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 **xxx**   Current Version: **3.5.0**

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

For submission to:	SA #9	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 ☐   ME **X**   UTRAN / Radio **X**   Core Network ☐
(at least one should be marked with an X)

Source:	Ericsson		**Date:**	2000-09-12

Subject:	Clarifications on the COUNT parameters.

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:	Alignment with TS 25.331, TS 25.321 and TS 25.322 1. "UEFN" and "CSN" should be removed since these terms have no validity 2. There are separate UL/DL COUNT-I respective separate UL/DL COUNT-C per radio bearer. 3. The length of CFN is 8 bits and not 7 bits. 4. Definition of ciphering unit 5. Editorial modifications

Clauses affected:	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:	For clarity reason, this CR includes the changes introduced by CR 105.

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~~up-link signalling radio bearer and one COUNT-I value per down-link signalling radio bearer using RLC AM or RLC UM.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number forms the least significant bits of COUNT-I while the "long" sequence number forms the most significant bits of COUNT-I. 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 hyper frame number (RRC HFN) which is incremented at each RRC SN cycle.
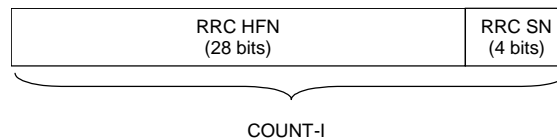
```
+----------------------------------------+------------+
|              RRC HFN                    |   RRC SN   |
|             (28 bits)                   |  (4 bits)  |
+----------------------------------------+------------+
            _____/
                           COUNT-I
```

Figure 16a: The structure of COUNT-I

The ~~hyperframe number~~ RRC HFN is initialised by means of the parameter START, which is described in subsection 6.4.8~~transmitted from ME to RNC during *RRC connection establishment*~~. The ME and the RNC then initialise the 20 most significant bits of the RRC HFN to START; the remaining bits of the RRC HFN are initialised to 0. ~~The RRC HFN are incremented independently for each logical channel used for signalling.~~

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~~ are one COUNT-C value per up-link radio bearer and one COUNT-C value per down-link radio bearer using ~~logical~~ RLC AM ~~channel, one per logical~~ or RLC UM. There are one up-link COUNT-C value and one down-link COUNT-C value~~channel and one~~ for all ~~logical channels~~radio bearers 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 "short" sequence number forms the least significant bits of COUNT-C while the "long" sequence number forms the most significant bits of COUNT-C. The update of COUNT-C depends on the transmission mode as described below (see figure 16c).
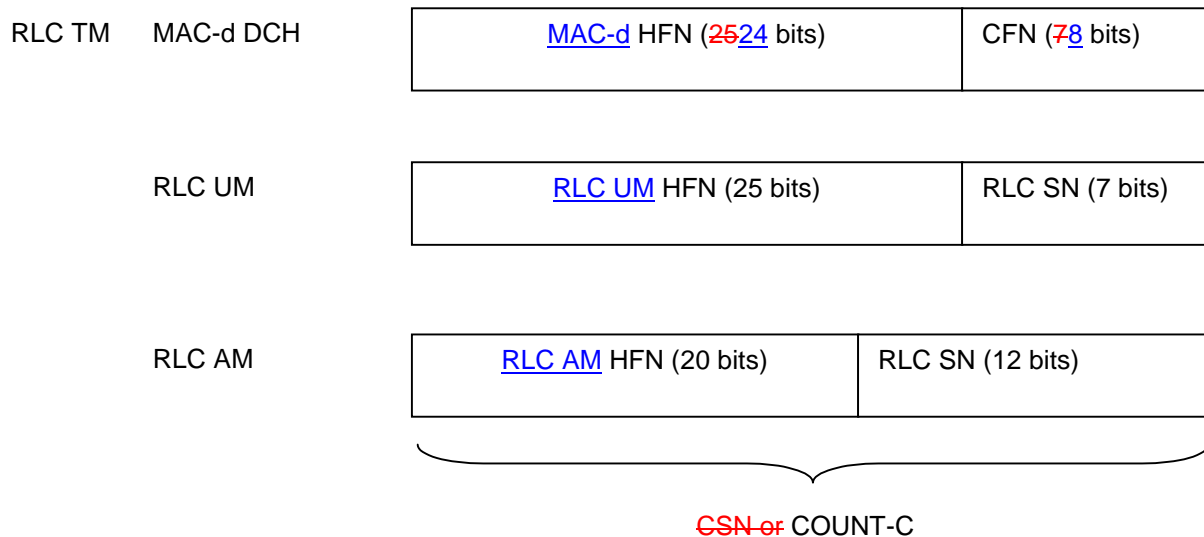
| RLC TM | MAC-d DCH | MAC-d HFN (~~25~~24 bits) | CFN (~~7~~8 bits) |

| RLC UM | | RLC UM HFN (25 bits) | RLC SN (7 bits) |

| RLC AM | | RLC AM HFN (20 bits) | RLC SN (12 bits) |

~~CSN or~~ COUNT-C

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

- For RLC TM on DCH, the "short" sequence number is the ~~7-bit~~ 8-bit ~~ciphering~~connection frame number CFN of ~~the UEFN~~COUNT-C. It is independently maintained in the ME MAC-d entity and the SRNC MAC-d entity. The "long" sequence number is the ~~25~~24-bit MAC-d 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~~ and this is part of the RLC UM PDU header~~(it is not ciphered)~~. The "long" sequence number is the 25-bit RLC UM 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~~ and this is part of the RLC AM PDU header~~(it is not ciphered)~~. The "long" sequence number is the 20-bit RLC AM HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is described in subsection 6.4.8~~transmitted from ME to RNC in~~ *RRC connection establishment*. The ME and the RNC then initialise the 20 most significant bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN to START.~~;~~ ~~the~~ The remaining bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN are initialised to ~~0~~zero. ~~The RRC HFN are incremented independently for each logical channel.~~

When a new radio bearer is established during a RRC connection in ciphered mode, the HFN is initialised by the current START value (see subsection 6.4.8).

The plaintext block~~ciphering unit~~, i.e. the data unit ~~(plaintext block)~~ that is ciphered, depends on the transmission mode as described below.

- For RLC UM mode, the ~~ciphering unit~~plaintext block is the UMD PDU excluding the first octet, i.e. excluding the RLC UM PDU header (see TS 25.322).

- For RLC AM mode, the plaintext block ~~ciphering unit~~ is the AMD PDU excluding the two first octets, i.e. excluding the RLC AM PDU header (see TS 25.322).

- For RLC TM on DCH, the plaintext block ~~ciphering unit~~ is the MAC SDU (see TS 25.321).