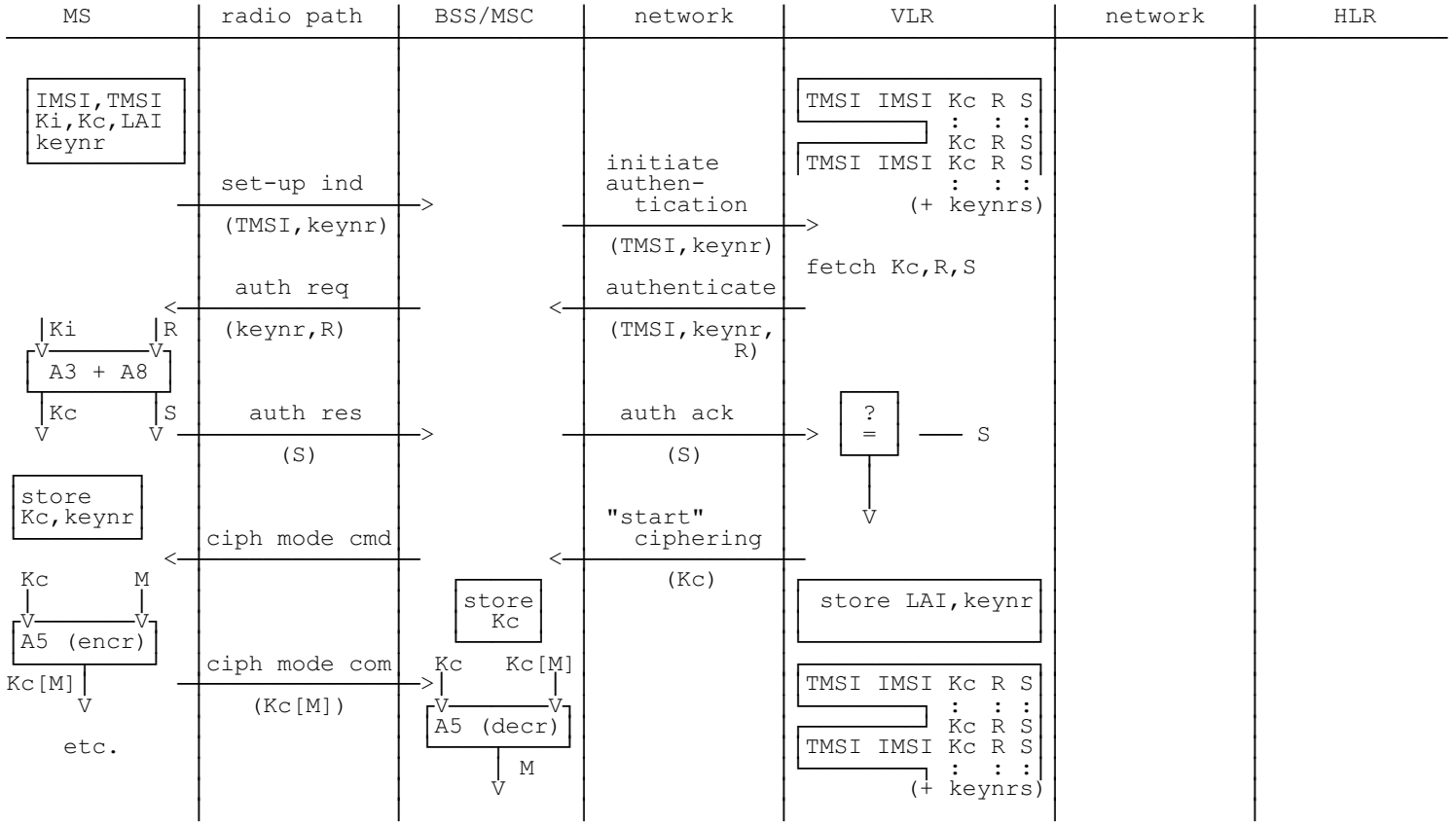
- MS not yet registered in VLR; no old LAI



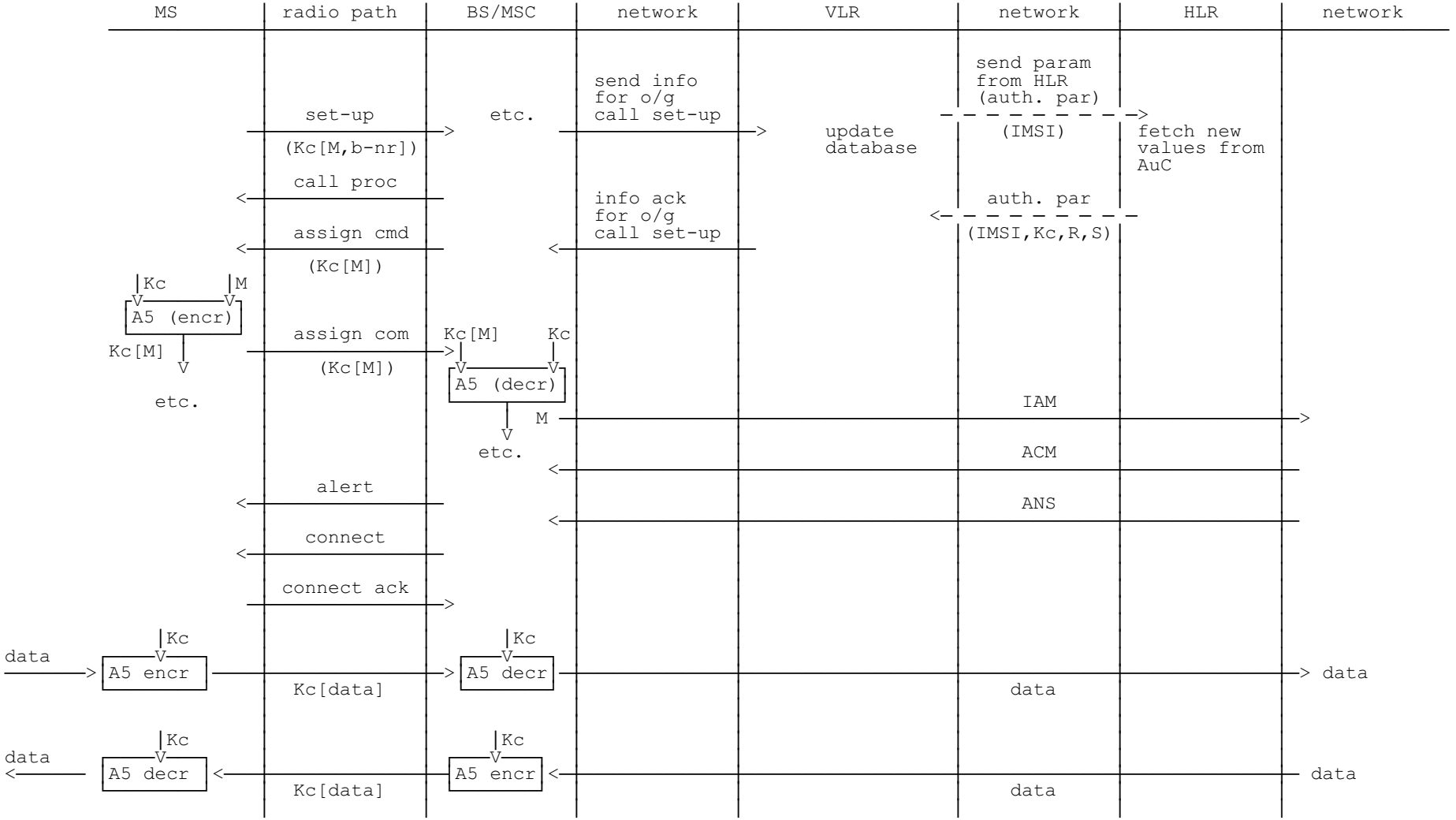
Scheme 5 Call set-up

- Mobile originated

- early assignment



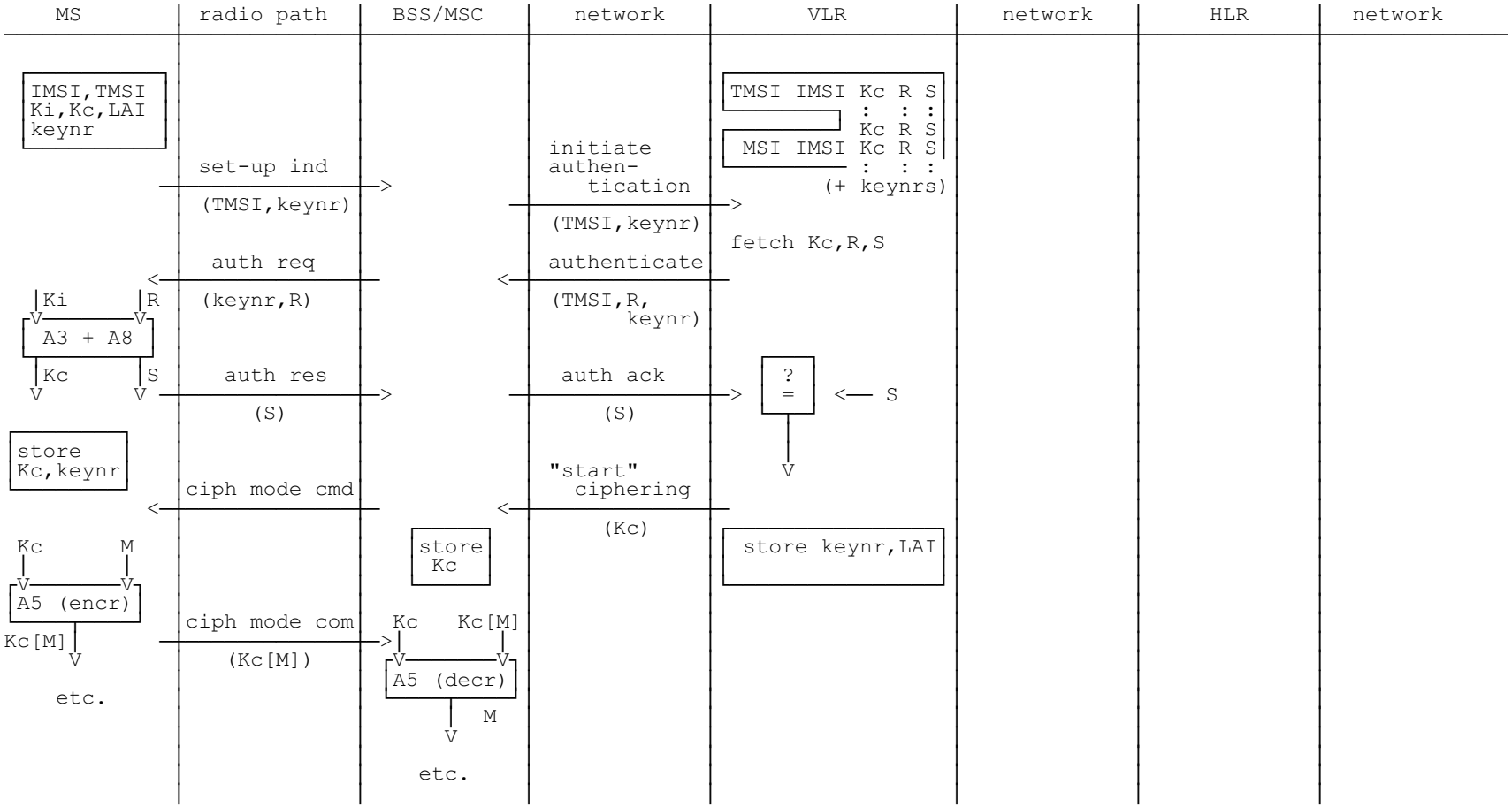
Scheme 5 (concluded)



