

ETSI/TC SMG
Released by : ETSI/PT 12
Release date: February 1992

RELEASE NOTE

Recommendation GSM 03.20

Security-related Network Functions

Previously distributed version : 3.3.2 (Updated Release 1/90)
New Released version February 92 : 3.3.2 (Release 92, Phase 1)

1. Reason for changes

No changes since the previously distributed version.

Blank page

UDC: 621.396.21

Key words: European Digital Cellular Telecommunications System, Global System for Mobile Communications (GSM)

**European digital cellular
telecommunication system (phase 1);
Security-related Network Functions**

ETSI

European Telecommunications Standards Institute

ETSI Secretariat: B.P.152 . F - 06561 Valbonne Cedex . France

TP. + 33 92 94 42 00 TF. + 33 93 65 47 16 Tx. 47 00 40 F

Copyright European Telecommunications Standards Institute 1992.
All rights reserved.

No part may be reproduced or used except as authorised by contract or other written permission. The copyright and the foregoing restriction on reproduction and use extend to all media in which the information may be embodied.

PREFATORY NOTE

ETSI has constituted stable and consistent documents which give specifications for the implementation of the European Cellular Telecommunications System. Historically, these documents have been identified as "GSM recommendations".

Some of these recommendations may subsequently become Interim European Telecommunications Standards (I-ETSS) or European Telecommunications Standards (ETSS), whilst some continue with the status of ETSI-GSM Technical Specifications. These ETSI-GSM Technical Specifications are for editorial reasons still referred to as GSM recommendations in some current GSM documents.

The numbering and version control system is the same for ETSI-GSM Technical Specifications as for "GSM recommendations".

TABLE OF CONTENTS

0. SCOPE	3
1. GENERAL	3
2. SUBSCRIBER IDENTITY CONFIDENTIALITY	4
2.1 Generality	4
2.2 Identifying method	4
2.3 Procedures	5
2.3.1 Location up-dating in the same MSC area	5
2.3.2 Location up-dating between MSCs area, within the same VLR area :	5
2.3.3 Location Updating between different VLRs	6
2.3.4 Re-allocation of a new TMSI	7
2.3.5 Local TMSI unknown	8
2.3.6 Location up-dating between VLRs in case of a loss of information :	9
3. SUBSCRIBER IDENTITY AUTHENTICATION	10
3.1 Generality	10
3.2 The authentication procedure	10
3.3 Subscriber Authentication Key Management	11
3.3.1 No transmitting of the key	11
3.3.2 Transmitting the authentication key	14
3.4 Ciphering key sequence number	15
4. CONFIDENTIALITY OF SIGNALLING INFORMATION ELEMENTS, CONNECTIONLESS DATA AND USER INFORMATION ELEMENTS ON PHYSICAL CONNECTIONS	16
4.1 Generality	16
4.2 The ciphering method	16
4.3 Key setting	17
4.4 Starting of the ciphering and deciphering processes	17
4.5 Synchronisation	18
4.6 Hand-over	18
5. SYNTHETIC SUMMARY	19
ANNEX 1	21
A1.1. Introduction	21
A1.2. Short description of the schemes	21
A1.3. List of abbreviations	23
A1.4. Schemes	24
ANNEX 2	38
A2.1. Introduction	38
A2.2. Entities and Security Information	38
ANNEX 3	40
A3.0. SCOPE	40
A3.1. SPECIFICATIONS FOR ALGORITHM A5	40
A3.1.1. Purpose	40
A3.1.2. Implementation indications	40
A3.1.3. External specifications of Algorithm A5	42
A3.1.4. Internal specification of Algorithm A5	42
A3.2. ALGORITHM A3	42
A3.2.1. Purpose	42
A3.2.2. Implementation and operational requirements	42
A3.2.3. Proposal for an Algorithm A3	43
A3.3. ALGORITHM A8	43
A3.3.1. Purpose	43
A3.3.2. Implementation and operational requirements	44
A3.3.3. Proposals for an Algorithm A8	44

0. SCOPE

This recommendation specifies the network functions needed to provide the security related service and functions specified in Recommendation GSM 02.09.

This recommendation does not address the cryptological algorithms that are needed to provide different security related features. This topic is addressed in Annex 3. Wherever a cryptological algorithm or mechanism is needed, this is signalled with a reference to Annex 3. The references refers only to functionalities, and some algorithms may be identical or use common hardware.

1. GENERAL

The different security related service and functions that are listed in Recommendation 02.09 are grouped as follows :

- Subscriber identity confidentiality;
- Subscriber identity authentication;
- Signalling information element and connectionless user data confidentiality;
- Data confidentiality for physical connections.

All functions must be implemented with minimum assumptions about the cryptological algorithms that are used, and it must be possible that these algorithms are changed during the system life time. Any change in these algorithms must not change the format of the messages exchanged via the interfaces of the system. The system must be prepared for a parallel operation of more than one algorithm during a transitional period.

The security procedures must include mechanisms to enable recovery in event of signalling failures. These recovery procedures must be designed in such a way that they cannot be used to breach the security of the system.

General note on figures :

- 1- In the figures below, signalling exchanges are referred by functional names. The exact messages and message types are specified in Rec. GSM 04.08 and Rec. GSM 09.02.
- 2- No assumptions are taken for function splitting between MSC (Mobile Switching Centre), VLR and BS (Base Station). Signalling is hence described directly between MS and the local network (i.e. MSC, VLR, and BS, denoted in the figures by BS/MSC/VLR). The splitting in Annex 1 is only given for illustrative purpose.
- 3- Addressing fields are not given; all information relate to the signalling layer. The TMSI allows addressing schemes without IMSI, but the actual implementation is specified in the 04. series.
- 4- The term HPLMN in the figures below is used as a general term which should be understood as HLR (Home Location Register) or AR (Authentication Centre).
- 5- 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 first a high level of confidentiality for user data and signaling, and additionally a protection against the tracing of the location of a user.

The provision of this function implies that the IMSI (International Mobile Subscriber Identity), or any information allowing a listener to derive easily the IMSI, should not normally be transmitted in clear text in any signaling 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 an addressing means on the radio path (see Recommendation GSM 02.09, 3.1.3.);
- Signalling information elements that convey an information about the mobile subscriber identity must be ciphered for transmission on the radio path.

The identifying method is specified in the following section. The ciphering of signalling elements is specified in Section 4.

2.2 Identifying method

The means used to identify a mobile subscriber on the radio path consists in 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 Rec. GSM 03.03.

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

A new TMSI must be allocated at least in each location up-dating 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 a 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 a MS, it is transmitted to the MS in a ciphered mode. This ciphered mode is the same as defined in Section 4 of this recommendation.

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 off.

2.3 Procedures

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

2.3.1 Location up-dating in the same MSC area

This procedure is part of the location up-dating procedure taking 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").

MS sends TMSIo as identifying fields at the beginning of the location up-dating procedure.

The procedure is schematised in Figure 2.1.

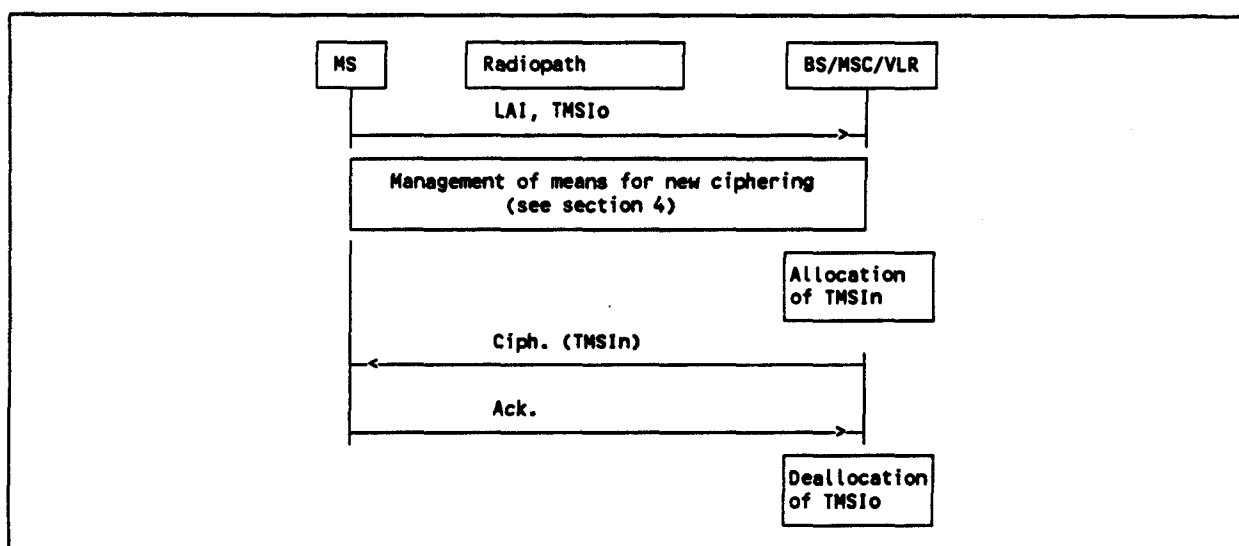


Figure 2.1 / GSM 03.20

Signalling Functionalities :

Management of means for new ciphering : The MS and BS/MSC/VLR agree on means for ciphering signaling information elements, in particular to transmit TMSIn.

2.3.2 Location up-dating between MSCs area, within the same VLR area :

This procedure is part of the location up-dating procedure taking place when the original location area and the new location area depend on different MSCs, but on the same VLR.

The procedure is schematised on Figure 2.2.

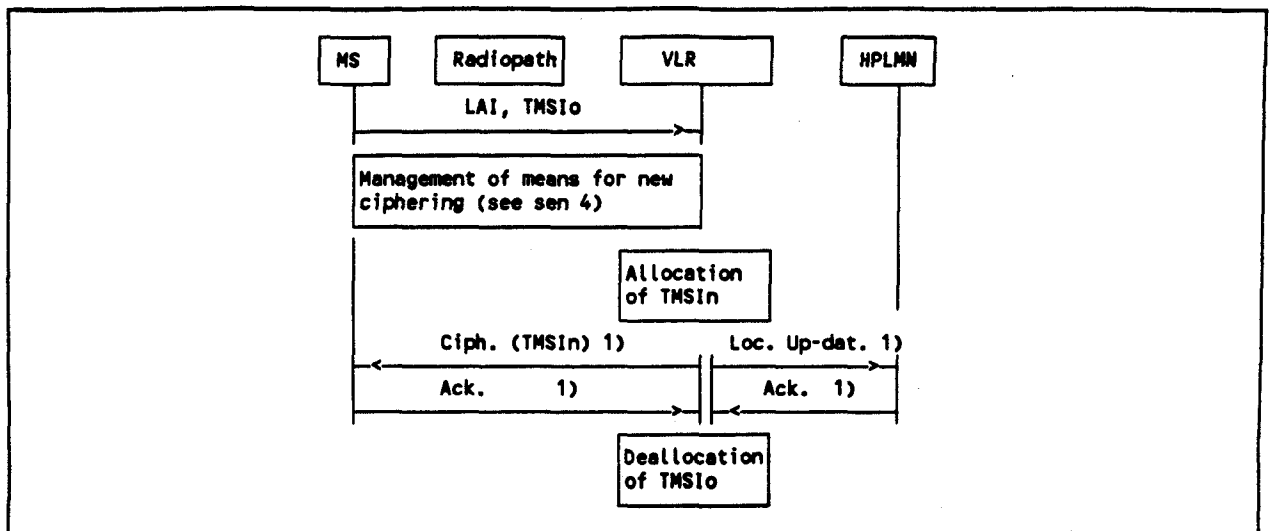


Figure 2.2 / GSM 03.20

Note (1) : From a security point of view, the order of the procedures is irrelevant.

Signalling functionalities :

Loc. Up-dat : stands for Location Up-dating. The BS/MSC/VLR indicates that the location of the MS must be up-dated.

2.3.3 Location Updating between different VLRs

This procedure is part of the normal location up-dating procedure, using TMSI and LAI, when the original location area and the new location area depend on different VLRs.

MS is still registered in VLR_o ("o" for old or original) and asks for its registration in VLR_n ("n" for new). LAI and TMSIo are sent by MS as identifying field during the location up-dating procedure.

The procedure is schematised on Figure 2.3.

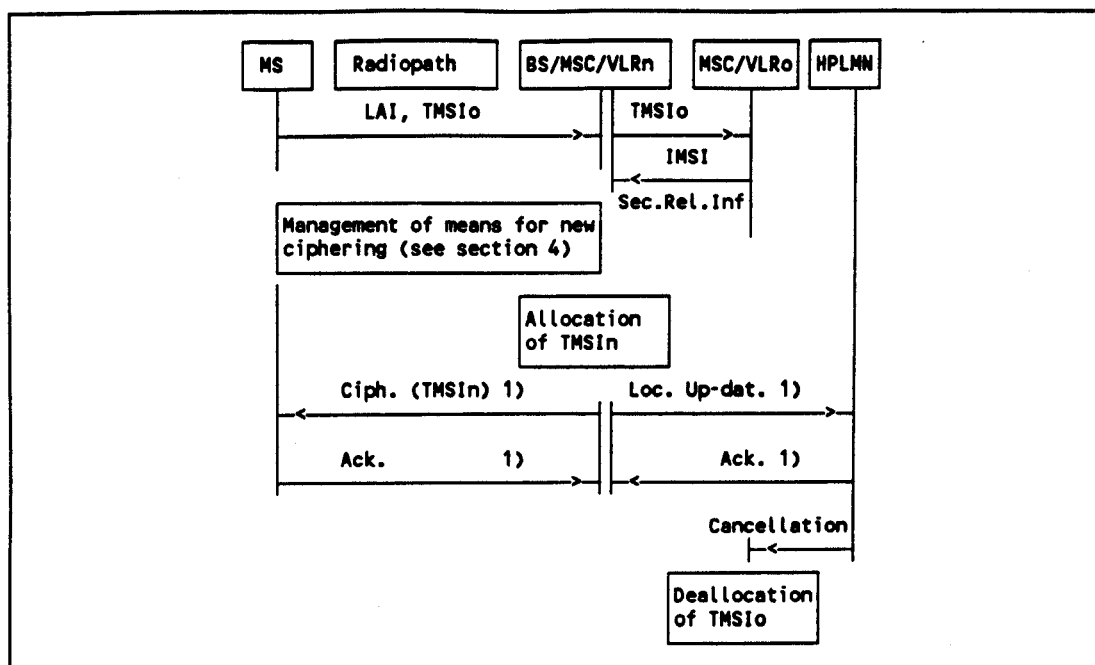


Figure 2.3 /GSM 03.20

Note (1) : From a security point of view, the order of the procedures is irrelevant.

