3GPP TSG SA WG 3 (Security) meeting #15
Washington (USA), 12—14 September, 2000

Document **S3-000537**

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 xxx 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	X	strategic	□	*(for SMG*
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 X UTRAN / Radio □ Core Network □
(at least one should be marked with an X)

Source: Ericsson **Date:** 2000-08-31

Subject: Removal of ME triggered authentication during RRC connection

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: ME triggered authentication during RRC connection is not part of Release 99

Clauses affected: 6.4.3.

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

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the values START_{CS} and START_{PS} of the bearers that were protected in that RRC connection are stored in the USIM. When the next RRC connection is established that values are read from the USIM.

The ME shall trigger the generation of a new access link key set (a cipher key and an integrity key) if START_{CS} or START_{PS} has reached a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out ~~or during an RRC connection~~. When this maximum value is reached the cipher key and integrity key stored on USIM shall be deleted.

This mechanism will ensure that a cipher/integrity key set cannot be reused beyond the limit set by the operator.