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

Document ***S3-000168***
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** **061r1** 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: Ericsson **Date:** 2000-02-17

Subject: Unsuccessful integrity check

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	□	

Release:

Phase 2	□
Release 96	□
Release 97	□
Release 98	□
Release 99	☒
Release 00	□

Reason for change: At detection of an integrity failure, the concerned message shall be discarded. In both the MS and the SRNC there shall be a supervision of failed integrity checks and if the failure situation persists, the connection shall be dropped.

Clauses affected: 6.4.6

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:

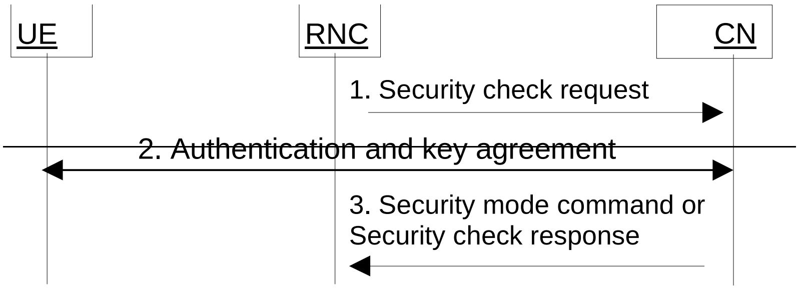
Other comments:

help.doc

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

6.4.6 Signalling procedures in the case of an unsuccessful integrity check

The supervision of failed integrity checks shall be performed both in the MS and the SRNC. In case of failed integrity check (i.e. faulty or missing MAC) is detected after that the integrity protection is started the concerned message shall be discarded. This can happen on the RNC side or on the MS side.~~The following procedure is used by the RNC to request the CN to perform an authentication and to provide a new CK and IK in case of unsuccessful integrity check. This can happen on the RNC side or in the UE side. In the latter case the UE sends a SECURITY CONTROL REJECT message to the RNC.~~


UE
RNC
CN
1. Security check request
~~2. Authentication and key agreement~~
3. Security mode command or Security check response

~~**Figure 15: Procedures at unsuccessful integrity check**~~

~~RNC detects that new security parameters are needed. This may be triggered by (repeated) failure of integrity checks (e.g. COUNT-I went out of synchronisation), or at handover the new RNC does not support an algorithm selected by the old RNC, etc.~~

1. ~~RNC sends a SECURITY CHECK REQUEST message to CN (indicating cause of the request).~~
2. ~~The CN performs the authentication and key agreement procedure.~~
3. ~~If the authentication is successful, the CN sends a Security mode command to RNC. This will restart the ciphering and integrity check with new parameters. If the authentication is not successful, the CN sends a SECURITY CHECK RESPONSE (Cause) to RNC.~~
4. ~~If the failure situation persists, the connection should be dropped.~~