TSG-SA WG 3 Security #30 **S3-030549**
Povoa de Varzim, Portugal, 6-10 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **33.102 CR CRNum** ⌘ **rev** ⌘ Current version: **5.3.0** ⌘

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:*** ⌘	30/09/2003
Category:	⌘	**F**	***Release:*** ⌘	REL-5

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 not 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.

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:

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				
		Y	**N**			
Other specs affected:	⌘	**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 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.

TSG-RAN Working Group 2 meeting #37 **R2-031724**
Budapest, Hungary 25th-29th Aug 2003

Source: Ericsson

Title: Handling of key sets at Inter-RAT Handover

Agenda item: 6.2

Document for: Information, discussion and decision

1. Introduction

This document discusses handling of key sets at Inter-RAT handover. We have discovered that specifications that describe the key set handling are currently not aligned. In this document, an analysis of the current status is presented, and a way forward is proposed.

2. Discussion

2.1 Key set handling at handover 2G to 3G according to TS 25.331

The current requirements on key set handling at handover 2G to 3G in TS 25.331 v3.15.0 (2003-06) are analysed from UE point of view by considering the following cases.

A. Handover 2G to 3G before ciphering has been activated in 2G

According to TS 25.331, section 8.3.6.3, UE shall not apply ciphering in 3G in case ciphering was not ongoing in 2G prior to handover.

With respect to possible key set assignment in 2G, the following cases are possible:

(A1) No new key set is assigned to UE in 2G prior to handover to 3G.
In this case, it is assumed that UE has previously stored a valid key set in USIM.

(A2) A new key set is assigned to UE in 2G prior to handover to 3G.

After the handover procedure has been completed, UTRAN shall initiate integrity protection for the RRC connection using the RRC Security Mode Control procedure. In both (A1) and (A2), UE will use the key set stored on USIM/SIM, since this is the only known key set by the UE.

B. Handover 2G to 3G after ciphering has been activated in 2G

According to TS 25.331, section 8.3.6.3, UE shall apply the ciphering key set used while in 2G prior to handover and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

With respect to possible key set assignment in 2G, the following cases are possible:

(B1) No new key set is assigned to UE in 2G prior to activation of ciphering.
In this case, the key set used is the same key set as memorised by the UE in USIM/SIM.

(B2) New key set is assigned to UE in 2G prior to activation of ciphering.
In this case, the key set used is the same key set as memorised by the UE in USIM/SIM.

(B3) New key set is assigned to UE in 2G after activation of ciphering, but prior to handover to 3G, i.e. the new key set has not been taken into use prior to the handover.
In this case, the key set used is not the same key set as memorised by the UE in USIM/SIM.

After the handover procedure has been completed, UTRAN shall initiate integrity protection for the RRC connection using the RRC Security Mode Control procedure.

In case (B1), it is clear that UE shall use (or derive) the key for integrity protection from the key set currently in use for ciphering, which is the same key set as memorised by the UE on USIM/SIM. There is obviously no other possibility.

In case (B2), it is not completely clear that UE shall use (or derive) the key for integrity protection from the key set assigned while in 2G and currently in use for ciphering. However, from a UE point of view, a straightforward is to use the key set assigned in 2G, since this is the same key set as memorised on USIM/SIM.

In case (B3), it is currently not clear which key set the UE shall use for integrity protection. Shall the UE use/derive the key for integrity protection from the key set stored on USIM/SIM (latest AKA) or from the key set currently in use for ciphering? Normally during a Security Mode Control procedure, UE uses/derives the key for integrity protection from the key set memorised on USIM/SIM. But this would lead to that ciphering of TM RBs and signalling radio bearers use a different key set than integrity protection, and is therefore not a preferred solution. Instead, we assume that UE shall use/derive the key for integrity protection from the key set currently in use for ciphering. In this case, the Security Mode Control procedure to start integrity protection becomes dependent on whether the RRC Connection was initiated at handover from 2G or not. This is currently not clear in TS25.331.

2.2 Principles for key set handling at Inter-RAT handover

In the previous section, we analysed the current requirements of TS 25.331 on key set handling at handover 2G to 3G. From this discussion, it seems clear that we need some principles:

1) UE shall for ciphering and integrity protection only use keys derived from one active key set.

2) Same key set handling principles should preferably apply both at 2G to 3G handover and 3G to 2G handover.

2.3 Analysis of related TSs

In this section, we analyse some related TS.

2.3.1 Analysis of TS 33.102

The following is extracted from TS 33.102 V3.13.0 (2002-12).

