3GPP TSG SA WG 3 (Security) meeting #11 **S3-000108**
Mainz, 22—24 February, 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**	**xx**	Current Version:	3.3.1

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

For submission to TSG (*list TSG meeting no. here ↑*): SA #7 — for approval **X** — for information — *(only one box should 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: (*at least one should be marked with an X*) USIM [ ] ME [ ] UTRAN [X] Core Network [X]

Source: Telenor **Date:** 2000-Feb-14

Subject: Clarification about CK and IK which are transmitted in clear over the Iu-interface

3G Work item: Security

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

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

Reason for change: The keys CK and IK is transmitted in clear over the Iu-interface. For R99 we merely acknowledge this.

Clauses affected: 7.6

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
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: This CR does not solve the problem, it just makes it clear that we have identified the problem.

help.doc

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

7.6 Distribution of security parameters to UTRAN

Confidentiality and integrity between the user and the network is handled by the UE/USIM and the RNC.

The security parameters for the confidentiality and integrity algorithms must be distributed from the core network to the RNC over the Iu-interface in a secure manner. The actual mechanism for securing these parameters has not yet been identified.