3GPP TSG SA 3 Meeting #12
Stockholm, Sweden, 11-14 April 2000

Document ***S3-000258***
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 ☐ 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 3 #12
list expected approval meeting # here ↑

for approval	☒	strategic	□	*(for SMG*
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: Siemens Atea **Date:** 4 April 2000

Subject: Limitation and reduction of the effective cipher key length by the serving network

Work item: Security

Category:
(only one category shall be marked with an X)

F	Correction	□	**Release:**	Phase 2	□
A	Corresponds to a correction in an earlier release	□		Release 96	□
B	Addition of feature	□		Release 97	□
C	Functional modification of feature	☒		Release 98	□
D	Editorial modification	□		Release 99	☒
				Release 00	☒

Reason for change: The definition of a second ciphering capability with reduced effective key length facilitates the deployment of UMTS in countries where lawful restrictions exist on the use of cipher keys with a long effective key length.

Clauses affected: 6.6.6

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: Is there a need to reserve some UEA-values for proprietary use?

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.6.6 ~~UEA identification~~Ciphering capabilities

Each UEA will be assigned a 4-bit identifier. Currently the following values have been defined:

"0000_2" : UEA0, no encryption.

"0001_2" : UEA1, f8 with Kasumi with effective key length of the cipher key up to 128 bits.

"0010_2" : UEA2, f8 with Kasumi with effective key length of the cipher key up to 64 bits.

"0011_2" : UEA3, f8 with Kasumi with effective key length of the cipher key up to 54 bits.

"0100_2" : UEA4, f8 with Kasumi with effective key length of the cipher key up to 40 bits.

The remaining values are not defined.

In case of UEA1, the RNC and the ME feed the cipher key CK (as it was provided by the VLR or SGSN and the USIM) as input to the Kasumi algorithm.

In case of UEA2-UEA4, the RNC and the ME derive from the cipher key CK (as it was provided by the VLR or SGSN and the USIM) a modified cipher key CK' with a reduced effective key length n (respectively 64, 54 and 40) bits, from the cipher key CK:

$$CK'[k] = CK[k \bmod n], \quad \text{for } 0 \leq k < 128.$$

The RNC and the ME then feed the modified cipher key CK' as input to the Kasumi algorithm.