3GPP TSG SA 3 Meeting #12
Stockholm, Sweden, 11-14 April 2000

***Document* S3-000256**
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		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 3 #12	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: *(at least one should be marked with an X)* (U)SIM [ ] ME [ ] UTRAN / Radio [X] Core Network [ ]

Source: Siemens Atea **Date:** 3 April 2000

Subject: 3G-3G Handover

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	X

Reason for change:

The length of the START parameter used to initialise the HFN is set to 20 bits.
At handover (with relocation of S-RNC) the old S-RNC sends the new S-RNC:

- a 20-bit START value, such that the new S-RNC can initialise the HFN and synchronisation can resume.
- the value FRESH, rather than that the new S-RNC generates a new FRESH value (current situation).
- the ciphering and integrity protection modes UEA and UIA.
- information on the cipher/integrity keys (CK_{CS}, CK_{PS}, IK_{CS}, IK_{PS} and information on which key set is used for signalling)

Clauses affected: 6.4.8 (new clause), 6.5.4, 6.6.4

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: The length of START (20 bits) is taken from TS 25.331.

help.doc

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

6.4.8 Handover with relocation of S-RNC

At handover with relocation of S-RNC, the old S-RNC derives a value START that equals the 20 most significant bits of the maximum value of the current COUNT-I and COUNT-C values for all existing user data and signalling connections, incremented by 1:

START = MSB_{16} (MAX {COUNT-C, COUNT-I | for all signalling and user data logical channels}) + 1

The old S-RNC sends the new S-RNC a container that is transparently sent through the core network and that:

- shall contain the START value;
- shall contain the FRESH value
- if CK_{CS} and IK_{CS} are being used for user data or signalling connections, shall contain the cipher/integrity keys from the CS domain;
- if CK_{PS} and IK_{PS} are being used for user data or signalling connections, shall contain the cipher/integrity keys from the PS domain;
- shall contain the ciphering and integrity protection modes UEA and UIA that are used;
- shall contain an indication on which cipher/integrity keys are used on the common signalling channels.

Upon receipt of this information, the new S-RNC initialises 20 most significant bits of the RRC HFN, the RLC HFN and the MAC-d HFN to the received START value and sets the remaining bits equal to 0. Also the RRC SN, the RLC HFN and the MAC-d HFN are set equal to 0.

Ciphering (if applied) and integrity protection is resumed with the same ciphering and integrity protection modes, the same cipher/integrity keys, the same value for FRESH, and the same cipher/integrity keys used on the common signalling channels.

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.

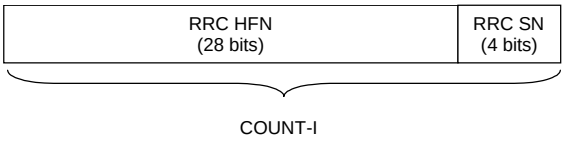

Figure 16a: The structure of COUNT-I

The hyperframe number RRC HFN is initialised by means of the parameter START, which is transmitted from the ~~UE~~ME to the RNC during *RRC connection establishment*. The ~~UE~~ME and the RNC then initialise the ~~X~~ 16 most significant bits of the RRC HFN to START; the remaining ~~(28-X) LSB~~bits 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~~ between the ~~UE~~ME and the USIM 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 f4, 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 Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the ~~UE~~ME. IK is sent from the USIM to the ~~UE~~ME upon request of the ~~UE~~ME. 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~~ME 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.

6.6.4 Input parameters to the cipher algorithm

6.6.4.1 COUNT-C

The ciphering sequence number COUNT-C is 32 bits long.

There is one COUNT-C value per logical RLC AM channel, one per logical RLC UM channel and one for all logical channels using the transparent RLC mode (and mapped onto DCH).

COUNT-C is composed of two parts: a "short" sequence number and a "long" sequence number. The update of COUNT-C depends on the transmission mode as described below (see figure 16c).

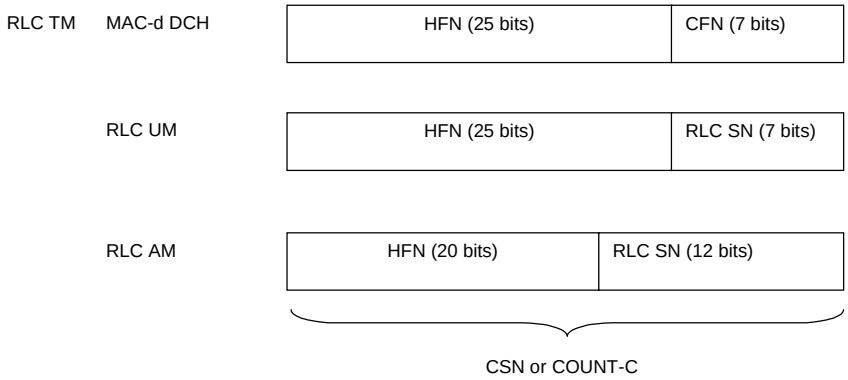

Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 7-bit ciphering frame number CFN of the UEFN. It is independently maintained in the ~~UE~~ME MAC entity and the SRNC MAC-d entity. The "long" sequence number is the 25-bit MAC HFN which is incremented at each CFN cycle. The ciphering sequence number CSN or COUNT-C is identical to the UEFN.

- 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 RLC 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 RLC HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is transmitted from ~~UE~~ME to RNC in *RRC connection establishment*. The ~~UE~~ME and the RNC then initialise the ~~X~~ 16 most significant bits of the RLC HFN and MAC HFN to START; the remaining ~~LSB~~ bits of the RLC HFN and MAC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel.

~~Editor's note: The value of X still needs to be decided.~~

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

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 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 Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the ~~UE~~ME. CK is sent from the USIM to the ~~UE~~ME upon request of the ~~UE~~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 ~~UE~~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. 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.~~

6.6.4.3 BEARER

The logical channel identifier BEARER is 4 bits long.

There is one BEARER parameter per logical channel associated with the same user and multiplexed on a single 10ms physical layer frame. The logical channel identifier is input to avoid that for different keystream an identical set of input parameter values is used.

6.6.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the an identical set of input parameter values.

6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

The length indicator determines the length of the required keystream block. LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.