3GPP TSG SA WG3 (Security) meeting #12
Stockholm, 11-14 April, 2000

Document S3-000289
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	CR		Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG SA #8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM	X	ME	X	UTRAN / Radio	X	Core Network	X

Source: Ericsson **Date:** 2000-04-13

Subject: Clarification on the HFN handling

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:
- to clarify that the initial HFN information contains one HFN per CN domain
- to clarify that the start usage of new generated IK and CK implies a reset of the initial HFN, i.e. a reset of the COUNT-C and COUNT-I parameters
- editorial modifications

Clauses affected: 6.4.1, 6.4.2, 6.4.5

Other specs affected:

Other 3G core specifications		→	List of CRs:
Other GSM core specifications		→	List of CRs:
MS test specifications		→	List of CRs:
BSS test specifications		→	List of CRs:
O&M specifications		→	List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.4 Local authentication and connection establishment

Local authentication is obtained by integrity protection functionality.

6.4.1 Cipher key and integrity key setting

Authentication and key setting are triggered by the authentication procedure and described in 6.3. Authentication and key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. P-TMSI, TMSI or IMSI) is known by the VLR/SGSN. The CK and IK are stored in the VLR/SGSN and transferred to the RNC when needed. The CK and IK for the CS domain are stored on the USIM and updated at the next authentication from this domain. The CK and IK for the PS domain are stored on the USIM and updated at the next authentication from this domain.

If an authentication procedure is performed during a connection (PS or CS mode), the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the UE as part of the security mode ~~negotiation~~ set-up procedure (see 6.4.5) that follows the authentication procedure.

6.4.2 Ciphering and integrity mode negotiation

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM Classmark which cipher and integrity algorithms the MS supports. This information itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving the MS/USIM Classmark this information must be stored in the RNC. The data integrity of the classmark is performed, during the security mode set-up procedure by use of the most recently generated IK (see section 6.4.5).

The network shall compare its integrity protection 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 ~~SN~~ have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the network ~~SN~~ have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UIA algorithm for use on that connection.

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 UEA 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 no versions of the UEA algorithm in common and the user (respectively the user's HE) and the network are willing to use an unciphered connection, then an unciphered connection shall be used.

~~2~~3) If the MS and the network have at least one version of the UEA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection.

~~3) If the MS and the network have no versions of the UEA algorithm in common and the user (respectively the user's HE) and the SN are willing to use an unciphered connection, then an unciphered connection shall be used.~~

Because of the separate mobility management for CS and PS services, one CN domain may, independent of the other CN, establish a connection to one and the same MS. Change of ciphering and integrity mode (algorithms) at establishment of a second MS to CN connection shall not be permitted. The preferences and special requirements for the ciphering and integrity mode setting shall be common for both domains. (e.g. the order of preference of the algorithms).

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and MSC/VLR respective SGSN. The three exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.

- If there is no MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), i.e. in the case of deactivation indication sent from the MS followed by connection release.