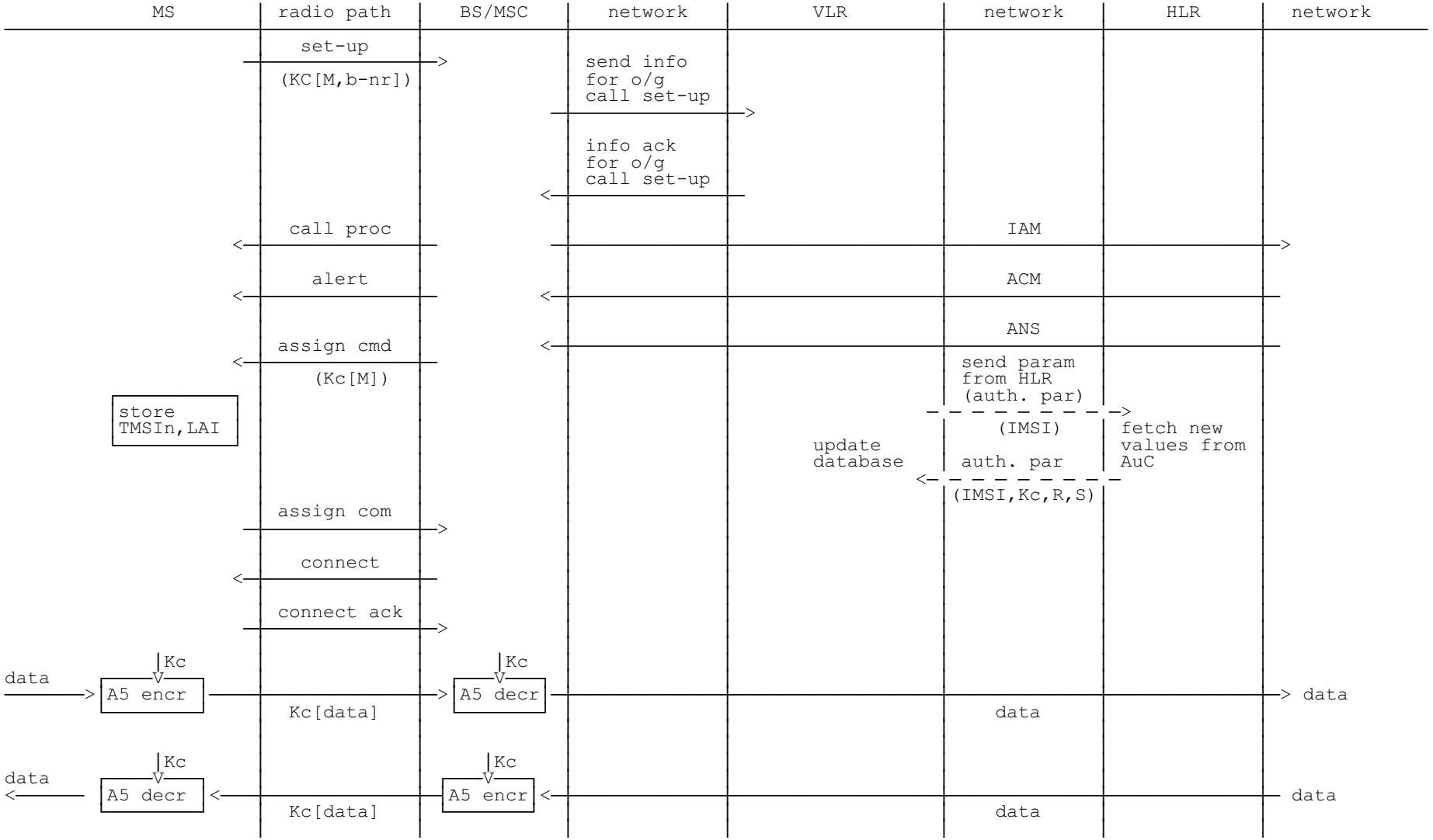
Scheme 6 Call set-up

- Mobile originated

- Off air call set-up



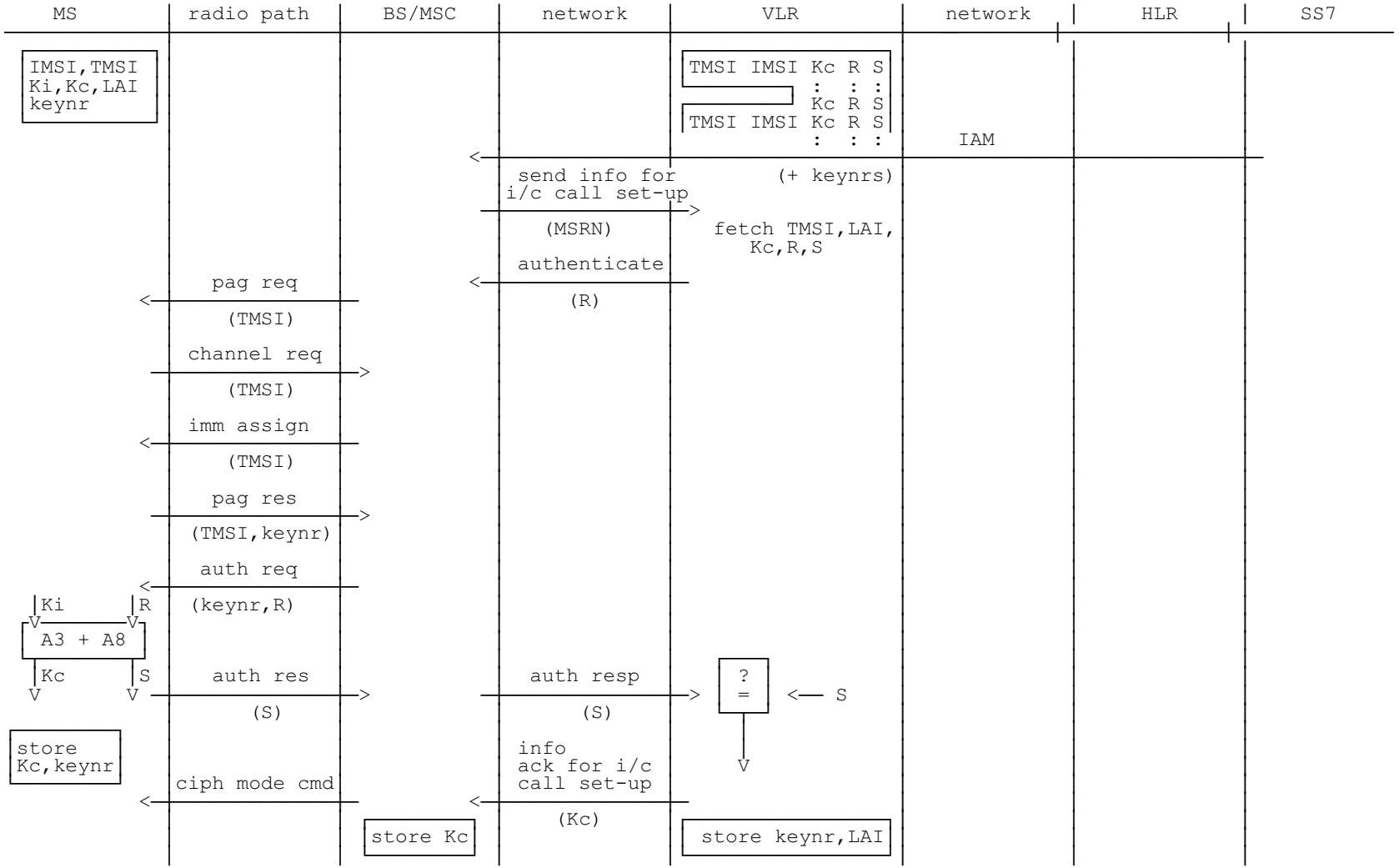
Scheme 6 (concluded)



