DRAFT 3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	CR	068	Current Version:	3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG	SA #7	for approval	X	*(only one box should*
list TSG meeting no. here ↑		for information		*be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)*	USIM	X	ME	X	UTRAN		Core Network	X

Source:	Siemens Atea	**Date:** 2000-Jan-17
Subject:	Interoperation and intersystem handover/change between UTRAN and GSM BSS	
3G Work item:	Security	

Category: *(only one category shall be marked with an X)*

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	X
D	Editorial modification	

Reason for change: All scenarios for authentication and intersystem handover/change are described in greater detail in order to clarify the existing section.

Clauses affected: 6.8

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other 2G core specifications		→ List of CRs:
MS test specifications		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments: This is a modified version of S3-000079 that was a contribution to SA-3 #10.


help.doc

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

6.8 Interoperation and handover between UMTS and GSM

6.8.1 Authentication and key agreement of UMTS subscribers

6.8.1.1 General

For UMTS subscribers, authentication and key agreement will be performed as follows:

- UMTS AKA shall be applied when the user is attached to a UTRAN.
- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has R99+ UE and also the MSC/VLR or SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK, by the MSC/VLR or SGSN on the network side and by the ~~USIM~~UE on the ~~MS~~user side.
- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the user has R98- UE ~~or the MSC/VLR or SGSN is R98~~. In this case, the GSM user response SRES and the GSM cipher key Kc are derived from the UMTS user response RES and the UMTS cipher/integrity keys CK and IK, by the MSC/VLR or SGSN on the network side and the USIM on the ~~MS~~user side.
- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the MSC/VLR or SGSN is R98-. In this case, the GSM user response SRES and the GSM cipher key Kc are derived from the UMTS user response RES and the UMTS cipher/integrity keys CK and IK, (usually) by the HLR/AuC on the network side and by the USIM on the MS side.

The execution of the UMTS (resp. GSM) AKA results in the establishment of a UMTS (resp. GSM) security context between the user and the serving network domain to which the MSC/VLR or SGSN belongs. The user needs to separately establish a security context with each serving network domain.

Figure 18 shows the different scenarios that can occur with UMTS subscribers using either R98- or R99+ UE in a mixed network architecture.

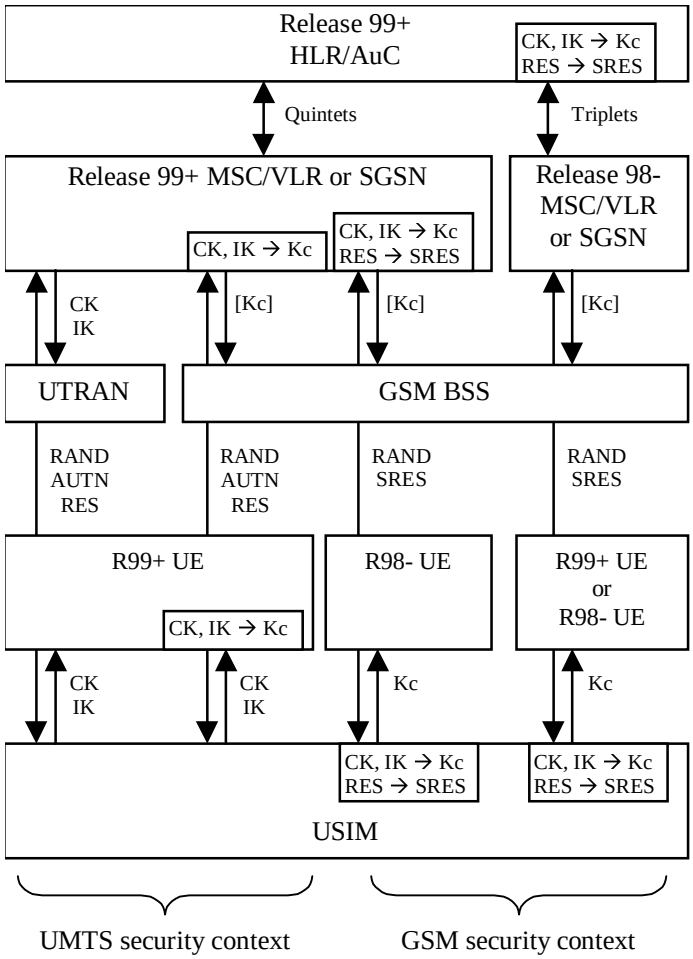

Figure 18: Authentication and key agreement of UMTS subscribers

Note that the UMTS parameters RAND, AUTN and RES are sent transparently through the UTRAN or GSM BSS and that the GSM parameters RAND and SRES are sent transparently through the GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering is always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

6.8.1.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* from a R99+ MSC/VLR or SGSN, a R99+ HLR/AuC shall send quintets, generated as specified in 6.3.

