**3GPP TSG SA 3 Meeting #14**
**Oslo, Norway, 01-04 July 2000**

***S3-000589***
***Document S3-000424***
*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 | for approval | ☒ | strategic | □ | *(for SMG use only)* |
| *list expected approval meeting # here ↑* | | 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:** TSG SA WG3 **Date:** 28 July 2000

**Subject:** Clarification on condition on rejecting keys CR and IK

**Work item:** Security

| | | | | | | |
|---|---|---|---|---|---|---|
| **Category:** | F | Correction | ☒ | **Release:** | Phase 2 | □ |
| | A | Corresponds to a correction in an earlier release | □ | | Release 96 | □ |
| *(only one category* | B | Addition of feature | □ | | Release 97 | □ |
| *shall be marked* | C | Functional modification of feature | □ | | Release 98 | □ |
| *with an X)* | D | Editorial modification | □ | | Release 99 | ☒ |
| | | | | | Release 00 | ☒ |

**Reason for change:** Conditions on rejecting keys CK and IK are not in line with the 3G security concept and TS 31.102.

**Clauses affected:** 6.5.4.2, 6.6.4.2

| | | | |
|---|---|---|---|
| **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:** Possible impact on T WG3 specifications

help.doc

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

### 6.5.4.2 IK

The integrity key IK is 128 bits long.

There may be one IK for CS connections (IK$_{CS}$), established between the CS service domain and the user and one IK for PS connections (IK$_{PS}$) established between the PS service domain and the user. Which integrity key to use for a particular connection is described in 6.5.6.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the ME. IK is sent from the USIM to the ME upon request of the ME. The USIM shall send IK under the condition that ~~1)~~ a valid IK is available. The UE shall reject the currently received IK if ~~, 2)~~ the current values of START$_{CS}$ or START$_{PS}$ in the USIM ~~is~~ are not up-to-date ~~and 3)~~or START$_{CS}$ or START$_{PS}$ ~~has~~ have ~~not~~ reached THRESHOLD. The ME shall delete IK from memory after power-off as well as after removal of the USIM.

IK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of a quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) *security mode command*.

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

### 6.6.4.2 CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK$_{CS}$), established between the CS service domain and the user and one CK for PS connections (CK$_{PS}$) established between the PS service domain and the user. Which cipher key to use for a particular logical channel is described in 6.6.6.For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the ME. CK is sent from the USIM to the ME upon request of the ME. The USIM shall send CK under the condition that ~~1)~~ a valid CK is available. The UE shall reject the currently received CK if ~~, 2)~~ the current value of START$_{CS}$ or START$_{PS}$ in the USIM ~~is~~ are not up-to-date ~~and 3)~~or START$_{CS}$ or START$_{PS}$ ~~has~~ have ~~not~~ reached THRESHOLD. The ME shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of the quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) security mode command.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.