3GPP TSG SA WG3 Security — S3#18 **S3-010182**

21-24 May, 2001

Phoenix, USA

CR-Form-v3

CHANGE REQUEST

⌘ **33.102** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☒ Core Network ☐

Title:	⌘	Correction to COUNT-C description
Source:	⌘	Siemens Atea
Work item code:	⌘	Security ***Date:*** ⌘ 17/05/2001
Category:	⌘	**A** ***Release:*** ⌘ Rel-4

Use one of the following categories:
- ***F*** *(essential correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(Addition of feature),*
- ***C*** *(Functional modification of feature)*
- ***D*** *(Editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	Clause 6.6.4.1 COUNT-Cof TS33.102 is inconsistent with TS25.331 V3.6.0 (2001-3) clause 8.5.8 Hyper Frame Numbers
Summary of change:	⌘	Alignment of Stage 2 specification with Stage 3 specifications
Consequences if not approved:	⌘	Inconsistent set of specifications

Clauses affected:	⌘	6.6.4.1 COUNT-C
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	Inconsistency to TS 33.102 was introduced with approval by TSG RAN#11 of R2-010673 [CR669R2 - March 2001] on TS 25.331

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.6.4.1 COUNT-C

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

There is one COUNT-C value per up-link radio bearer and one COUNT-C value per down-link radio bearer using RLC AM or RLC UM. For all transparent mode RLC radio bearers of the same CN domain COUNT-C is the same, and COUNT-C is also the same for uplink and downlink. ~~There is one up-link COUNT-C value and one down-link COUNT-C value for all radio bearers using the transparent RLC mode that are connected to the same CN domain (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).

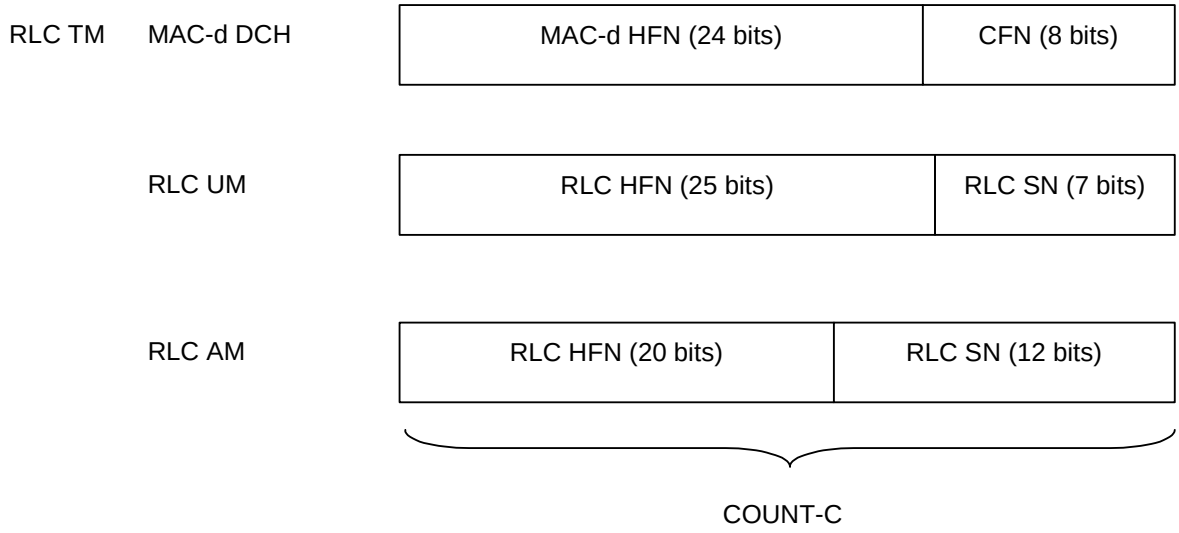

Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 8-bit connection frame number CFN of COUNT-C. It is independently maintained in the ME MAC-d entity and the SRNC MAC-d entity. The "long" sequence number is the 24-bit MAC-d HFN, which is incremented at each CFN cycle.
- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number (RLC SN) and this is part of the RLC UM PDU header. 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) and this is part of the RLC AM PDU header. 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 subclause 6.4.8. 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 remaining bits of the RLC AM HFN, RLC UM HFN and MAC-d HFN are initialised to zero.

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