> ### *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. The RNC may request the MS to send the MS Classmarks 2 and 3 which include information on the GSM ciphering algorithm capabilities of the MS. This is necessary only if the MS Classmarks 2 and 3 were not transmitted from UE to UTRAN during the RRC Connection Establishment. The intersystem handover will imply a change of ciphering algorithm from a UEA to a GSM A5. The GSM BSS includes the selected GSM ciphering mode in the handover command message sent to the MS via the RNC.*
>
> *The integrity protection of signalling messages is stopped at handover to GSM BSS.*
>
> *The START values (see section 6.4.8) shall be stored in the ME/USIM at handover to GSM BSS.*
>
> #### *6.8.4.1 UMTS security context*
>
> *A UMTS security context in UTRAN is only established for a UMTS subscriber with a R99+ 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 last UMTS AKA procedure.

Comment: The underlined text above seems to indicate that ME shall use the key set from the latest AKA.

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.

Comment: The text in this section seems ambiguous on whether the ME shall use the key set from USIM/SIM at the handover from 3G to 2G, or if the ME shall use the key set used prior to the handover.

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 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.

Comment: The text in this section seems ambiguous on whether the ME shall use the key set from USIM/SIM at the handover from 2G to 3G, or if the ME shall use the key set used prior to the handover.

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) and applies them.

Comment: The text in this section seems ambiguous on whether the ME shall use the key set from USIM/SIM at the handover from 2G to 3G, or if the ME shall use the key set used prior to the handover.

2.3.2 Analysis of TS 24.008

The following is extracted from TS 24.008 v3.16.0 (2003-06). Comments are added, highlighted in yellow.

4.3.2.7 Handling of keys at intersystem change from UMTS to GSM

At intersystem change from UMTS to GSM, ciphering may be started (see 3GPP TS 04.18) without any new authentication procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GSM ciphering key according to table 4.3.2.7.1.

Table 4.3.2.7.1/3GPP TS 24.008: Intersystem change from UMTS to GSM

Security context established in MS and network in UMTS	*At intersystem change to GSM:*
GSM security context	*An ME shall apply the GSM cipher key received from the GSM security context residing in the SIM.*
UMTS security context	*An ME shall apply the GSM cipher key derived by the SIM from the UMTS cipher key and the UMTS integrity key.*
NOTE A SIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.	

Comment: The text in this section seems to indicate that the ME uses the key set currently residing in USIM/SIM at the handover from UMTS to GSM.

4.3.2.7a Use of established security contexts

In GSM, in the case of an established GSM security context, the GSM ciphering key shall be loaded from the SIM and taken into use by the ME when any valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in 3GPP TS 04.18 clause 3.4.7.2).

In GSM, in the case of an established UMTS security context, the GSM ciphering key shall be loaded from the SIM and taken into use by the MS when a valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in 3GPP TS 04.18 clause 3.4.7.2). The network shall derive a GSM ciphering key from the UMTS ciphering key and the UMTS integrity key by using the conversion function named "c3" defined in 3GPP TS 33.102.

In UMTS, in the case of an established GSM security context, the ME shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102. The GSM ciphering key shall be loaded from the SIM and the derived UMTS ciphering key and UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331). The network shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102.

In UMTS, in the case of an established UMTS security context, the UMTS ciphering key and UMTS integrity key shall be loaded from the SIM and taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during a RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331).

NOTE: In UMTS and GSM, during an ongoing, already ciphering and/or integrity protected RR connection, the network might initiate a new Authentication procedure in order to establish a new GSM/UMTS security context. The new keys are taken into use in the MS when a new valid SECURITY MODE COMMAND indicating CS domain in UMTS, or a new valid CIPHERING MODE COMMAND in GSM, is received during the RR connection.

Comment: The underlined text in the note above seems to indicate that the RRC procedure Security Mode Control used to activate integrity protection after handover from GSM to UMTS shall use the key set stored on USIM/SIM.

The fact that “Inter-system change” is not specifically mentioned in this section could be interpreted both as that “Inter-system change” has been covered in sections 4.3.2.7 and 4.3.2.8, or that UE shall not start to use a new key set at “Inter-system change”.

4.3.2.8 Handling of keys at intersystem change from GSM to UMTS

At intersystem change from GSM to UMTS, ciphering and integrity may be started (see 3GPP TS 25.331) without any new authentication procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the UMTS cipher key and the UMTS integrity key according to Table 4.3.2.8.1.

Table 4.3.2.8.1/3GPP TS 24.008: Intersystem change from GSM to UMTS

Security context established in MS and network in GSM	*At intersystem change to UMTS:*
GSM security context	*An ME shall derive the UMTS cipher key and UMTS integrity key from the GSM cipher key provided by the SIM. The conversion functions named "c4" and "c5" in 3GPP TS 33.102 are used for this purpose.*
UMTS security context	*An ME shall apply the UMTS ciphering key and the UMTS integrity key received from the UMTS security context residing in the SIM.*
NOTE A SIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.	