Signalling functionalities :

Sec.Rel.Info.: Stands for Security Related information. The MSC/VLRn needs some information for ciphering; these information are 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 Re-allocation of a new TMSI

This function can be initiated by the network side at any time. The procedure can be included in other procedures, through the means of optional parameters. The execution of this function is left to the network operator.

This procedure is schematised in Figure 2.4.

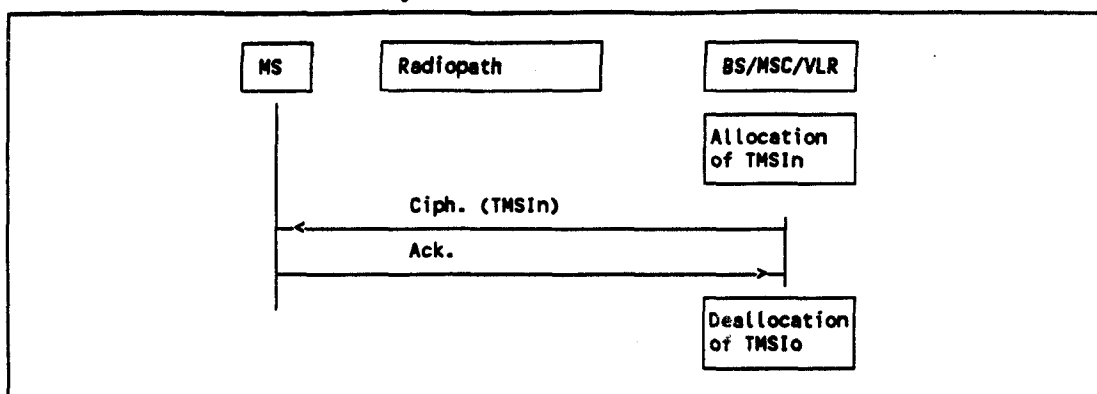


Figure 2.4 /GSM 03.20

2.3.5 Local TMSI unknown

This procedure is a variant of the procedure described in Section 2.3.1 and Section 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 up-dating request in a location area managed by the same VLR.

This procedure is schematised in Figure 2.5.

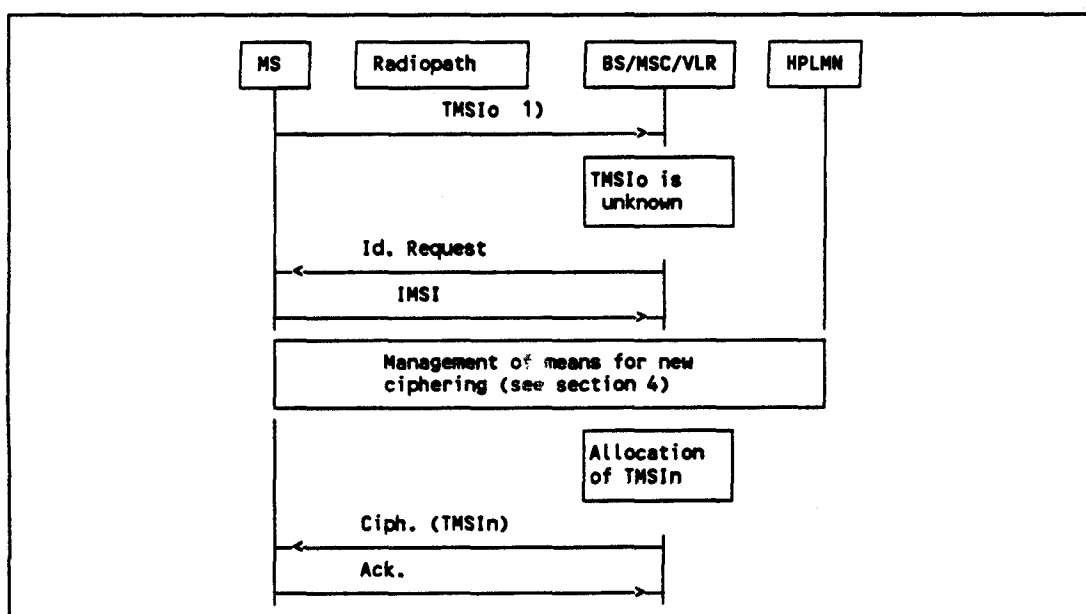


Figure 2.5 /GSM 03.20

Note (1) : Any message in which TMSIo is used as an identifying means in a location area managed by the same VLR.

2.3.6 Location up-dating between VLRs in case of a loss of information :

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

The procedure is schematised in Figure 2.6.

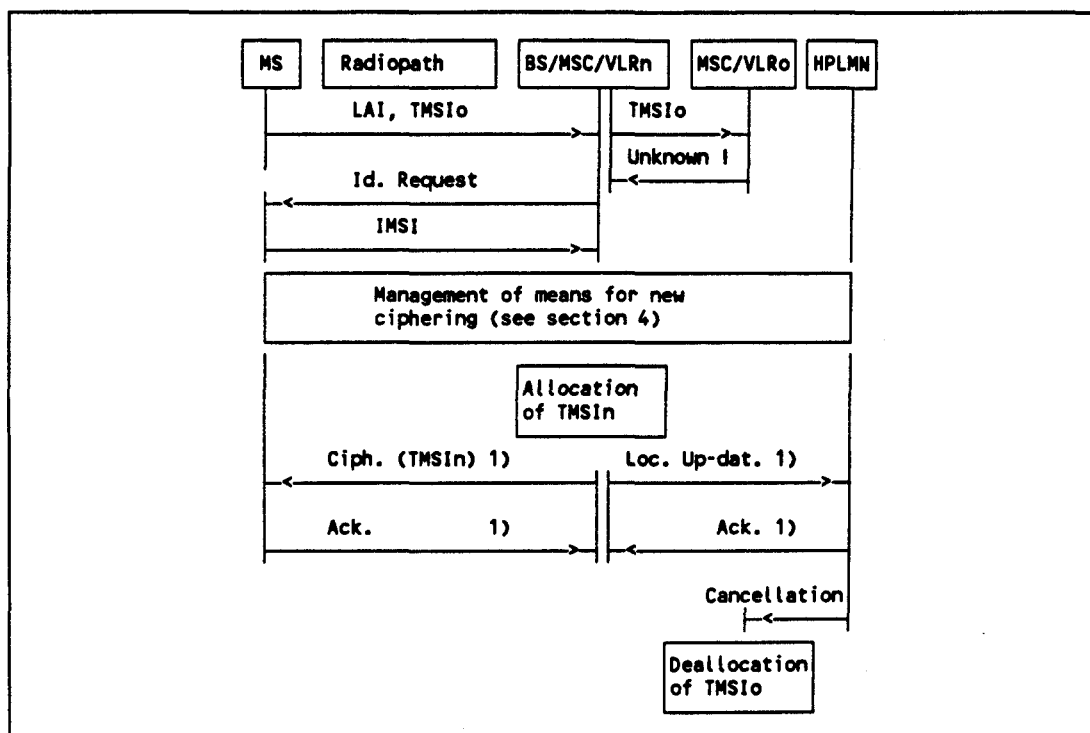


Figure 2.6 / GSM 03.20

Note (1) : Form a security point of view, the order of the procedures is irrelevant.

3. SUBSCRIBER IDENTITY AUTHENTICATION

3.1 Generality

Definition and operational requirements of subscriber identity authentication are given in Recommendation GSM 02.09.

The authentication procedure will be also used to perform the cipher key-setting (see Section 4) on dedicated signalling channels. 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 sub-system.

3.2 The authentication procedure

The authentication procedure consists in the following exchange between the fixed sub-system and the MS.

- The fixed sub-system 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 Subscriber Authentication Key, denoted Ki in the sequel.
- The MS transmits the signature SRES to the fixed sub-system.
- The fixed sub-system tests SRES for validity.

The general procedure is schematised in Figure 3.1.

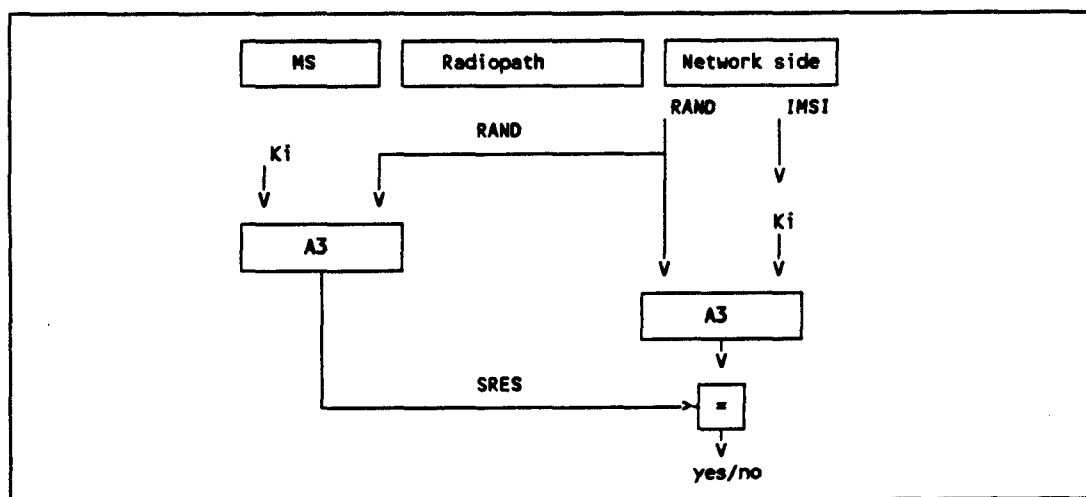


Figure 3.1 / GSM 03.20

Algorithm A3 is specified in Annex 3.

3.3 Subscriber Authentication Key Management

The Subscriber Authentication Key Ki is allocated at subscription time, together with the IMSI.

The Subscriber Authentication Key is stored on the network side in the HPLMN (Home Public Land Mobile Network), in an Authentication Centre. A PLMN may contain one or more Authentication Centres. An Authentication Centre can be implemented together with other functions, e.g. in a HLR (Home Location Register).

Two management modes are specified. The second one, specified in Section 3.3.2, is less secure than the first one, specified in Section 3.3.1, and should not be used between two PLMNs. The procedures are such that the decision to use one or the other of the two methods inside one PLMN is done by the network operator.

3.3.1 No transmitting of the key

3.3.1.1 General authentication procedure

When needed for each MS, the BS/MSC/VLR requests to the Authentication Centre corresponding to the MS, either through the HLR or directly, Security Related Informations. This includes an array of pairs of corresponding RAND and SRES. These pairs are obtained by applying on each RAND Algorithm A3 and the key Ki as shown in Figure 3.1 above. The pairs are stored in the VLR.

The procedure needed for up-dating the vectors RAND/SRES is schematised in Figure 3.2.

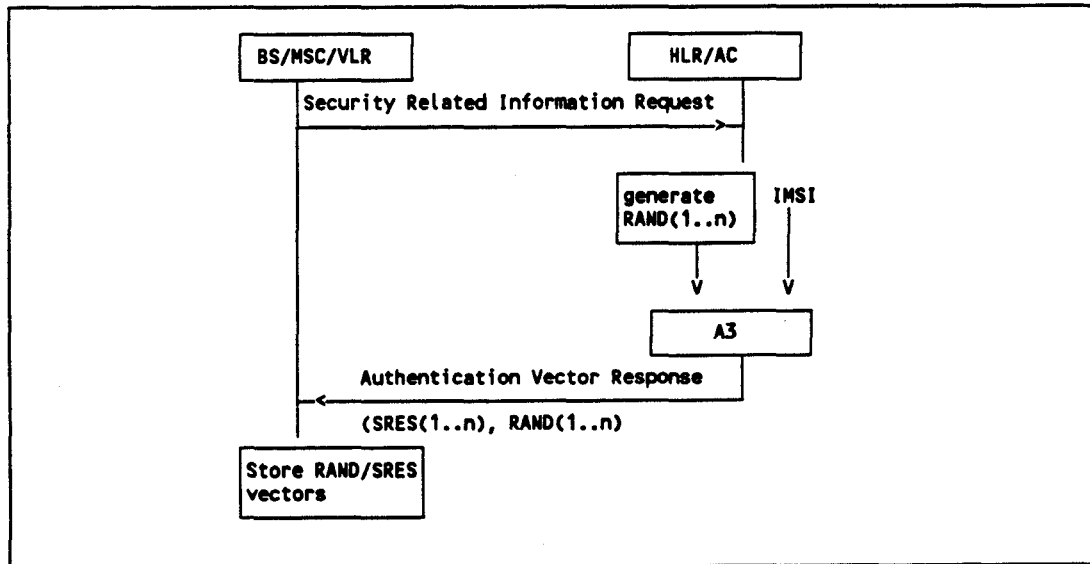


Figure 3.2 / GSM 03.20

When a MSC/VLR performs an authentication, including the case of a location up-dating within the same VLR area, it chooses a RAND value in the array corresponding to the MS. It then tests the answer by the MS by comparing it with the corresponding SRES, as schematised in Figure 3.3 below. Any pair RAND/SRES is used only once and deleted after usage.

