3GPP TSG-SA3 Meeting #34
Acapulco, Mexico, 6-9 July 2004

Tdoc ⌘S3-040529

CR-Form-v7

CHANGE REQUEST

⌘ **43.020** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **5.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Introducing the special RAND mechanism as a principle for GSM/GPRS
Source:	⌘	Orange, Nokia
Work item code:	⌘	GERAN Security
Date:	⌘	28/06/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	As there is no cryptographic key separation between GSM / GPRS encryption algorithms, it cannot be controlled with which algorithm the ciphering key may be used.
Summary of change:	⌘	Introduces the special RAND mechanism described in [S3-030588] to restrict the ciphering algorithms with which a particular GSM or GPRS ciphering key may be used.
Consequences if not approved:	⌘	There is no mean to restrict the algorithms with which the ciphering key may be used.
Clauses affected:	⌘	3.2, 4.3, 4.5, B.2.4, C.4, D.3.3.1, D.4.5, D.4.3

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 24.008, 44.018, 33.102
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** BEGIN SET OF CHANGES *****

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.

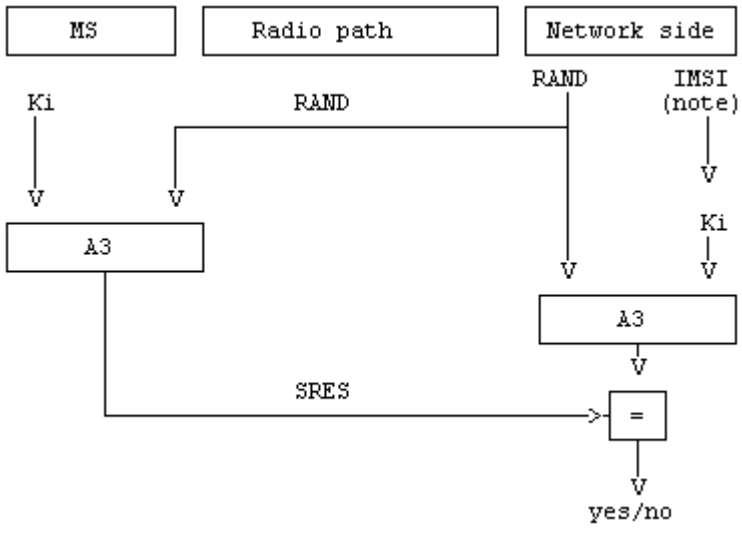
Two network functions are necessary: the authentication procedure itself, and the key management inside the fixed subsystem.

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~~128-bit A3 and A8 input parameter RAND to the MS. The exact structure of RAND is specified in Annex C. RAND contains a non-predictable number, and also allows an Encryption Algorithms Restriction Vector (EARV) to be derived that describes restrictions on the set of encryption algorithms the MS is authorized to use with the ciphering key (see Annex C, Section C.4).
- 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.

***** END SET OF CHANGES *****

***** BEGIN SET OF CHANGES *****

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 and the encryption algorithms restriction vector (EARV) derived from RAND are~~is~~ stored by the mobile station until it is updated at the next authentication.

If for any reason the encryption algorithms restriction vector (EARV) associated with Kc is lost, the MS behaves as if no Kc value is available in the mobile when a "start cipher" message is received from the network without prior Kc update and when the CKSN value associated with Kc has to be sent to the network.

Key setting is schematized in figure 4.1.

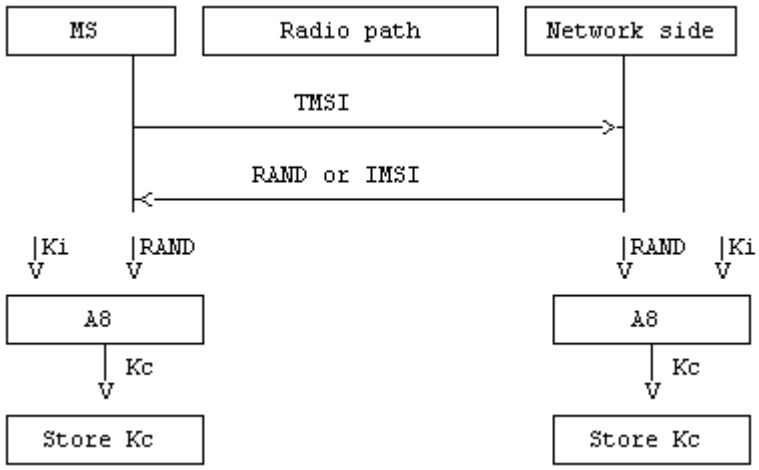


Figure 4.1: Key setting

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". The MS checks that the requested encryption algorithm is authorized by the Encryption Algorithms Restriction Vector (EARV) associated with Kc. 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.