Comment: The text in this section seems to indicate that the ME uses the key set currently residing in USIM/SIM at the handover from GSM to UMTS.

2.3.3 Analysis of TS 04.18

The following is extracted from TS 04.18 V8.18.0 (2003-02).

3.4.4.1 Handover initiation

The network initiates the handover procedure by sending a HANDOVER COMMAND message to the mobile station on the main DCCH. It then starts timer T3103.

If the HANDOVER COMMAND message refers to a cell to which the mobile station is not synchronised to, this shall not be considered as an error (see 3GPP TS 05.08).

NOTE 1: The network should take into account limitations of certain mobile stations to understand formats used in the Frequency List IE, Frequency Short List IE, and Cell Channel Description IE used in the HANDOVER COMMAND message, see clause 10.5.2.13, clause 10.5.2.14, and clause 10.5.2.1b.

When sending this message on the network side, and when receiving it on the mobile station side, all transmission of signalling layer messages except for those RR messages needed for this procedure and for abnormal cases, is suspended until resuming is indicated. These RR messages can be deduced from clause 3.4.3 and clause 8.5.1.

Upon receipt of the HANDOVER COMMAND message, the mobile station initiates, as described in clause 3.1.4, the release of link layer connections, disconnects the physical channels (including the packet resources, if in class A mode of operation), commands the switching to the assigned channels and initiates the establishment of lower layer connections (this includes the activation of the channels, their connection and the establishment of the data links).

The HANDOVER COMMAND message contains:

- *The characteristics of the new channels, including for the multislot configuration and the TCH/H + TCH/H + ACCHs configuration the exact ACCHs to be used. The message may also contain definitions of the channel mode to be applied for one or several channel sets. If a previously undefined channel set is defined by the HANDOVER COMMAND message, a definition of the channel mode for the new channel set shall be included in the message.*

- *The characteristics of the new cell that are necessary to successfully communicate (e.g. frequency list in the case of slow frequency hopping), including the data that allows the mobile station to use the pre-knowledge about synchronization it acquires by the measurement process (i.e. BSIC + BCCH frequency).*

- *A power command (see 3GPP TS 05.08). The power level defined in this power command shall be used by the mobile station for the initial power on the new channel(s). It shall not affect the power used on the old channel(s).*

- *An indication of the physical channel establishment procedure to be used.*

- *A handover reference, used as specified in the following clause. The choice of the handover reference by the network is out of the scope of the present document and left to the manufacturers.*

- *Optionally a timing advance to be used on the new cell.*

- *Optionally a cipher mode setting. In that case, this ciphering mode has to be applied on the new channel. If no such information is present, the ciphering mode is the same as on the previous channel. In either case the ciphering key shall not be changed. In case of 2G to 2G handover, the HANDOVER COMMAND message shall not contain a cipher mode setting IE that indicates "start ciphering" unless a CIPHERING MODE COMMAND message has been transmitted previously in this instance of the dedicated mode: if such a HANDOVER COMMAND message is received it shall be regarded as erroneous, a HANDOVER FAILURE message with cause "Protocol error unspecified" shall be returned immediately, and no further action taken. In the case of UTRAN to GSM handover, the HANDOVER COMMAND message, which is sent transparently via RNC from BSS to the mobile station, shall always contain the cipher mode setting IE to indicate the ciphering mode to be used in GSM. In the case of CDMA2000 to GSM handover, the HANDOVER COMMAND message, which is sent transparently via RNC from BSS to the mobile station, shall always contain the cipher mode setting IE.*

Comment: The underlined text above indicates that the ciphering key is not changed at handover. But it could be questioned if this text is applicable for 3G to 2G handover, since in this case the GSM ciphering key Kc is always “changed” to a UMTS ciphering key CK.

- *Optionally, in a voice group call, a VGCS target mode information element defining which RR mode is to be used on the new channel (i.e. dedicated mode or group transmit mode). If this information element is not present, the mode shall be assumed to be the same as on the previous channel. The VGCS target mode information element shall also indicate the group cipher key number for the group cipher key to be used on the new channel or if the new channel is non ciphered. If the information element is not present, the ciphering mode and ciphering key shall be the same as on the previous channel. Mobile stations not supporting VGCS talking shall ignore the HANDOVER COMMAND message if the VGCS target mode information element is included in the message and shall send an RR STATUS message to the network with cause #96. If a VGCS target mode information element and a cipher mode setting information element is included in the same message, then a mobile station supporting VGCS talking shall regard the HANDOVER COMMAND message as erroneous, an HANDOVER FAILURE message with cause "Protocol error unspecified" shall be returned immediately, and no further action taken.*

- *Optionally, when the channel mode indicates that a multi-rate speech codec must be applied, the MultiRateconfiguration to be used in the new cell. The MultiRate Configuration IE defines the set of codec mode and related information to use after the handover. When accessing the new channel, the mobile station shall use for the Initial Codec Mode the mode specified in the MultiRate Configuration IE, if present, or apply by default the implicit rule defined in 3GPP TS 05.09.*

In addition, a HANDOVER COMMAND message may indicate a frequency change in progress, with a starting time and possibly alternative channel descriptions.