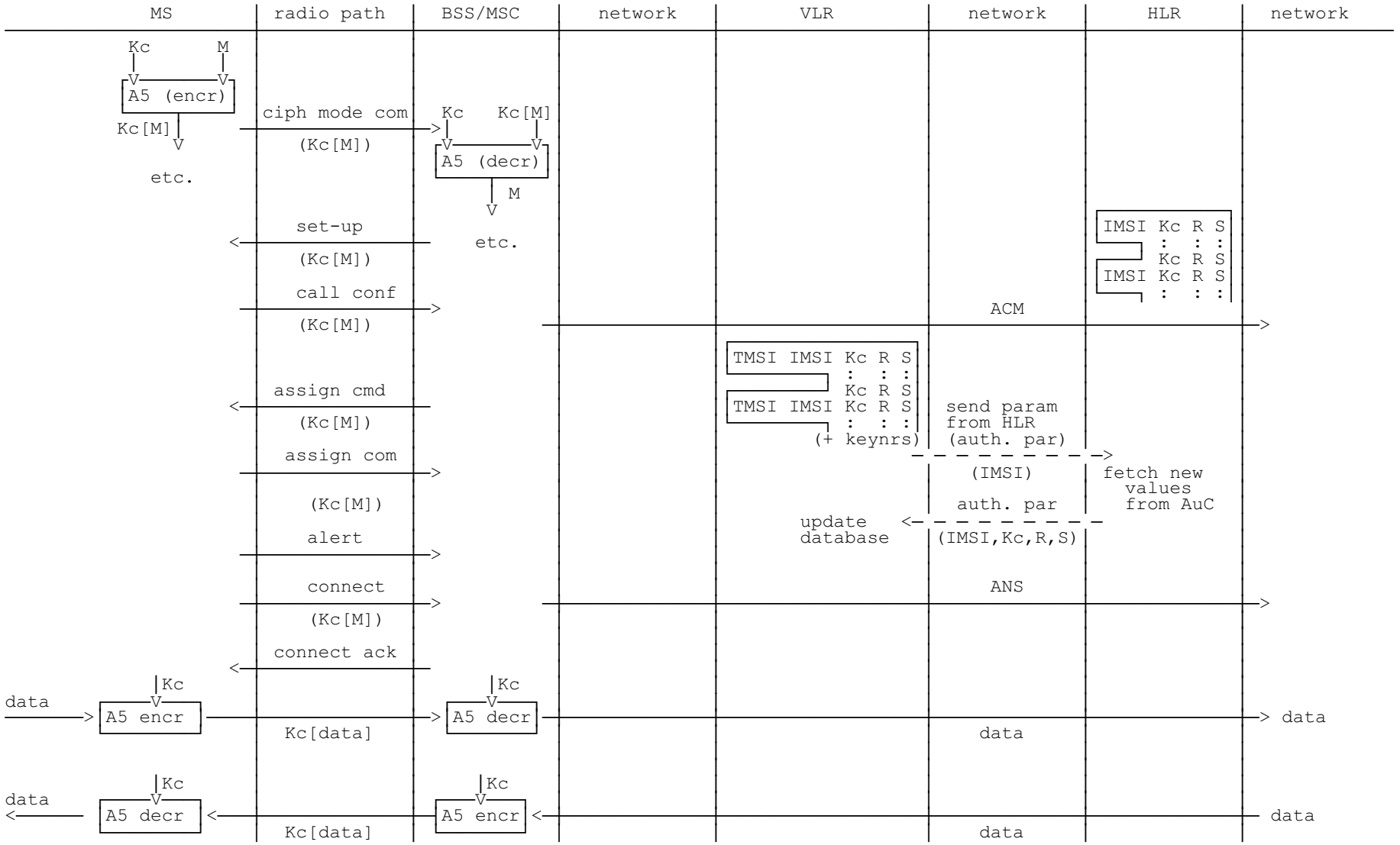
Scheme 7 Call set-up

- Mobile terminated

- Early assignment



Scheme 7 (concluded)



Annex B (informative): Security information to be stored in the entities of the GSM system

B.1 Introduction

This annex gives an overview of the security related information and the places where this information is stored in the GSM network.
The entities of the GSM network where security information is stored are:

- home location register;
- visitor location register;
- mobile services switching centre;
- base station system;
- mobile 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, 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 Centre (MSC)/Base Station System (BSS)

Encryption algorithm A5 is stored in the MSC/BSS.
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 Station (MS)

The mobile station stores permanently:
- authentication algorithm A3;
- encryption algorithm A5;
- ciphering key generating algorithm A8;
- individual subscriber authentication key Ki;
- ciphering key Kc;
- ciphering key sequence number;
- TMSI.

The mobile station generates and stores:
- ciphering key Kc.

The mobile station receives and stores:
- ciphering key sequence number;
- TMSI;
- 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 of each subscriber are stored in an authentication centre.

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

C.0 Scope

This annex specifies the cryptological algorithms which are needed to provide the various security features and mechanisms defined in, respectively, GSM 02.09 and GSM 03.20.
The following three algorithms are considered in GSM 03.20:

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

Algorithm A5 must be common to all GSM PLMNs and all mobile stations (in particular, to allow roaming). The external specifications of Algorithm A5 are defined in subclause C.1.3. The internal specifications of Algorithm A5 are managed under the responsibility of GSM/MoU; 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 must be specified. It is also desirable that the processing times of these algorithms remain below a maximum value. Proposals for Algorithm A3 and A8 are managed by GSM/MoU and available, for those PLMN operators who wish to use them, in response to an appropriate request.

C.1 Specifications for Algorithm A5

C.1.1 Purpose

As defined in GSM 03.20, Algorithm A5 realizes the protection of both user data and signalling information elements at the physical layer on the dedicated channels (TCH or DCCH).
Synchronization of both the enciphering and deciphering (especially at hand-over) must be guarantied.

C.1.2 Implementation indications

Algorithm A5 is implemented into both the MS and the BSS. On the BSS side description below assumes that one algorithm A5 is implemented for each physical channel (TCH or DCCH).
The ciphering takes place before modulation and after interleaving (see GSM 05.01); the deciphering takes place after demodulation symmetrically. Both enciphering and deciphering need Algorithm 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 114 bits. Then, each block is incorporated into a normal burst (see GSM 05.02) and transmitted during a time slot. According to GSM 05.03, the useful information bits into a block are numbered e0 to e56 and e59 to e115 (the flag bits e57 and e58 are ignored). Successive slots for a given physical channel are separated at least by a frame duration, approximately 4.615 ms (see GSM 05.01).

For ciphering, Algorithm A5 produces, each 4.615 ms, a sequence of 114 encipher/decipher bits (here called BLOCK) which is combined by a bit-wise modulo 2 addition with the 114-bit plain text block. The first encipher/decipher bit produced by A5 is added to e0, the second to e1 and so on. As an indication, the resulting 114-bit block is then applied to the burst builder (see GSM 05.01).
For each slot, deciphering is performed on the MS side with the first block (BLOCK1) of 114 bits produced by 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 A5 must produce two blocks of 114 bits (i.e. BLOCK1 and BLOCK2) each 4.615 ms.
Synchronization is guarantied by driving Algorithm A5 by an explicit time variable, COUNT, derived from the TDMA frame number. Therefore each 114-bit block produced by A5 depends only on the TDMA frame numbering and the ciphering key Kc.
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 A5. The coding of COUNT is shown in figure C.1.

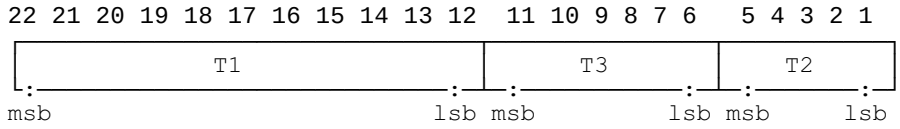


Figure C.1: The coding of COUNT

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 GSM 05.02).
Figure C.2 summarizes the implementation indications listed above, with only one enciphering/deciphering procedure represented (the second one for deciphering/enciphering is symmetrical).

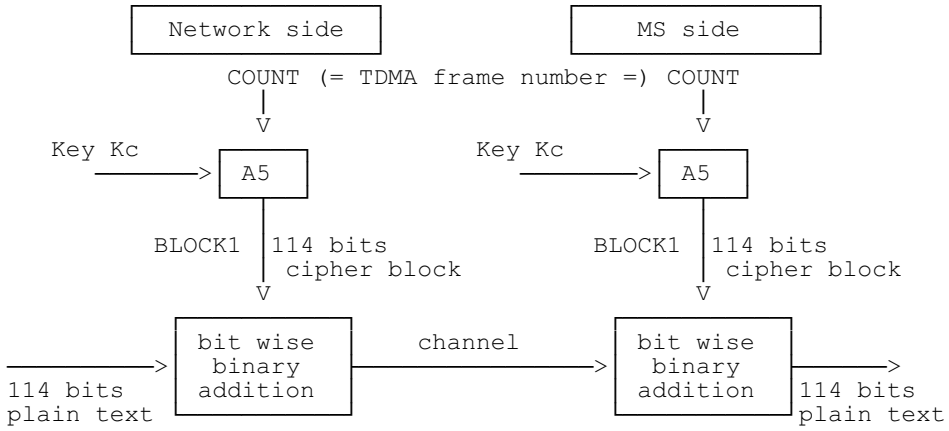


Figure C.2: Deciphering on the MS side

C.1.3 External specifications of Algorithm A5

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

- length of Kc: 64 bits;
- length of COUNT: 22 bits;
- length of BLOCK1: 114 bits;
- length of BLOCK2: 114 bits.

Algorithm A5 shall produce BLOCK1 and BLOCK2 in less than a TDMA frame duration, i.e. 4.615 ms.

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 A5

The internal specification of Algorithm A5 is managed under the responsibility of GSM/MoU; it will be made available to in response to an appropriate request.

C.2 Algorithm A3

Algorithm A3 is considered as a matter for GSM PLMN operators. Therefore, only external specifications are given. However a proposal for a possible Algorithm A3 is managed by GSM/MoU and available upon appropriate request.

C.2.1 Purpose

As defined in GSM 03.20, 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 MS side, Algorithm A3 is contained in a Subscriber Identity Module, as specified in GSM 02.17.
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 GSM PLMN operators as is Algorithm A3.
A proposal for a possible Algorithm A8 is managed by GSM/MoU and available upon appropriate request.

C.3.1 Purpose

As defined in GSM 03.20, 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 MS side, Algorithm A8 is contained in the SIM, as specified in GSM 02.17.
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.

Since the maximum length of the actual ciphering key is fixed by GSM/MoU, 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 has to considered to be 64 unstructured bits.

