

CR-Form-v7	CHANGE REQUEST
# TS 33.102 CR CRNum # rev - # Current version: 5.2.0 #	

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:	#	IMEISV retrieval before completion of security mode setup procedure
Source:	#	SA WG3
Work item code:	#	LATE_UE
		Date: # 27/08/2003
Category:	#	F
		Use <u>one</u> of the following categories: <i>F</i> (correction) <i>A</i> (corresponds to a correction in an earlier release) <i>B</i> (addition of feature), <i>C</i> (functional modification of feature) <i>D</i> (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .
		Release: # Rel-5 Use <u>one</u> 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:	#	The Serving Network needs to be able to retrieve the IMEISV before ciphering is started to be able to handle faulty ciphering behavior of not fully ciphering tested early UE's. TS 33.102 currently forbid the retrieval of IMEISV before completion of security mode set-up procedure. Such a restriction has not been implemented within Stage-3 specification (i.e. TS 24.008).
Summary of change:	#	Remove the restriction to retrieve IMEISV before security mode setup procedure has been completed.
Consequences if not approved:	#	The Serving Network will not be able to recognise and handle Early UE with faulty ciphering behavior when ciphering is activated.

Clauses affected:	#	6.4.5; 5.1.5								
Other specs affected:	#	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td style="text-align: center;">Y</td><td style="text-align: center;">N</td></tr> <tr><td style="text-align: center;">#</td><td style="text-align: center;">N</td></tr> <tr><td style="text-align: center;">#</td><td style="text-align: center;">N</td></tr> <tr><td style="text-align: center;">#</td><td style="text-align: center;">N</td></tr> </table> Other core specifications	Y	N	#	N	#	N	#	N
	Y	N								
	#	N								
#	N									
#	N									
#	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td style="text-align: center;">#</td><td style="text-align: center;">N</td></tr> <tr><td style="text-align: center;">#</td><td style="text-align: center;">N</td></tr> </table> Test specifications	#	N	#	N					
#	N									
#	N									
#	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr><td style="text-align: center;">#</td><td style="text-align: center;">N</td></tr> </table> O&M Specifications	#	N							
#	N									
Other comments:	#									

***** Start of change *****

5.1.5 Mobile equipment identification

~~In certain cases, The~~ SN may request the MS to send it the ~~mobile equipment identity~~ IMEI or IMEISV of the terminal. ~~The mobile equipment identity shall only be sent after authentication of SN with exception of emergency calls.~~ The IMEI should be securely stored in the terminal. However, the presentation of this identity to the network is not a security feature and the transmission of the IMEI or IMEISV ~~may~~ ~~is not~~ ~~be~~ ~~un~~protected. Although it is not a security feature, it should not be deleted from UMTS however, as it is useful for other purposes.

***** End of change *****

***** Start of change *****

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 VLR/SGSN. The four 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-VLR/SGSN signalling after the initial L3 signalling message sent from MS to VLR/SGSN, i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-VLR/SGSN signalling after the initial L3 signalling message sent from MS to VLR/SGSN, and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.
- If the call is an emergency call teleservice as defined in TS 22.003, see section 6.4.9.2 below.