In the case of the reception of a HANDOVER COMMAND message which contains only the description of a channel to be used after the starting time, the mobile station shall wait up to the starting time before accessing the channel. If the starting time has already elapsed, the mobile shall access the channel as an immediate reaction to the reception of the message (see 3GPP TS 05.10 for the timing constraints).

In the case of a handover towards a GSM cell to which the mobile station is not synchronised to and in the case of an intersystem handover to GSM, at the reception of a HANDOVER COMMAND message which contains only the description of a channel to be used after the starting time, the mobile station shall wait up to the starting time before accessing the new channel. If the starting time has already elapsed, the mobile shall access the new channel as an immediate reaction to the reception of the message (see 3GPP TS 05.10 for the timing *constraints). Between the reception of the HANDOVER COMMAND and the starting time there is no requirement for the mobile station to receive or transmit on the old channel.*

NOTE 2: This case may result to a long interruption and should not be used.

If the message contains both the description of a channel to be used after the indicated time and of a channel to be used before, the mobile station accesses a channel as an immediate reaction to the reception of the message. If the moment the mobile station is ready to access is before the indicated time, the mobile station accesses the channels described for before the starting time. The mobile station then changes to the channel described for after the starting time at the indicated time. New parameters can be frequency list, MAIO and HSN. Other parameters describing the allocated channels must be identical to the parameters described for before the starting time. If the moment the mobile station is ready to access is after the starting time, the mobile station accesses the channel described for after the starting time.

If the channel mode indicates that a multi-rate speech codec must be applied, and the MultiRateConfiguration IE is not included in the HANDOVER COMMAND message, then the mobile station shall use on the new channel the AMR configuration it was using on the old channel when it received the HANDOVER COMMAND message. The MultiRate Configuration IE shall be included in the case of full rate channel to half rate channel handover. If not included in this case, the mobile station shall behave as if the MultiRate Configuration IE was inconsistent.

2.4 Comparision of the different interpretations

From the analysis presented in the previous sections, it is clear that key set handling at Inter-RAT handover is currently ambiguously specified in the TSs concerned.

It is not clear which of the following interpretations that are valid:

Interpretation 1: Same key set used prior to the handover is used also after the handover

Interpretation 2: Key set stored on USIM/SIM is used after the handover

For handover 2G to 3G, the following table lists the differences between the interpretations:

	Scenario	**1. Same key set used prior to the handover is used also after the handover**	**2. Key set stored on USIM/SIM is used after the handover**
1	Handover 2G->3G before ciphering started in 2G, no AKA performed in 2G.	Ciphering: Security Mode Control triggers start of ciphering and integrity protection. The key set previously stored on USIM/SIM is used.. Integrity protection: Security Mode Control triggers start of integrity protection. The key set previously stored on USIM/SIM is used.	Same as in scenario 1.
2	Handover 2G->3G before ciphering started in 2G, AKA performed in 2G prior to the handover	Ciphering: Security Mode Control triggers start of ciphering The new key set stored on USIM/SIM is used. Integrity protection: Security Mode Control triggers start of integrity protection. The new key set stored on USIM/SIM is used.	Same as in scenario 1.

3	Handover 2G->3G, AKA performed in 2G and ciphering ongoing prior to the handover.	Ciphering: Ciphering is continued to be ongoing in 3G using the same key set as used in GSM (and stored on USIM/SIM), i.e. the latest performed AKA. Integrity protection: Security Mode Control triggers start of integrity protection. The key set stored on USIM/SIM is used.	Same as in scenario 1.
4	Handover 2G->3G with ciphering ongoing, AKA in 2G has provided a new key set currently not in use in 2G	Ciphering: Ciphering is continued to be ongoing in 3G using the same key set as used in GSM (not the same as stored on USIM/SIM). Integrity protection: Security Mode Control triggers start of integrity protection using the same key set as used in GSM (not the same as stored on USIM/SIM).	Ciphering: Ciphering is continued to be ongoing in 3G taking the new key set stored on USIM/SIM into use, i.e. the key set from the latest AKA. Integrity protection: Security Mode Control triggers start of integrity protection using the new key set stored on USIM/SIM.

