3GPP TSG SA 3 meeting #11
Mainz, Germany, 22-24 February 2000

***Document* S3-000129**
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 067 Current Version: 3.2.0

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

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

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
(at least one should be marked with an X)

Source: Siemens Atea **Date:**

Subject: Data integrity

Work item: Security

Category:				**Release:**		
	F	Correction			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	X		Release 98	
with an X)	D	Editorial modification			Release 99	X
					Release 00	

Reason for change: Detail is added to the description of the integrity protection mechanism: the layer of integrity protection is identified and the input values are discussed.

Clauses affected: 6.5

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 Access link data integrity

6.5.1 General

Most RRC, MM and CC signalling information elements are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the ~~MS~~ UE and the ~~SN~~RNC.

~~The UMTS Integrity Algorithm (UIA) shall be used with an Integrity Key (IK) to compute a message authentication code for a given message.~~

All signalling messages except the following ones shall be integrity protected:

- Notification
- Paging Type 1
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete
- RRC Connection Reject
- All System Information messages.

6.5.2 Layer of integrity protection

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

Integrity protection shall be apply at the RRC layer.

~~6.5.2~~6.5.3 ~~Integrity algorithm~~Data integrity protection method

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

Figure 6.5.1 illustrates the use of the ~~UIA~~ integrity algorithm f9 to authenticate the data integrity of a signalling message.

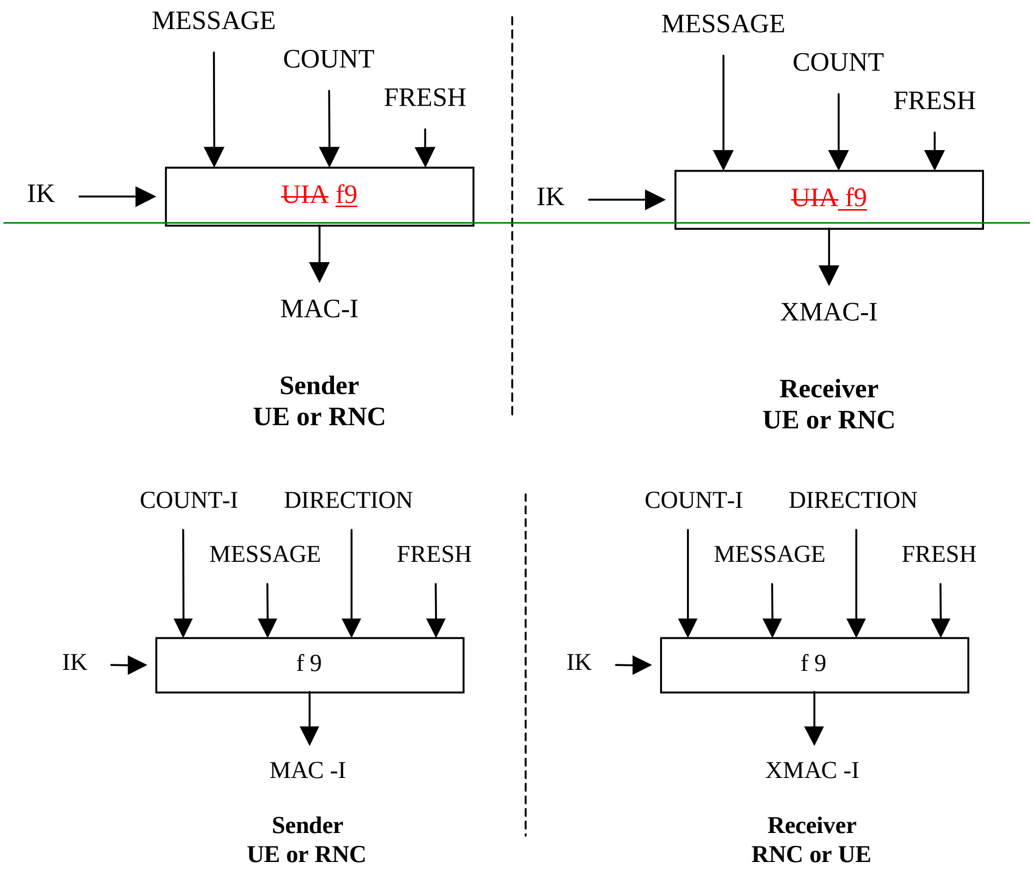

Figure 6.5.1: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the ~~Integrity Key~~ integrity key ~~(~~IK~~)~~, ~~a time dependent input~~the integrity sequence number ~~(~~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)~~integrity algorithm f9. 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.

