3GPP TSG SA 3 Meeting #12
Stockholm, Sweden, 11-14 April 2000

Document S3-000257
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   Current Version: 3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑   *↑ CR number as allocated by MCC support team*

For submission to:	SA 3 #12	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:	Siemens Atea	**Date:**	3 April 2000
Subject:	3G-2G and 2G-3G Handover for CS services		
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:	Removal of storage of CK and IK in the non-anchor MSC/VLR, as it is the anchor MSC/VLR that provides the new keys in the event of handover.
Clauses affected:	6.8.4, 6.8.5

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.

6.8.4 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.

6.8.4.1 UMTS security context

A UMTS security context in UTRAN is only established for a UMTS subscriber with a R99+ ~~UE~~ME.

At the network side, three 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 target BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by ~~other R98~~ 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 target BSC via the new MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.

~~c) In case of a handover to a GSM BSS controlled by another R99+ MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new MSC/VLR. The initial MSC/VLR also derives Kc and sends it to the new MSC/VLR. The new MSC/VLR store the keys and sends the received GSM cipher key Kc to the target BSC (which forwards it to the BTS). The initial MSC/VLR remains the anchor point throughout the service.~~

At the user side, in either case, the ~~UE~~ME applies the derived GSM cipher key Kc received from the USIM during the last UMTS AKA procedure.

6.8.4.2 GSM security context

A GSM security context in UTRAN is only established for a GSM subscribers with a R99+ ~~UE~~ME.

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 target BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by another MSC/VLR ~~(R99+ or R98-)~~, the initial MSC/VLR sends the stored GSM cipher key Kc to the BSC via the new MSC/VLR controlling the target BSC. The initial MSC/VLR remains the anchor point throughout the service.

~~If the non-anchor MSC/VLR is R99+, then the anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the UMTS cipher/integrity keys CK and IK. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.~~

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

6.8.5 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.

6.8.5.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with R99+ ~~UE~~ME under GSM BSS controlled by a R99+ VLR/SGSN.

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 target 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 new MSC/VLR that controls the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

~~The anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the GSM cipher key Kc. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.~~

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

6.8.5.2 GSM security context

Handover from GSM BSS to UTRAN with a GSM security context is only possible for a GSM subscriber with a R99+ ~~UE~~ME. At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same MSC/VLR, UMTS cipher/integrity keys CK and IK are derived from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sent to the target RNC.

b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR ~~(R99+ or R98-)~~ sends the stored GSM cipher key Kc to the new MSC/VLR controlling the target RNC. That MSC/VLR derives UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

At the user side, in either case, the ~~UE~~ME derives the UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and applies them.