

<h1>CHANGE REQUEST</h1>			<i>Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.</i>		
<b>33.102 CR xxx</b>		Current Version: <b>3.6.0</b>			
<small>GSM (AA.BB) or 3G (AA.BBB) specification number ↑</small>		<small>↑ CR number as allocated by MCC support team</small>			
For submission to: <b>SA #10</b> <small>list expected approval meeting # here ↑</small>	for approval for information	<input checked="" type="checkbox"/>	strategic	<input type="checkbox"/>	<small>(for SMG use only)</small>
		<input type="checkbox"/>	non-strategic	<input type="checkbox"/>	

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:** 2000-11-23

**Subject:** Intersystem handover for CS Services – from GSM BSS to UTRAN

**Work item:** Security

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

**Reason for change:** Cases where a GSM security context has been established for a UMTS subscriber and a handover to a UTRAN is performed have not been taken into account.

**Clauses affected:** 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:**



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

## 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, START 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 GSM BSS requests the MS to send the UMTS capability information, which includes information on the START values and UMTS security capabilities of the MS. The intersystem handover will imply a change of ciphering algorithm from a GSM A5 to a UEA. The target UMTS RNC includes the selected UMTS ciphering mode in the handover to UTRAN command message sent to the MS via the GSM BSS.

The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed. The Serving RNC will do this by initiating the RRC security mode control procedure when the first RRC message (i.e. the Handover to UTRAN complete message) has been received from the MS. The UE security capability information, that has been sent from MS to RNC via the GSM radio access and the system infrastructure before the actual handover execution, will then be included in the RRC Security mode command message sent to MS and then verified by the MS (i.e. verified that it is equal to the UE security capability information stored in the MS)

### 6.8.5.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with R99+ 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 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+ ME or for a UMTS subscriber with a R99+ ME when the initial MSC/VLR is R98-. 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. Note that In case of subsequent handover in a non-anchor R99+ MSC/VLR, a GSM cipher key Kc has been is received for a UMTS subscriber if the anchor MSC/VLR is R98-.
- 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 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.