3GPP TSG SA WG3 Security — SA3#33
10-14 May 2004, Beijing, China

S3-040274

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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Handling of key sets at inter-system change
Source:	⌘	Siemens, Ericsson
Work item code:	⌘	GERAN network access security/ UTRAN network access security
Date:	⌘	03/05/2004
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). The correction is done according to following rationales which were also adopted within NP-040099 which was approved at NP#32 (March 2004) For PS services, the intention is that the key set from the latest AKA run shall be used after the inter-system change, since ciphering (and/or integrity protection) is started after the inter-system change. For CS services, at handover, ciphering is continued after the handover (if ciphering was ongoing), but integrity protection is started with an RRC Security Mode Control procedure. In certain scenarios the target MSC will not know if an AKA procedures has been run just before the inter system handover. Therefore after an inter-system handover, the UE shall use the key set that was in use before the inter-system handover. The target system waits for the RANAP security mode control procedure initiated by the anchor MSC to take the new key set into use.
Summary of change:	⌘	For the PS domain, it is clarified that UE shall use the key set received during the latest AKA procedure after an inter-system handover. For the CS domain after an inter-system handover, it is clarified that UE shall use the key set that was in use before the inter-system handover.
Consequences if not approved:	⌘	The indicated unclarities will remain in the specification. Misalignment between different specifications (TS 24.008, TS 25.331)

Clauses affected:	⌘	6.8.4, 6.8.5, 6.8.6, 6.8.7			
Other specs affected:	⌘	Y / N X / [ ] Other core specifications [ ] / X Test specifications [ ] / X O&M Specifications	⌘	TS24.008; 25.331	
Other comments:	⌘				

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 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 used before the intersystem handover (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 used before the intersystem handover (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 used before the intersystem handover to the new MSC/VLR. The initial MSC/VLR also derives Kc and sends it to the new MSC/VLR. The new MSC/VLR stores 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~~ from the key set which was used before the intersystem handover~~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+ 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 from the key set used before the intersystem handover 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 from the key set used before the intersystem handover 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 from the key set which was used before the intersystem 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. In this case, the RRC security mode control procedure is initiated by the Serving RNC without receipt of a corresponding RANAP security mode control procedure from the MSC/VLR. 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 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 from the key set used before the intersystem handover 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 from the key set used before the intersystem handover 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 from the key set which was used before the intersystem 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 used before the intersystem handover (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 used before the intersystem handover 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) which was used before the intersystem handover and applies them.

6.8.6 Intersystem change for PS Services – from UTRAN to GSM BSS

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 agreed during the latest UMTS AKA procedure (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 agreed during the latest UMTS AKA procedure 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 from the UMTS cipher/integrity keys CK and IK agreed during the latest UMTS AKA procedure 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 agreed during the latest GSM AKA procedure.

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 agreed during the latest GSM AKA procedure 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~~.

6.8.7 Intersystem change for PS services – from GSM BSS to UTRAN

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 agreed during the latest UMTS AKA procedure 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 agreed during the latest UMTS AKA procedure 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 agreed during the latest GSM AKA procedure 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) agreed during the latest GSM AKA procedure 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 agreed during the latest GSM AKA procedure 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 agreed during the latest GSM AKA procedure 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.