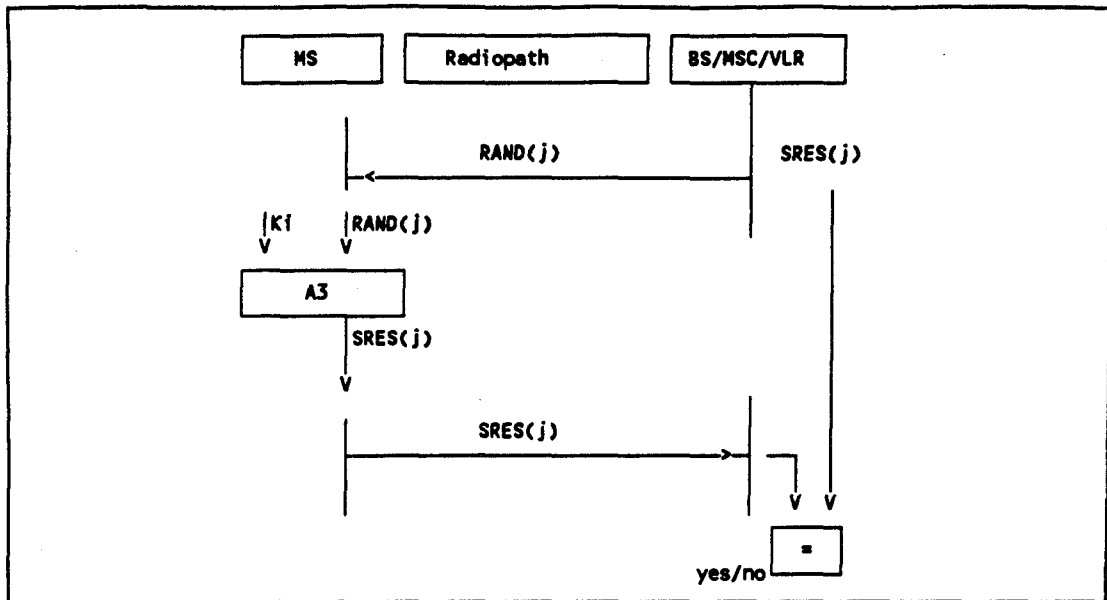


Figure 3.3 / GSM 03.20

3.3.1.2 Authentication at location up-dating between different VLRs, using TMSI

During a location up-dating between different VLRs, the procedure to get pairs for subsequent authentication and the procedure for authentication are particular. In the case when identification is done through the means of TMSI, pairs for authentication are given by the old VLR.

The procedure is schematised in Figure 3.4.

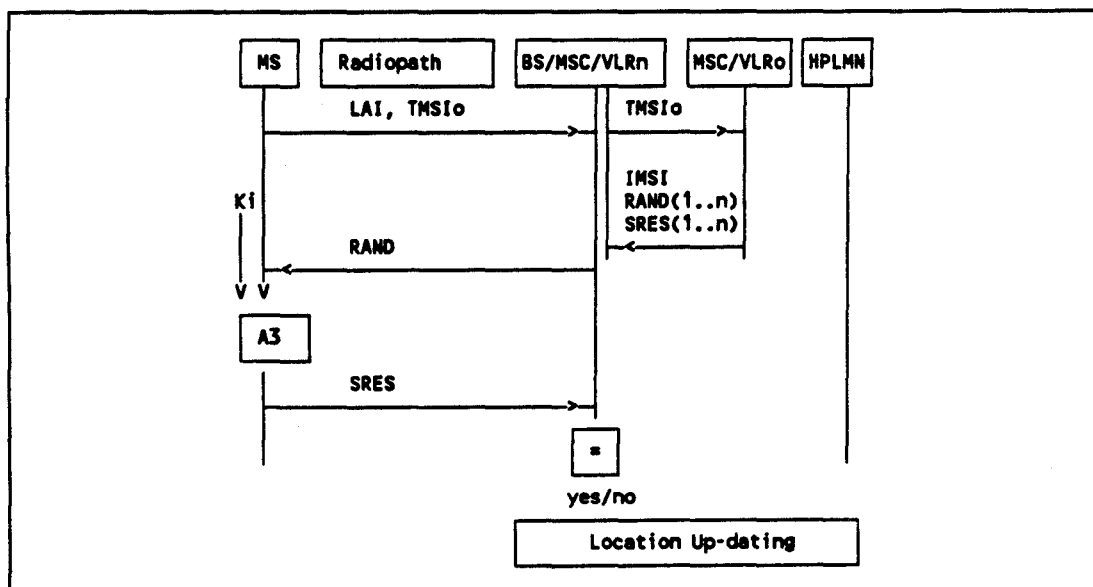


Figure 3.4 / GSM 03.20

3.3.1.3 Authentication at location up-dating between different VLRs, using IMSI and not transmitting LAI

When the IMSI is used as a mean for identification, or more generally when the MS does not transmit the LAI of its last location area, the procedure described in 3.3.1.2 cannot be used. Instead, the first pairs of RAND/SRES are requested directly to the HPLMN.

The procedure is schematised in Figure 3.5.

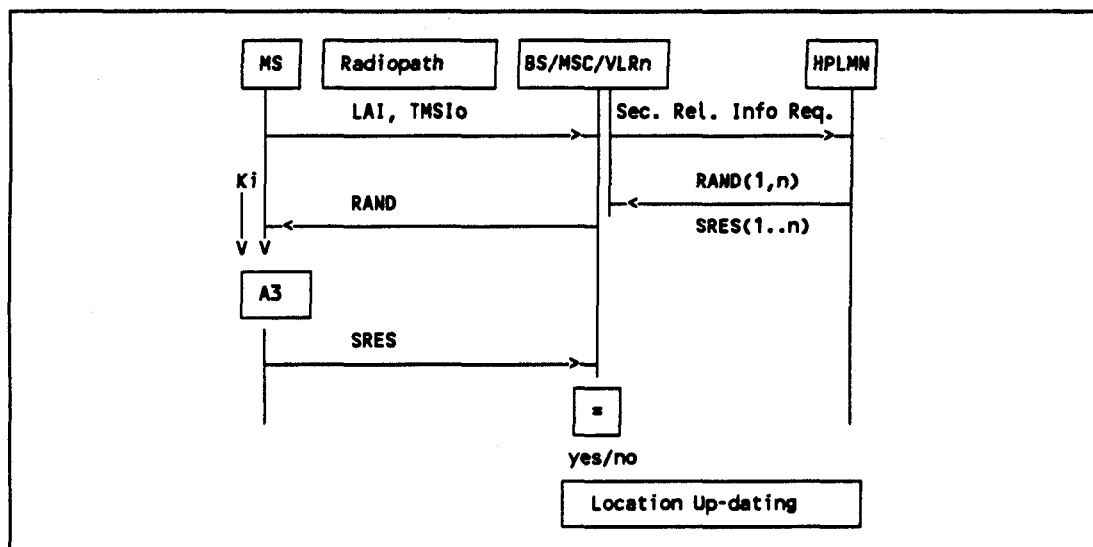


Figure 3.5 GSM 03.20

3.3.1.4 Authentication at location up-dating between different VLRs, using TMSI, TMSI unknown

This case is an abnormal one, when a data loss has occurred in a VLR.

The procedure is schematised in Figure 3.6.

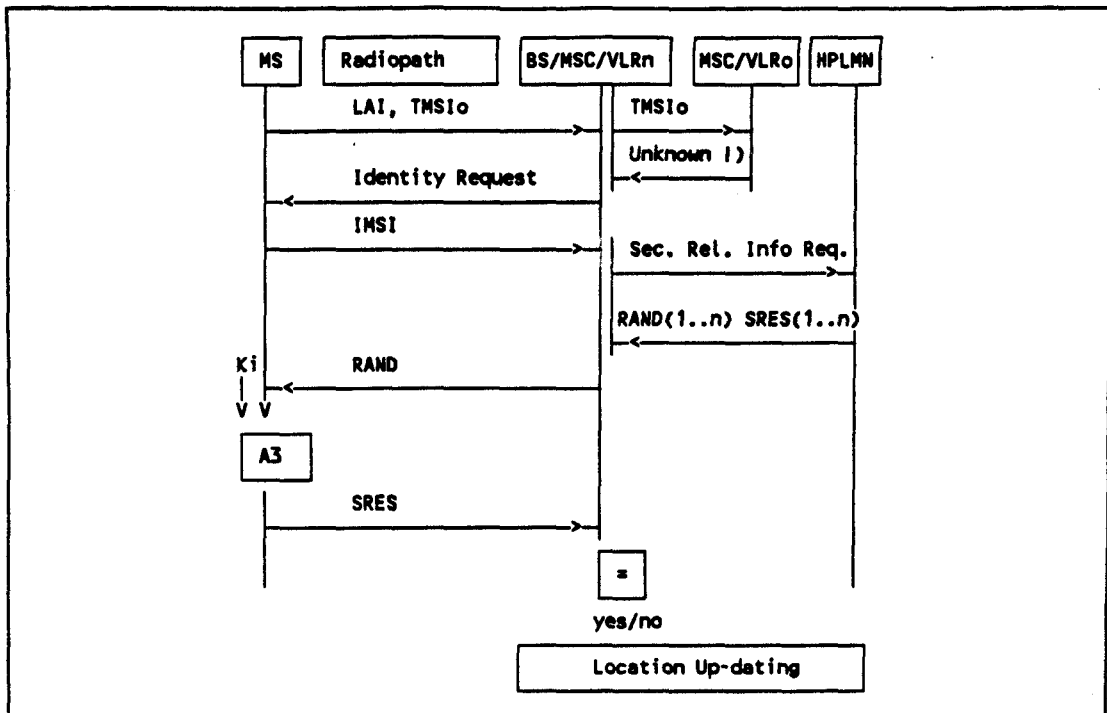


Figure 3.6 / GSM 03.20

3.3.2 Transmitting the authentication key

This procedure, which is less secure than the preceding one because secret information have to be known in several places of the network. It should be used within the same PLMN only. When the MS enters first a VLR area, the MSC/VLR requests from the HLR the Security Related Information for the MS. The HLR sends back the Authentication Key K_i which is used directly by the MSC/VLR. To cope with several possible different algorithms A3, the HLR also sends the type of algorithm A3 used by the MS.

The procedure is schematised in Figure 3.7.

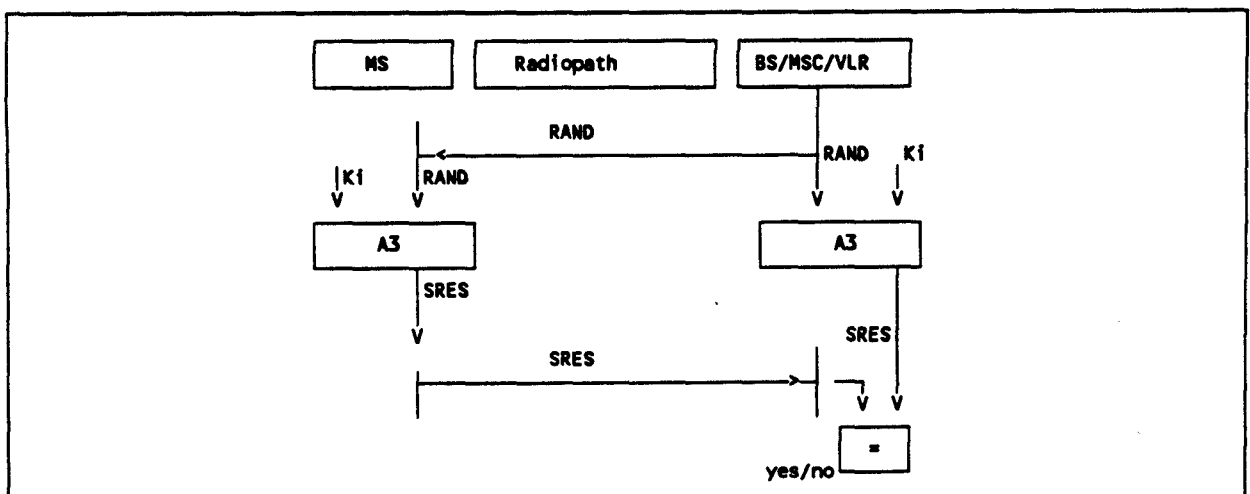


Figure 3.7 / GSM 03.20

3.4 Ciphering key sequence number

The cipheringkey sequence number is a number which is associated to the cipher key K_c . However since it is not directly involved into any security mechanism, it is not addressed in this recommendation but in Recommendation GSM 04.08 instead.

4. CONFIDENTIALITY OF SIGNALLING INFORMATION ELEMENTS, CONNECTIONLESS DATA AND USER INFORMATION ELEMENTS ON PHYSICAL CONNECTIONS

4.1 Generality

In Recommendation GSM 02.09, some signalling information elements are considered sensitive and must be protected.

To ensure the identity confidentiality (see Section 2), the following information must be transferred in a protected mode:

- Temporary Mobile Subscriber Identity at allocation time

The confidentiality of connection less user data requires at least the protection of the message part pertaining to layers 4 and upper.

The user information confidentiality on physical connections concerns the information transmitted on a traffic channel on the MS-BS interface (e.g. for speech). It is not an end to end confidentiality service.

These four needs for a protected mode of transmission are fulfilled with the same mechanism where the confidentiality function is a 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 CCH (Common Control Channel) is only used for the allocation of

Four points have to be specified :

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

4.2 The ciphering method

The layer 1 information 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 Section 4.3. The key is denoted by K_c in the sequel, and is called "Ciphering Key".

The deciphering is performed by exactly the same method.

Algorithm A5 is specified in Annex 3

The ciphering/deciphering function is placed on the transmission chain between the interleaver and the modulator (see Recommendation GSM 05.01).

4.3 Key setting

Mutual key setting is the procedure that allows the mobile subscriber and the network to agree on the key K_c to use in the cipher and decipher algorithms A5.

A key setting is triggered by the authentication procedure. In addition to the authentication procedures listed in Recommendation GSM 02.09, a key-setting may be initiated by the network as often as the network operator wishes.

A key setting must occur on a DCCH not yet encrypted and as soon as the identity of the mobile subscriber (e.g. TMSI/IMSI) is known by the network.

