DRAFT 3G 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:	3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG		for approval	X	*(only one box should*
list TSG meeting no. here ↑		for information		*be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

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

Source:	Siemens Atea	**Date:**	2000-Feb-20

Subject: HE control over accepting non-ciphered connections

3G Work item: Security

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

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	X
D	Editorial modification	

Reason for change: Provide the HE with the ability to allow non-ciphered connections only on certain serving networks by means of the AMF in AUTN.
To enable that, the ciphering mode negotiation has to be changed, because the current negotiation mechanism already sends the user's capabilities before the user (possibly) receives AUTN. The change also allows the negotiation to take the user's preferences fully into account (a security requirement!) while saving on signalling.

Clauses affected: 6.4.2, 6.4.5, Annex F

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other 2G 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.

6.4.2 Cipher ~~key~~ mode 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 message itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving the~~ The MS/USIM Classmark ~~the cipher and i~~must be stored in the RNC ~~and the integrity of the classmark with the newly generated IK and this value is transmitted to the RNC after the authentication procedure is complete~~.

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 SN have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the 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 now send the security mode command to the user with the selected integrity mode, a copy of the received user's integrity capabilities and the network's ciphering capabilities. The security mode command message is the first integrity protected message. Upon receipt, the user verifies the integrity of the received information, and compares the received user's integrity capabilities with the stored user's integrity capabilities.

The ~~network~~ user equipment shall compare its ciphering capabilities ~~and preferences~~, and any special ~~requirements~~ preferences of the ~~subscription of the MS~~USIM, with ~~those~~ the capabilities indicated by the ~~MS~~ network 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 or the MS is not prepared to use an unciphered connection, then the connection shall be released.

2) If the MS and the network have at least one version of the UEA algorithm in common, then the ~~network~~ UE shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection, and if the USIM has indicated a preference, it shall take that preference into account.

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

The user sends shall now send the network the security mode response with the selected ciphering mode.

Both service domains (CS and PS) that belong to the same serving network shall allow the same cipher modes, i.e., $UEA\text{-}CN_{CS} = UEA\text{-}CN_{PS}$. When a connection is already established with a first service domain, it is not allowed that the cipher mode for the connection with the second service domain is different.

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.

