3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

Document S3-000207
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**	**078**	Current Version:	3.3.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG SA #7	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:	Siemens Atea	**Date:**	2000-02-27
Subject:	Conversion functions		
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: Following SAGE recommendation, when the effective cipher key is shorter than 128 bits is repeated. To prevent that the derived Kc would only depend on the IK, the conversion function c3: (CK, IK) → Kc is modified. To have maintain the reversibility also the conversion function c4: Kc → CK and c5: Kc → IK are modified.

Clauses affected: 6.8.1.2, 6.8.2.2

Other specs affected:	Other 3G core specifications	☒	→ List of CRs:	33.105 CR 079
	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.

6.8.1.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* from a R99+ MSC/VLR or SGSN, a R99+ HLR/AuC shall send quintets, generated as specified in 6.3.

Upon receipt of an *authentication data request* from a R98- MSC/VLR or SGSN, a R99+ HLR/AuC shall send triplets, derived from quintets using the following conversion functions:

a) c1: $RAND_{[GSM]} = RAND$

b) c2: $SRES_{[GSM]} = XRES_1$ [xor $XRES_2$ [xor $XRES_3$ [xor $XRES_4$]]]

c) c3: $Kc_{[GSM]} = CK_1$ ~~xor CK_2~~ xor IK_1 xor Complement[IK_2]

whereby $XRES_i$ are all 32 bit long and $XRES = XRES_1$ [|| $XRES_2$ [|| $XRES_3$ [|| $XRES_4$]]] dependent on the length of XRES, and CK_i and IK_i are both 64 bits long and $CK = CK_1 \| CK_2$ and $IK = IK_1 \| IK_2$.

6.8.2.2 R99+ MSC/VLR or SGSN

The R99+ MSC/VLR or 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 MSC/VLR or SGSN. Note that all triplets are originally provided by the R98- 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 MSC/VLR or SGSN.

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

a) c4: $CK_{[UMTS]}$ = ~~0…0~~Kc || Kc;

b) c5: $IK_{[UMTS]}$ = Kc || Complement[Kc~~;~~].

~~whereby in , Kc occupies the 64 least significant bits of CK~~.

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

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