3GPP TSG SA WG3 (Security) meeting #10
Antwerpen, 19-21 January, 2000

***Document* S3-000043**
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 XX 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: SA#7
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: Ericsson **Date:** 2000-01-17

Subject: Clarification on cipher key and integrity key lifetime

Work item: Release 99

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

F	Correction	□	**Release:**	Phase 2	□
A	Corresponds to a correction in an earlier release	□		Release 96	□
B	Addition of feature	□		Release 97	□
C	Functional modification of feature	☒		Release 98	□
D	Editorial modification	□		Release 99	☒
				Release 00	□

Reason for change: Clarification needed on how the USIM shall trigger the generation of new security keys.

Clauses affected: 6.4.3, 6.4.4

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 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 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. 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 more times than the limit set by the operator.

6.4.4 Cipher key and integrity key identification

The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. The key set identifier is allocated by the network and sent with the authentication request message to the mobile station where it is stored together with the calculated cipher key CK and integrity key IK.

The purpose of the key set identifier is to make it possible for the network to identify the cipher key CK and integrity key IK which is stored in the mobile station without invoking the authentication procedure. This is used to allow re-use of the cipher key CK and integrity key IK during subsequent connection set-ups.

The key set identifier is three bits. Seven values are used to identify the key set. A value of "111" is used by the mobile station to indicate that a valid key is not available for use. At deletion of the cipher key and integrity key, the KSI is set to “111”. The value '111' in the other direction from network to mobile station is reserved.