The transmission of K_c to the MS is indirect and uses the authentication RAND value; K_c is derived from RAND by using algorithm A8 and the Subscriber Authentication key K_i , as defined in Annex 3

As a consequence, the procedures for the management of K_c are the authentication procedures described in Sec. 3.3.

The values K_c are computed together with the SRES values. When pairs are given by the old VLR, the K_c values are given also (see Section 3.3.1.2). Similarly, when pairs are given by the HPLMN, the K_c values are given also (see Section 3.3.1.3 and Section 3.3.1.4). When K_i is known by the VLR, it is used to directly compute K_c (see Section 3.3.2).

The key K_c may be stored by the mobile station until it is updated at the next authentication.

A key setting is schematized in Figure 4.1.

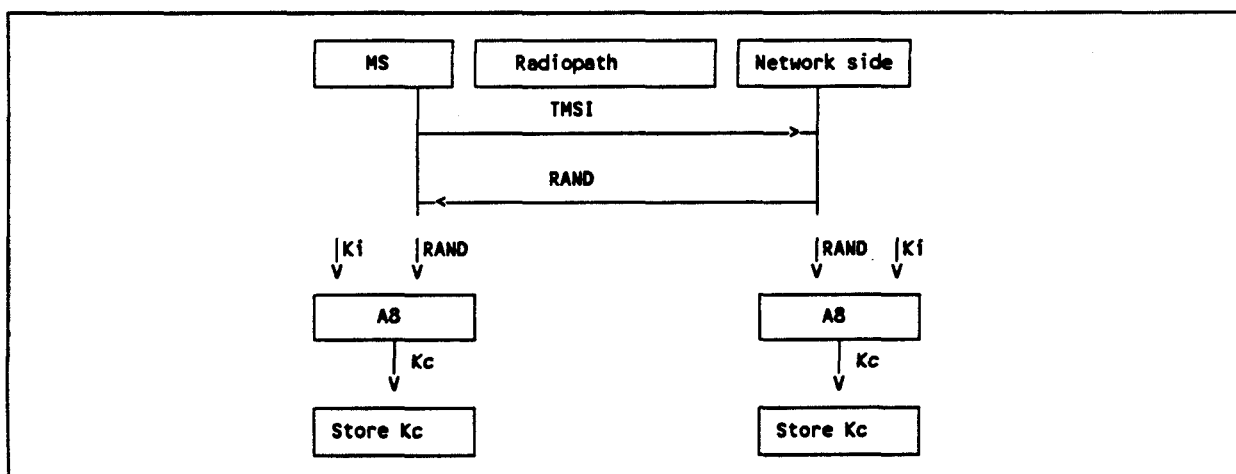


Figure 4.1 / GSM 03.20

4.4 Starting of the ciphering and deciphering processes

The MS and the BS must choose into a coordinate way the instants at which respectively 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 K_c has been made available at the BS.

No information elements for which protection is needed must be sent before the completion of the starting of the ciphering and deciphering processes.

The deciphering process starts on the BS which sends to the MS a specific message, here called "Start cipher". Both the enciphering and deciphering processes start on the MS side after the message "Start cipher" has been correctly received by the MS. Finally, the enciphering process on the BS side starts as soon as a frame or a message from the MS has been correctly received at the BS.

The starting of enciphering and deciphering processes is schematised in Figure 4.2.

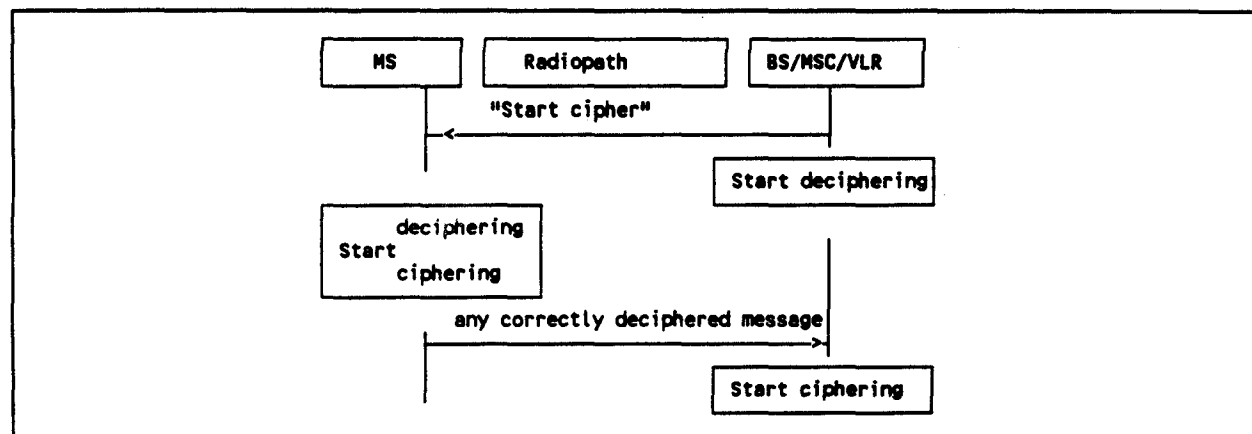


Figure 4.2 / GSM 03.20

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.

4.5 Synchronisation

The ciphering stream at one end the deciphering stream at the other end must be synchronised, for the ciphering bit stream and the deciphering bit streams to coincide.

Specific functions are needed to obtain the synchronization in the first place, i.e. at the beginning of the call, or during a hand-over.

The underlying synchronisation of the radio sub-system provides the synchronisation of the ciphering-deciphering streams by the following mechanism. A slot numbering in the radio sub-system is maintained by the BS, and periodically transmitted. Algorithm A5 will use this information to produce on both the MS side and the BS side a synchronized stream, as described in Annex 3

4.6 Hand-over

When a hand-over 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 BS to the new one, the synchronisation procedure is resumed. The key Kc remains unchanged at handover.

5. SYNTHETIC SUMMARY

Figure 5.1 shows in a synopsis a normal location up-dating procedure with all elements pertaining to security functions, i.e. to TMSI management, authentication and Kc management.

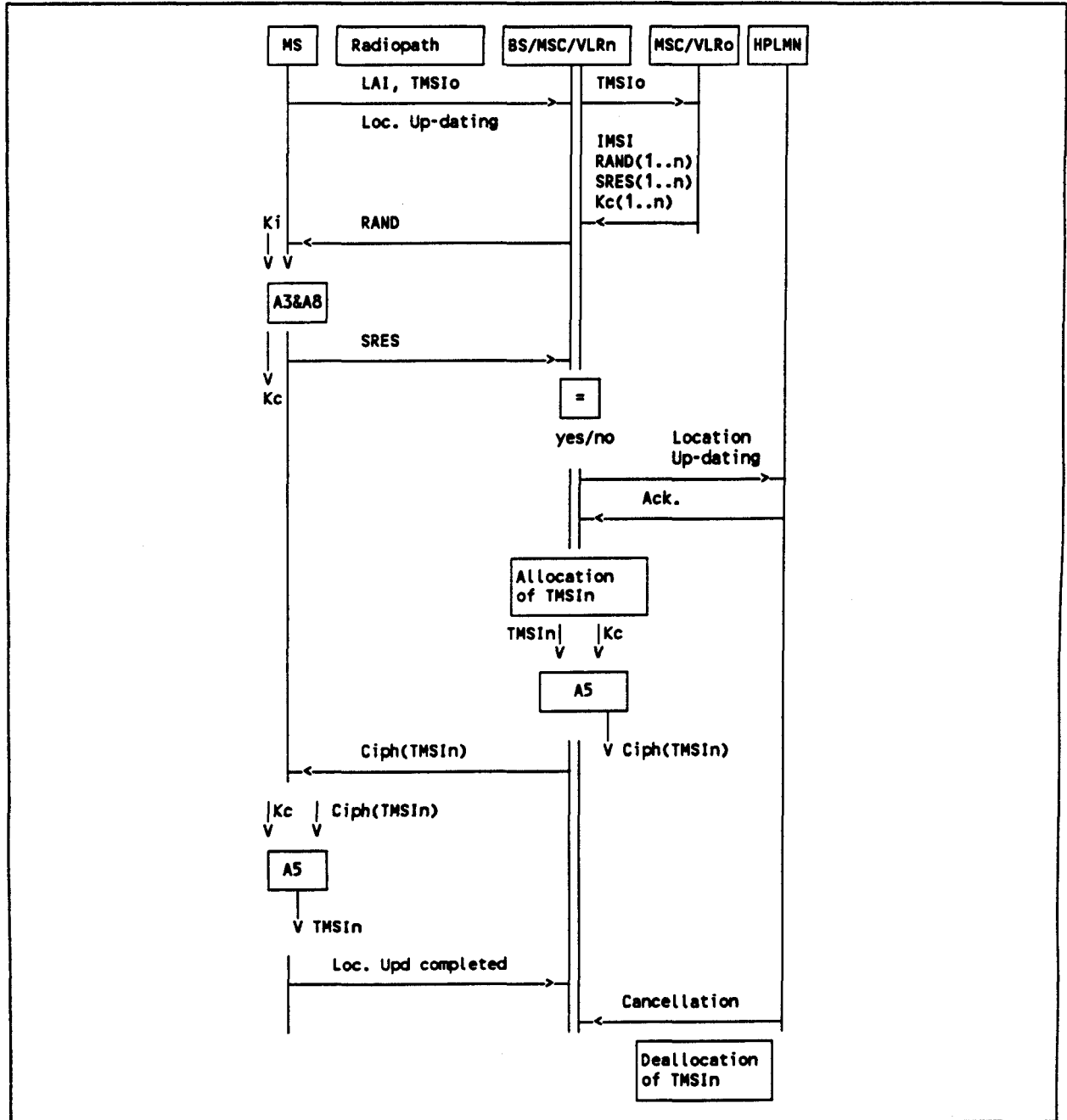


Figure 5.1 / GSM 03.20

ABBREVIATIONS GLOSSARY :

AC	:	Authentication Centre
BS	:	Base Station
CCCH	:	Common Control Channel
DDCH	:	Dedicated Control Channel
HLR	:	Home Location Register
HPLMN	:	Home Public Land Mobile Network
IMSI	:	International Mobile Subscriber Identity
Ki	:	Individual Subscriber Authentication Key
Kc	:	Ciphering Key
LAI	:	Location Area Identity
MS	:	Mobile Station
MSC	:	Mobile Switching Centre
PLMN	:	Public Land Mobile Network
RAND	:	A random number
SRES	:	A signed response to RAND
TCH	:	Traffic Channel
TMSI	:	Temporary Mobile Subscriber Identity
VLR	:	Visited Location Register

ANNEX 1

A1.1. 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. In this annex the option of transmitting the authentication key Ki is not described. The security functions between VLR and BSS/MSC are split. In case of inconsistency between the diagrams in this annex and the text in Recommendation GSM 03.20 or other GSM recommendations then the text in these recommendations has preference.

A1.2. Short description of the schemes

Scheme 1 : Location registration

- no TMSI available

The situation is represented where an MS wants registration and for some reason, e.g. TMSI is lost or 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 VLR, so no connection with HLR is necessary. Identification is done by the LAI and TMSI. For authentication a new set of Kc, R, and S 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
- no location confidentiality feature

This PLMN does not offer the location confidentiality feature (as defined in Recommendation GSM 02.09). Identification is therefore done by using the IMSI. MS was not yet registered in any 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 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

Like in scheme 5 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".

Scheme 8 : Location updating

- MS not yet registered in VLR
- no location confidentiality feature
- old LAI still available

This PLMN does not offer location confidentiality feature. The MS has roamed to an area controlled by another VLR. The LAI is used to address the "old" VLR. The IMSI 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.