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

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

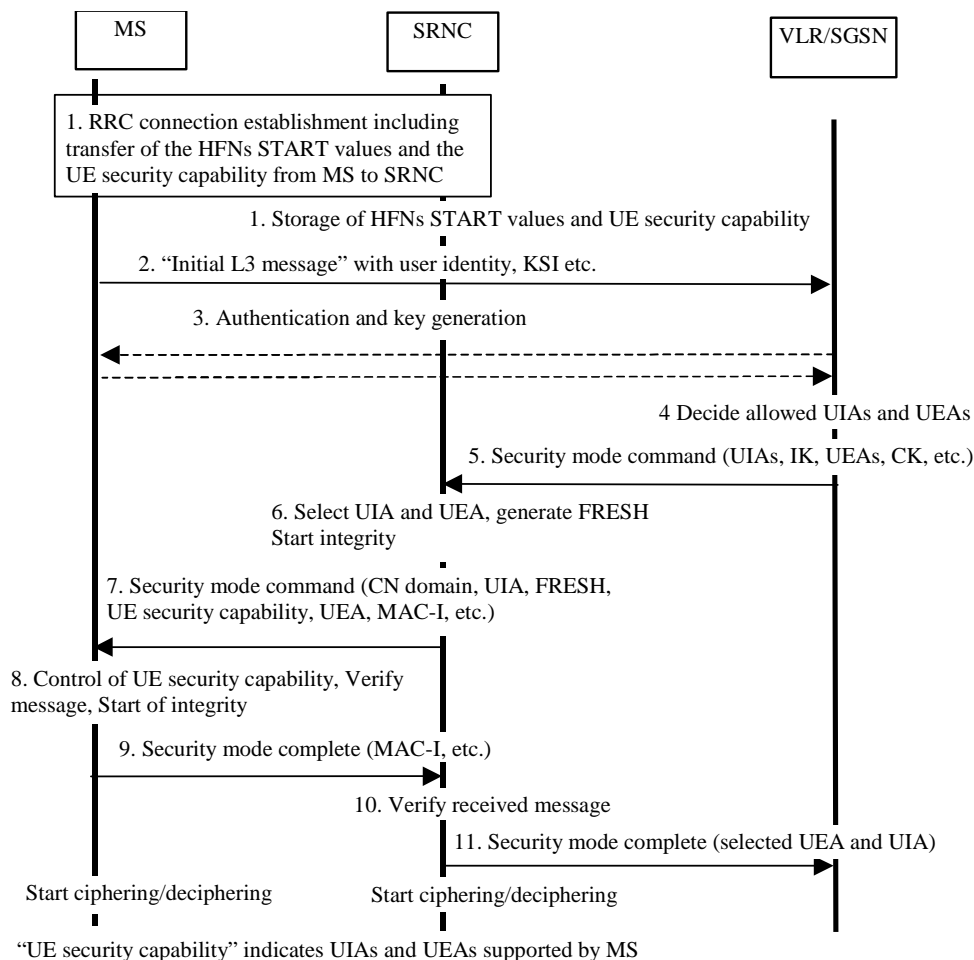


Figure 14: Local authentication and connection set-up

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.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ME security capability optionally the GSM Classmarks 2 and 3 and the START values 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 START values and the UE security capability information are stored in the SRNC. If the GSM Classmarks 2 and 3 are transmitted during the RRC Connection establishment, the RNC must store the GSM ciphering capability of the UE (see also message 7).
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 VLR/SGSN. This message contains e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the 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 VLR/SGSN determines which UIAs and UEAs that are allowed to be used in order of preference.

5. The VLR/SGSN initiates integrity and ciphering by sending the RANAP message Security Mode Command to SRNC. This message contains an ordered list of allowed UIAs in order of preference, and the IK to be used. If ciphering shall be started, it contains the ordered list of allowed UEAs in 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 START value to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the START value already available in the SRNC that shall be used (see 1. above).
6. The SRNC decides which algorithms to use by selecting the highest preference algorithm from the list of allowed algorithms that matches any of the algorithms supported by the MS (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 sends a SECURITY MODE REJECT message to the requesting VLR/SGSN. The further actions are described in 6.4.2.
7. The SRNC generates the RRC message Security mode command. The message includes the ME security capability, optionally the GSM ciphering capability (if received during RRC Connection establishment), the UIA and FRESH to be used and 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, the network must indicate which key set to use. This is obtained by including a CN type indicator information in the Security 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 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 same applies to the GSM ciphering capability if it was included in the RRC Connection Establishment. 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 mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in 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 VLR/SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. this and all following downlink messages sent to the MS are integrity protected using the new integrity configuration. The Security mode complete from MS starts the uplink integrity protection, i.e. this and all following messages sent from the MS are integrity protected using the new integrity configuration. When ciphering shall be started, the Ciphering Activation time information that is exchanged between SRNC and MS during the Security mode set-up procedure sets the RLC Sequence Number/Connection Frame Number when to start ciphering in Downlink respective Uplink using the new ciphering configuration.

***** End of change *****