

<h2 style="margin: 0;">CHANGE REQUEST</h2>				<i>Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.</i>	
33.102		CR	xxx	Current Version: 3.5.0	
<small>GSM (AA.BB) or 3G (AA.BBB) specification number ↑</small>			<small>↑ CR number as allocated by MCC support team</small>		
For submission to: SA #9		for approval for information		strategic	
<small>list expected approval meeting # here ↑</small>		<input checked="" type="checkbox"/>		<input type="checkbox"/> (for SMG use only)	
		<input type="checkbox"/>		<input type="checkbox"/>	

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

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

Source: Ericsson **Date:** 2000-09-07

Subject: Clarifications on integrity and cipherring of radio bearers.

Work item: Security

Category: <small>(only one category shall be marked with an X)</small>	F Correction	<input checked="" type="checkbox"/>	Release: Phase 2 <input type="checkbox"/> Release 96 <input type="checkbox"/> Release 97 <input type="checkbox"/> Release 98 <input type="checkbox"/> Release 99 <input checked="" type="checkbox"/> Release 00 <input type="checkbox"/>
	A Corresponds to a correction in an earlier release	<input type="checkbox"/>	
	B Addition of feature	<input type="checkbox"/>	
	C Functional modification of feature	<input type="checkbox"/>	
	D Editorial modification	<input type="checkbox"/>	

Reason for change: Alignment with TS 25.331.
 - Use of "radio bearer" instead of "logical channel"
 - There is only one RRC connection established between MS and Serving RNC.
 - Editorial modifications.

Clauses affected: 6.4.8, 6.5.5, 6.6.2, 6.6.4.2, 6.6.5

Other specs affected:	Other 3G core specifications	<input type="checkbox"/>	→ List of CRs:	
	Other GSM core specifications	<input type="checkbox"/>	→ List of CRs:	
	MS test specifications	<input type="checkbox"/>	→ List of CRs:	
	BSS test specifications	<input type="checkbox"/>	→ List of CRs:	
	O&M specifications	<input type="checkbox"/>	→ List of CRs:	

Other comments:



help.doc

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

6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a START_{CS} value for the CS cipher/integrity keys and a START_{PS} value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the START_{CS} and the START_{PS} value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting START_{CS} and START_{PS} to THRESHOLD.

The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to the START value of the corresponding service domain; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection), the RLC SN (for ciphering) and the MAC-d HFN (for ciphering) are initialised to 0.

During an ongoing radio connection, the START_{CS} value in the ME is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and CS user data logical channels protected using CK_{CS} and/or IK_{CS}, incremented by 1, i.e.:

$$\text{START}_{\text{CS}} = \text{MSB}_{20} (\text{MAX} \{ \text{COUNT-C}, \text{COUNT-I} \mid \text{all } \text{logical channels} \text{ radio bearers (including signalling) protected with CK}_{\text{CS}} \text{ and IK}_{\text{CS}} \}) + 1.$$

Likewise, during an ongoing radio connection, the START_{PS} value in the ME is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling radio bearers and PS user data radio bearers logical channels protected using CK_{PS} and/or IK_{PS}, incremented by 1, i.e.:

$$\text{START}_{\text{PS}} = \text{MSB}_{20} (\text{MAX} \{ \text{COUNT-C}, \text{COUNT-I} \mid \text{all } \text{radio bearers (including signalling) logical channels protected with CK}_{\text{PS}} \text{ and IK}_{\text{PS}} \}) + 1.$$

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates START_{CS} and START_{PS} in the USIM with the current values.

During authentication and key agreement the ME sets the START values of the corresponding service domain to 0 in the USIM and in the ME itself.

6.5.5 Integrity key selection

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user.

The data integrity of radio bearers logical channels for user data is not protected.

The signalling radio bearers are used for transfer of sSignalling data for services delivered by either of both CS and PS service domains is sent over common logical (signalling) channels. These signalling radio bearers logical channels are data integrity protected by the IK of the service domain for which the most recent security mode negotiation took place. This may require that the integrity key of an (already integrity protected) ongoing signalling connection has to be changed, when a new RRC-connection is established (with another service domain), or when a security mode negotiation follow a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.

6.6.2 Layer of ciphering

The ciphering function is performed either in the RLC sub-layer or in the MAC sub-layer, according to the following rules:

- If a logical channel is expected to be supported on a common transport channel and has to be ciphered, it shall use UM RLC mode and ciphering is performed at the RLC sub-layer.

- If a ~~radio bearer logical channel~~ is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-layer.
- If a ~~radio bearer logical channel~~ is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).

Ciphering when applied is performed in the S-RNC and the ME and the context needed for ciphering (CK, HFN, etc.) is only known in S-RNC and the ME.

6.6.4.2 CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. ~~Which The CK cipher key~~ to use for a particular ~~radio bearer logical channel~~ is described in 6.6.65. For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key K_c , as described in 8.2.

CK is stored in the USIM and a copy is stored in the ME. CK is sent from the USIM to the ME upon request of the ME. The USIM shall send CK under the condition that 1) a valid CK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The ME shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of the quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) security mode command.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.

6.6.5 Cipher key selection

There is one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user.

The ~~radio bearers logical channels~~ for CS user data are ciphered with CK_{CS} .

The ~~radio bearers logical channels~~ for PS user data are ciphered with CK_{PS} .

~~The signalling radio bearers are used for transfer of signalling data (for services delivered by both CS and PS services) domains is sent over common logical channels.~~ These ~~signalling radio bearers logical channels~~ are ciphered by the CK of the service domain for which the most recent security mode negotiation took place. This may require that the cipher key of an (already ciphered) ongoing signalling connection ~~is has to be~~ changed, when a new ~~RRC-connection is establishment established with another service domain occurs~~, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.