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

***Document* S3-000259**
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	X	ME	X	UTRAN / Radio		Core Network	

Source:	Siemens Atea
Date:	3 April 2000
Subject:	Initialisation of synchronisation for ciphering and integrity protection
Work item:	Security

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

F	Correction	
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	X
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
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. A description is added on how START is managed between the ME and the USIM such that a COUNT-C or COUNT-I value is never re-used.

Clauses affected: 6.4.8 (new clause), 6.5.4.1, 6.6.4.1

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.

6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a $START_{CS}$ value for the CS cipher/integrity keys and a $START_{PS}$ value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the corresponding START value to the RNC in the *RRC connection setup complete* message. The ME also indicates to the USIM that a radio connection has been established, with again an indication of the serving network domain. The USIM marks the corresponding START value as invalid. The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to START; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection), the RLC SN (for ciphering) and the MAC-d HFN (for ciphering) are initialised to 0.

During an ongoing radio connection, the START value in the ME is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values, incremented by 1, i.e.,

$$START = MSB_{20}\,(\,MAX\,\{COUNT\text{-}C, COUNT\text{-}I \mid \text{for all signalling and user data logical channels}\}) + 1$$

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME informs the USIM and indicates the serving network domain and the current START value for that serving network domain. The USIM updates the corresponding START value and marks it as up-to-date.

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.

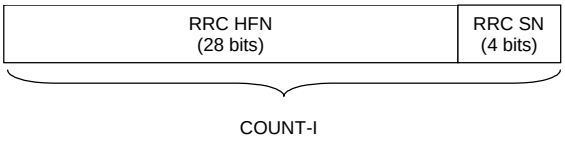

Figure 16a: The structure of COUNT-I

The hyperframe number RRC HFN is initialised by means of the parameter START, which is transmitted from ~~UE~~ME to RNC during *RRC connection establishment*. The ~~UE~~ME and the RNC then initialise the ~~X~~ 20 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 the UE needs to be added.~~

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).

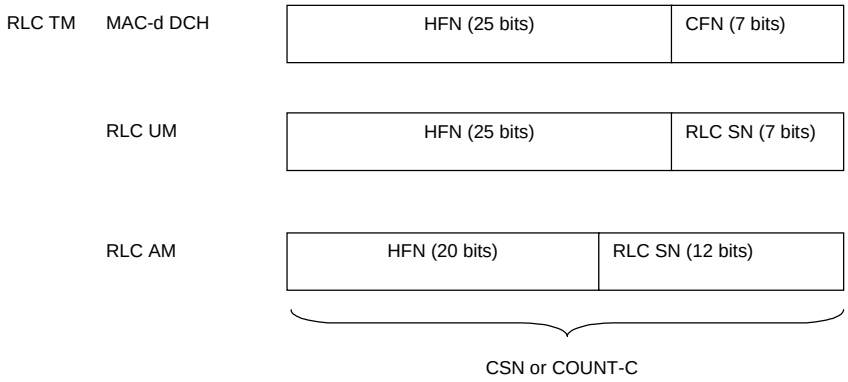

Figure 16c: The structure of COUNT-C for all transmission modes

- 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~~ $_{20}$ 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 needs to be added.~~