Technical Specification Group Services and System Aspects
Meeting #10, Bangkok, Tailand, 11-14 December 2000

TSGS#10(00)0627

Source: **SA WG3**

Title: **CR to TS 33.105**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CR was agreed at SA WG3 meeting #16 and is presented to TSG SA #10 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
33.105	015		R99	Layer 2 related corrections	F	3.5.0	S3	S3-16	S3-000667

S3-000667

CR-Form-v3

CHANGE REQUEST

⌘ **33.105** **CR** **015** ⌘ rev **-** ⌘ Current version: **3.5.0** ⌘

*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 **X** Radio Access Network **X** Core Network ☐

Title:	⌘	Layer 2 related corrections
Source:	⌘	SA WG3
Work item code:	⌘	***Date:*** ⌘ 2000-11-21
Category:	⌘	**F** ***Release:*** ⌘ R99

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:	⌘	- The maximum size of RLC PDU / MAC SDU has been clarified. - The definition of the plaintext block has been corrected.
Summary of change:	⌘	Clarification of MAX RLC PDU/MAC SDU. Correction of plaintext block definition
Consequences if not approved:	⌘	Possible incorrect interpretation of Maximum RLC PDU/MAC SDU.

Clauses affected:	⌘	5.2.5, 5.2.7.5, 5.2.7.7
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

5.2.5 Implementation and operational considerations

The algorithm should be designed to accommodate a range of implementation options including hardware and software implementations. For hardware implementations, it should be possible to implement one instance of the algorithm using less than 10,000 gates (working assumption).

A wide range of UE with different bearer capabilities is expected, so the encryption throughput requirements on the algorithm will vary depending on the implementation. However, based on the likely maximum user traffic data rates, it must be possible to implement the algorithm to achieve an encryption speed in the order of 2Mbit/s on the downlink and on the uplink.

1. RLC-transparent mode:
   - New keystream block required every physical layer frame (10ms)
   - Maximum number of bits per physical layer frame of 20000~~5114~~ bits
   - Minimum number of bits per physical layer frame of 1 bit.
   - Granularity of 1 bit on all possible intermediate values
2. For UM RLC mode:
   - New keystream block required per every UMD PDU~~RLC frame (minimum 156μs)~~
   - Maximum number of bits in UMD PDU is 5000 bits~~per UM RLC frame of 1016 bits (ongoing specification work in TSG-R2 could extend this to 5000 bits)~~
   - Minimum number of bits in UMD PDU is ~~per UM RLC frame of~~ 16 bits.
   - Granularity of 8 bit on all possible intermediate values
3. For AM RLC mode:
   - New keystream block required per every AMD PDU ~~RLC frame (minimum 156μs)~~
   - Maximum number of bits in AMD PDU is 5000 bits~~per AM RLC frame of 1024 bits (ongoing specification work in TSG-R2 could extend this to 5000 bits)~~
   - Minimum number of bits in AMD PDU is ~~per AM RLC frame of~~ 24 bits.
   - Granularity of 8 bit on all possible intermediate values

The encryption throughput requirements should be met based on clock speeds upwards of 20MHz (typical clock speeds are expected to be much greater than this).

5.2.7.5 LENGTH

LENGTH: the required length of keystream.

LENGTH[0], LENGTH[1], …, LENGTH[15]

The length of LENGTH is 16 bits.

For a given bearer and transmission direction the length of the plaintext block that is transmitted during a single physical layer frame may vary. The algorithm shall generate a keystream block of variable length based on the value of the length parameter.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

~~The format of LENGTH cannot be specified at present since the number and sizes of RLC PDUs / MAC SDUs in each 10ms physical layer frame have not yet been fully specified. However, a maximum RLC PDU / MAC SDU size in the region of 1000 bits has been informally indicated by 3GPP TSG RAN2.~~ The maximum RLC PDU / MAC SDU size is

5000 bits. The range of values of the length parameter will depend not only on the RLC PDU / MAC SDU size but also the number of RLC PDUs / MAC SDUs which may be sent in a single physical layer 10ms frame for a given bearer and transmission direction.

Not all values between the maximum and minimum values shall be required but it is expected that the ability to produce length values of whole numbers of octets between a minimum and a maximum value will be required.

5.2.7.7 PLAINTEXT

PLAINTEXT: the plaintext.

PT[0], PT[1], …, PT[LENGTH-1]

The length of a keystream block equals the value of the input parameter LENGTH.

This plaintext block consists of the payload of the particular RLC PDUs / MAC SDUs to be encrypted ~~in a single 10ms physical layer frame~~ for a given bearer and transmission direction. It may consist of user traffic or signalling data. ~~The structure of the plaintext block cannot be specified at present.~~

- For RLC UM mode, the plaintext block is the UMD PDU excluding the first octet, i.e. excluding the RLC UM PDU header (see TS 25.322 [19]).
- For RLC AM mode, the plaintext block is the AMD PDU excluding the two first octets, i.e. excluding the RLC AM PDU header (see TS 25.322 [19]).
- For RLC TM on DCH, the plaintext block consists of all the MAC SDUs containing data for one and the same radio bearer and sent in one Transmission Time Interval. In this case, the CFN part of COUNT-C for the plaintext block is the CFN for the first radio frame of the Transmission Time Interval containing the plaintext block. (see TS 25.321 [18]).