Upon receipt of an *authentication data request* from a R98- MSC/VLR or SGSN, a R99+ HLR/AuC shall send triplets, derived from quintets using the following conversion functions:

a) c1: $RAND_{[GSM]} = RAND$

b) c2: $SRES_{[GSM]} = XRES_1$ [xor $XRES_2$ [xor $XRES_3$ [xor $XRES_4$]]]

c) c3: $Kc_{[GSM]} = CK_1$ xor CK_2 xor IK_1 xor IK_2

whereby $XRES_i$ are all 32 bit long and XRES = $XRES_1$ [|| $XRES_2$ [|| $XRES_3$ [|| $XRES_4$]]] dependent on the length of XRES, and CK_i and IK_i are both 64 bits long and CK = CK_1 || CK_2 and IK = IK_1 || IK_2.

6.8.1.3 R99+ MSC/VLR or SGSN

The AKA procedure will depend on the terminal capabilities, as follows:

UMTS subscriber with R99+ UE

When the user has R99+ UE, UMTS AKA shall be performed using a quintet that is either

a) ~~a)~~ retrieved from the local database,

b) ~~b)~~ provided by the HLR/AuC, or

c) ~~c)~~ provided by the previously visited R99+ MSC/VLR or SGSN. Note that originally all quintets are provided by the HLR/AuC.

UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are stored in the MSC/VLR or SGSN.

When the user is attached to a UTRAN, the UMTS cipher/integrity keys are sent to the RNC, where the cipher/integrity algorithms are allocated.

When the user is attached to a GSM BSS, UMTS AKA is followed by the derivation of the GSM cipher key from the UMTS cipher/integrity keys. When the user receives service from an MSC/VLR, the derived cipher key Kc is then sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the derived cipher key Kc is applied in the SGSN itself.

UMTS ~~authentication and key freshness~~AKA is always provided to UMTS subscribers with R99+ UE independently of the radio access network since the UMTS RAND, AUTN and RES are ~~sent~~ transmitted transparently over the radio access network between the network and ~~to~~ the MS.

UMTS subscriber with R98- UE

When the user has R98- UE, the R99+ MSC/VLR or SGSN shall perform GSM AKA using a triplet that is either

a) derived by means of the conversion functions c2 and c3 in the R99+ MSC/VLR or SGSN from a quintet that is i) retrieved from the local database, ii) provided by the HLR/AuC, or iii) provided by the previously visited R99+ MSC/VLR or SGSN, or

b) provided as a triplet by the previously visited R98- MSC/VLR or SGSN. Note that R99+ MSC/VLR or SGSN will always provide quintets for UMTS subscribers.

Note that all triplets are derived from quintets, be it in the HLR/AuC or in an MSC/VLR or SGSN.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the MSC/VLR or SGSN.

~~This results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the MSC/VLR or SGSN.~~

In this case the user is attached to a GSM BSS. When the user receives service from an MSC/VLR, the GSM cipher key is sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the derived cipher key Kc is applied in the SGSN itself.

UMTS ~~authentication and key freshness~~AKA cannot be provided to UMTS subscriber with R98- UE.

Note 1: How does the VLR/SGSN know the UE release in order to decide whether to send the UMTS AUTN, RES or the derived GSM SRES?

6.8.1.4 R99+ UE

R99+ UE with a USIM inserted and attached to a UTRAN shall only support UMTS AKA and shall not support GSM AKA.

R99+ UE with a USIM inserted and attached to a GSM BSS shall support UMTS AKA and may support GSM AKA. Support of GSM AKA is required to allow registration in a R98- MSC/VLR or SGSN.

The execution of UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are stored in the USIM~~UE~~ and a copy is stored in the UE.

The execution of GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the USIM~~UE~~ and a copy is stored in the UE.

When the user is attached to a GSM BSS and the user participates in UMTS AKA, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK using conversion function c3.

6.8.1.5 USIM

The USIM shall support UMTS AKA and may support GSM AKA. Support of GSM AKA is required to allow registration in a GSM BSS with a R98- UE or in a GSM BSS connected to a R98- MSC/VLR or SGSN.