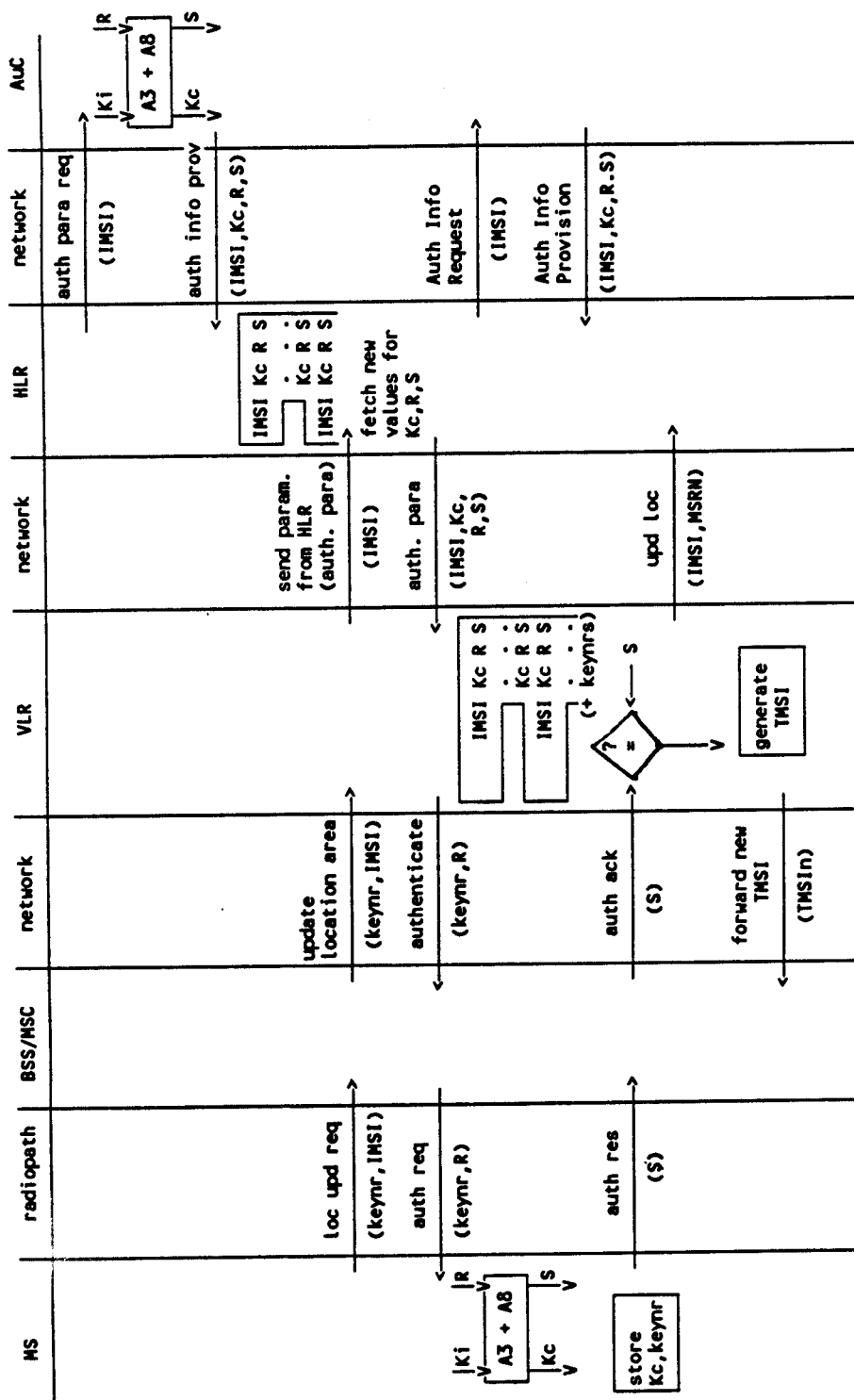
A1.3. List of abbreviations

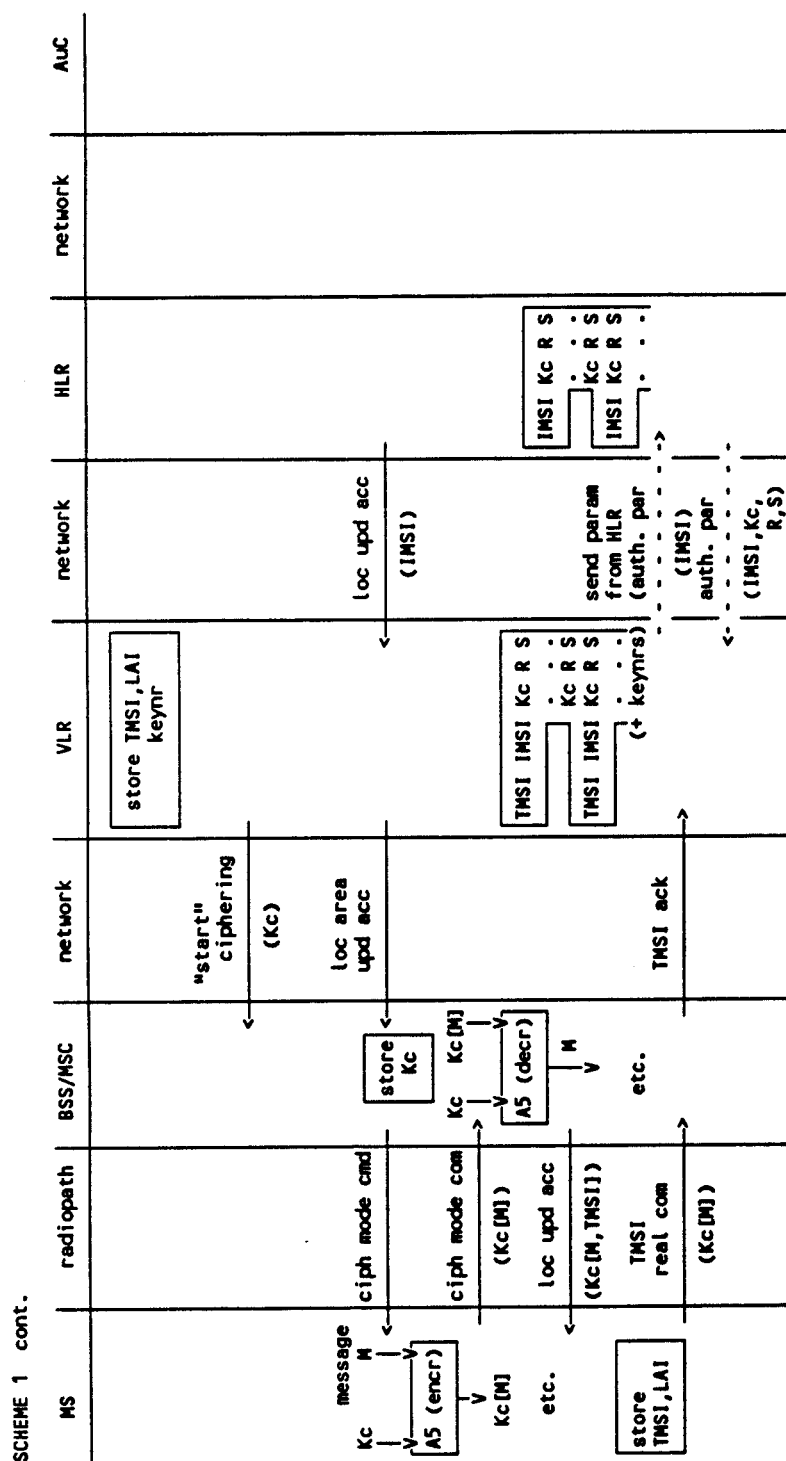
A3	authentication algorithm
A5	signalling data and user data encryption algorithm
A8	ciphering key generating algorithm
BSS	base station system
HLR	home location register
IMSI	international mobile subscriber identity
Kc	ciphering key
Kc[M]	message encrypted with ciphering key Kc
Kc[TMSI]	TMSI encrypted with ciphering key Kc
Ki	individual subscriber authentication key
LAI	location area identity
MS	mobile station
MSC	mobile services 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

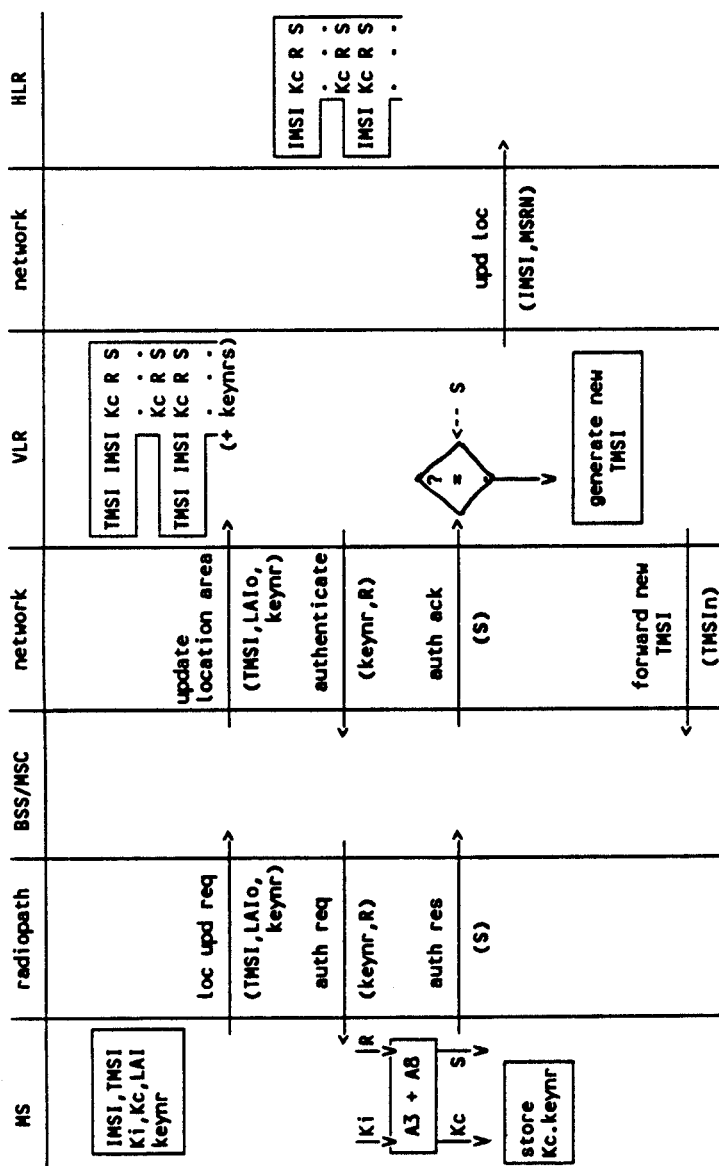
A1.4. Schemes

Scheme 1

SCHEME 1 Location registration
- no TMSI available

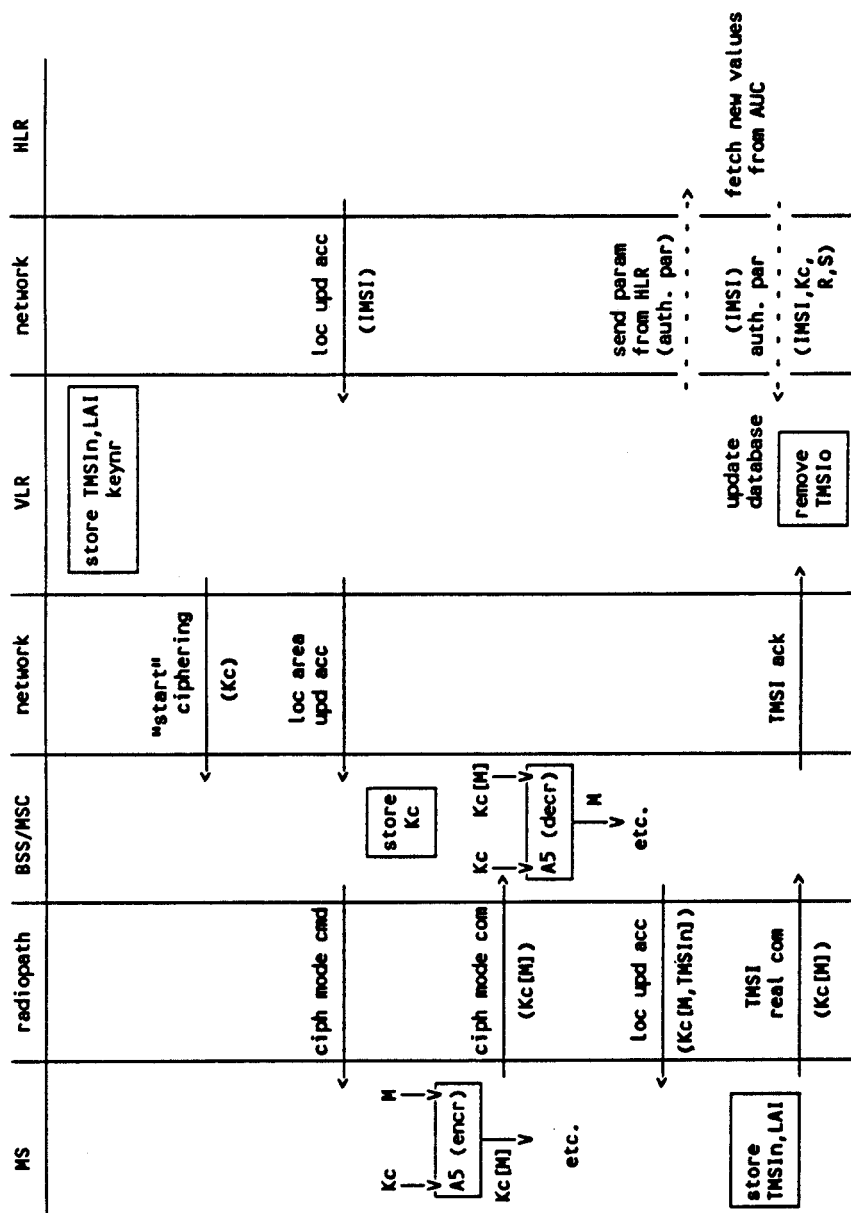




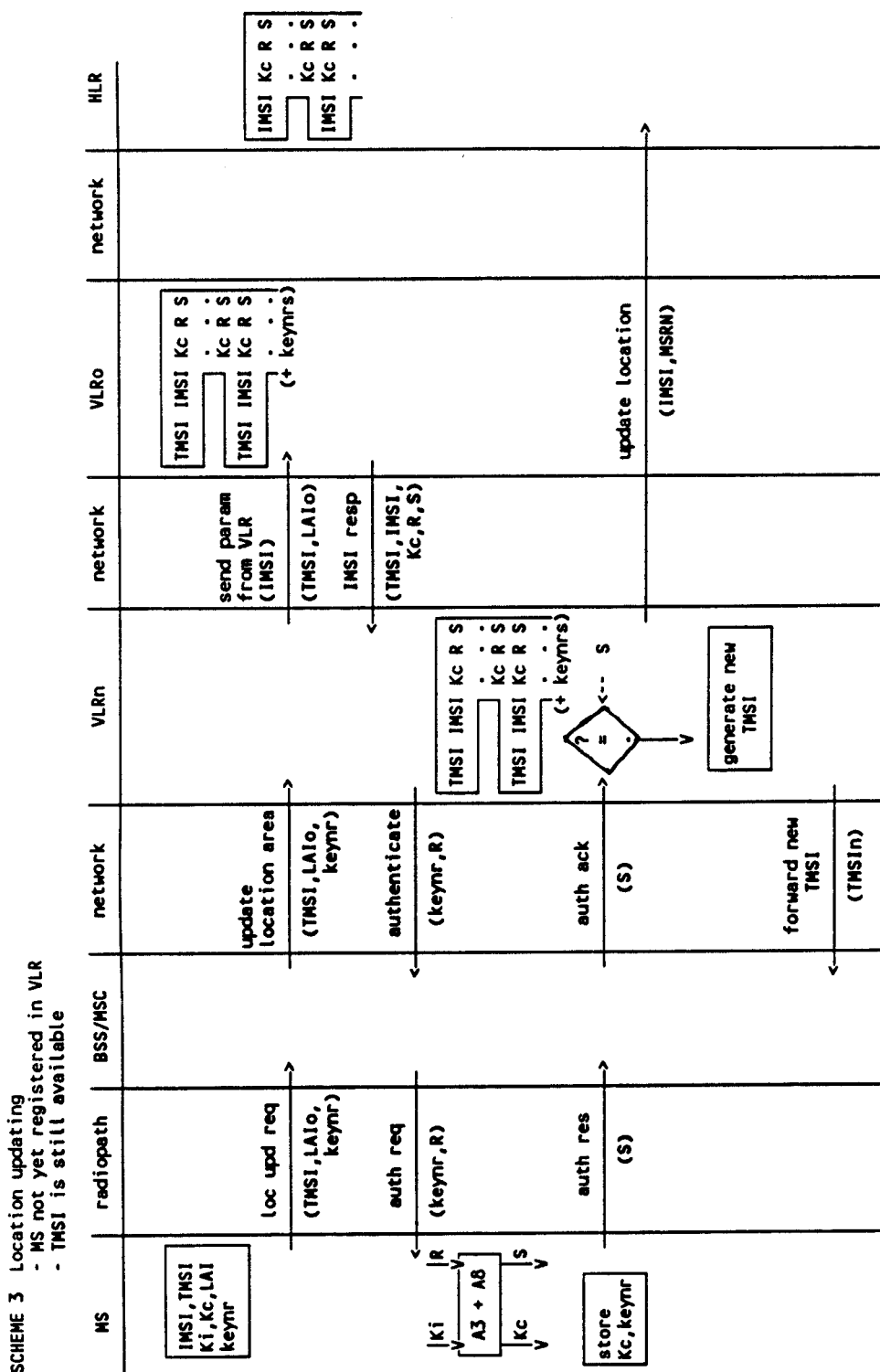


Scheme 2 cont

SCHEME 2 cont.