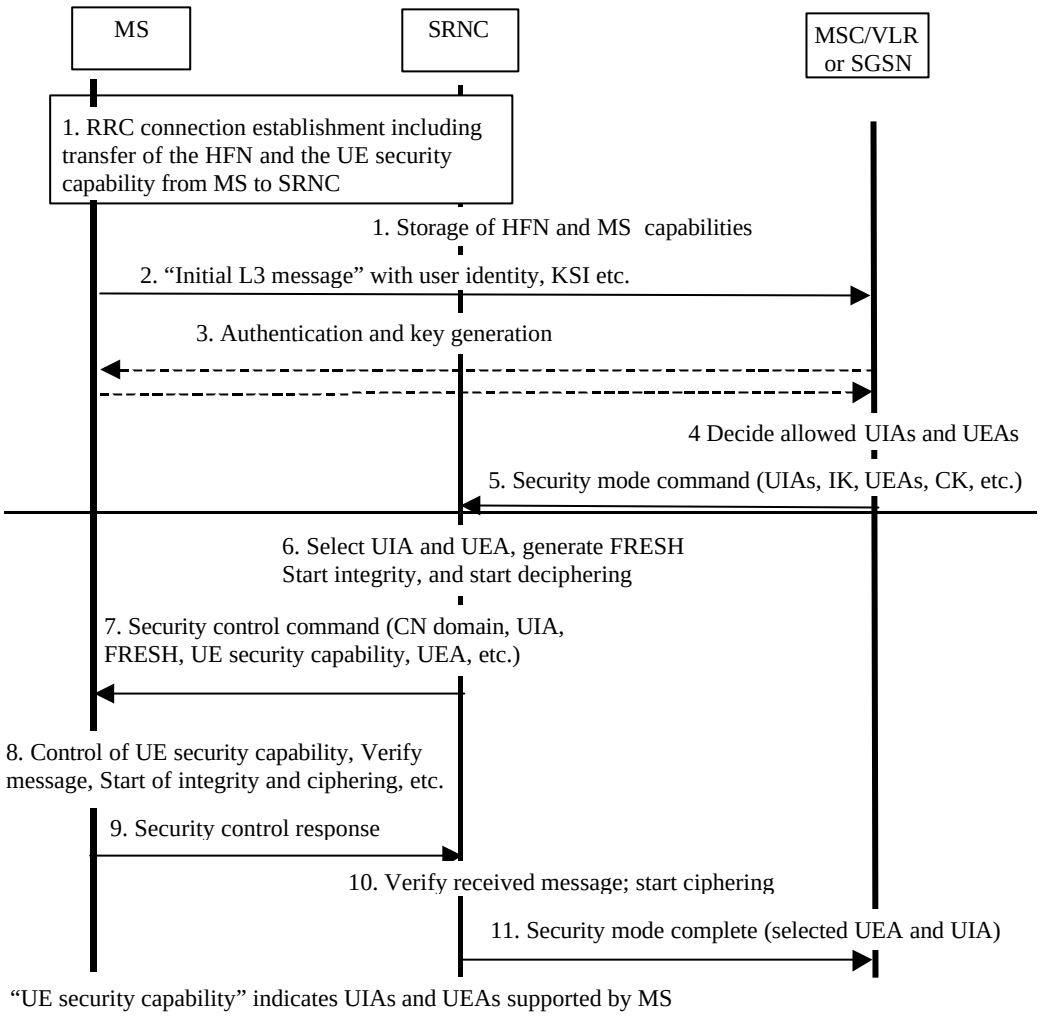
- If the only MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.

When the integrity protection shall be started, the only procedures between MS and MSC/VLR respective SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to MSC/VLR or SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and

- Authentication and key agreement

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.