Only in scenario 4 (“currently used key set not same as stored in USIM/SIM”), the two interpretations give different UE behaviour.

2.5 Analysis of TS 25.413

Currently, TS TS 25.413 (UTRAN Iu interface RANAP signalling) does not give any advice on how a CN node shall behave towards the Target RNC with respect to key sets at handover from 2G to 3G. This section describes how RANAP procedures should be used in order to align with the two interpretations of key set handling at Inter-RAT handover.

Interpretation 1 (“same key set used prior to the handover is used also after the handover”):

At relocation due to handover from 2G to 3G (RANAP Relocation Preparation procedure):

If ciphering is ongoing in 2G prior to the handover, the RANAP message RELOCATION REQUEST shall include the keys from the currently used key set, which may not be keys from the latest AKA.

If ciphering is not ongoing in 2G prior to the handover, the RANAP message RELOCATION REQUEST shall include the integrity key from the latest AKA (no other key is available in the UE) and no ciphering key. This integrity protection key will be used to start integrity in UTRAN. If there is no existing key set agreement (e.g. case of emergency call), no keys shall be included in the relocation message.

At invocation of security procedure (RANAP Security Mode Control procedure)

If ciphering is ongoing in 2G prior to the handover, and (according to scenario 4) there is a new key set stored on USIM/SIM currently not in use, this new key set cannot be taken into use by a security mode control procedure after a handover 2G to 3G for this CS signalling connection. The reason for this is that UE does not (according to what is currently stated TS25.331, sections 8.1.12.3.1 and 8.3.6.3) does not regard this key set received in GSM (but yet not in use) as ‘new’. Either a new AKA must be performed in 3G, or the new key set can be activated in the next signalling connection, in which case the key status shall be "old".

Interpretation 2 (“Key set stored on USIM/SIM is used after the handover”):

At relocation due to handover from 2G to 3G (RANAP Relocation Preparation procedure):

If ciphering is ongoing in 2G prior to the handover, the RANAP message RELOCATION REQUEST shall include the key set from the latest AKA.

If ciphering is not ongoing in 2G prior to the handover, the RANAP message RELOCATION REQUEST shall include the integrity key from the latest AKA and no ciphering key. This integrity protection key will be used to start integrity protection UTRAN. If there is no existing key set agreement (e.g. case of emergency call), no keys shall be included in the relocation message.

3. Conclusion and Proposal

In this document, we have analysed the key set handling at Inter-RAT Handover, and found that currently, specifications that cover different parts and interfaces (TS25.331, TS24.008, TS33.102, TS04.18, TS25.413), are not complete and not aligned.

We propose that key set handling at Inter-RAT handover is aligned according to the principle that after the Inter-RAT Handover, the key set from the latest performed AKA (i.e. the key set stored in USIM/SIM of the UE) shall be used. It should be noted that it is only in case the “currently used key set” prior to the handover is not same as the key set stored in USIM/SIM, that the 2 different interpretations give different UE behaviour.

If this proposal is agreed upon, the concerned standardisation groups should be contacted.
Ericsson will prepare the necessary CRs. Attached is a proposed CR to TS 25.331.

If this proposal cannot be agreed upon, we recommend that, due to the late stage, Inter-RAT handover is not supported in R99 for the case “currently used key set” prior to the handover is not same as the key set stored in USIM/SIM.

References

[1] TS 25.413, UTRAN Iu interface RANAP signalling,V3.13.0 (2003-06)

[2] TS 04.18, Radio Resource Control Protocol, V8.18.0 (2003-02)

[3] TS 24.008, Core Network Protocols Stage 3, V3.16.0 (2003-06)

[4] TS 33.102, 3G Security, Security Architecture, V3.13.0 (2002-12)

[5] TS 25.331, Radio Resource Control (RRC) protocol specification, V3.15.0 (2003-06)

TSG-RAN Working Group 2 meeting #37 **R2-031724**
Budapest, Hungary 25th-29th Aug 2003

CR-Form-v7

CHANGE REQUEST

⌘	**25.331**	**CR**		⌘ **rev**		⌘	Current version:	**3.f.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-RAT Handover to UTRAN		
Source:	⌘	Ericsson		
Work item code:	⌘	TEI	***Date:*** ⌘	Aug 2003
Category:	⌘	**F**	***Release:*** ⌘	R99

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: ⌘ It is currently not clear that UE shall consider a key set as ‘new’ only in case UE recieves the key set for the ongoing signalling connection while in UMTS. This clarification is needed in order to prevent the UE from assuming that a key set received in another RAT is ‘new’ (and initialise the HFNs to zero), instead of assuming that the key set is ‘not new’ (and initialise HFNs to the values send to UTRAN in e.g. HANDOVER TO UTRAN COMLETE).