Annex D (normative): Security related network functions for General Packet Radio Service $(GPRS)$

This annex is only applicable if GPRS is supported.

D.1 General

This annex gives an overview of the different security related services and functions for General Packet Radio Service (GPRS) which is described in GSM 02.60 and GSM 03.60. They are grouped as follows:

- Subscriber identity confidentiality;
- Subscriber identity authentication;
- Confidentiality of user information and signalling between MS and SGSN;
- Security of the GPRS backbone.

It shall be possible to introduce new authentication and ciphering algorithms during the systems lifetime. The fixed part of the network may support more than one authentication and ciphering algorithm.
The security procedures include mechanisms to enable recovery in the event of signalling failures. These recovery procedures are designed to minimise the risk of a breach in the security of the system.
In this annex, the terms GPRS-Kc and GPRS-CKSN are introduced to provide a clear distinction from the ciphering parameters (Kc and CKSN) used for circuit switched. The GPRS-Kc is the ciphering key used for GPRS, and GPRS-CKSN is the corresponding Ciphering Key Sequence Number used for GPRS. The use of these parameters is described in clause D.4.

D.2 Subscriber identity confidentiality

D.2.1 Generality

The purpose of this function is to avoid the possibility for an intruder to identify which subscriber is using a given resource on the radio path by listening to the signalling exchanges or the user traffic on the radio path. This allows both a high level of confidentiality for user data and signalling and protection against the tracing of users location.
The provision of this function implies that the IMSI (International Mobile Subscriber Identity), 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 radio 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 radio path;
- the IMSI is not normally used as addressing means on the radio path (see GSM 02.09);
- when the signalling procedures permit it, signalling information elements that convey information about the mobile subscriber identity must be ciphered for transmission on the radio path.

The identifying method is specified in the following subclause. The ciphering of communication over the radio path is specified in clause D.4.
Furthermore, Anonymous Access allows a user to access the network without a subscriber identity (see GSM 03.60). Therefore, Anonymous Access always guarantees by its nature subscriber identity confidentiality. The following parts of the clause D.2 are not applicable for Anonymous Access.

D.2.2 Identifying method

The means used to identify a mobile subscriber on the radio path consists of a Temporary Logical Link Identity (TLLI). This TLLI is a local number, having a meaning only in a given RA (Routing Area); the TLLI must be accompanied by the Routing Area Identity (RAI) to avoid ambiguities. The maximum length and guidance for defining the format of a TLLI are specified in GSM 03.03.
The SGSN manages suitable data bases to keep the relation between TLLIs and IMSIs. When a TLLI is received with an RAI that does not correspond to the current SGSN, the IMSI of the MS must be requested from the SGSN in charge of the indicated routing area if its address is known; otherwise the IMSI is requested from the MS.

A new TLLI may be allocated in each routing area updating procedure. The allocation of a new TLLI corresponds implicitly for the MS to the de-allocation of the previous one. In the fixed part of the network, the cancellation of the record for an MS in a SGSN implies the de-allocation of the corresponding TLLI.
To cope with some malfunctioning, e.g. arising from a software failure, the fixed part of the network can require the identification of the MS in clear. This procedure is a breach in the provision of the service, and should be used only when necessary.
When a new TLLI is allocated to an MS, it is transmitted to the MS in a ciphered mode. This ciphered mode is the same as defined in clause D.4.
The MS must store its current TLLI in a non volatile memory, together with the RAI, so that these data are not lost when the MS is switched off.

D.2.3 Procedures

This subclause presents the procedures, or elements of procedures, pertaining to the management of TLLIs.
These security procedures may also be applied between two PLMNs of different operators for seamless service when the PLMN is changed.

D.2.3.1 Routing area updating in the same SGSN area

This procedure is part of the routing area updating procedure which takes place when the original routing area and the new routing area depend on the same SGSN. The part of this procedure relative to TLLI management is reduced to a TLLI re-allocation (from TLLIo with "o" for "old" to TLLIn with "n" for "new").
The MS sends TLLIo as an identifying field at the beginning of the routing area updating procedure.
The procedure is schematised in figure D.2.1.

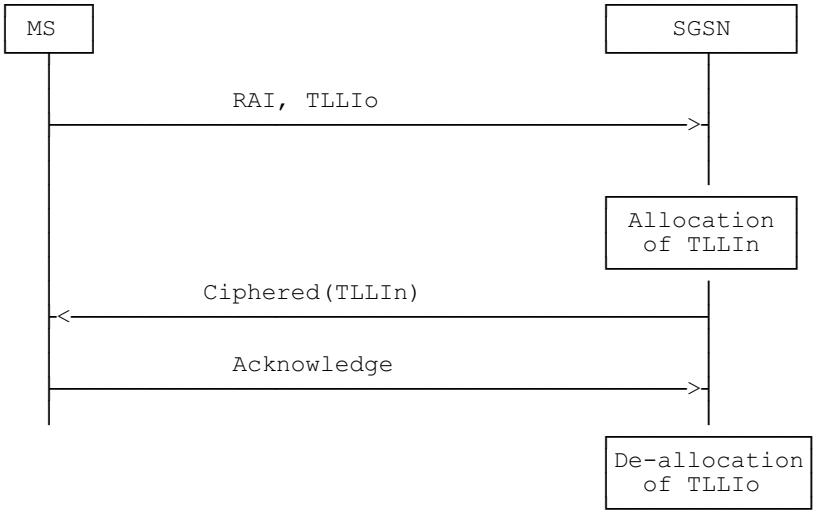
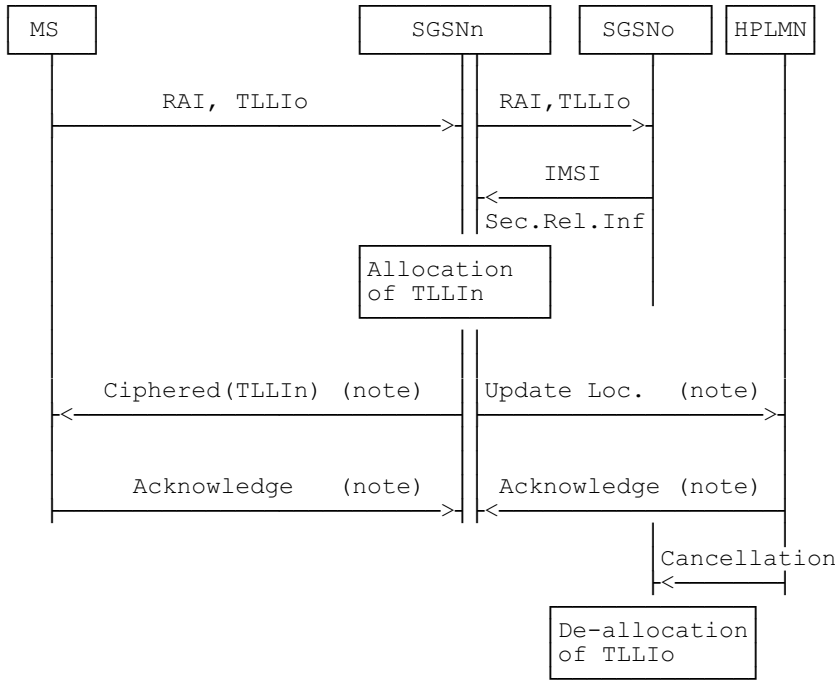


Figure D.2.1: Routing area updating in the same SGSN area

D.2.3.2 Routing area updating in a new SGSN; old SGSN reachable

This procedure is part of the routing area updating procedure, using TLLI and RAI, when the original routing area and the new routing area depend on different SGSNs.
The MS is still registered in SGSNo ("o" for old or original) and requests registration in SGSNn ("n" for new). RAI and TLLIo are sent by the MS as identifying fields during the routing area updating procedure. The Routing Area Update Request is not ciphered to allow the new SGSN to read RAI and TLLIo.
The procedure is schematised in figure D.2.2.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure D.2.2: Routing area updating in a new SGSN; old SGSN reachable

Signalling functionalities:

Update Loc. stands for Update Location

The new SGSN informs the HLR that it is now handling the MS.

Sec.Rel.Info.:

Stands for Security Related information

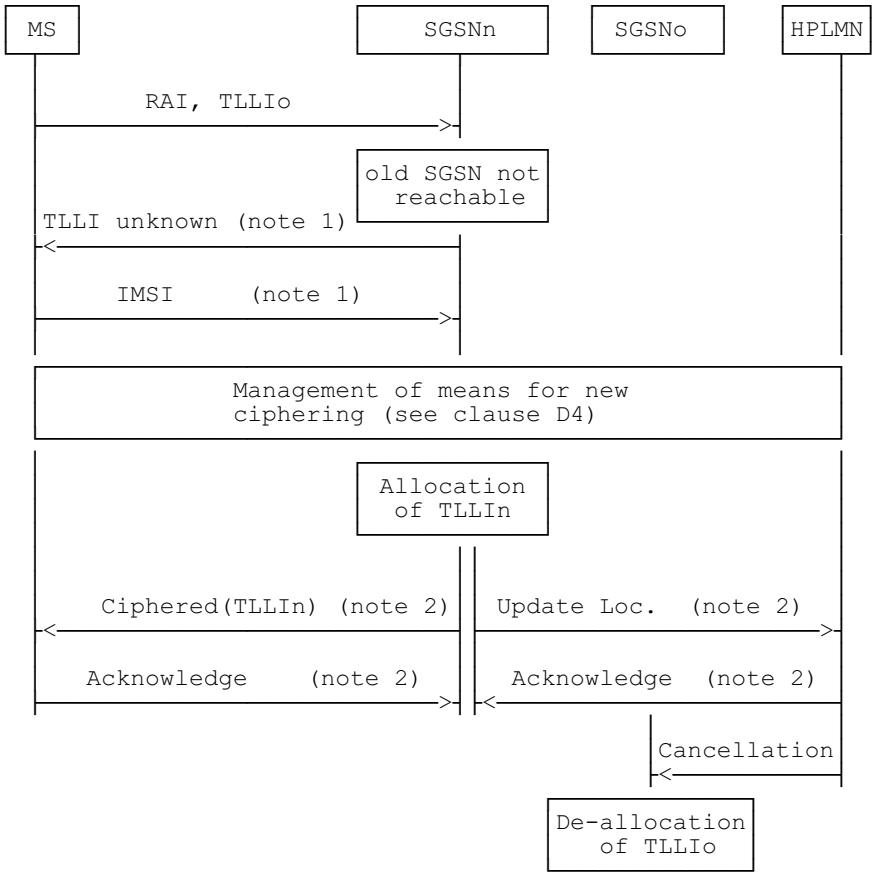
The SGSNn needs some information for authentication and ciphering; this information is obtained from SGSNo.

