3GPP TSG SA 3 Meeting #14
Oslo, Norway, 1-4 August 2000

Document ***S3-000460***

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**	**105**		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:	Siemens Atea	**Date:**	1 August 2000

Subject:	Length of CFN

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:	The length of the CFN was set to 7 bits. It is 8 bits.

Clauses affected:	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.

6.6.4.1　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).
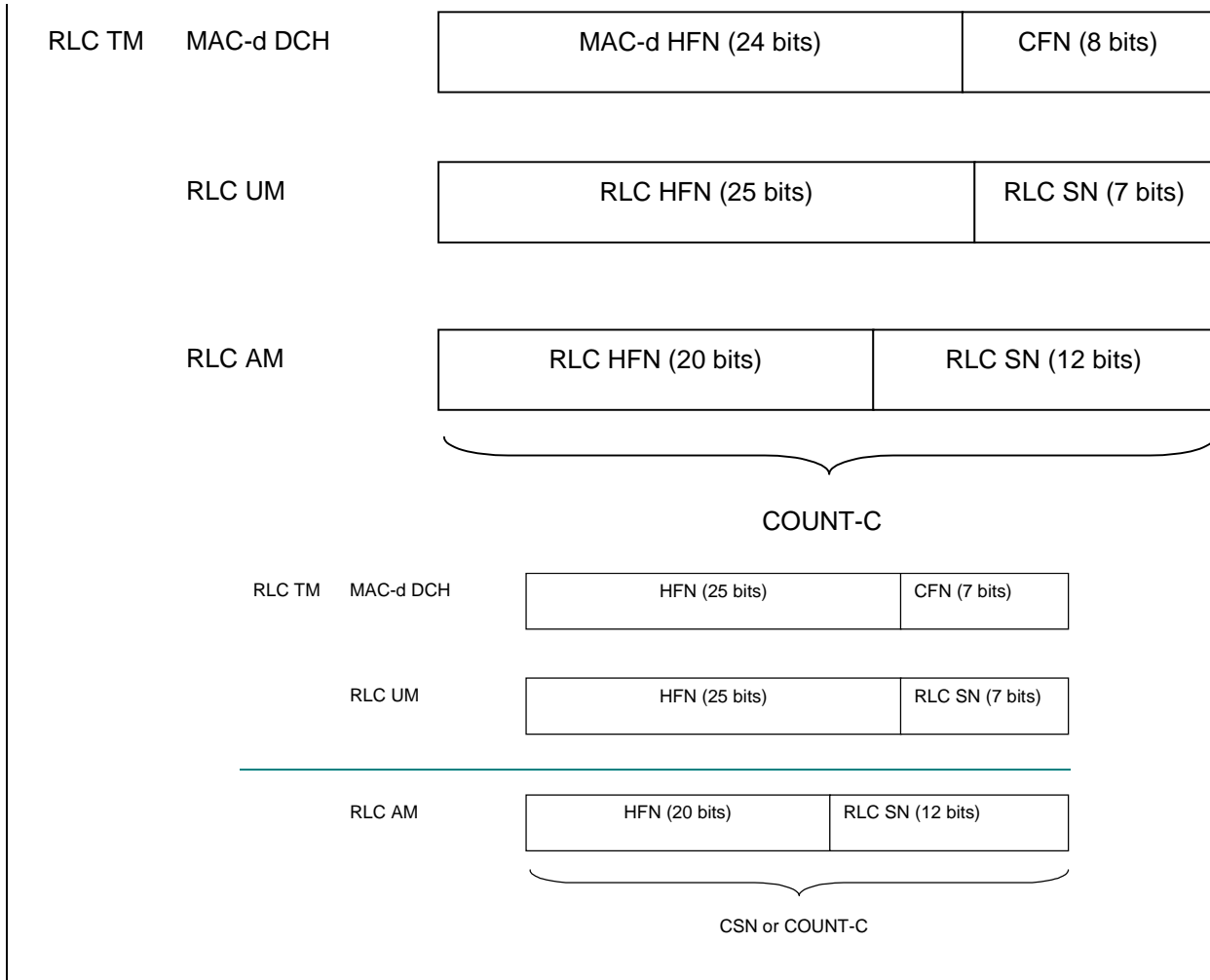

Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 7̶8-bit ciphering frame number CFN of the UEFN. It is independently maintained in the ME MAC entity and the SRNC MAC-d entity. The "long" sequence number is the 2̶5̶24-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 ME to RNC in *RRC connection establishment*. The ME and the RNC then initialise the 20 most significant bits of the RLC HFN and MAC HFN to START; the remaining bits of the RLC HFN and MAC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel.