3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000120**
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	060	Current Version:	3.3.1

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

For submission to:	TSG SA #7	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		ME	X	UTRAN / Radio	X	Core Network	X

Source:	Ericsson	**Date:** 2000-02-17
Subject:	Clarification on the security mode set-up message sequence flow	
Work item:	Security	

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

F	Correction	X
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change:
The HFN information that is sent from MS to RNC at connection establishment contains one HFN value for each CN domain (i.e. one HFN for each established security key set).
The start of usage of new generated security keys implies a reset of the COUNT parameter.
Editorial modifications

Clauses affected: 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.

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. This procedure is mandatory. The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

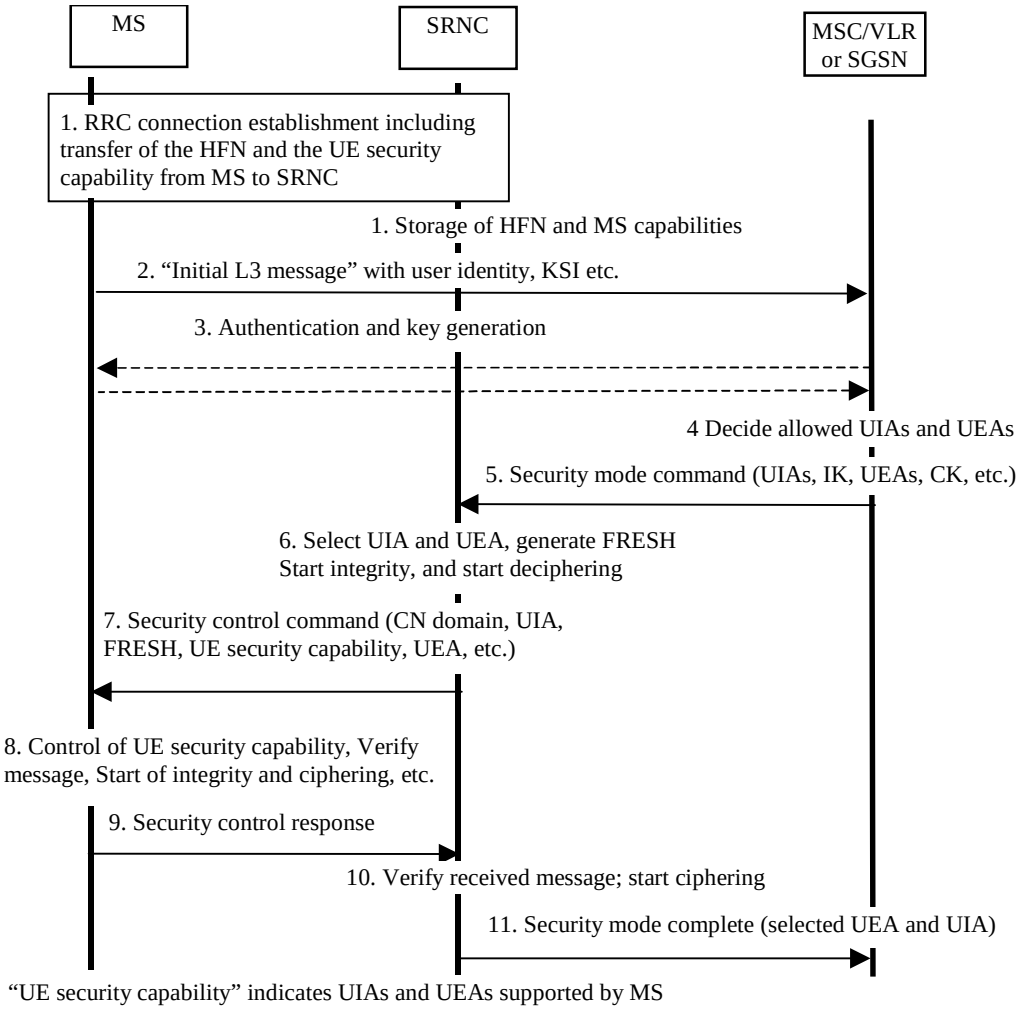

Figure 14: Local authentication and connection set-up

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 in a protected message will give UE 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 information and the hyperframe numbers (HFN) for the CS service domain respective PS service domain. The HFN is ~~to be~~ used as part of one of the input parameters for the integrity algorithm and for the ciphering algorithm (see 6.5.2). The HFN and MS capability information is stored in the SRNC.~~The COUNT-I parameter (together with COUNT which is used for ciphering) is 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 section 6.2). In addition, ~~A~~authentication of the user and generation of new security keys (IK and CK) may be performed (see section 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 MSC/VLR (or SGSN)~~CN~~ initiates integrity ~~(~~and ~~possible also~~ ciphering~~)~~ by sending the RANAP message Security Mode Command to SRNC. This message contains a list of allowed UIAs and the IK to be used. If ciphering shall be started, it ~~It may~~ also contains the allowed UEAs and the CK to be used. If a new authentication and security key generation has been performed (see point 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.

6. The SRNC decides which algorithms to use by selecting from the list of allowed algorithms, the ~~first~~ most preferred UEA and the ~~first~~ most preferred UIA ~~it~~ that both the SRNC and the MS supports. 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 the requesting MSC/VLR (or SGSN)~~CN~~. The further actions are description in 6.4.2.

7. The SRNC generates the RRC message Security control 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 key set~~IK~~ to use. This is obtained by including a CN type indicator information in "Security control command". 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 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 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~~ MSC/VLR (or SGSN)~~node~~ 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 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.