It is currently not clear what key set UE shall use after Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set currently in use for ciphering of the connection in the other RAT.

Summary of change: ⌘ Section 8.1.12.3.1:
It is clarified in a note that the actions in this section are performed only in case UE recieves a new key set for the ongoing signalling connection while in UMTS.

Section 8.3.6.3:
It is clarified in a note that Keys received while in another RAT shall not be regarded as ‘new’

It is added in a note that UE (after handover from another RAT) at a subsequent security mode control procedure in UTRAN activates ciphering and/or integrity protection using the key set stored in USIM/SIM.

It is corrected that UE shall, after the Inter-RAT handover to UTRAN, use the ciphering key set stored in the USIM/SIM, not the key set that was in use prior to the handover.

T1 impact:

No impact on T1 specifications is foreseen

		Backward compatibility: Backwards compatible for a UE and UTRAN that have assumed the indicated behaviour. In case UE and UTRAN are not complying with the correction ciphering and/or integrity protection will fail after an Inter-RAT handover to UTRAN, in case the key set stored on USIM/SIM is different from the key set in use prior to the handover.
Consequences if not approved:	⌘	The indicated unclarities will remain in the specification:

Clauses affected:	⌘	8.1.12.3, 8.1.12.3.1, 8.3.6.3				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			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.

8.1.12.3.1 New ciphering and integrity protection keys

NOTE: The actions in this subclause are to be performed only if the new keys were received for an ongoing signalling connection while in UMTS.

If a new security key set (new ciphering and integrity protection keys) has been received from the upper layers [40] for the CN domain as indicated in the variable LATEST_CONFIGURED_CN_DOMAIN, the UE shall:

1> set the START value for the CN domain indicated in the variable LATEST_CONFIGURED_CN_DOMAIN to zero;

1> if the SECURITY MODE COMMAND message contained the IE "Integrity protection mode info":

2> for integrity protection in the downlink on each signalling radio bearer except RB2:

3> if IE "Integrity protection mode command" has the value "start":

4> for the first received message on this signalling radio bearer:

5> start using the new integrity key;

5> for this signalling radio bearer:

6> set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero.

3> else:

4> for the first message for which the RRC sequence number in a received RRC message for this signalling radio bearer is equal to or greater than the activation time as indicated in IE "Downlink integrity protection activation info" as included in the IE "Integrity protection mode info":

5> start using the new integrity key;

5> for this signalling radio bearer:

6> set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero.

2> for integrity protection in the uplink on each signalling radio bearer except RB2:

3> for the first message for which the RRC sequence number in a to be transmitted RRC message for this signalling radio bearer is equal to the activation time as indicated in IE "Uplink integrity protection activation info" included in the transmitted SECURITY MODE COMPLETE message:

4> start using the new integrity key;

4> for this signalling radio bearer:

5> set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero.

2> for integrity protection in the downlink on signalling radio bearer RB2:

3> at the received SECURITY MODECOMMAND:

4> start using the new integrity key;

4> set the IE "Downlink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the downlink COUNT-I to zero.

2> for integrity protection in the uplink on signalling radio bearer RB2 :

3> at the transmitted SECURITY MODE COMPLETE:

4> start using the new integrity key;

4> set the IE "Uplink RRC HFN" in the variable INTEGRITY_PROTECTION_INFO of the uplink COUNT-I to zero.

1> if the SECURITY MODE COMMAND message contained the IE "Ciphering mode info":

2> for each signalling radio bearer and for each radio bearer for the CN domain indicated in the variable LATEST_CONFIGURED_CN_DOMAIN:

3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers using RLC-TM:

4> at the CFN as indicated in the IE "Ciphering activation time for DPCH" in the IE "Ciphering mode info":

5> start using the new key in uplink and downlink;

5> set the HFN component of the COUNT-C to zero.

3> if the IE "Status" in the variable CIPHERING_STATUS has the value "Started" for this CN domain, then for ciphering on radio bearers and signalling radio bearers using RLC-AM and RLC-UM:

4> in the downlink, at the RLC sequence number indicated in IE "Radio bearer downlink ciphering activation time info" in the IE "Ciphering mode info":

5> start using the new key;

5> set the HFN component of the downlink COUNT-C to zero.

4> in the uplink, at the RLC sequence number indicated in IE "Radio bearer uplink ciphering activation time info":

5> start using the new key;

5> set the HFN component of the uplink COUNT-C to zero.

1> consider the value of the latest transmitted START value to be zero.

