3GPP TSG SA WG 3 (Security) meeting #15
Washington (USA), 12—14 September, 2000

Document **S3-000587**
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.

33.105 CR Xxx 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 #9	for approval	☒	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 ☒ UTRAN / Radio ☒ Core Network □
(at least one should be marked with an X)

Source: Nokia **Date:** 2000-09-08

Subject: L2 related corrections

Work item: Security

Category:	F	Correction	☒	**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	☒
					Release 00	□

Reason for change:

- The theoretical maximum number of bits to be ciphered in one 10 ms physical layer frame is 20 000 bits for transparent mode RLC (corresponds to 2 Mbit/s).
- Maximum RLC PDU size is 5000 bits.
- PLAINTEXT has been defined more precisely.

Clauses affected: 5.2.5, 5.2.7

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

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 RLC PDU~~ frame (minimum 156µs)~~
   - Maximum number of bits in RLC 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 RLC 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 RLC PDU~~frame (minimum 156µs)~~
   - Maximum number of bits in RLC 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 RLC 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 transparent mode RLC, the plaintext block consists of the MAC SDUs in one Transmission Time Interval. For unacknowledged mode RLC, the plaintext block is the UMD PDU minus the first octet. For acknowledged mode RLC, the plaintext block is the AMD PDU minus the two first octets.