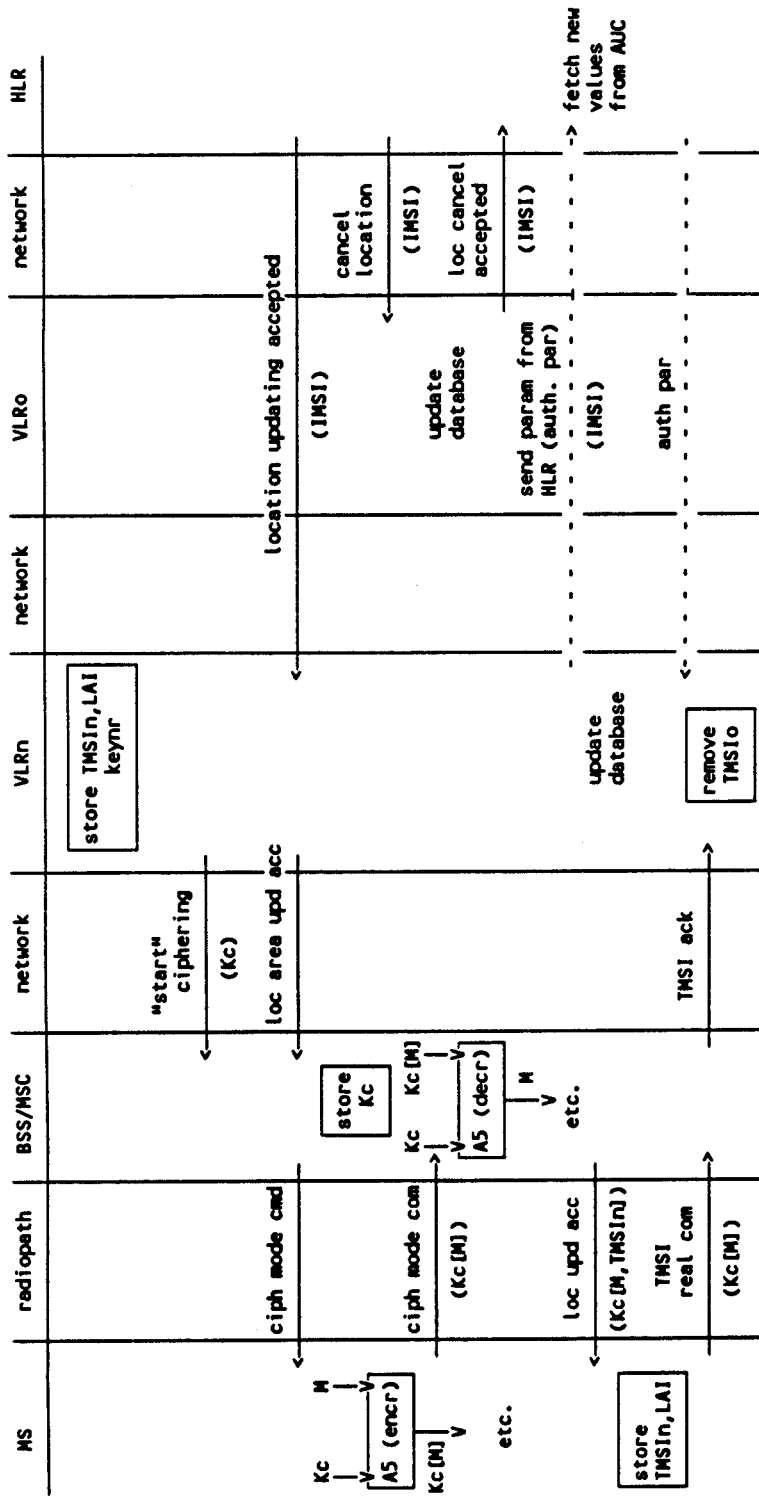


Scheme 3

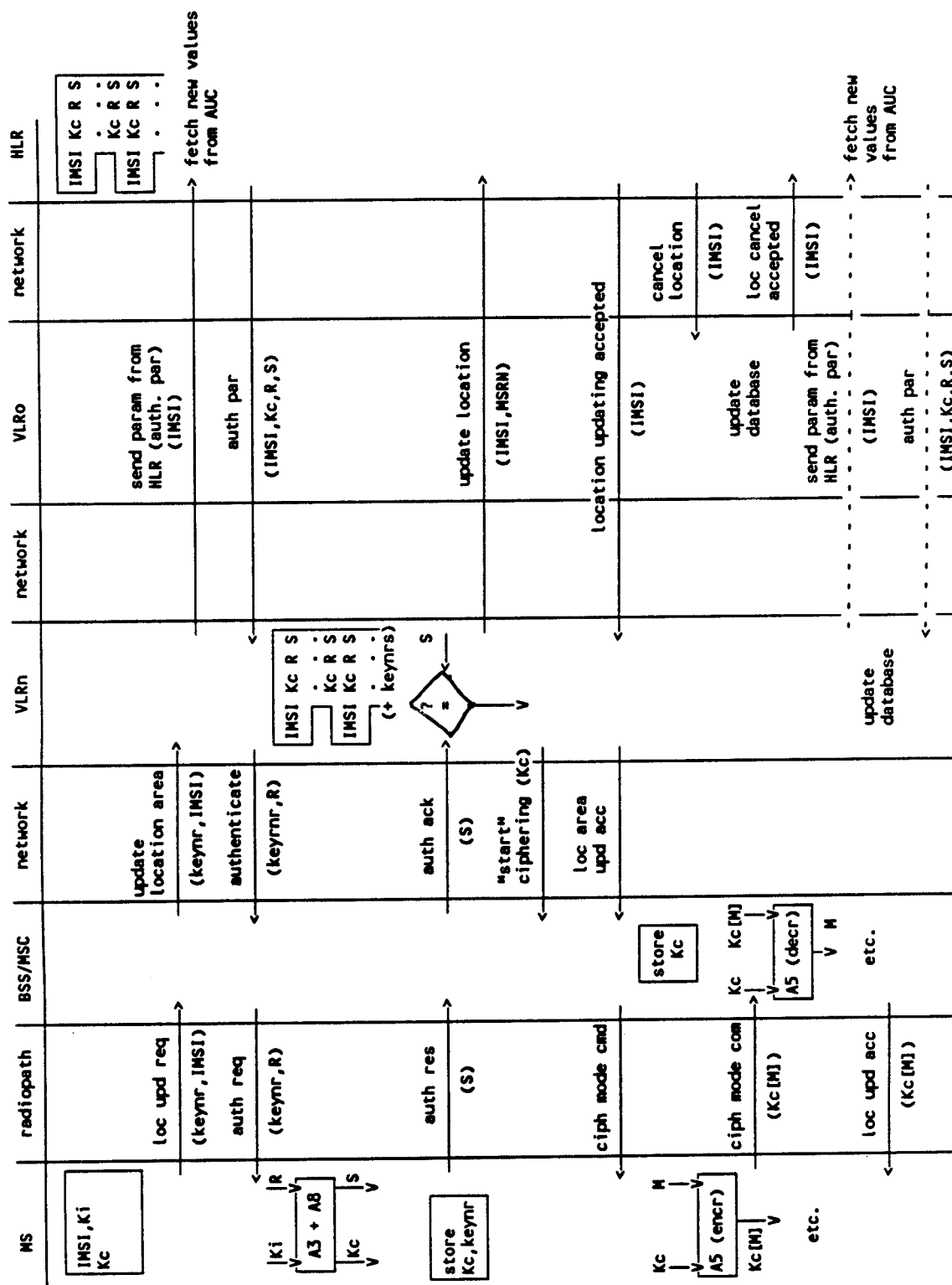


Scheme 3 cont

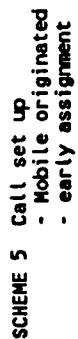
SCHEME 3 cont.



- Location updating
- MS not yet registered in VLR; no old LAI
- no location confidentiality function