8.3.6.3 Reception of HANDOVER TO UTRAN COMMAND message by the UE

The UE shall be able to receive a HANDOVER TO UTRAN COMMAND message and perform an inter-RAT handover, even if no prior UE measurements have been performed on the target UTRAN cell and/or frequency.

The UE shall act upon all received information elements as specified in subclause 8.6, unless specified otherwise in the following. The UE shall:

1> store a U-RNTI value (32 bits), which is derived by the IEs "SRNC identity" (12 bits) and "S-RNTI 2" (10 bits) included in IE "U-RNTI-short". In order to produce a full size U-RNTI value, a full size "S-RNTI" (20 bits) shall be derived by padding the IE "S-RNTI 2" with 10 zero bits in the most significant positions; and

1> initialise the variable ESTABLISHED_SIGNALLING_CONNECTIONS with the signalling connections that remains after the handover according to the specifications of the source RAT;

1> initialise the variable UE_CAPABILITIES_TRANSFERRED with the UE capabilities that have been transferred to the network up to the point prior to the handover, if any;

1> initialise the variable TIMERS_AND_CONSTANTS to the default values and start to use those timer and constants values;

1> if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Predefined configuration":

2> initiate the radio bearer and transport channel configuration in accordance with the predefined parameters identified by the IE "Predefined configuration identity";

2> initiate the physical channels in accordance with the predefined parameters identified by the IE "Predefined radio configuration identity" and the received physical channel information elements;

2> store information about the established radio access bearers and radio bearers according to the IE "Predefined configuration identity"; and

2> set the IE "RAB Info Post" in the variable ESTABLISHED_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED_RABS to "useT314".

1> if IE "Specification mode" is set to "Preconfiguration" and IE "Preconfiguration mode" is set to "Default configuration":

2> initiate the radio bearer and transport channel configuration in accordance with the default parameters identified by the IE "Default configuration mode" and IE "Default configuration identity";

2> initiate the physical channels in accordance with the default parameters identified by the IE "Default configuration mode" and IE "Default configuration identity" and the received physical channel information elements;

NOTE: IE "Default configuration mode" specifies whether the FDD or TDD version of the default configuration shall be used

2> set the IE "RAB Info Post" in the variable ESTABLISHED_RABS and the IE "Re-establishment timer" in the IE "RAB Info" in the variable ESTABLISHED_RABS to "useT314".

1> if IE "Specification mode" is set to "Preconfiguration":

2> use the following values for parameters that are neither signalled within the HANDOVER TO UTRAN COMMAND message nor included within pre-defined or default configuration:

3> 0 dB for the power offset $P_{\text{Pilot-DPDCH}}$ bearer in FDD;

3> calculate the Default DPCH Offset Value using the following formula:

3> in FDD:

$$\text{Default DPCH Offset Value} = (\text{SRNTI 2 mod } 600) * 512$$

3> in TDD:

Default DPCH Offset Value = (SRNTI 2 mod 7)

3> handle the above Default DPCH Offset Value as if an IE with that value was included in the message, as specified in subclause 8.6.6.21.

1> if IE "Specification mode" is set to "Complete specification":

2> initiate the radio bearer, transport channel and physical channel configuration in accordance with the received radio bearer, transport channel and physical channel information elements.

1> perform an open loop estimation to determine the UL transmission power according to subclause 8.5.3;

1> set the IE "START" for each CN domain, in the IE "START list" in the HANDOVER TO UTRAN COMPLETE message equal to the START value for each CN domain stored in the USIM if the USIM is present, or as stored in the UE for each CN domain if the SIM is present;

NOTE: ~~Reception of new k~~Keys received while in another RAT shall not be regarded as ‘new’ (i.e. ~~does~~ not trigger the actions in subclause 8.1.12.3.1) in a subsequent security control procedure in UTRAN, irrespective of whether the keys are already being used in the other RAT or not. If the UE has received new keys in the other RAT before handover, then the START values in the USIM (sent in the HANDOVER TO UTRAN COMPLETE message and in the INTER_RAT_HANDOVER_INFO sent to the BSS while in the other RAT) will not reflect the receipt of these new keys. At a subsequent security mode control procedure in UTRAN, UE activates ciphering and/or integrity protection using the key set stored in USIM/SIM.