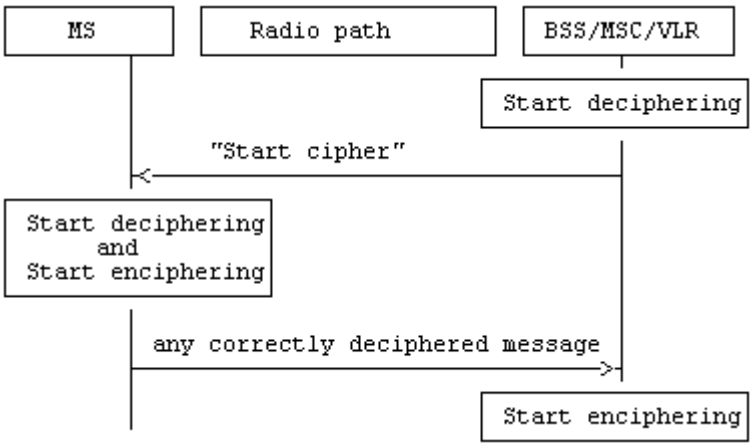


Figure 4.2: Starting of the enciphering and deciphering processes

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.

***** END SET OF CHANGES *****

***** BEGIN SET OF CHANGES *****

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;
- encryption algorithms restriction vector;
- 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.

***** END SET OF CHANGES *****

***** BEGIN SET OF CHANGES *****

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.

C.4 Structure of RAND

This Section describes how the MS shall interpret the 128-bit values RAND it receives from the network at authentication. The received 128-bit RAND value may be either a special RAND value, the structure of which is depicted in the scheme hereafter, or simply be an unstructured value consisting of 128 non predictable bits. It is left as a home operator option to use either structure. In both cases, the received RAND value is taken (unmodified) as the input to the authentication and ciphering key generation algorithms A3 and A8, and also allows the MS to derive the Encryption Algorithms Restriction Vector (EARV) associated with the ciphering key derived from RAND.

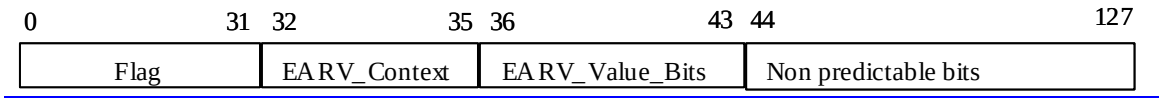
The Encryption Algorithms Restriction Vector (EARV) consists of the EARV_Context and EARV_Value_Bits. The EARV derivation procedure in the MS is the following: The MS checks whether bits 0 to 31 of RAND (contained in the first 4 octets of RAND) are all set to 1. If this is the case, the received RAND is treated as a special RAND value, and the EARV_Context value is extracted from bits 32-35 and EARV_Value_Bits from bits 36-43 of RAND as explained below. Otherwise, the received RAND value is interpreted as an unstructured value: bits 32-43 have no specific signification, the 4 EARV_Context bits to be set in the MS are set to 0000 (GSM) or 0001 (GPRS) depending on the domain in which authentication is performed and the 8 EARV_Value_Bits to be stored in the MS are set to 1.

If the EARV_Context bits are set to GSM, the EARV_Value_Bits consists of 8 binary values indicating which of the algorithms A5/0 to A5/7 are authorised (namely which associated binary value is equal to 1). If the EARV_Context bits are set to GPRS, the EARV_Value_Bits consists of 8 binary values indicating which of the algorithmsGEA0 to GEA7 are authorised (namely which associated binary value is equal to 1).

In GSM/GPRS, the EARV value derived from RAND is stored in the MS at the same time as the associated ciphering key. Each time a command governing the encryption state of the MS is received from the network (e.g. CIPHER

MODE COMMAND in circuit-switched GSM, AUTHENTICATION AND ENCRYPTION REQUEST in GPRS, etc.), the consistency of the requested algorithm with the EARV value associated with the current ciphering key value (Kc or GPRS-Kc) shall be checked by the MS, and the command shall not be executed if the binary value corresponding to the requested algorithm is set to 0. The binary value associated with A5/0 (circuit switched GSM) or GEA0 (GPRS) shall be checked every time a command instructing the MS not to cipher is received from the network, and the command shall not be executed if the binary value associated with A5/0 (resp. GEA0) is set to 0. In GSM, if the EARV_Context bits are not set to GSM access, all the algorithms A5/0 to A5/7 are forbidden. In GPRS, if the EARV_Context bits are not set to GPRS access, all the algorithms GEA0 to GEA7 are forbidden.