Cancellation:

The HLR indicates to SGSNo that the MS is now under control of another SGSN. The "old" TLLI is free for allocation.

D.2.3.3 Routing area updating in a new SGSN; old SGSN not reachable

This variant of the procedure in subclause D.2.3.2 arises when the SGSN receiving the RAI and TLLIo cannot identify the SGSNo. In that case the relation between TLLIo and IMSI is lost, and the identification of the MS in clear is necessary. The procedure is schematised in figure D.2.3.



NOTE 1: From a security point of view, the exact signalling messages (described in GSM 03.60) used to indicate that the TLLI is unknown, or to send the IMSI are irrelevant.

NOTE 2: From a security point of view, the order of the procedures is irrelevant.

Figure D.2.3: Routing area updating in a new SGSN; old SGSN not reachable

D.2.3.4 Reallocation of a TLLI

This function may be initiated by the network at any time for a GPRS attached MS. The procedure can be included in other procedures, e.g. through the means of optional parameters. The execution of this function is left to the network operator. When a new TLLI is allocated to an MS the network must prevent the old TLLI from being allocated again until the MS has acknowledged the allocation of the new TLLI.
If an MM context of an MS is deleted in the SGSN by O&M action, the network must prevent any TLLI associated with the deleted MM context from being allocated again until a new TLLI is successfully allocated to that IMSI.
If an IMSI record is deleted in the HLR by O&M action, it is not possible to prevent any TLLI associated with the IMSI record from being allocated again. However, if the MS whose IMSI record was deleted should attempt to access the network using the TLLI after the TLLI has been allocated to a different IMSI, then authentication or ciphering of the MS whose IMSI was deleted will fail, which will cause the TLLI to be deleted from the MS.
The case where allocation of a new TLLI is unsuccessful is described in subclause D.2.3.7.
This procedure is schematised in figure D.2.4.

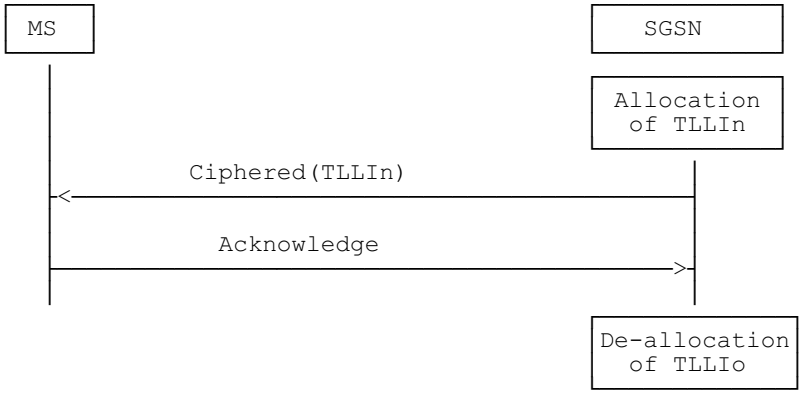
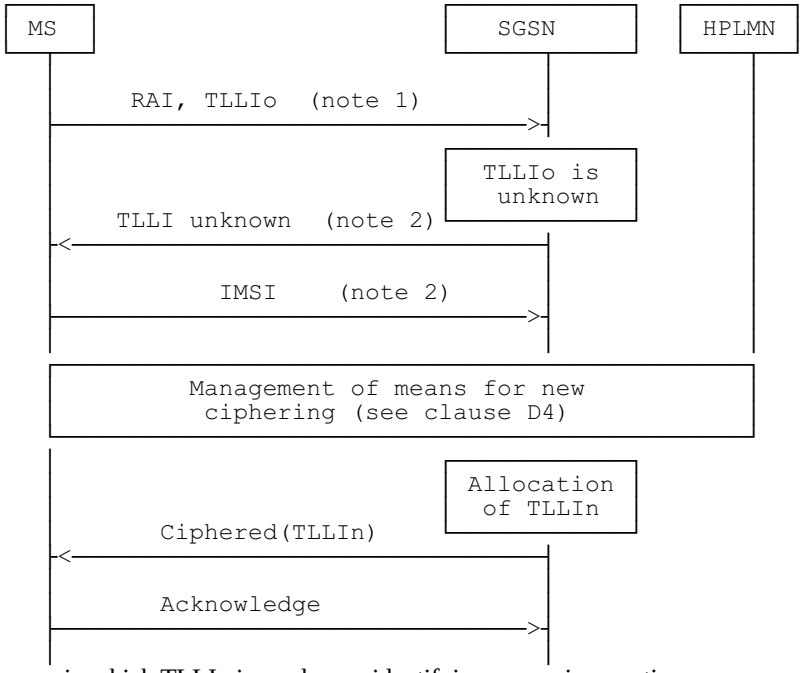


Figure D.2.4: Reallocation of a new TLLI

D.2.3.5 Local TLLI unknown

This procedure is a variant of the procedure described in subclauses D.2.3.1 and happens when a data loss has occurred in a SGSN and when a MS uses an unknown TLLI, e.g. for a communication request or for a routing area updating request in a routing area managed by the same SGSN. The SGSN indicates to the MS that the TLLI is unknown and and the identification of the MS in clear is necessary.
This procedure is schematised in figure D.2.5.

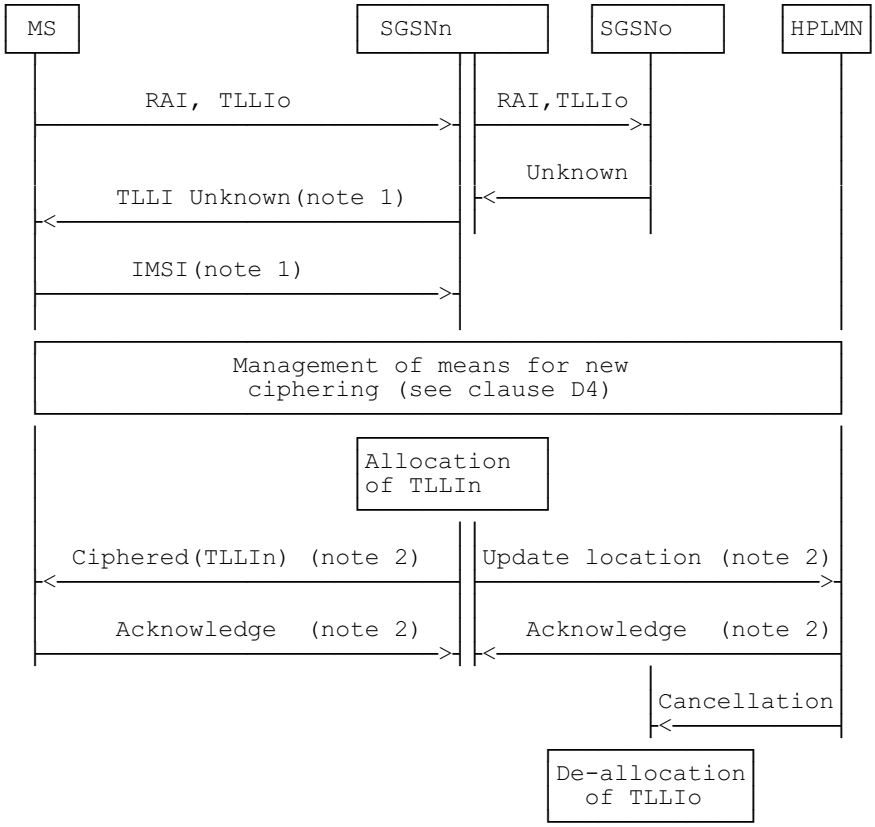


NOTE 1: Any message in which TLLIo is used as an identifying means in a routing area managed by the same SGSN.
NOTE 2: From a security point of view, the exact signalling messages (described in GSM 03.60) used to indicate that the TLLI is unknown, or to send the IMSI are irrelevant.

Figure D.2.5: Routing area updating in the same SGSN area; local TLLI unknown

D.2.3.6 Routing area updating in a new SGSN in case of a loss of information

This variant of the procedure described in D.2.3.2 arises when the SGSN in charge of the MS has suffered a loss of data. In that case the relation between TLLIo and IMSI is lost, and the identification of the MS in clear is necessary.
The procedure is schematised in figure D.2.6.



NOTE 1: From a security point of view, the exact signalling messages (described in GSM 03.60) used to indicate that the TLLI is unknown, or to send the IMSI are irrelevant.
NOTE 2: From a security point of view, the order of the procedures is irrelevant.

Figure D.2.6: Routing area updating in a new SGSN in case of a loss of information

D.2.3.7 Unsuccessful TLLI allocation

If the MS does not acknowledge the allocation of a new TLLI, the network shall maintain the association between the old TLLI and the IMSI and between the new TLLI and the IMSI.
For an MS-originated transaction, the network shall allow the MS to identify itself by either the old TLLI or the new TLLI. This will allow the network to determine the TLLI stored in the MS; the association between the other TLLI and the IMSI shall then be deleted.
For a network-originated transaction, the network shall identify the MS by its IMSI. When radio contact has been established, the network shall instruct the MS to delete any stored TLLI. When the MS has acknowledged this instruction, the network shall delete the association between the IMSI of the MS and any TLLI.
In either of the cases above, the network may initiate the normal TLLI reallocation procedure.
Repeated failure of TLLI reallocation (passing a limit set by the operator) may be reported for O&M action.

