

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: 3.4.0	
GSM (AA.BB) or 3G (AA.BBB) specification number ↑	↑ CR number as allocated by MCC support team	
For submission to: TSG SA # 8 <i>list expected approval meeting # here</i> ↑	for approval <input checked="" type="checkbox"/> for information <input type="checkbox"/>	strategic <input type="checkbox"/> non-strategic <input type="checkbox"/> (for SMG use only)

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: Nokia **Date:** 9. April 2000

Subject: Inclusion of the radio bearer identity to the integrity mechanism

Work item:

Category:	F Correction <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 checked="" type="checkbox"/> D Editorial modification <input 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"/>
------------------	--	-----------------	--

(only one category shall be marked with an X)

Reason for change: The radio bearer identity has to affect the message authentication code calculated by the integrity algorithm.

Clauses affected:

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.

6.5.4 Input parameters to the integrity algorithm

6.5.4.1 COUNT-I

The integrity sequence number COUNT-I is 32 bits long.

There is one COUNT-I value per logical signalling channel.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number is the 4-bit RRC sequence number RRC SN that is available in each RRC PDU. The "long" sequence number is the 28-bit RRC hyperframe number RRC HFN which is incremented at each RRC SN cycle.

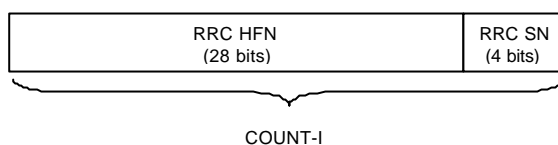


Figure 16a: The structure of COUNT-I

The hyperframe number RRC HFN is initialised by means of the parameter *START*, which is transmitted from UE to RNC during *RRC connection establishment*. The UE and the RNC then initialise the *X* most significant bits of the RRC HFN to *START*; the remaining (28-*X*) LSB of the RRC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel used for signalling.

Editor's note: The value of *X* still needs to be added.

Editor's note: The description of how *START* is managed in the UE needs to be added.

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.

6.5.4.3 FRESH

The network-side nonce FRESH is 32 bits long.

There is one FRESH parameter value per user. The input parameter FRESH protects the network against replay of signalling messages by the user. At connection set-up the RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any

old MAC-Is.

At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it in a new *security mode command* to the user.

6.5.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the integrity algorithm used to compute the message authentication codes would use an identical set of input parameter values for the up-link and for the down-link messages.

6.5.4.5 MESSAGE

The signalling message itself with the radio bearer identity. The latter is appended in front of the message. Note that the radio bearer identity is not transmitted with the message but it is needed to avoid that for different instances of message authentication codes the same set of input parameters is used.