

## 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**  
list expected approval meeting # here  
↑

for approval   
for information

strategic   
non-strategic  (for SMG 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:** Vodafone **Date:** 4 September 2000

**Subject:** Addition of authentication parameter lengths.

**Work item:** Security

**Category:** F Correction   
A Corresponds to a correction in an earlier release   
B Addition of feature   
C Functional modification of feature   
D Editorial modification   
(only one category shall be marked with an X)

**Release:** Phase 2   
Release 96   
Release 97   
Release 98   
Release 99   
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	<input type="checkbox"/>	→ List of CRs:	
Other GSM core specifications	<input type="checkbox"/>	→ List of CRs:	
MS test specifications	<input type="checkbox"/>	→ List of CRs:	
BSS test specifications	<input type="checkbox"/>	→ List of CRs:	
O&M specifications	<input type="checkbox"/>	→ 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 16 octets.

The random challenge (RAND) shall have a length of 16 octets.

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

The anonymity key (AK) shall have a length of 6 octets.

The authentication management field (AMF) shall have a length of 2 octets.

The message authentication codes MAC in AUTN and MACS in AUTS shall have a length of 8 octets.

The cipher key (CK) shall have a length of 16 octets.

The integrity key (IK) shall have a length of 16 octets.

The authentication response (RES) shall have a variable length of 4-16 octets.