D.3 Subscriber identity authentication

D.3.1 Generality

The definition and operational requirements of subscriber identity authentication are given in GSM 02.09.
The authentication procedure may be performed at any time by the network.
The authentication procedure will also be used to set the ciphering key (see clause D.4). Therefore, it is performed after the subscriber identity (TLLI/IMSI) is known by the network for the management of new ciphering.
Two network functions are necessary: the authentication procedure itself, and the key management.

D.3.2 The authentication procedure

The authentication procedure is described in subclause 3.2.

D.3.3 Subscriber Authentication Key management

The management of Subscriber Authentication Key (Ki) is described in subclause 3.3.

D.3.3.1 General authentication procedure

When needed, the SGSN requests security related information for a MS from the HLR/AuC corresponding to the IMSI of the MS. 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 3.1. The pairs are stored in the SGSN as part of the security related information.
The procedure used for updating the vectors RAND/SRES is schematised in figure D.3.2.

NOTE: The Authentication Vector Response contains also GPRS-Kc(1..n) which is not shown in this and the following figures. For discussion of GPRS-Kc see clause D.4.

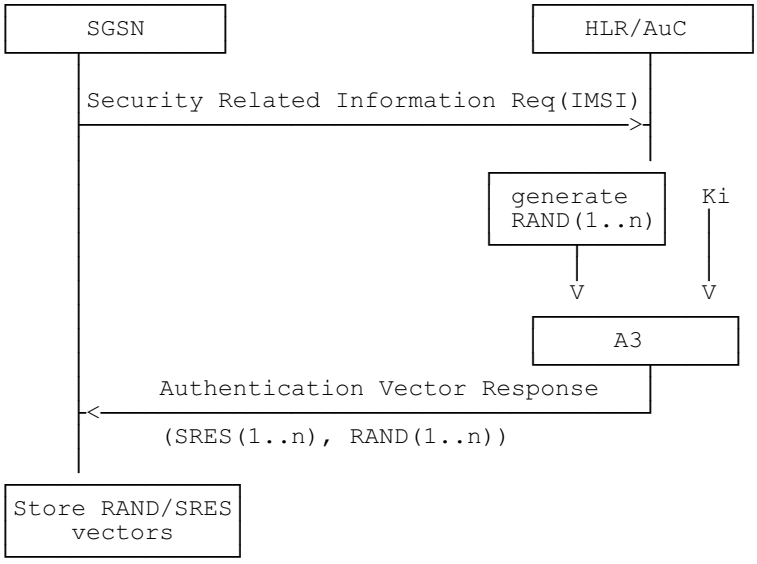


Figure D.3.2: Procedure for updating the vectors RAND/SRES

When an SGSN performs an authentication, including the case of a routing area updating within the same SGSN area, it chooses a RAND value in the array corresponding to the MS. It then tests the answer from the MS by comparing it with the corresponding SRES, as schematised in figure D.3.3.

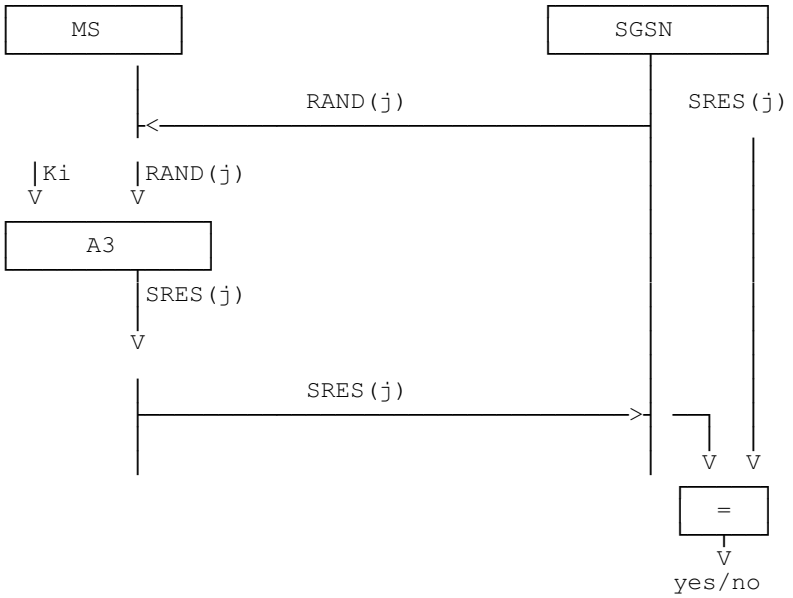


Figure D.3.3: General authentication procedure

D.3.3.2 Authentication at routing area updating in a new SGSN, using TLLI

During routing area updating in a new SGSN (SGSNn), the procedure to get pairs for subsequent authentication may differ from that described in the previous subclause. In the case when identification is done using TLLI, pairs for authentication as part of security related information are given by the old SGSN (SGSNo). The old SGSN shall send to the new SGSN only those pairs which have not been used. SGSNn may also request the triplets directly from HLR.
The procedure is schematised in figure D.3.4.

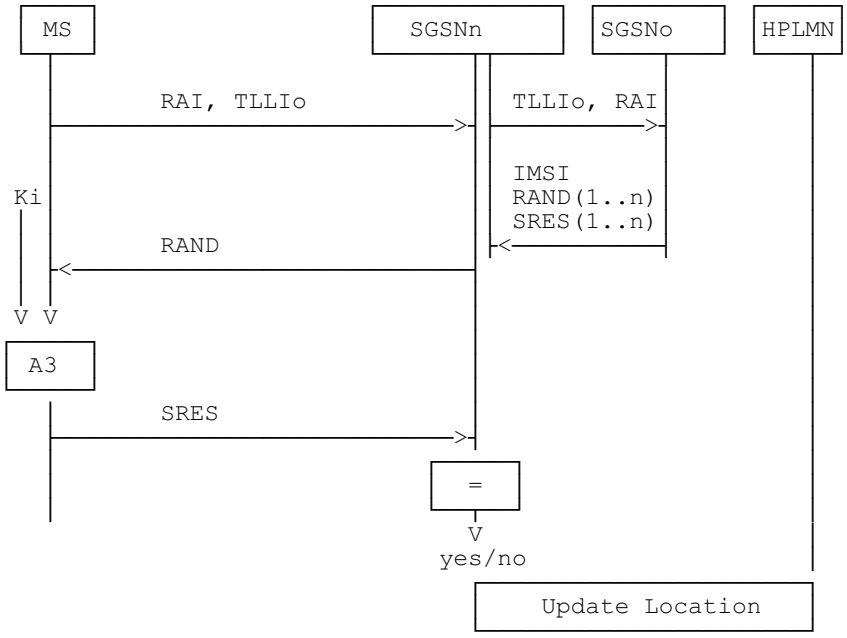


Figure D.3.4: Authentication at routing area updating in a new SGSN, using TLLI

D.3.3.3 Authentication at routing area updating in a new SGSN, using IMSI

When the IMSI is used for identification, or more generally when the old SGSN is not reachable, the procedure described in subclause D.3.3.2 cannot be used. Instead, pairs of RAND/SRES contained in the security related information are requested directly from the HPLMN.
The procedure is schematised in figure D.3.5.

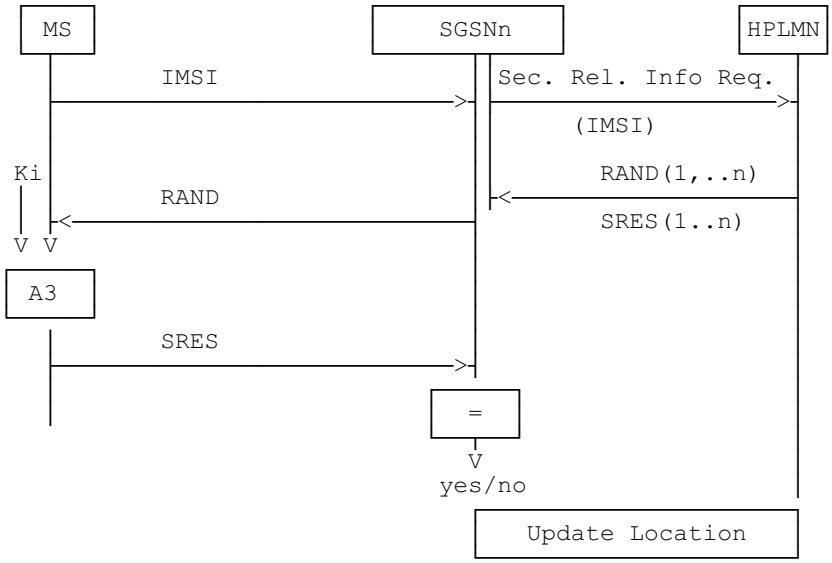


Figure D.3.5: Authentication at routing area updating in a new SGSN, using IMSI

D.3.3.4 Authentication at routing area updating in a new SGSN, using TLLI, TLLI unknown in 'old' SGSN

This case is an abnormal one, when a data loss has occurred in the 'old' SGSN.
The procedure is schematised in figure D.3.6.

