CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **CRNum** ⌘**rev** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Handling of key sets at inter-system change
Source:	⌘	Ericsson
Work item code:	⌘	GERAN network access security/ UTRAN network access security
Date:	⌘	09/10/2003
Category:	⌘	**A**
Release:	⌘	REL-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘ Currently, it is ambiguously specified in the stage 2 description what key set that shall be used for ciphering (and/or integrity protection) after an inter-system handover (inter-system change) for the case ciphering (and/or integrity protection) was started in the original system, but there was a UMTS or GSM AKA performed prior to the inter-system handover (inter-system change) and this key set has not yet been taken into use.

In sections 6.8.4.1, UMTS security context (for Intersystem handover for CS Services – from UTRAN to GSM BSS) and 6.8.6.1, UMTS security context (for Intersystem change for PS Services – from UTRAN to GSM BSS), it seems clear that UE shall use the key set from the latest AKA procedure. But in all other sections for inter-system handover and inter-system change, TS33.102 simply refers to the 'stored' key set, which could be interpreted both as the 'key set currently in use' and the 'key set stored in SIM/USIM'.

For PS services, it is obvious that the intention is that the 'key set stored in SIM/USIM' shall be used after the inter-system change, since ciphering (and/or integrity protection) is started after the inter-system change by e.g. a Security Mode Control procedure (UMTS).

For CS services, at handover from GSM to UMTS, ciphering is continued after the handover (if ciphering was ongoing in GSM), but integrity protection is started with a Security Mode Control procedure. This indicates that the 'key set stored in SIM/USIM' shall be used after the inter-system handover.

In RAN2, a R99-CR in R2-031856 has already been approved to correct TS 25.331.

Summary of change: ⌘ It is clarified that UE shall use the key set received during the latest AKA procedure after an inter-system handover (inter-system change).

Consequences if not approved:	⌘	The indicated unclarities will remain in the specification. Misalignment between different specifications.

Clauses affected:	⌘	6.8.4.1, 6.8.4.2, 6.8.5.1, 6.8.5.2, 6.8.6.1, 6.8.6.2, 6.8.7.1, 6.8.7.2			
Other specs affected:	⌘	**Y** / **N** **X** / ☐	Other core specifications	⌘	TS24.008
		☐ / **X**	Test specifications		
		☐ / **X**	O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.8.4.1 UMTS security context

A UMTS security context in UTRAN is only established for a UMTS subscriber with a ME that is capable of UMTS AKA. 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- 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 ME applies the derived GSM cipher key Kc received from the USIM during the latest 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+ 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 ME applies the ~~stored~~ GSM cipher key Kc received from the SIM during the latest GSM AKA procedure

********** NEXT CHANGE **********

6.8.5.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with a ME that is capable of UMTS AKA 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 received from the USIM during the latest UMTS AKA procedure.

6.8.5.2 GSM security context

Handover from GSM BSS to UTRAN with a GSM security context is 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. In case of subsequent handover in a non-anchor R99+ MSC/VLR, a GSM cipher key Kc 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) received from the SIM or USIM during the latest GSM AKA procedure, and applies them.

********** NEXT CHANGE **********

6.8.6.1 UMTS security context

A UMTS security context in UTRAN is only established for UMTS subscribers. At the network side, three cases are distinguished:

a) In case of an intersystem change to a GSM BSS controlled by the same SGSN, the SGSN derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and applies it.

b) In case of an intersystem change to a GSM BSS controlled by another R99+ SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the new SGSN. The new SGSN stores the keys, derives the GSM cipher key Kc and applies the latter. The new SGSN becomes the new anchor point for the service.

c) In case of an intersystem change to a GSM BSS controlled by a R98- SGSN, the initial SGSN derives the GSM cipher key Kc and sends the GSM cipher key Kc to the new SGSN. The new SGSN stores the GSM cipher key Kc and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in all cases, the ME applies the derived GSM cipher key Kc received from the USIM during the latest UMTS AKA procedure.

6.8.6.2 GSM security context

A GSM security context in UTRAN is only established for GSM subscribers. At the network side, two cases are distinguished:

a) In case of an intersystem change to a GSM BSS controlled by the same SGSN, the SGSN starts to apply the stored GSM cipher key Kc.

b) In case of an intersystem change to a GSM BSS controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the BSC. The new SGSN stores the key and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in both cases, the ME applies the GSM cipher key Kc received from the SIM during the latest GSM AKA procedure~~that is stored~~.

********** NEXT CHANGE **********

6.8.7.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with a ME that is capable of UMTS AKA and connected to a R99+ VLR/SGSN. At the network side, two cases are distinguished:

a) In case of an intersystem change to a UTRAN controlled by the same SGSN, the stored UMTS cipher/integrity keys CK and IK are sent to the target RNC.

b) In case of an intersystem change to a UTRAN controlled by another SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN then stores the UMTS cipher/integrity keys CK and IK and sends them to the target RNC.

At the user side, in both cases, the ME applies the ~~stored~~ UMTS cipher/integrity keys CK and IK received from the USIM during the latest UMTS AKA procedure.

6.8.7.2 GSM security context

A GSM security context in GSM BSS can be either:

- **Established for a UMTS subscriber**

  A GSM security context for a UMTS subscriber is established in case the user has a ME not capable of UMTS AKA, where intersystem change to UTRAN is not possible, or in case the user has a R99+ ME but the SGSN is R98-, where intersystem change to UTRAN implies a change to a R99+ SGSN.

  As result, in case of intersystem change to a UTRAN controlled by another R99+ SGSN, the initial R98- SGSN sends the stored GSM cipher key Kc to the new SGSN controlling the target RNC.

  Since the new R99+ SGSN has no indication of whether the subscriber is GSM or UMTS, a R99+ SGSN shall perform a new UMTS AKA when receiving Kc from a R98- SGSN. A UMTS security context using fresh quintets is then established between the R99+ SGSN and the USIM. The new SGSN becomes the new anchor point for the service.

  At the user side, new keys shall be agreed during the new UMTS AKA initiated by the R99+ SGSN.

- **Established for a GSM subscriber**

  Handover from GSM BSS to UTRAN for GSM subscriber is only possible with R99+ ME. At the network side, three cases are distinguished:

  a) In case of an intersystem change to a UTRAN controlled by the same SGSN, the SGSN derives UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sends them to the target RNC.

  b) In case of an intersystem change from a R99+ SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN stores the GSM cipher key Kc and derives the UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC.

  c) In case of an intersystem change from an R98-SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. To ensure use of UMTS keys for a possible UMTS subscriber (superfluous in this case), a R99+ SGSN will perform a new AKA when a R99+ ME is coming from a R98- SGSN.

  At the user side, in all cases, 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) received from the SIM during the latest GSM AKA procedure and applies them. In case c) these keys will be over-written with a new CK, IK pair due to the new AKA.