When the UE provides the USIM with RAND and AUTN, UMTS AKA shall be executed. If ~~The USIM shall support UMTS AKA. When the UE provides the USIM with RAND and AUTN and~~ the verification of AUTN is successful, the USIM shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. In case the verification of AUTN is not successful, the USIM shall respond with an appropriate error message to the R99+ UE.

When the UE provides the USIM with only RAND, GSM AKA shall be executed, if supported. The ~~USIM may support GSM AKA. In that case, when the UE provides the USIM with RAND, the~~ USIM first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The USIM then sends the GSM user response SRES and the GSM cipher key Kc to the UE.

In case the USIM does not support GSM AKA, the USIM responds with an appropriate message to the R99+ UE. USIM that do not support GSM AKA cannot operate in R98- UE.

6.8.2 Authentication and key agreement for GSM subscribers

6.8.2.1 General

For GSM subscribers, GSM AKA shall always be used.

The execution of the GSM AKA results in the establishment of a GSM security context between the user and the serving network domain to which the MSC/VLR or SGSN belongs. The user needs to separately establish a security context with each serving network domain.

When in a UTRAN, the UMTS cipher/integrity keys CK and IK are derived from the GSM cipher key Kc by the UE and the MSC/VLR or SGSN, both R99+ entities.

Figure 19 shows the different scenarios that can occur with GSM subscribers using either R98- or R99+ UE in a mixed network architecture.

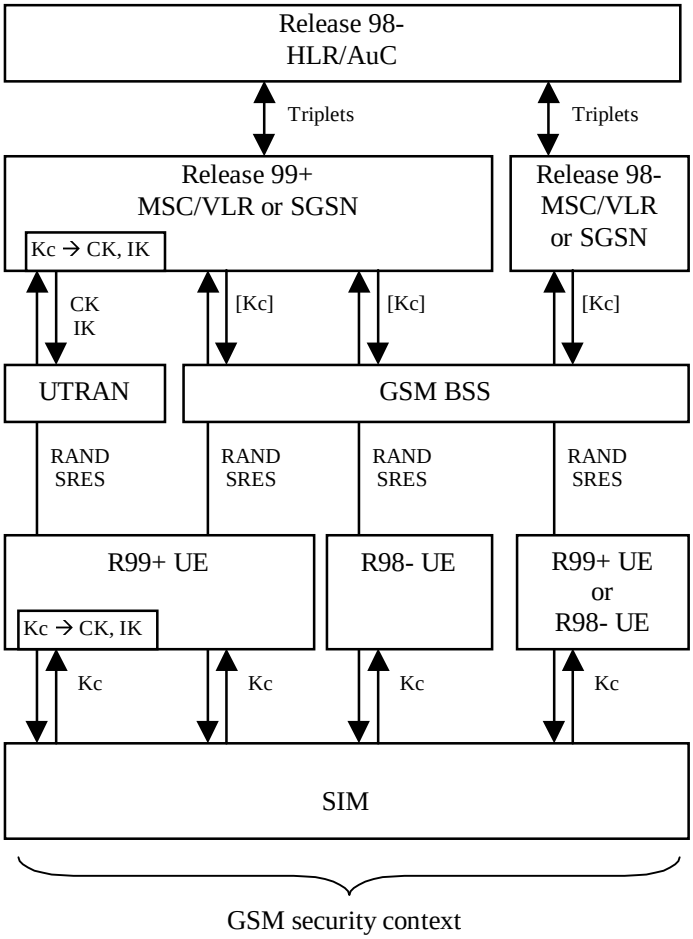

Figure 19: Authentication and key agreement for GSM subscribers

Note that the GSM parameters RAND and RES are sent transparently through the UTRAN or GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering is always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

6.8.2.2 R99+ MSC/VLR or SGSN

The R99+ MSC/VLR or SGSN shall perform GSM AKA using a triplet that is either:

a) ~~a)~~ retrieved from the local database,

b) ~~b)~~ provided by the HLR/AuC, or

c) ~~c)~~ provided by the previously visited MSC/VLR or SGSN. Note that all triplets are originally provided by the R98- HLR/AuC.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the MSC/VLR or SGSN.

When the user is attached to a UTRAN, the R99+ MSC/VLR or SGSN derives the UMTS cipher/integrity keys from the GSM cipher key using the following conversion functions:

a) c4: $CK_{[UMTS]} = 0 \ldots 0 \parallel Kc$;

b) c5: $IK_{[UMTS]} = Kc \parallel Kc$;

whereby in c4, Kc occupies the 64 least significant bits of CK.

The UMTS cipher/integrity keys are then sent to the RNC where the ciphering and ~~message authentication~~ integrity algorithms are allocated.

