3GPP TSG SA 3 Meeting #15
Washington, 12-14 September 2000

Document S3-000617
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**	**0xx**	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	X	UTRAN / Radio	X	Core Network	X

Source:	S3	**Date:**	13 September 2000

Subject: Addition of authentication parameter lengths.

Work item: Security

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

F	Correction	
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	X

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change:

Only the sequence number length is given in the authentication mechanism specifications. To improve readability of the specifications, it is necessary to include all parameter lengths in 33.102. The lengths of the parameters used in other security mechanisms are already given in 33.102.

For clarity 33.105 should refer to 33.102 for the lengths of parameters. There may be some extra duplication with 33.103 but this can be tolerated in the short term.

Clauses affected: 6.3.7

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.

6.3.7 Length of ~~sequence numbers~~authentication parameters

The authentication key (K) shall have a length of 128 bits.

The random challenge (RAND) shall have a length of 128 bits.

Sequence numbers (SQN) shall have a length of ~~6 octets~~48 bits.

The anonymity key (AK) shall have a length of 48 bits.

The authentication management field (AMF) shall have a length of 16 bits.

The message authentication codes MAC in AUTN and MACS in AUTS shall have a length of 64 bits.

The cipher key (CK) shall have a length of 128 bits.

The integrity key (IK) shall have a length of 128 bits.

The authentication response (RES) shall have a variable length of 32-128 bits.