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

***Document* S3-000148**
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 072 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	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: Ericsson **Date:** 2000-02-17

Subject: Clarification on ciphering and integrity protection at intersystem handover

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: A clarification is needed on that the communication is continued in ciphered mode at intersystem handover.
A clarification is needed on that integrity protection is started at intersystem handover from GSM BSS to UTRAN.

Clauses affected: 6.8.3, 6.8.4

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.

6.8.3 Intersystem handover for CS Services – from UTRAN to GSM BSS

If ciphering has been started when an intersystem handover occurs from UTRAN to GSM BSS, the necessary information (e.g. Kc, supported/allowed GSM ciphering algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old RNC to the new GSM BSS, and to continue the communication in ciphered mode.

6.8.3.1 UMTS security context

At the network side, two cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same MSC/VLR, the MSC/VLR derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and sends Kc to the BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by another MSC/VLR, the initial MSC/VLR derives the GSM cipher key from the stored UMTS cipher/integrity keys (using the conversion function c3) and sends it to the BSC via the (second) MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.

At the user side, in either case, the UE derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and applies Kc.

6.8.3.2 GSM security context

At the network side, two cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same MSC/VLR, the MSC/VLR sends the stored GSM cipher key Kc to the BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by another MSC/VLR, the initial MSC/VLR sends the stored GSM cipher key Kc to the BSC via the (second) MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.

At the user side, in either case, the UE applies the stored GSM cipher key Kc.

6.8.4 Intersystem handover for CS Services – from GSM BSS to UTRAN

If ciphering has been started when an intersystem handover occurs from GSM BSS to UTRAN, the necessary information (e.g. CK, IK, initial HFN value information, supported/allowed UMTS algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old GSM BSS to the new RNC, and to continue the communication in ciphered mode.

The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed.

6.8.4.1 UMTS security context

At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same MSC/VLR, the stored UMTS cipher/integrity keys CK and IK are sent to the new RNC.

b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new RNC via the (second) MSC/VLR that controls the new RNC. The initial MSC/VLR remains the anchor point for throughout the service.

At the user side, in either case, the UE applies the stored UMTS cipher/integrity keys CK and IK.