The structure of special RAND values is the following:



Bit 0 is the most significant bit of RAND and bit 127 is the least significant bit of RAND.

- length of Flag: 32 bits;
- lenth of EARV_Context: 4 bits;
- length of EARV_Value_Bits : 8 bits;
- length of Non predictable bits: 84 bits.

Flag :

In special RAND values, the flag is set to a particular binary pattern (all 32 bits set to 1) to indicate that bits 32-43 shall be interpreted by the MS as the EARV value.

EARV_Context:

The following values are defined:

- GSM: 0000
- GPRS: 0001
- WLAN scenario 2: 0010
- WLAN scenario 3: 0011

Other values are reserved for future use.

EARV_Value_Bits:

When EARV_Context is set to 0000, the EARV_Value_Bits parameter indicates which encryption algorithms the ciphering key value K_C derived from RAND may be used with. Bits 36-43 indicate which of A5/0…A5/7 it may be used with,. For each of these 8 bits, value 1 indicates that the corresponding algorithm is allowed and value 0 indicates that the corresponding algorithm is forbidden.

When EARV_Context is set to 0001, the EARV_Value_Bits parameter indicates which encryption algorithms the ciphering key value GPRS-Kc derived from RAND may be used with. Bits 36-43 indicate which of GEA0…GEA7 it may be used with. For each of these 8 bits, value 1 indicates that the corresponding algorithm is allowed and value 0 indicates that the corresponding algorithm is forbidden.

When EARV_Context is set to 0010, EARV_Value_Bits parameter indicates which authentication algorithms the ciphering key value Kc may be used with when performing WLAN scenario 2 authentication. Bit 36 indicates EAP-SIM version 1 with IEEE 802.11i. Other bits are reserved for future use.

When EARV_Context is set to 0011, EARV_Value_Bits parameter indicates which authentication algorithms the ciphering key value Kc may be used with when performing WLAN scenario 3 authentication. Bit 36 indicates EAP-SIM version 1 inside IKEv2 (assuming this protocol is chosen; otherwise FFS).

NOTE : The permitted encryption algorithm settings should be maintained and kept homogeneous per operator's network in order to keep open the possibility for pre-calculation of Authentication Vectors at the AuC

***** END SET OF CHANGES *****

***** BEGIN SET OF CHANGES *****

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.

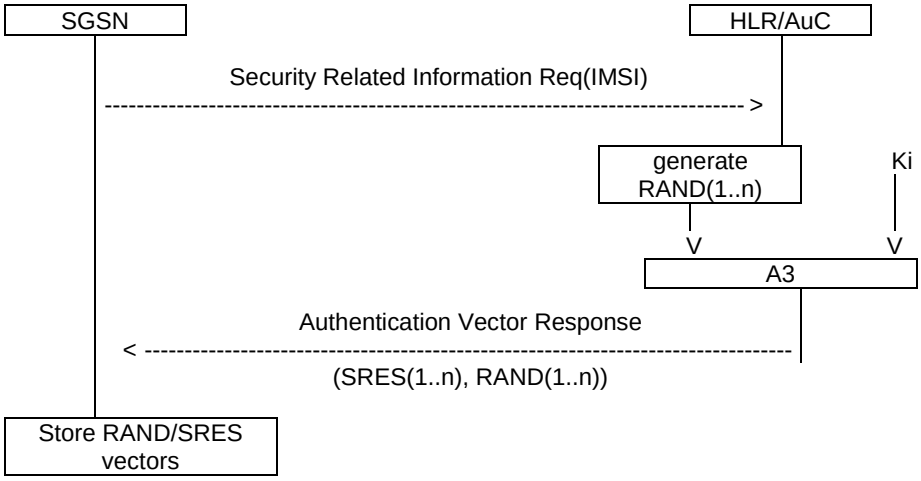


Figure D.3.2: Procedure for updating the vectors RAND/SRES

When an SGSN performs an authentication, including the case of a routing area updating within the same SGSN area, it chooses a 128-bit 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. The exact structure of RAND is specified in Annex C. RAND contains a non-predictable number, and also allows an Encryption Algorithms Restriction Vector

(EARV) to be derived that describes restrictions on the set of encryption algorithms the MS is authorized to use with the ciphering key (see Annex C, Section C.4).