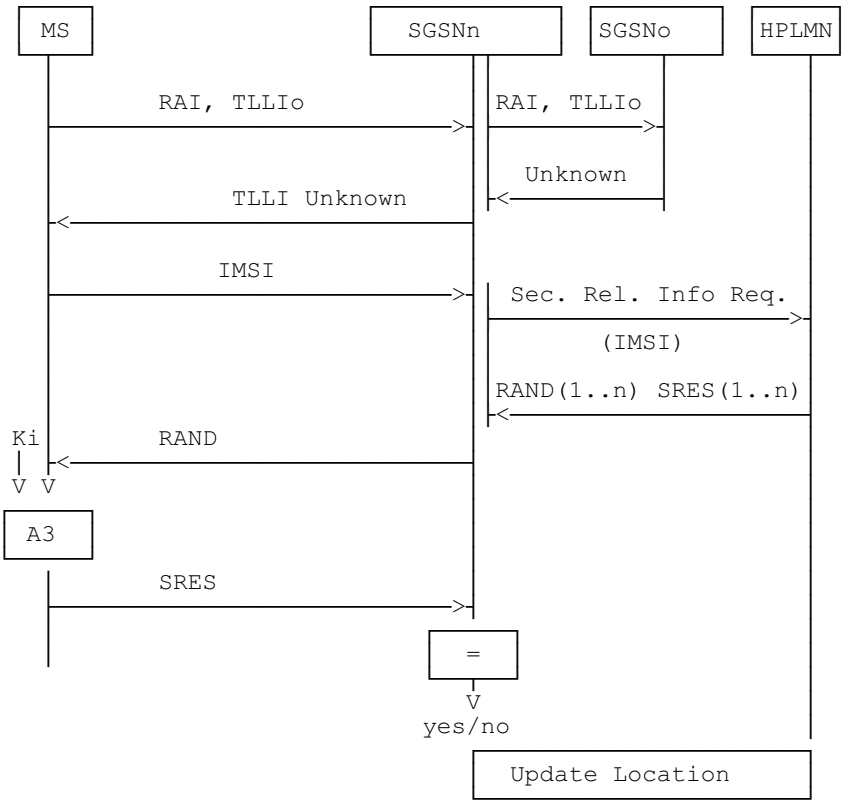


Figure D.3.6: Authentication at routing area updating in a new SGSN, using TLLI, TLLI unknown in 'old' SGSN

D.3.3.5 Authentication at routing area updating in a new SGSN, using TLLI, old SGSN not reachable

The case occurs when an old SGSN cannot be reached by the new SGSN.
The procedure is schematised in figure D.3.7

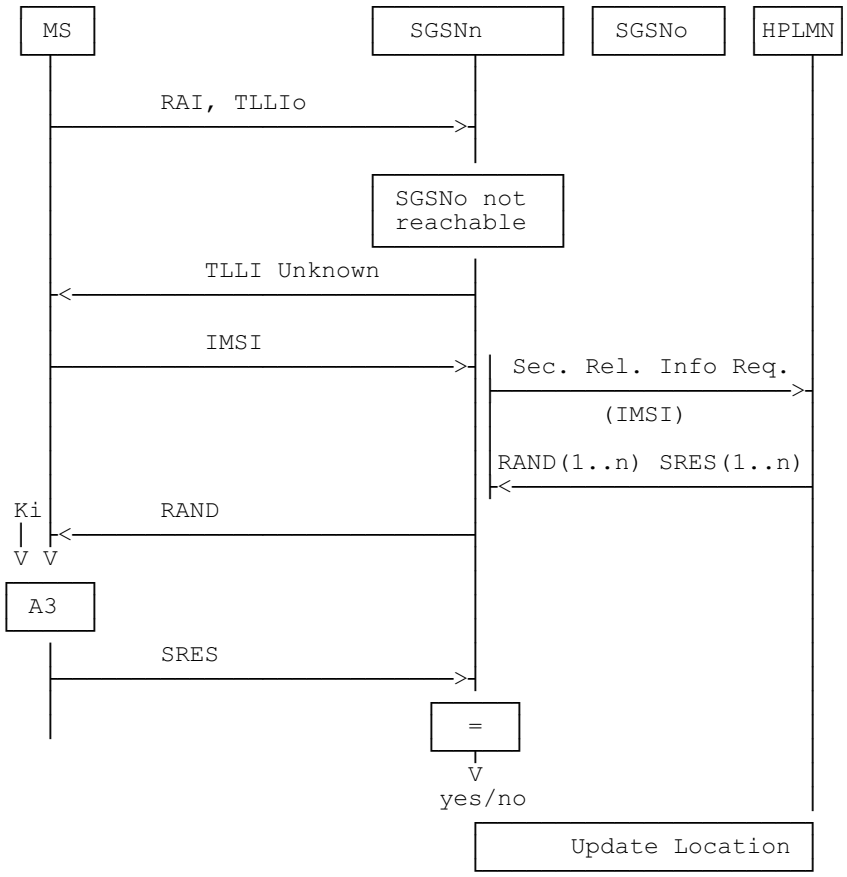


Figure D.3.7: Authentication at routing area updating in a new SGSN, using TLLI, old SGSN not reachable

D.3.3.6 Authentication with IMSI if authentication with TLLI fails

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

D.3.3.7 Re-use of security related information in failure situations

Security related information consisting of sets of RAND, SRES and a ciphering key (GPRS-Kc) is stored in the SGSN and in the HLR.
When a SGSN has used a set of security related information to authenticate an MS, it shall delete the set of security related information or mark it as used. When a SGSN 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 SGSN 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 SGSN; 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 SGSN successfully requests security related information from the HLR, it shall discard any security related information which is marked as used in the SGSN.
If a SGSN receives from another SGSN 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 send 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.

D.4 Confidentiality of user information and signalling between MS and SGSN

D.4.1 Generality

In GSM 02.09, some signalling information elements are considered sensitive and must be protected.
To ensure identity confidentiality (see clause 2), the new TLLI must be transferred in a protected mode at allocation time.
The confidentiality of user information concerns the information transmitted on the logical connection between MS and SGSN.
These needs for a protected mode of transmission are fulfilled by a ciphering function in the LLC layer. It is not an end-to-end confidentiality service.
Four points have to be specified:

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

D.4.2 The ciphering method

The LLC layer information flow is ciphered by the algorithm GPRS-A5 as described in GSM 01.61.

D.4.3 Key setting

Mutual key setting is the procedure that allows the mobile station and the network to agree on the key GPRS-Kc to use in the ciphering and deciphering algorithms GPRS-A5. This procedure corresponds to the procedure described in subclause 4.3 besides the different confidential subscriber identity. The GPRS-Kc is handled by the SGSN independently from the MSC. If a MS is using both circuit switched and packet switched, two different ciphering keys will be used independently, one (Kc) in the MSC and one (GPRS-Kc) in the SGSN.
A key setting is triggered by the authentication procedure. Key setting may be initiated by the network as often as the network operator wishes. If an authentication procedure is performed during a data transfer, the new ciphering parameters shall be taken in use immediately at the end of the authentication procedure in both SGSN and MS.
Key setting may not be encrypted and shall be performed as soon as the identity of the mobile subscriber (i.e. TLLI or IMSI) is known by the network.
The transmission of GPRS-Kc to the MS is indirect and uses the authentication RAND value; GPRS-Kc is derived from RAND by using algorithm A8 and the Subscriber Authentication key Ki, in the same way as defined in annex C for Kc.
As a consequence, the procedures for the management of GPRS-Kc are the authentication procedures described in subclause D.3.3.
The values GPRS-Kc are computed together with the SRES values. The security related information (see subclause D.3.3.1) consists of RAND, SRES and GPRS-Kc.
The key GPRS-Kc is stored by the mobile station until it is updated at the next authentication.
Key setting is schematised in figure D.4.1.

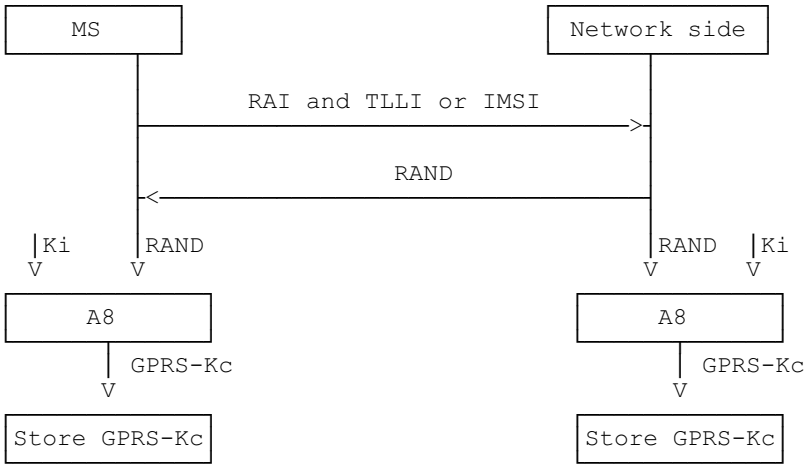


Figure D.4.1: Key setting

D.4.4 Ciphering key sequence number

The GPRS-CKSN (Ciphering Key Sequence Number) is a number which is associated with each ciphering key GPRS-Kc. The GPRS-CKSN and GPRS-Kc are stored together in the mobile station and in the network. It permits the consistency check of the keys stored in the MS and in the network. Two independent pairs, Kc and CKSN (for circuit switched), and GPRS-Kc and GPRS-CKSN (for packet switched) may be stored in the MS simultaneously.
However since it is not directly involved in any security mechanism, it is not addressed in this specification but in [GSM 04.08] instead.

D.4.5 Starting of the ciphering and deciphering processes

The MS and the SGSN must co-ordinate the instants at which the ciphering and deciphering processes start. The authentication procedure governs the start of ciphering. The SGSN indicates if ciphering shall be used or not in the authentication request message. If ciphering is used, the MS starts ciphering after sending the Authentication Response message. The SGSN starts ciphering when a valid Authentication Response is received from the MS.
As an option, the network may decide to start ciphering without authentication. Both the MS and the network shall use the latest ciphering parameters. The MS starts ciphering after a receiving a valid ciphered Attach Accept message from the network. The SGSN starts ciphering when sending the Attach Accept message to the MS.
After the attach procedure, the GPRS Mobility and Management entity in both SGSN and MS shall be aware if ciphering has started or not. LLC provides the capability to send both ciphered and unciphered PDUs. The synchronisation of ciphering at LLC frames level is done by a bit in the LLC header indicating if the frame is ciphered or not. Only a few identified signalling messages (e.g., Routing Area Update Request message) described in GSM 04.08 may be sent unciphered, any other frames sent unciphered shall be deleted. Once the encryption has been started, neither the MS nor the network shall go to an unciphered session.

D.4.6 Synchronisation

The enciphering stream at one end and the deciphering stream at the other end must be synchronised, for the enciphering bit stream and the deciphering bit streams to coincide. Synchronisation is guaranteed by driving Algorithm GPRS-A5 by an explicit variable INPUT per established LLC and direction.
These initial INPUT values shall not be identical for the different LLC link. The initial INPUT value shall be determined by the network. It may be identical for uplink and downlink value because the direction is given to the ciphering algorithm as described in GSM 01.61 and illustrated on the figure D.4.2. In a given direction, the INPUT value shall be unique for each frame.
The calculation of the INPUT value is described in GSM. The use of the INPUT value is described in GSM 01.61 and illustrated on the figure D.4.2.

