3GPP TSG SA 3 Meeting #13
Yokohama, Japan May 23 - 26

Document ***S3-000435***
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**	**r1**	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#13	for approval	☒	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑		for information	□	non-strategic	□	

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:	TSG SA WG 3	**Date:**	26 May, 2000
Subject:	Conversion functions for GSM-UMTS interoperation		
Work item:	Security		

Category:	F Correction	☒	**Release:**	Phase 2	□
(only one category	A Corresponds to a correction in an earlier release	□		Release 96	□
shall be marked	B Addition of feature	□		Release 97	□
with an X)	C Functional modification of feature	□		Release 98	□
	D Editorial modification	□		Release 99	☒
				Release 00	□

Reason for change: The suggested modifications to the conversion functions accommodate the SAGE recommendation and greatly improves the previously proposed conversion function .

Clauses affected: 6.8.2.3

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: In the current translation function, the string of the key is 64 bits, based on the GSM calculated K_C. This proposal is adding a practical difficulty to protect against a brute force attack by adding 32 IMSI bits to the function input . Cryptographically speaking one cannot have more than 64 bit strength if we began with 64 bit secret. However, adding $IMSI_{32}$ adds a practical difficulty to the attacker who does not know the IMSI. Adding IMSI into the mix means brute force searching requires more than 2^{96} tries which is not feasible with current hardware.

help.doc

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

6.8.2.3 VLR/SGSN

The R99+ VLR/SGSN shall perform GSM AKA using a triplet that is either:

a) retrieved from the local database,

b) provided by the HLR/AuC, or

c) provided by the previously visited VLR/SGSN.

NOTE: All triplets are originally provided by the HLR/AuC.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the VLR/SGSN.

When the user is attached to a UTRAN, the R99+ VLR/SGSN derives the UMTS cipher/integrity keys from the GSM cipher key using the following conversion functions:

a) C4: CK$_{[UMTS]}$ = KC || IMSI$_{64}$ ~~CK$_{[UMTS]}$ = Kc || Kc~~;

b) **C5: IK$_{[UMTS]}$ = KC xor IMSI$_{64}$ || KC** ~~c5: IK$_{[UMTS]}$ = Kc$_1$ xor Kc$_2$ || Kc || Kc$_1$ xor Kc$_2$~~; ||

whereby in. IMSI$_{64}$ = IMSI$_{32}$ || IMSI$_{32}$ while the IMSI$_{32}$ is the least significant 32 bits (most unique part to the MS) of the International Mobile Station Identity (IMSI) stored in the USIM and the VLR/SGSN ~~whereby in , are both 32 bits long and KC = Kc$_1$ || Kc$_2$.~~

The UMTS cipher/integrity keys are then sent to the RNC where the ciphering and integrity algorithms are allocated.

When the user is attached to a GSM BSS and the user receives service from an MSC/VLR, the cipher key Kc is sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the cipher key Kc is applied in the SGSN itself.