3GPP TSG SA WG 3 (Security) meeting #11 **S3-000101**
Mainz, 22—24 January, 2000

3G 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 050 Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG	SA #7	for approval	X	*(only one box should*
list TSG meeting no. here ↑		for information		*be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: USIM ☒ ME ☒ UTRAN □ Core Network □
(at least one should be marked with an X)

Source: T-Mobil **Date:** 2000-Feb-09

Subject: Refinement of Cipher key and integrity key lifetime

3G Work item: Security

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

F	Correction	X
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Reason for change: Generation of a new access link key set shall be triggered by UE instead of USIM

Clauses affected: 6.4.3

Other specs affected:

Other 3G core specifications	□	→ List of CRs:	31.102
Other 2G 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 highest value of the hyperframe number (the current value of COUNT) of the bearers that were protected in that RRC connection is stored in the USIM. When the next RRC connection is established that value is read from the USIM and incremented by one.

The ~~USIM~~ UE shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out.

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