"UE security capability" indicates UIAs and UEAs supported by MS

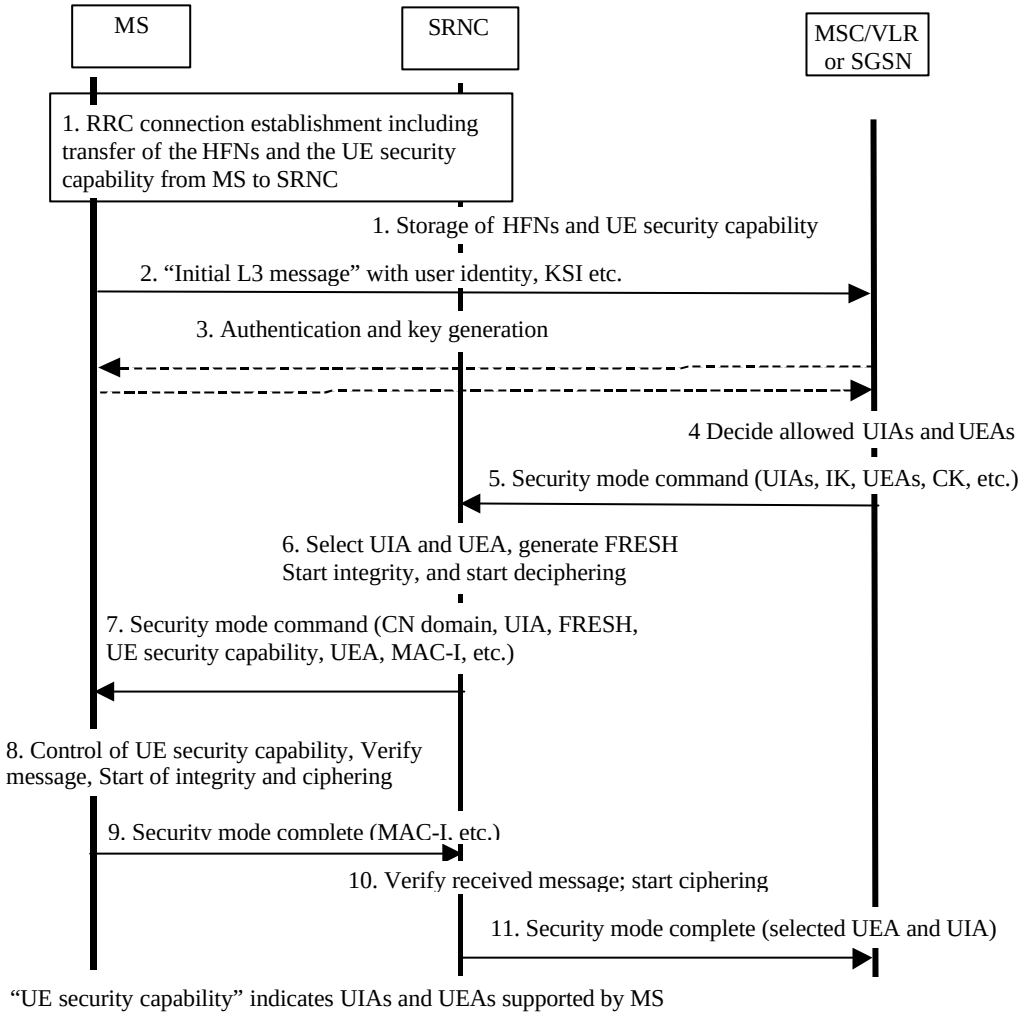


Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "UE security capability" information before the integrity protection can start, i.e. the "UE security capability" must be sent to the network in an unprotected message. Returning the "UE security capability" later on to the ~~UE~~ ME in a protected message will give ~~UE~~ ME the possibility to verify that it was the correct "UE security capability" that reached the network.
~~This latter point, as well as the RRC interwork described below, is yet to be agreed in RAN WG2.~~

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the UE security ~~capabiltiy~~ capability and the initial hyperframe numbers (HFN) for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The initial HFN is used to initialise the HFN to be used as part of ~~one of~~ the input parameters COUNT-I, for the integrity algorithm, and COUNT-C, for the ciphering algorithm. The ~~COUNT-I parameter (together with COUNT which is used for ciphering) is~~ initial HFNs and the UE security capability information are stored in the SRNC.

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the ~~relevant CN domain~~ MSC/VLR or SGSN. This message contains ~~relevant MM information~~ e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the ~~number~~ KSI allocated by the ~~CN~~ CS service domain or PS service domain at the last authentication for this CN domain.

3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.

4. The ~~CN node~~ MSC/VLR or SGSN determines which UIAs and UEAs that are allowed to be used.

5. The ~~CN~~ MSC/VLR or SGSN initiates integrity ~~(~~and ~~possible also~~ ciphering~~)~~ by sending the RANAP message Security Mode Command to SRNC. This message contains a list of allowed UIAs in the order of preference and the IK to be used. If ciphering shall be started, it ~~It may also~~ contains the allowed UEAs in the order of preference and the CK to be used. If a new authentication and security key generation has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of new generated keys implies that the initial HFN to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the HFN already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting from the list of allowed algorithms, ~~the first UEA and the first UIA it~~ and the list of algorithms supported by the MS ~~supports~~ (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC ~~supports no UIA algorithms in the list, it~~ sends a SECURITY MODE REJECT message to ~~Cn~~the requesting MSC/VLR or SGSN. The further actions are described in 6.4.2.

7. The SRNC generates the RRC message Security ~~control~~ mode command. The message includes the UE security capability, the UIA and FRESH to be used and ~~possibly~~ if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. Because of that the MS can have two ciphering and integrity key sets ~~Since we have two CNs with an IK each~~, the network must indicate which ~~IK~~ key set to use. This is obtained by including a CN type indicator information in the ~~"~~Security ~~control~~ mode command~~"~~ message. Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security ~~control~~ mode command message, the MS controls that the UE security capability received is equal to the UE security capability sent in the initial message. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security ~~control command response~~mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in the MS~~a SECURITY CONTROL REJECT message is sent from the MS~~.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the ~~CN node~~ MSC/VLR or SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. also all following downlink messages sent to the MS are integrity protected and possibly ciphered. The Security mode ~~command response~~complete from MS starts the uplink integrity protection and possible ciphering, i.e. also all following messages sent from the MS are integrity protected and possibly ciphered.