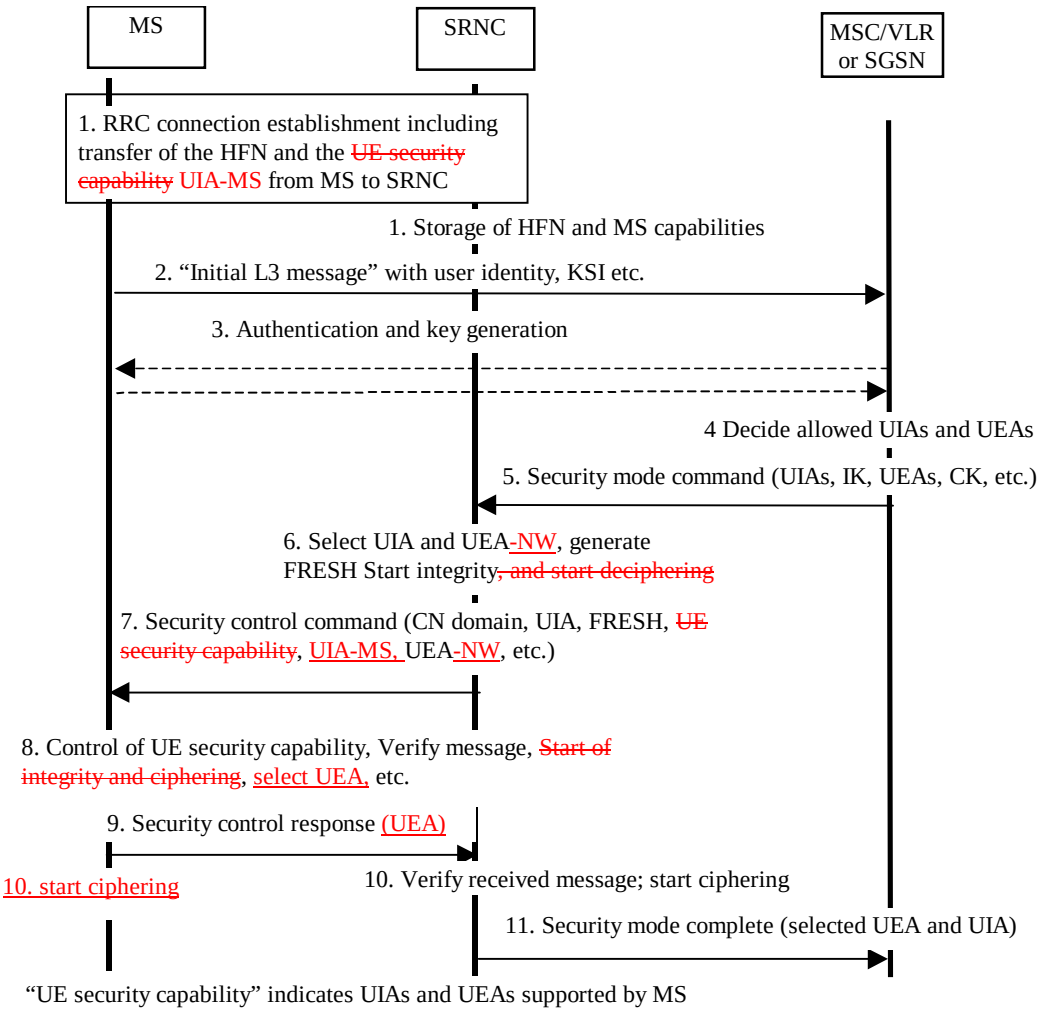

Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the ~~"UE security capability"~~user's integrity capabilities (UIA-MS) information before the integrity protection can start, i.e. the UIA-MS ~~"UE security capability"~~ must be sent to the network in an unprotected message. Returning the UIA-MS ~~"UE security capability"~~ later on to the UE in a protected message will give UE the possibility to verify that it was the correct UIA-MS ~~"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 user's integrity capabilities (UIA-MS) ~~UE security capabiltiy~~ and the hyperframe number to be used as part of one of the input parameters for the integrity algorithm and for the ciphering algorithm. 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. This message contains relevant MM information e.g. KSI. The KSI (Key Set Identifier) is the number allocated by the CN at the last authentication for this CN domain.

3. Authentication of the user and generation of new security keys (IK and CK) may be performed. A new KSI will

then also be allocated.

4. The CN node determines which UIAs and UEAs that are allowed to be used.

5. The 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. It may also contain the allowed UEAs and the CK to be used.

6. The SRNC decides which integrity ~~algorithms~~ algorithm to use by selecting from the list of allowed algorithms, ~~the first UEA and the first UIA it supports~~and the list of integrity algorithms supported by the user. The SRNC determines the list of ciphering algorithms UEA-NW that are allowed by the CN and supported by the SRNC. The SRNC generates a random value FRESH and initiates the downlink integrity protection. If SRNC supports no UIA algorithms in the list, it sends a SECURITY MODE REJECT message to CN.

7. The SRNC generates the RRC message Security control command. The message includes the ~~UE security capability~~UIA-MS, the UIA and FRESH to be used, the ciphering algorithms supported by the network UEA-NW ~~and possibly also the UEA to be used~~. ~~Additional information (start of ciphering) may also be included.~~ Since we have two CNs with an IK each, the network must indicate which 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~~ UIA-MS received is equal to the ~~UE security capability~~ UIA-MS 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. The MS then selects a ciphering mode UEA according to the received network's capabilities -UEA-NW an the user's ciphering capabilities and preferences (controlled by the USIM).

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, a SECURITY CONTROL REJECT message is sent from the MS.

10. After sending the response message, the UE starts ciphering and deciphering. 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. At receipt of the response message, the SNRC starts ciphering and deciphering.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the CN node ends the procedure.

The Security mode command to MS starts ~~the downlink~~ integrity protection, i.e. also all following ~~downlink~~ messages ~~sent to~~ exchanged between ~~the~~ MS and RNC are integrity protected ~~and possibly ciphered~~. The first message following the ~~Security~~ security mode command response from MS possibly starts ~~the uplink integrity protection and possible~~ ciphering (if UEA ≠ 0), i.e. also all following messages ~~sent from~~ exchanged between the MS and the RNC are ~~integrity protected and~~ (possibly) ciphered.

Annex F (informative): Example uses of AMF

F.1 Support multiple authentication algorithms and keys

A mechanism to support the use of multiple authentication and key agreement algorithms is useful for disaster recovery purposes. AMF may be used to indicate the algorithm and key used to generate a particular authentication vector.

The USIM keeps track of the authentication algorithm and key identifier and updates it according to the value received in an accepted network authentication token.

F.2 Changing list parameters

This mechanisms is used in conjunction with the window and list mechanisms described in C.2.

Parameters which may be used to manage a lsit are the number of entries in a list (the list size) and an upper list on the admissible $SEQ_{MS} - SEQ$ between the highest batch number SEQ_{MS} in the list and an accepted batch number SEQ. A mechanism to change these parameters dynamically is useful since the optimum for these parameters may change over time. AMF is used to indicate the maximum admissible list size or maximum admissible difference $SEQ_{MS} - SEQ$ to be used by the user when verifying the authentication token and deciding whether it is still accepted.

The USIM keeps track of the maximum admissible list size and maximum admissible difference $SEQ_{MS} - SEQ$ and updates them according to the received value providing that $SEQ > SEQ_{MS}$.

F.3 Setting threshold values to restrict the lifetime of cipher and integrity keys

According to section 6.4.3, the USIM contains a mechanism to limit the amount of data that is protected by an access link key set. The AMF field may be used by the operator to set or adjust this limit in the USIM. For instance, there could be two threshold values and the AMF field instructs the USIM to switch between them.

The USIM keeps track of the limit to the key set life time and updates it according to the value received in an accepted network authentication token.

F.4 Ciphering capability management

The AMF can be used to manage the ciphering capabilities that are supported or acceptable to the UE/USIM. The mechanism can be used to allow non-ciphered connections only on certain serving networks.