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 in RLC AM channel, one per logical RLC UM channel and one for all logical channels using the transparent RLC mode (and mapped onto DCH).

The initialisation at the start of a connection and the synchronisation of COUNT-I throughout a connection are detailed in 6.5.5.

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 f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, 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.

For GSM subscribers that access the UTRAN, the IK can be derived from the GSM cipher key Kc, as described in 8.2.

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.

~~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 an 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. The user stores 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.~~

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 network against replay of signalling messages by the user. At connection set-up the ~~network~~ 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.

6.5.5 Synchronisation of data integrity protection

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The update of COUNT-I depends on the transmission mode as described below (see Figure 6.5.2):

- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 25-bit HFN which is incremented at each RLC SN cycle.

- For RLC AM mode, the "short" sequence number is the 12-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 20-bit HFN which is incremented at each RLC SN cycle.

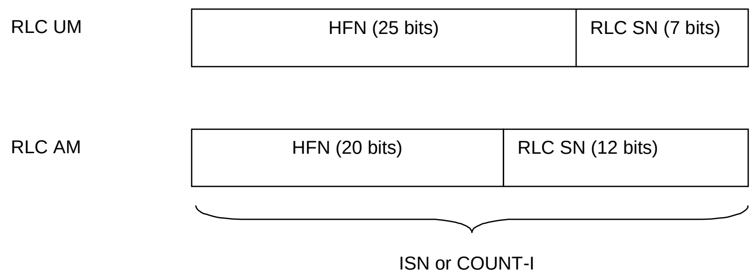

Figure 6.5.2: The structure of COUNT-I for both acknowledged and unacknowledged mode

The hyperframe number HFN is initialised by means of the parameter START, which is stored in the UE (and a copy is stored in the USIM, and is transmitted from UE to RNC during RRC connection establishment, to prevent that the integrity algorithm is re-used with an identical set of input parameter values.

The UE stores a parameter START, which is equal to the highest HFN that the UE is currently using or the highest HFN that the UE has been using in the past with the current IK. If the current IK has not been used yet, then START is 0.

The START parameter is 25 bits long.

A copy of start is stored on the USIM. During an ongoing (integrity protected) RRC connection, only the counter in the UE will be updated. Therefore the UE informs the USIM of connection establishment and the USIM from then on knows its START value is no longer up-to-date.

At connection establishment, the UE sends the RNC the START value in the RRC connection establishment message. For RLC UM logical channels, the initial HFN is initialised to START; for RLC AM logical channels, the HFN is initialised to the 20 MSB of START. The HFN parameters are then incremented independently from one another, at each cycle of the "short" sequence number. Throughout the RRC connection, the UE and the RNC maintain a parameter START, which is equal to the highest HFN value currently in use, incremented by 1.

When a new logical channel is created during an RRC connection, the initial value of HFN is again set to the current START value (or the 20 MSB thereof).

After connection release, the UE sends the up-to-date version of START to the USIM.

When the UE is powered-on, the UE reads the value of START from the USIM. When the copy on the USIM is up-to-date, the USIM will send it to the UE, otherwise it will indicate that a new authentication and key agreement is required. The latter may occur when the UE has been powered-off or the USIM has been removed during an ongoing connection, and the UE did not see a change to update the START value in the USIM.

6.5.6 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 logical channels for user data is not protected.

Signalling data for services delivered by either of both service domains is sent over common logical (signalling) channels. These 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.

6.5.~~3~~7 UIA identification

Each UMTS Integrity Algorithm (UIA) will be assigned a 4-bit identifier. Currently the following values have been defined:

"0001_2" : UIA1, Kasumi.

The remaining values are not defined.

~~**Table1 - UIA identifiation**~~

~~Information Element~~	~~Length~~	~~Value~~	~~Remark~~
~~UIA Number~~	4	~~0000_2~~	~~Standard UMTS Integrity Algorithm, UIA1~~
		~~0001_2~~	~~Standard UMTS Integrity Algorithm, UIA2~~
		~~0010_2~~	~~Standard UMTS Integrity Algorithm, UIA3~~
		~~0011_2 to 0111_2~~	~~Reserved for future expansion~~
		~~$1xxx_2$~~	~~Proprietary UMTS Algorithms~~