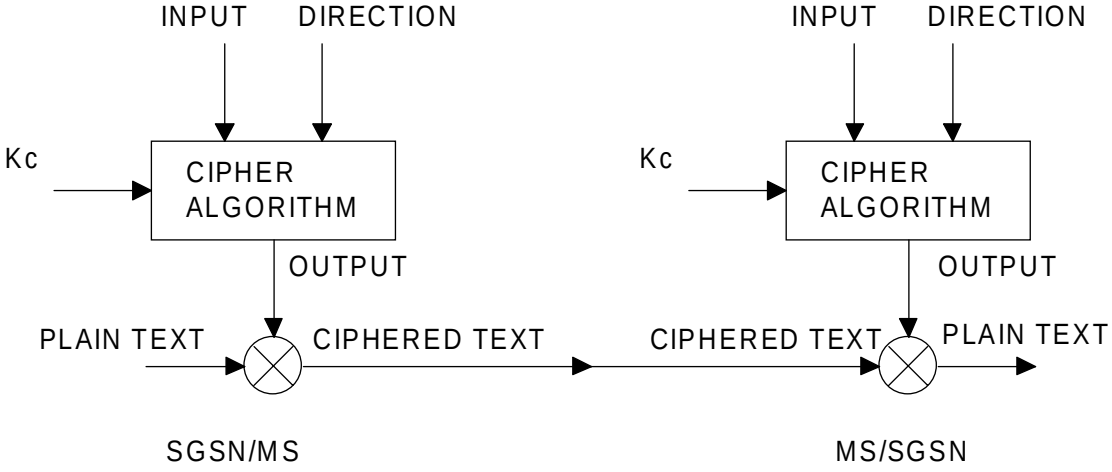


Figure D.4.2: Use of the INPUT parameter

D.4.7 Inter SGSN routing area update

When an Inter SGSN routing area update occurs, the necessary information (e.g. key Kc, INPUT parameters) is transmitted within the system infrastructure to enable the communication to proceed from the old SGSN to the new one, and the Synchronisation procedure is resumed. The key Kc may remains unchanged at Inter SGSN routing area update.

D.4.8 Negotiation of GPRS-A5 algorithm

When an MS wishes to establish a connection with the network, the MS shall indicate to the network which version(s) of the GPRS-A5 algorithm it supports. The negotiation of GPRS-A5 algorithm happens during the authentication procedure. The network may renegotiate the version of the GPRS-A5 algorithm in use at inter SGSN routing area update by performing an authentication procedure.
The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and may take one of the following decisions:

1) The network decides to release the connection because no common version of the GPRS-A5 algorithm is available or because the MS indicated an illegal combination of supported algorithms.
2) The network selects one of the mutually acceptable versions of GPRS-A5 to be used.

D.5 Synthetic summary

Figure D.5.1 shows in a synopsis a routing area updating procedure with all elements pertaining to security functions, i.e. to TLLI management, authentication and GPRS-Kc management.

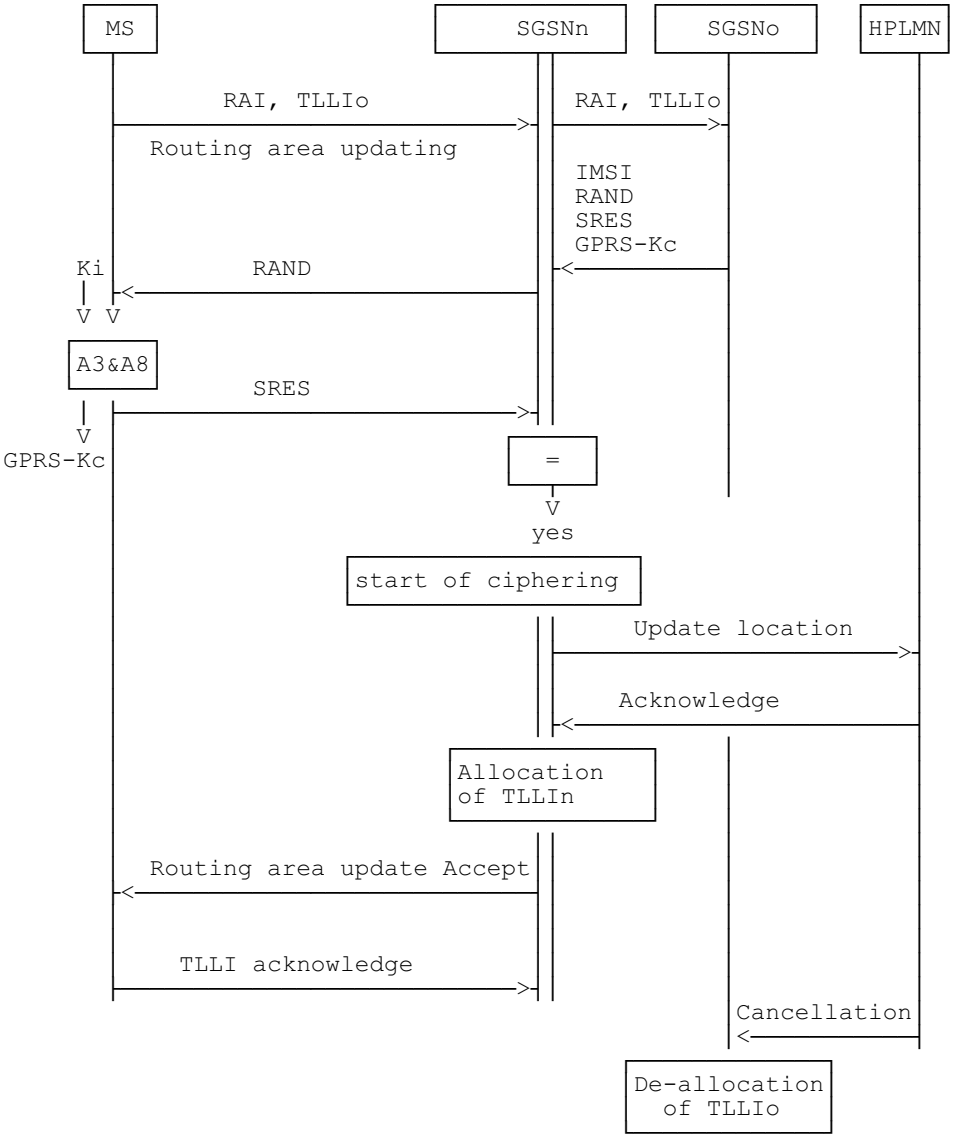


Figure D.5.1: Routing area updating procedure

D.6 Security of the GPRS backbone

The operator is responsible for the security of its own Intra-PLMN backbone which includes all network elements and physical connections. The operator shall prevent unauthorised access to its Intra-PLMN backbone. A secure Intra-PLMN backbone guarantees that no intruder can eavesdrop or modify user information and signalling in the Intra-PLMN backbone.

The GPRS architecture utilises GPRS tunnelling and private IP addressing within the backbone to restrict unauthorised access to the backbone. User traffic addressed to a network element shall be discarded. Firewall functionality may provide these means at the access points (Gi reference point and Gp interface) of the Intra-PLMN backbone.

The Inter-PLMN links shall be negotiated between operators as part of the roaming agreement. They shall ensure that the Inter-PLMN links are secure providing integrity and confidentiality. For example, secure links can be achieved by point to point links, private Inter-PLMN backbones or encrypted tunnels over the public Internet.

Operators shall be able to determine the origin of packets coming from the inter-PLMN backbone. One example is to use a Frame Relay PVC between two operators.

Annex E (informative): Status of Technical Specification GSM 03.20

Status of Technical Specification GSM 03.20		
Date	Version	Information about changes
Release 92	3.3.2	Last common Phase 1/Phase 2 version
August 1992	4.0.0	Working version 4 (in CR 03.20-16 (category D) CR 03.20- 11 rev 2 (category B) / CR 03.20- 13 rev 2 (category B) CR 03.20- 14 (category C); all approved by SMG#03
October 1992	4.1.0	CR 03.20-15 rev 2 (category C) approved by SMG#04
January 1993	4.2.0	CR 03.20-17 rev 1 (category D) approved by SMG#05 Titles of annexes are added from version 3.3.0. Annexes are renamed to annex A, B and C (PNE!). Some figures in section 2 are renumbered.
June 1993	4.2.1	CR 03.20-22 (category D) approved by SMG#07
October 1993	4.2.2	TS changed to prETS 300 534
April 1994	4.3.0	CR 03.20-24 r1 category F) CR 03.20-25 (category F) approved by SMG#10: TS frozen for Phase 2 by SMG#10
September 1994	4.3.1	ETS 300 534 1st edition
February 1996	4.3.2	CR 03.20-A001 (category D) approved by SMG#17:
	4.3.3	ETS 300 534 2nd edition Last common Phase 2/Phase 2+ version
December 1996	5.0.0	GTS converted to draft prETR 300 929 for Release 96
February 1997	5.1.0	CR 03.20-A002 r1 (category F) CR 03.20-A004 r1 (category A) all approved by SMG#21:
May 1997	5.0.1	ETS 300 929 first edition (version 5.1.0 already exists because of CRs approved by SMG#21 in Febr. 1997)
August 1997	5.1.1	ETS 300 929 second edition
October 1997	5.2.0	CR 03.20-A006 r1 (category B) (**GPRS Release 97**) CR 03.20-A007 r1 (category B) (**GPRS Release 97**); all approved by SMG#23 New section 2.3.9 related to GPRS and New normative annex D related to GPRS
March 1998	6.0.0	ETS converted to version 6.0.0 because of GPRS Release 97 contents.
July 1998	6.0.1	Specification published as TS 100 929
Text and figures: WinWord 7.0 **Stylesheet**: etsiw_70.dot **Rapporteur**: Henri Gilbert		

History

Document history		
V6.0.1	July 1998	Publication

ISBN 2-7437-2365-3
Dépôt légal : Juillet 1998