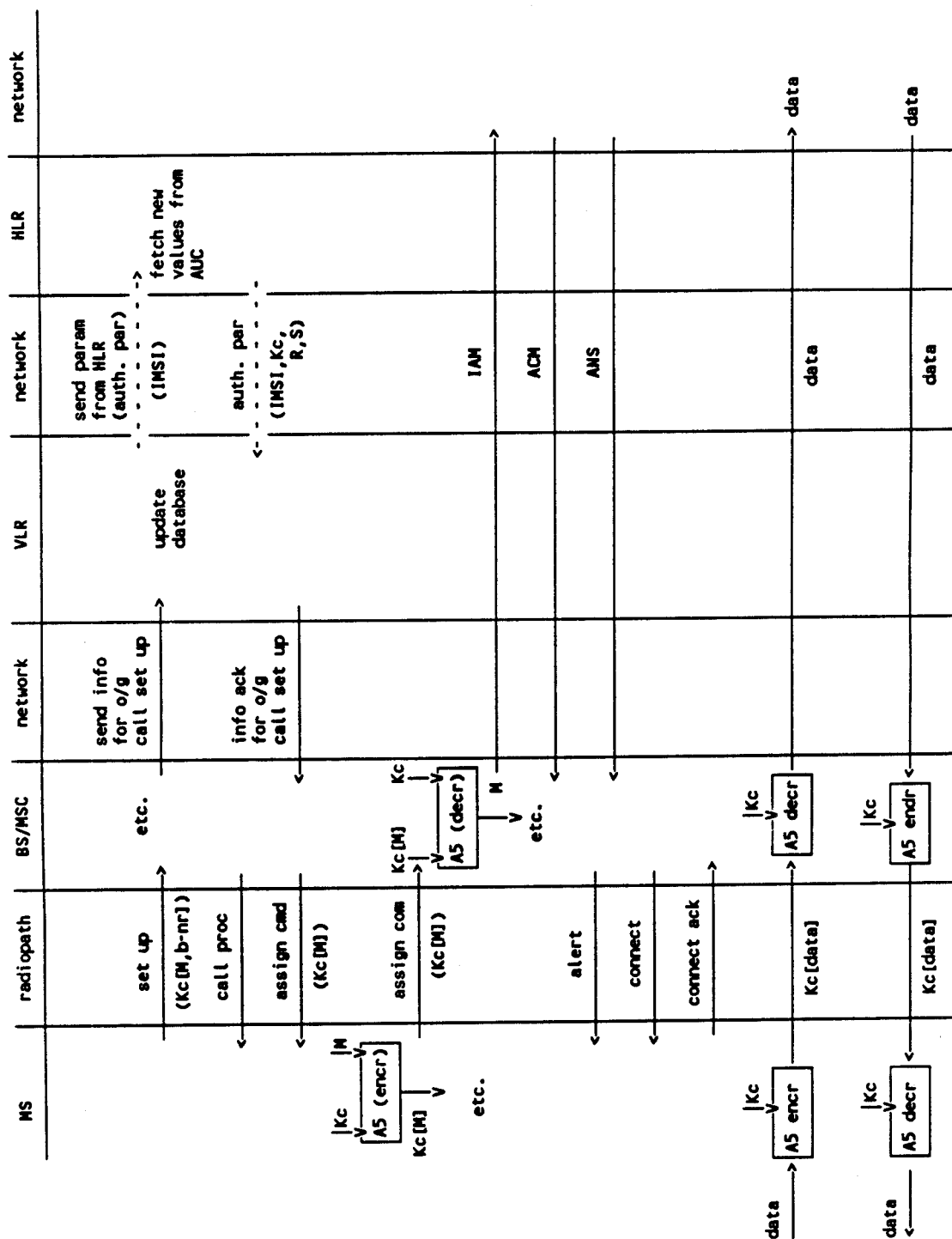


Scheme 5



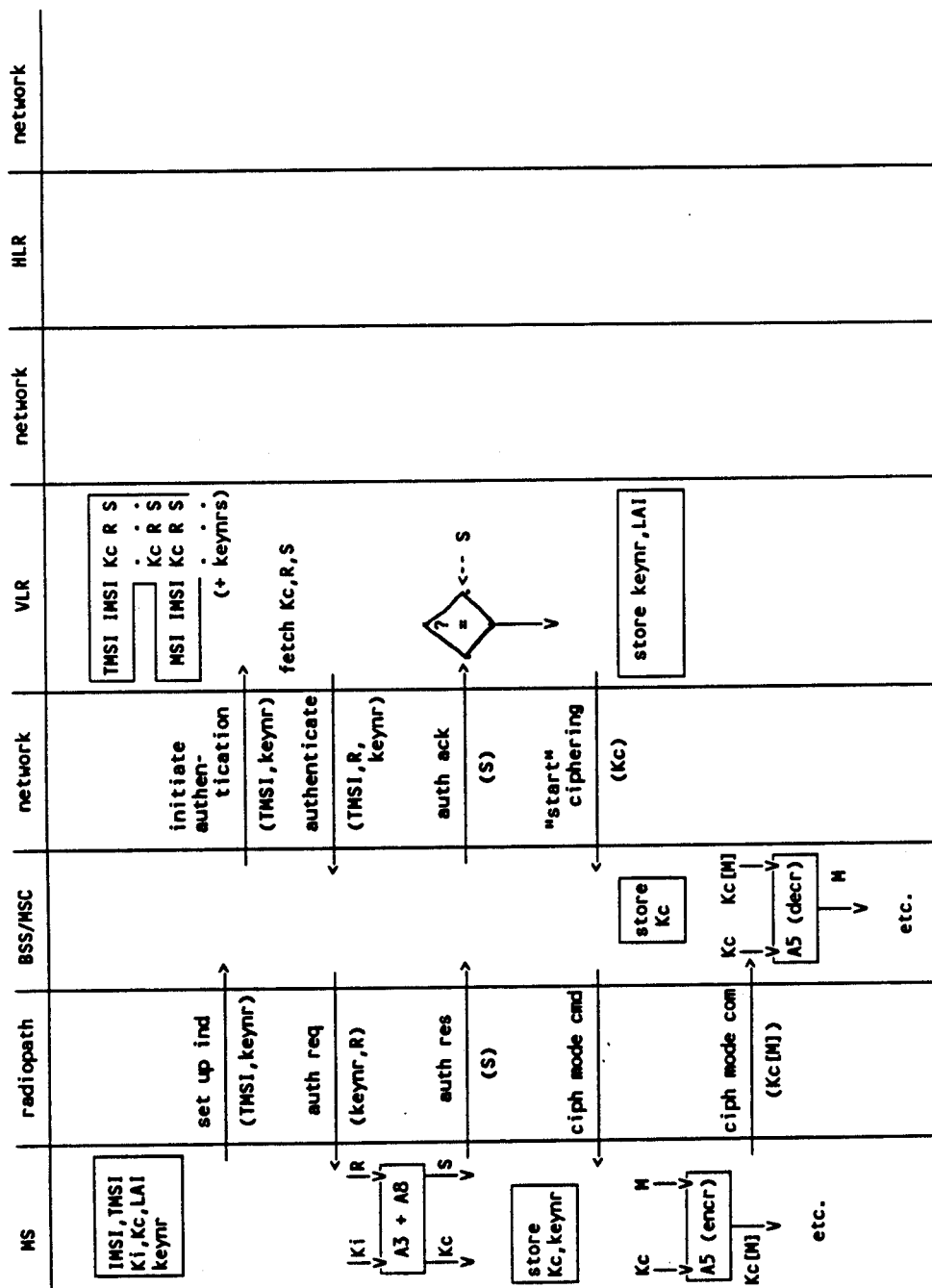
Scheme 5 cont

SCHEME 5 cont.



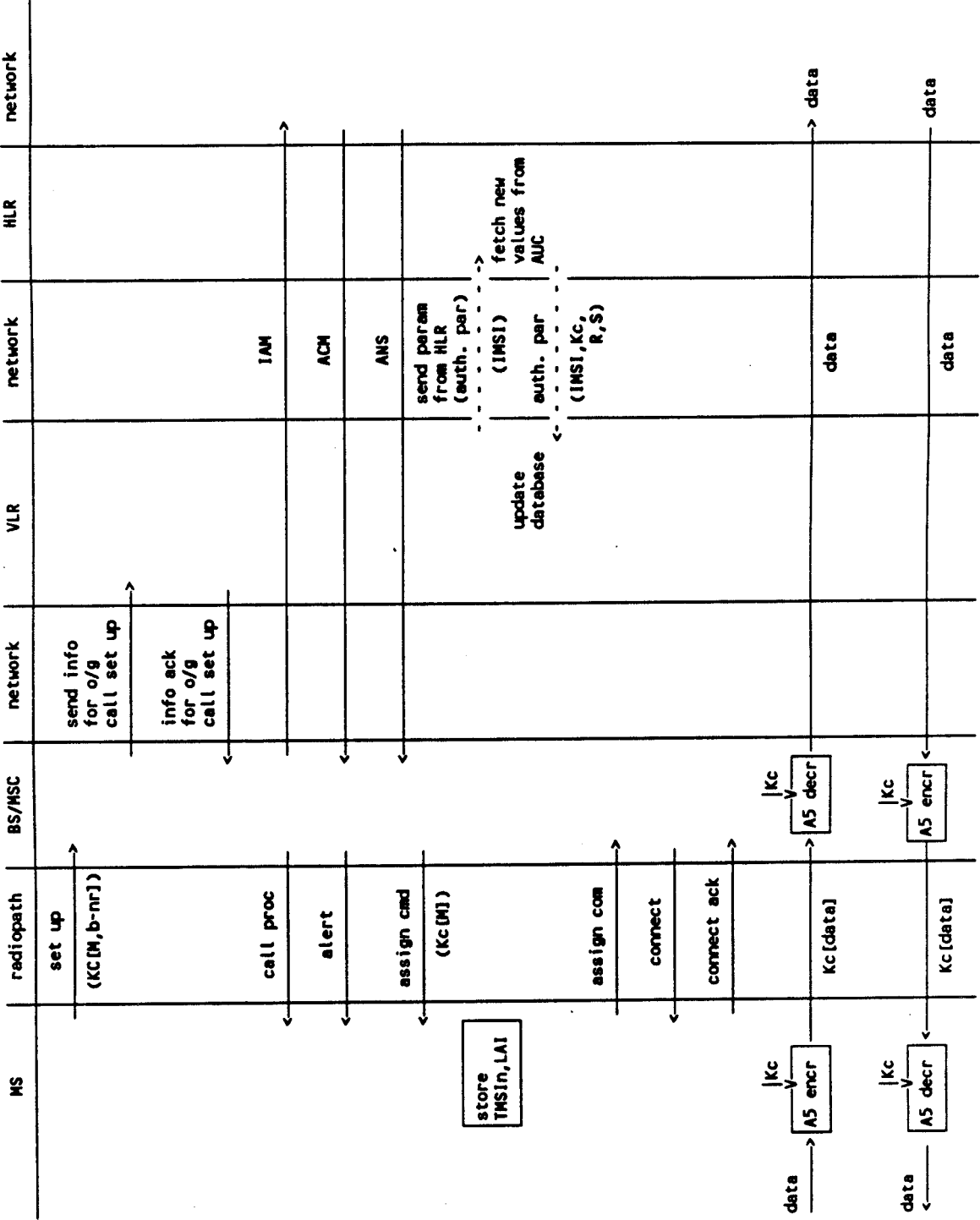
Scheme 6

SCHEME 6 Call set up
 - Mobile originated
 - Off air call set up

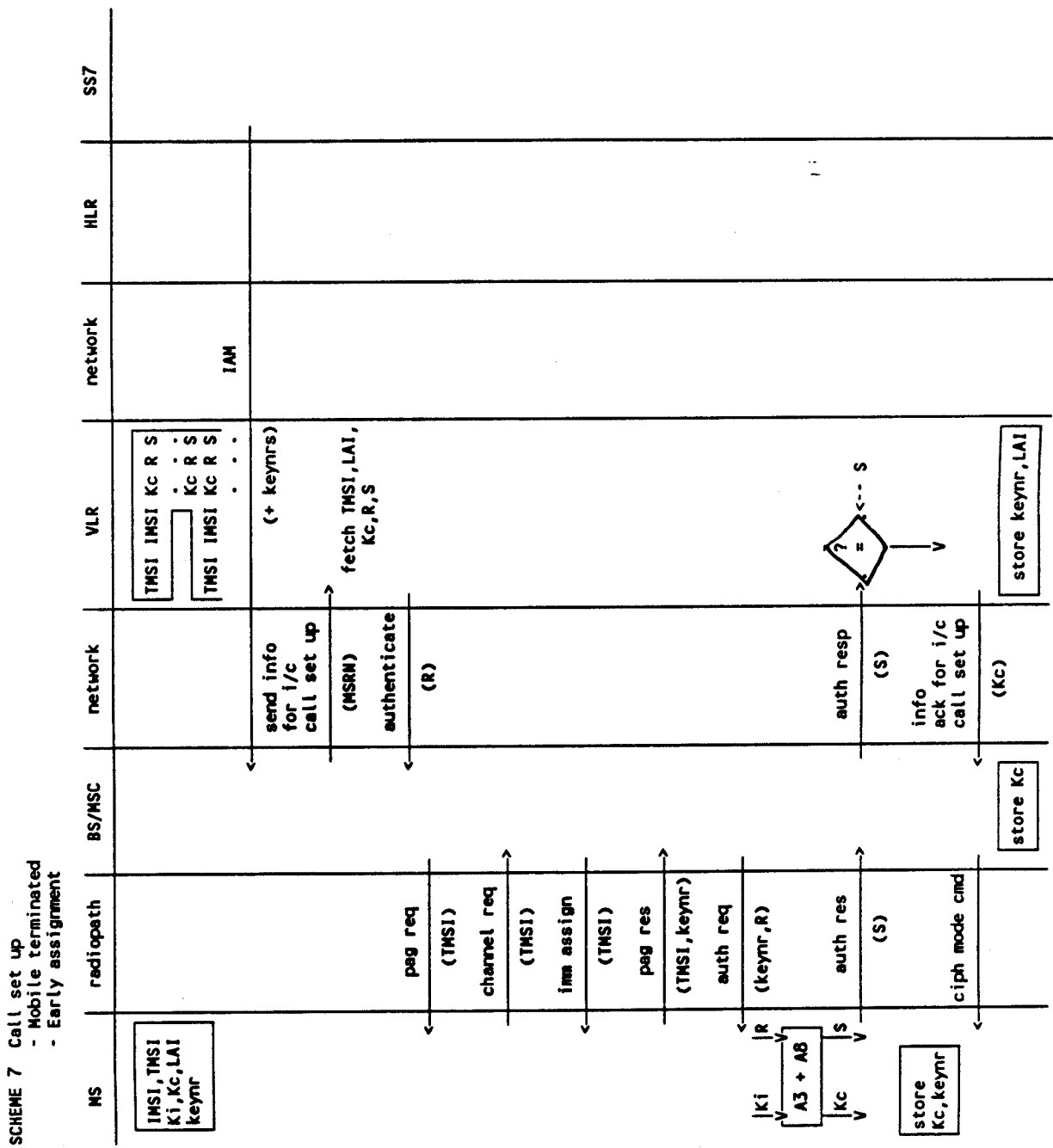


Scheme 6 cont

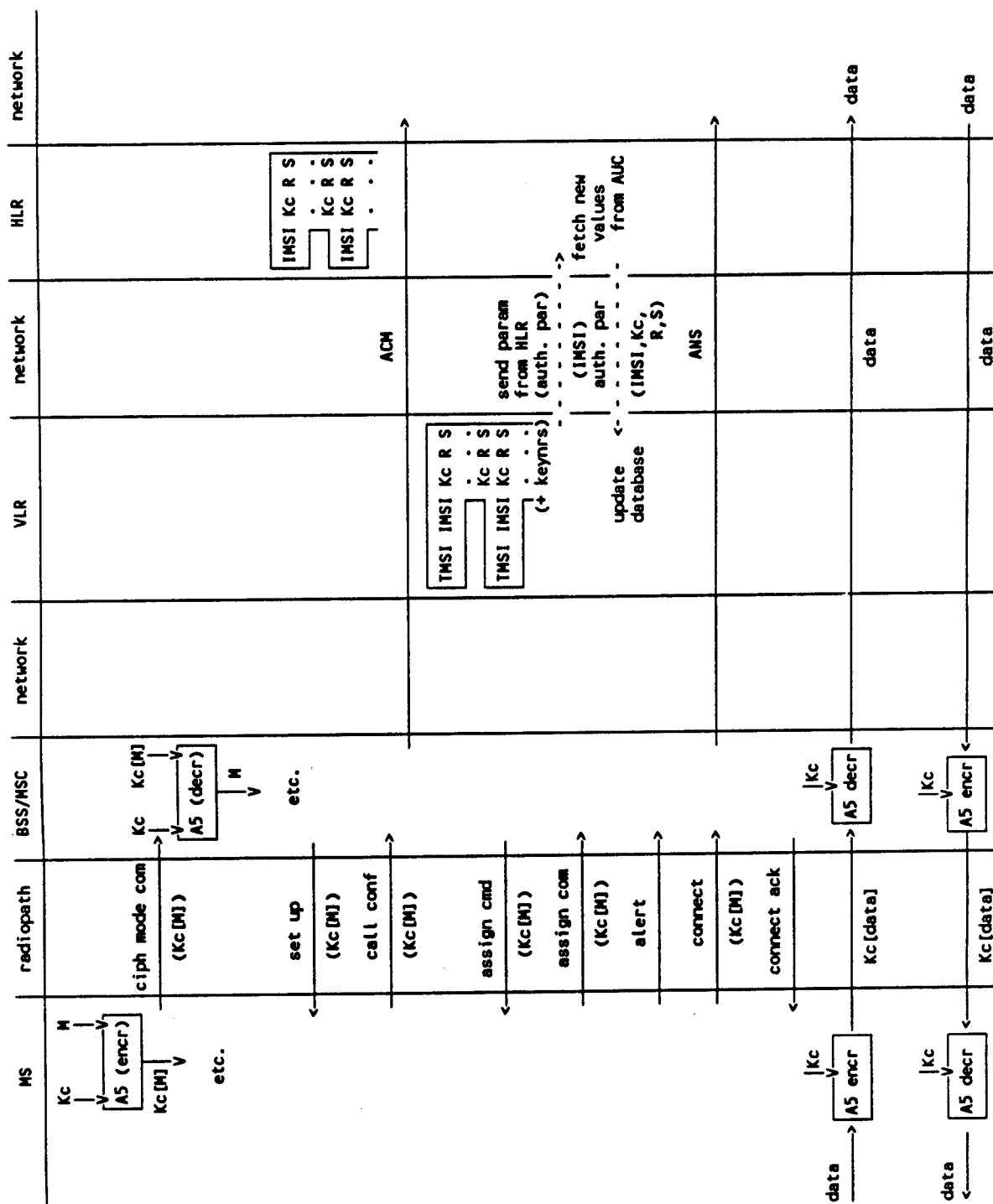
Scheme 6 cont.



