

<h1>CHANGE REQUEST</h1>		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: SA #8 <i>list expected approval meeting # here ↑</i>	for approval <input checked="" type="checkbox"/> for information <input type="checkbox"/>	strategic <input type="checkbox"/> (for SMG Use only) non-strategic <input type="checkbox"/>

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

Source: Ericsson **Date:** 2000-04-14

Subject: Cipher and integrity key update once every 24 hours

Work item: Security

Category: (only one category shall be marked with an X)	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: The indication that "the VLR/SGSN shall assure that IK and CK are updated at least

Clauses affected: 6.5.4.2, 6.6.4.2

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: This does not exclude that for R00 a procedure to better control the lifetime of the keys is fully specified.



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

6.5.4.2 IK

The integrity key IK is 128 bits long.

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. Which integrity key to use for a particular connection is described in 6.5.6.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f_4 , that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key K_c , as described in 6.8.2.

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

IK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of a quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) *security mode command*. ~~The MSC/VLR or SGSN shall assure that the IK is updated at least once every 24 hours.~~

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

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 cipher key to use for a particular logical channel is described in 6.6.6. For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f_3 , 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 UE. CK is sent from the USIM to the UE upon request of the UE. 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 UE 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. ~~The VLR or SGSN shall assure that CK is updated at least once every 24 hours.~~

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.