1> set the value of "THRESHOLD" in the variable "START_THRESHOLD" equal to the 20 MSBs of the value stored in the USIM [50] for the maximum value of START for each CN Domain, or to the default value in [40] if the SIM is present;

1> if ciphering has been activated and ongoing in the radio access technology from which inter- RAT handover is performed:

2> for the CN domain included in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup", or the CS domain when these IEs are not present:

3> set the variable LATEST_CONFIGURED_CN_DOMAIN to the value indicated in the IE "CN domain identity", or to the CS domain when this IE is not present;

3> set the 20 MSB of the HFN component of the COUNT-C variable for all radio bearers using RLC-TM and all signalling radio bearers to the "START" value included in the IE "UE security information" in the variable "INTER_RAT_HANDOVER_INFO_TRANSFERRED";

3> set the remaining LSBs of the HFN component of COUNT-C for all radio bearers using RLC-TM and all signalling radio bearers to zero;

3> not increment the HFN component of COUNT-C for radio bearers using RLC-TM, i.e. keep the HFN value fixed without incrementing every CFN cycle;

3> set the CFN component of the COUNT-C variable to the value of the CFN as calculated in subclause 8.5.15;

3> set the IE "Status" in the variable CIPHERING_STATUS to "Started";

3> apply the algorithm according to IE "Ciphering Algorithm" with the ciphering key set stored in the USIM/SIM~~used while in the other radio access technology prior to handover~~ and apply ciphering immediately upon reception of the HANDOVER TO UTRAN COMMAND.

NOTE: If ciphering has been activated and ongoing in the radio access technology from which inter RAT handover is performed, UTRAN should not include the IE "Ciphering mode info" in the SECURITY MODE COMMAND message that starts Integrity protection, and should not send a SECURITY MODE COMMAND including IE "Ciphering mode info" and IE "CN domain identity" set to the same value as UE variable LATEST_CONFIGURED_CN_DOMAIN until all pending ciphering activation times have been reached for the radio bearers using RLC-TM.

1> if ciphering has not been activated and ongoing in the radio access technology from which inter-RAT handover is performed:

2> for the CN domain included in the IE "CN domain identity" which is included in the IE "RAB info" of the IE "RAB information to setup", or the CS domain when these IEs are not present:

3> set the IE "Status" in the variable CIPHERING_STATUS to "Not Started".

If the UE succeeds in establishing the connection to UTRAN, it shall:

1> if the IE "Status" in the variable CIPHERING_STATUS of a CN domain is set to "Started" and transparent mode radio bearers have been established by this procedure for that CN domain:

2> set the START value stored in the USIM [50] if present, and as stored in the UE if the SIM is present for any CN domain to the value "THRESHOLD" of the variable START_THRESHOLD;

2> include the IE "COUNT-C activation time" in the response message and specify a CFN value other than the default, "Now", that is a multiple of 8 frames (CFN mod 8 =0) and lies at least 200 frames ahead of the CFN in which the response message is first transmitted;

2> at the CFN value as indicated in the response message in the IE "COUNT-C activation time" for radio bearers using RLC-TM:

3> set the 20 MSB of the HFN component of the COUNT-C variable common for all transparent mode radio bearers of this CN domain to the START value as indicated in the IE "START list" of the response message for the relevant CN domain; and

3> set the remaining LSBs of the HFN component of COUNT-C to zero;

3> increment the HFN component of the COUNT-C variable by one even if the "COUNT-C activation time" is equal to zero;

3> set the CFN component of the COUNT-C to the value of the IE "COUNT-C activation time" of the response message. The HFN component and the CFN component completely initialise the COUNT-C variable;

3> step the COUNT-C variable, as normal, at each CFN value. The HFN component is no longer fixed in value but incremented at each CFN cycle.

1> if the IE "Status" in the variable CIPHERING_STATUS of a CN domain is set to "Not Started" and transparent mode radio bearers have been established by this procedure for that CN domain:

2> initialise the 20 MSB of the HFN component of COUNT-C common for all transparent mode radio bearers of this CN domain with the START value as indicated in the IE "START list" of the response message for the relevant CN domain;

2> set the remaining LSBs of the HFN component of COUNT-C to zero;

2> do not increment the COUNT-C value common for all transparent mode radio bearers for this CN domain.

1> transmit a HANDOVER TO UTRAN COMPLETE message on the uplink DCCH, using, if ciphering has been started, the new ciphering configuration;

1> when the HANDOVER TO UTRAN COMPLETE message has been submitted to lower layers for transmission:

2> enter UTRA RRC connected mode in state CELL_DCH;

2> initialise variables upon entering UTRA RRC connected mode as specified in subclause 13.4;

2> update the variable UE_CAPABILITY_TRANSFERRED with the UE capabilities stored in the variable INTER_RAT_HANDOVER_INFO_TRANSFERRED;

2> for all radio bearers using RLC-AM or RLC-UM:

3> set the 20 MSB of the HFN component of the uplink and downlink COUNT-C variable to the START value indicated in the IE "START list" of the response message for the relevant CN domain; and

3> set the remaining LSBs of the HFN component of COUNT-C to zero;

3> increment the HFN component of the COUNT-C variable by one;

3> start incrementing the COUNT-C values.

1> and the procedure ends.