3GPP TSG SA 3 Meeting #14
Oslo, Norway, 1-4 August 2000

Document S3-000464
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	106	Current Version:	3.5.0

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

For submission to:	SA#9	for approval	X	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: *(at least one should be marked with an X)*	(U)SIM	X	ME		UTRAN / Radio		Core Network	X

Source: Siemens Atea **Date:** 1 August 2000

Subject: Conversion function c2

Work item: Security

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

F	Correction	X	**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	X
				Release 00	

Reason for change:

The conversion function c2 only specified the case whereby the length of XRES is a multiple of 32.

The proposed c2 definition specifies also the case whereby the length of XRES is not a multiple of 32.

Clauses affected: 6.8.1.2

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.

6.8.1.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* from a R99+ VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send quintuplets, generated as specified in 6.3.

Upon receipt of an *authentication data request* from a R98- VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send triplets, derived from quintuplets 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 IK_2

whereby XRES is 128 bits long and XRES* = XRES if XRES is 128 bits long and XRES* = XRES || 0...0 if XRES is shorter than 128 bits, $XRES^*_i$ 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 $IK = IK_1 || IK_2$.