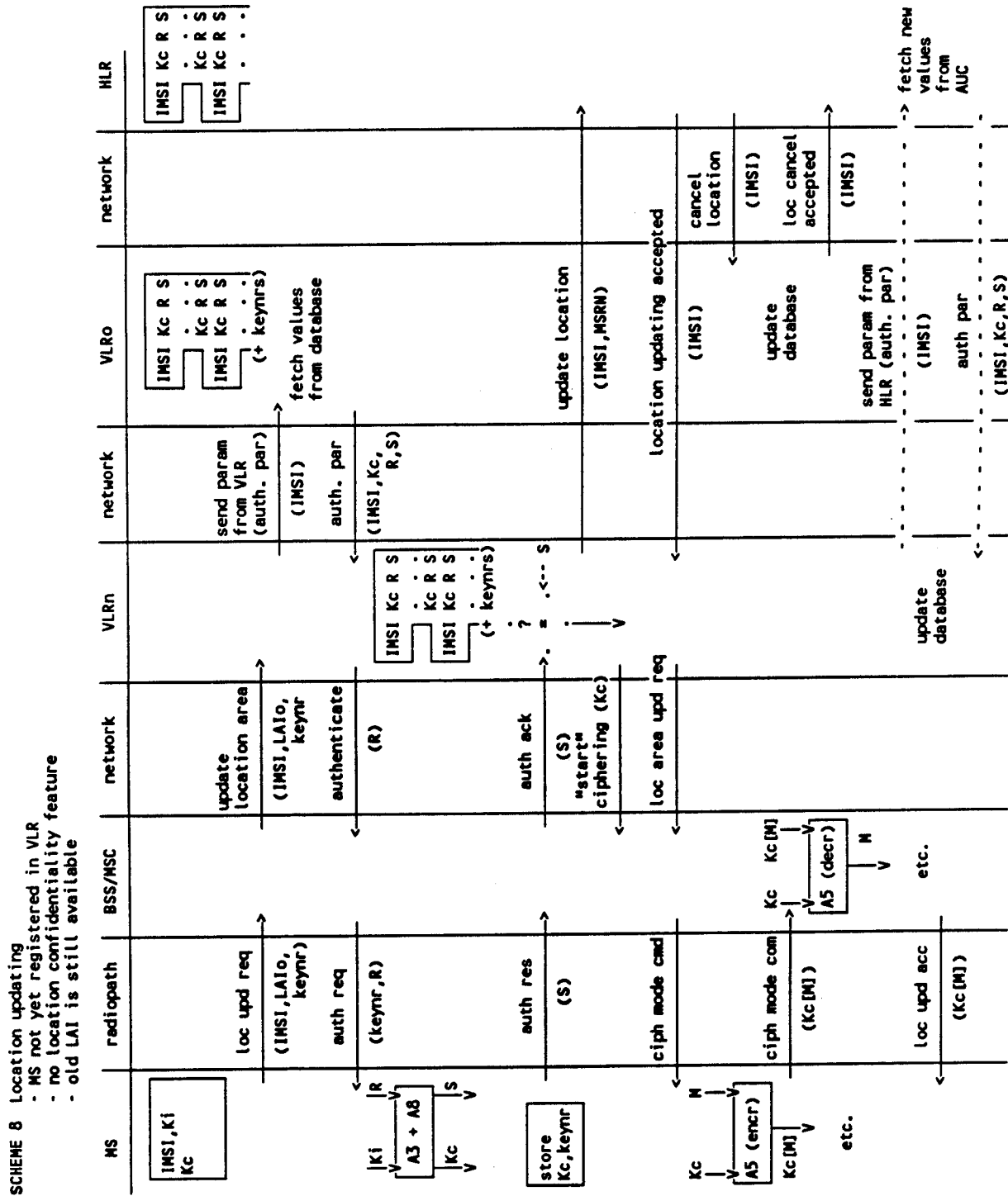
Scheme 7



SCHEME 7 cont.



Scheme 8



ANNEX 2

A2.1. 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 service switching center
- base station
- mobile station
- authentication center

A2.2. Entities and Security Information

* home location register (HLR)

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

* visitor location register (VLR)

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

* mobile services switching center (MSC) / base station (BS)

In the MSC/BS are installed:

- user data encryption algorithm A5
- signalling data encryption algorithm A5

Pairs of TMSI (or IMSI) and cipher key Kc are stored in the database.

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.

* mobile station (MS)

The mobile station contains/receives:

- authentication algorithm A3
- user data encryption algorithm A5
- signalling data encryption algorithm A5
- cipher key generating algorithm A8
- individual subscriber authentication key Ki
- cipher key Kc
- cipher key sequence number
- TMSI

*** authentication center (see note)**

In the authentication center are implemented:

- authentication algorithm A3
- cipher key generating algorithm A8

The secret individual authentication keys K_i of all subscribers of a PLMN are stored in the authentication center of the PLMN.

Note : The authentication center is a functional entity, the implementation of which may vary from one network to another network.

ANNEX 3

A3.0. SCOPE

This document specifies the cryptological algorithms which are needed to provide the various security features and mechanisms defined in, respectively, Recommendation GSM 02.09 and Recommendation GSM 03.20.

Three algorithms have been addressed in Recommendation GSM 03.20 as follows:

- Algorithm A3 : Authentication algorithm;
- Algorithm A5 : Ciphering/deciphering algorithm;
- Algorithm A8 : Cipher 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 is specified in Section 1. The internal specifications of Algorithm A5 are managed under the responsibility of MOU; they will be made available by 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. For those PLMN operators who wish to, proposals for Algorithm A3 and A8 are managed by MOU and available upon an appropriate request.

A3.1. SPECIFICATIONS FOR ALGORITHM A5

A3.1.1. Purpose

As defined in Recommendation GSM 03.20, Algorithm A5 realized 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 encipherment and decipherment processes (especially at hand-over) must be guaranteed.

A3.1.2. Implementation Indications

Algorithm A5 is implemented into both the MS and the BS. On the BS side, as it concerns the evaluations made in the sequel, it is assumed that one algorithm A5 is implemented for each physical channel (TCH or DCCH).

The ciphering takes place just before modulation and after interleaving (see the figure in Annex 1 of Rec. GSM 05.01); the deciphering takes place just after demodulation symmetrically. Both the encipherment and decipherment processes need Algorithm A5. They start at different times (see Rec. GSM 03.20, Section 4.4).

As an indication, recall that, due to the TDMA techniques used into the system, the useful information 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 Rec. GSM 05.02) and transmitted during a time slot. According to Rec. 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 Rec. GSM 05.01).

For ciphering, Algorithm A5 produces, each 4.615 ms, a sequence of 114 cipher/decipher bits (here called BLOCK) which is combined by a bit wise modulo 2 addition to the 114 bits plain text block. The first cipher/decipher bit produced by A5 is added to e0, the second to e1 and so on. As an indication, the resulting 114 bits block is then applied to the burst builder (see the figure in Annex 1 of Rec. GSM 05.01). Deciphering is quite symmetrical: A5 produces a sequence of 114 cipher/decipher bits and the first produced bit is added to e0, etc...

For each slot, the decipherment is performed on the MS side with the first block (BLOCK1) of 114 bits produced by A5, and the encipherment is performed with the second produced block (BLOCK2). As a consequence, on the network side, BLOCK1 is used for encipherment and BLOCK2 for decipherment. Therefore, Algorithm A5 must produce twice 114 bits each 4.615 ms (i.e. BLOCK1 and BLOCK2).

Synchronization is guaranteed by driving Algorithm A5 by an explicit time variable, COUNT, derived from the TDMA frame number. Therefore, each 114 bits block produced by A5 only depends on the TDMA frame numbering, and of the cipher key Kc.

COUNT is expressed on 22 bits as the concatenation of the binary representation of T1, T3 and T2 and is an input parameter of Algorithm A5. The coding of COUNT is shown in figure 1.1a/GSM 03.20-Annex 3.

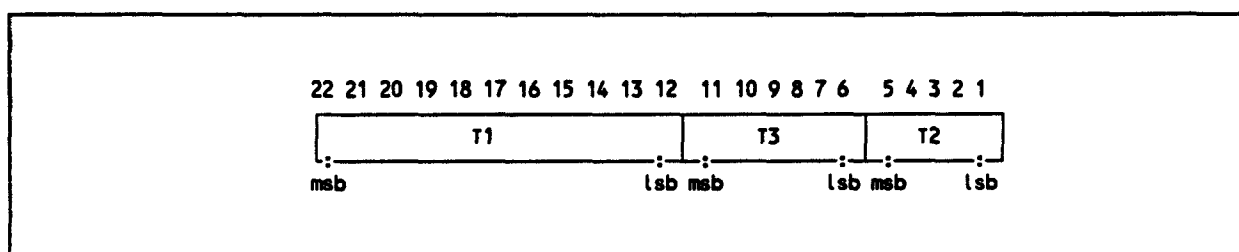


Figure 1.1a/GSM 03.20-Annex 3

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 binary represented. (For definition of T1, T3 and T2 see Recommendation GSM 05.02)

Figure 1.1 summarizes the above listed implementation indications, with only one ciphering/deciphering procedure represented (the second one for deciphering/ciphering is symmetrical).

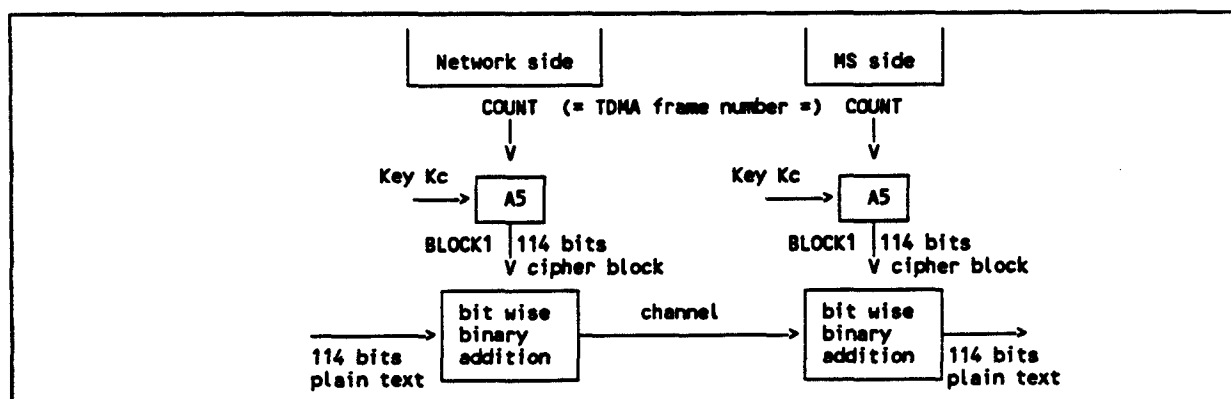


Figure 1.1 / GSM 03.20 - Annex 3
Decipherment on the MS side.

A3.1.3. External specifications of Algorithm A5

The two input parameters (COUNT and Kc) and the output parameters (BLOCK1 and BLOCK2) of Algorithm A5 shall follow 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 cipher key is less than 64 bits, then it is assumed that the actual cipher key corresponds to the most significant bits of Kc, and that the remaining and less significant bits are set to zero.

A3.1.4. Internal specification of Algorithm A5

Contact MOU

A3.2. ALGORITHM A3

Algorithm A3 is considered as a national matter by GSM. Therefore, only external specifications are given. However a proposal for a possible Algorithm A3 is managed by MOU and available upon request.

A3.2.1. Purpose

As defined in Recommendation GSM 03.20, the purpose of Algorithm A3 is to provide an authentication of a mobile subscriber.

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 authenticating key Ki (as an indication, recall that Ki is a secret key allocated to a mobile subscriber at subscription, and that it must be protected).

A3.2.2. Implementation and operational requirements

On the MS side, Algorithm A3 is contained in a Subscriber Identity Module, as specified in Recommendation GSM 02.17.

On the network side, it may be implemented in various entities (HLR/AC or VLR), as specified in Recommendation GSM 03.20 (see Section 3.3.1 and 3.3.2).

The two input parameters (RAND and Ki) and the output parameter (SRES) of Algorithm A3 shall follow the following formats:

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

The run-time of Algorithm A3 must be less than 500 ms.

A3.2.3. Proposal for an Algorithm A3

Contact MOU

A3.3. ALGORITHM A8

Algorithm A8 is considered as a national matter as Algorithm A3. However, since the maximum length of the actual cipher key, i.e. the bits which are significant and non-predictable by a third party, is fixed by a mutual agreement within MOU, this impacts on the internal specifications of A8

A proposal for a possible Algorithm A8 is managed by MOU and available upon request.

A3.3.1. Purpose

As defined in Recommendation GSM 03.20, Algorithm A8 must compute the cipher key Kc from the random challenge RAND sent during the authentication procedure, using the authentication key Ki.

A3.3.2. Implementation and operational requirements

On the MS side, Algorithm A8 is contained in the SIM, as specified in Recommendation GSM 02.17.

On the network side, Algorithm A8 should be 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.

The maximum length of the actual cipher key being fixed by MOU, Algorithm A8 shall produce this actual cipher key and present it into a 64 bit word where the non-significant bits are forced to zero. It is assumed that these (eventual) non-significant bits are the least significant bits and that, the actual cipher key contains the most significant bits

A3.3.3. Proposals for an Algorithm A8

Contact MOU