3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000177**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

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 063r1 Current Version: 3.3.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG SA #7	for approval	X	strategic	□	*(for SMG*
list expected approval meeting # here ↑		for information	□	non-strategic	□	*use only)*

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

Source:	Ericsson	**Date:**	2000-02-17
Subject:	Clarification of the HFN handling		
Work item:	Security		

Category:	F	Correction	X	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	X
					Release 00	□

Reason for change: A reset of the HFN is performed at start using new generated security keys.
Editorial changes (e.g. COUNT-I introduced in the figure 16)

Clauses affected: 6.5.2

Other specs affected:	Other 3G core specifications	□	→ List of CRs:
	Other GSM 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.

6.5.2 Integrity algorithm

The UIA shall be implemented in the UE and in the RNC.

Figure 16 illustrates the use of the UIA to authenticate the data integrity of a signalling message.

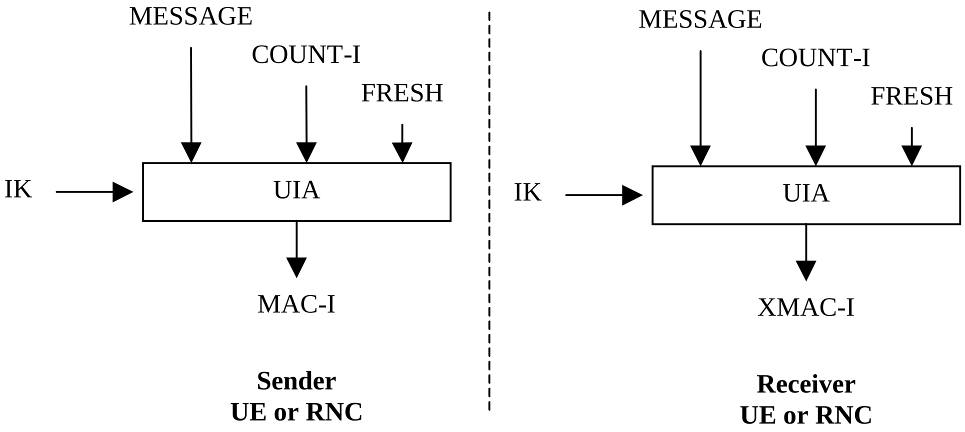

Figure 16: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), a time dependent input (COUNT-I), a random value generated by the network side (FRESH), the direction bit (DIRECTION) and the signalling data (MESSAGE). Based on these input parameters the user computes message authentication code for data integrity (MAC-I) using the UMTS Integrity Algorithm (UIA). The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I.

The input parameter COUNT-I protects against replay during a connection. It is a value incremented by one for each integrity protected message. COUNT-I consists of two parts: the HYPERFRAME NUMBER (HFN) as the most significant part and a RRC Sequence Number as the least significant part. The initial value of the hyperframe number is sent by the user to the network at connection set-up (see 6.4.5). The user stores, on the USIM, the greatest used hyperframe number from the previous connection and increments it by one ~~(see 6.4.5xxx)~~. In this way the user is assured that no COUNT-I value is re-used (by the network) with the same integrity key. A reset of the HFN (HFN=0) is performed when the new generated security key set is used for the first time. The user stores one HFN per established security key set.

The input parameter FRESH protects network against replay of signalling messages by the user. At connection set-up the network generates a random value FRESH and sends it to the user. 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.