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

***Document* S3-000194**
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 0xx 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
list expected approval meeting # here ↑

for approval	☒	strategic	□	*(for SMG use only)*
for information	□	non-strategic	□	

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:** 2000-02-22

Subject: Cipher key and integrity key setting

Work item: Security

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

F	Correction	☒	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	□

Release:

Reason for change: It is required to clarify that after an authentication the new keys are taken into use as part of the security mode control procedure that follows in both the PS and CS domain.

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 setting

Mutual key setting is the procedure that allows the MS and the RNC to agree on the key IK used to compute message authentication codes using algorithm UIA. Authentication and key setting is triggered by the authentication procedure and described in 6.3. Authentication and key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. TMUI or IMUI) is known by the SN/VLR. The key IK is stored in the SN/VLR and transferred to the RNC when it is needed. The key IK is stored in the USIM until it is updated at the next authentication.

If an authentication procedure is performed during ~~a data transfer in the PS mode~~a connection (PS or CS mode), the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the UE as part of the security mode negotiation (see 6.4.5) that follows the authentication procedure.