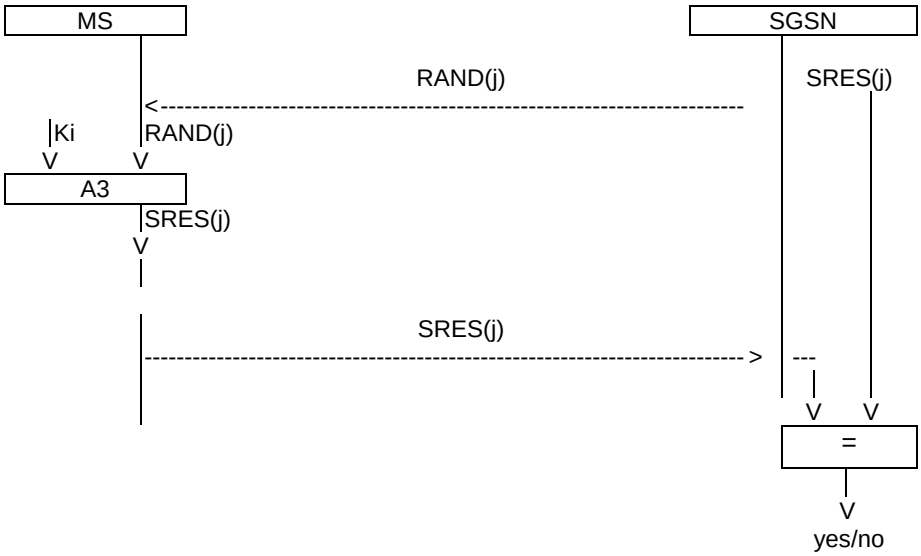


Figure D.3.3: General authentication procedure

***** END SET OF CHANGES *****

***** BEGIN SET OF CHANGES *****

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 and the encryption algorithms restriction vector (EARV) derived from RAND are ~~is~~ stored by the mobile station until it is updated at the next authentication.

If for any reason the encryption algorithms restriction vector (EARV) associated with GPRS-Kc is lost, the MS behaves as if no Kc value is available in the mobile when an authentication and ciphering request is received from the network without prior GPRS-Kc update and when the GPRS-CKSN value associated with GPRS-Kc has to be sent to the network.

Key setting is schematised in figure D.4.1.

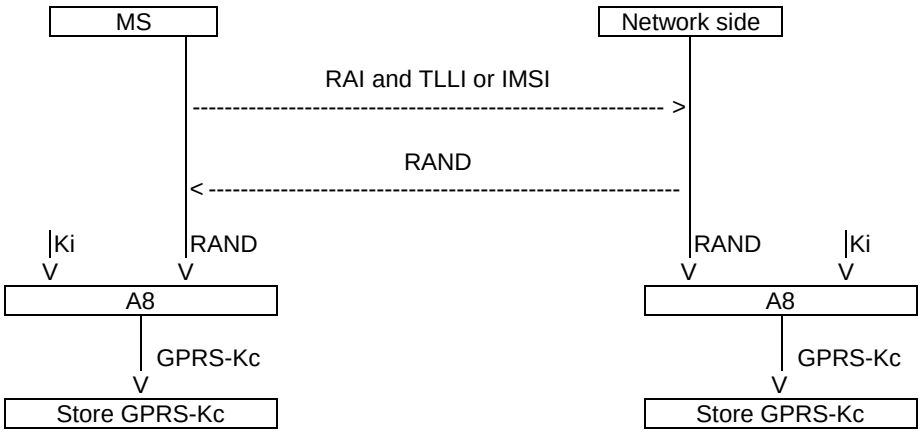


Figure D.4.1: Key setting

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 and Ciphering Request message. If ciphering is used, the MS starts ciphering after checking that the requested encryption algorithm is authorized by the Encryption Algorithms Restriction Vector (EARV) associated with GPRS-Kc and sending the Authentication and Ciphering Response message. The SGSN starts ciphering when a valid Authentication and Ciphering Response message is received from the MS.

Upon GPRS Attach, if ciphering is to be used, an Authentication and Ciphering Request message shall be sent to the MS to start ciphering.

If the GPRS-CKSN stored in the network does not match the GPRS-CKSN received from the MS in the Attach Request message, then the network should authenticate the MS.

As an option, the network may decide to continue ciphering without authentication after receiving a Routing Area Update Request message with a valid GPRS-CKSN. Both the MS and the network shall use the latest ciphering parameters. The MS starts ciphering after a receiving a valid ciphered Routing Area Update Accept message from the network. The SGSN starts ciphering when sending the ciphered Routing Area Update Accept message to the MS.

Upon delivery of the Authentication and Ciphering Response message or the Routing Area Update Accept message, 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.

***** END SET OF CHANGES *****