When the user is attached to a GSM BSS and the user receives service from an MSC/VLR, the ~~derived~~ cipher key Kc is sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the ~~derived~~ cipher key Kc is applied in the SGSN itself.

6.8.2.3 R99+ UE

R99+ UE with a SIM inserted, shall participate only in GSM AKA.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the SIM~~UE~~ and a copy is stored in the UE.

When the user is attached to a UTRAN, R99+ UE shall derive the UMTS cipher/integrity keys CK~~k~~ and IK from the GSM cipher key Kc using the conversion functions c4 and c5.

6.8.3 Distribution of authentication vectors between VLRs/SGSNs

The following four cases are distinguished related with the distribution of authentication vectors between VLR/SGSN:

a) R99+ VLR/SGSN to R99+ VLR/SGSN

UMTS and GSM authentication vectors can be distributed between R99+ VLR/SGSN. Note that originally all quintets are provided by a R99+ HLR/AuC for UMTS subscribers and all triplets are provided by a R98- HLR/AuC for GSM subscribers. When a R99+ VLR or SGSN receives quintets (from the user's HLR/AuC or from another VLR or SGSN) it marks the user as a UMTS subscriber. When a R99+ VLR or SGSN receives triplets (from the user's HLR/AuC or from another VLR or SGSN) it marks the user as a GSM subscriber.

b) R98- VLR/SGSN to R98- VLR/SGSN

Only triplets can be distributed by R98- VLR/SGSN. Note that ~~originally~~ triplets are generated by R98- HLR/AuC for GSM subscribers and (usually) derived from UMTS authentication vector by R99+ HLR/AuC for UMTS subscribers. UMTS AKA is not supported and only GSM security context can be established by a R98- VLR/SGSN.

c) R99+ VLR/SGSN to R98- VLR/SGSN

Only triplets can be distributed to R98- VLR/SGSN. R99+ VLR/SGSN can provide triplets originally provided by a R98- HLR/AuC for GSM subscribers ~~or~~ and can derive triplets from stored quintets originally provided by R99+ HLR/AuC for UMTS subscribers and forward them to a new R98- VLR/SGSN. Note that R98- VLR/SGSN can only establish GSM security context.

d) R98- VLR/SGSN to R99+ VLR/SGSN.

Only triplets can be distributed by a R98- VLR/SGSN. Upon receipt of triples, the new VLR/SGSN shall request authentication data from the HLR/AuC. When the HLR/AuC responds with triplets, the VLR/SGSN marks the user as a GSM subscriber and the triplets received from the previous VLR/SGSN may be stored and used. When the HLR/AuC responds with quintets, the VLR/SGSN marks the user as a UMTS subscriber and the triplets received from the previous VLR/SGSN must be deleted. ~~Triplets provided by R98- VLR/SGSN can only be used by a R99+ VLR/SGSN to establish a GSM security context. Note that as a consequence of not knowing the origin of the triplets, provided by R98- HLR/AuC of derived from quintets in R99+ HLR, they shall not be used with a R99+ UE in order not to establish a GSM security context for a UMTS subscriber.~~

~~Note: This means that triplets received from R98- VLR/SGSN shall not be used for GSM subscribers under UTRAN either. New AVs shall be requested to HE/AuC in this case with the corresponding load increase at MAP-D interface.~~

A R99+ VLR or ~~/~~SGSN ~~shall not~~ may distribute triplets ~~received from a R98- VLR/SGSN~~ to ~~any~~ other ~~R99+ MSC/~~VLR or SGSN (after he has asserted that the user is a GSM subscriber by contacting the HLR/AuC). ~~since it is unknown if the triplets belong to a GSM subscriber or UMTS subscriber (derived from quintets).~~

6.8.43 Intersystem handover for CS Services – from UTRAN to GSM BSS

6.8.43.1 UMTS security context

A UMTS security context in UTRAN is only established for UMTS subscribers.

At the network side, threetwo cases are distinguished:

a) 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 BSC (which forwards it to the BTS).

b) b) In case of a handover to a GSM BSS controlled by another a 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 BSC via the (second) 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. That MSC/VLR derives the GSM cipher key Kc and sends it to the BSC (which forwards it to the BTS). The initial MSC/VLR remains the anchor point throughout the service.

At the user side, in either case, the UE derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and applies Kc.

6.8.43.2 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 a handover to a GSM BSS controlled by the same MSC/VLR, the MSC/VLR sends the stored GSM cipher key Kc to the 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(second) MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.

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

6.8.54 Intersystem handover for CS Services – from GSM BSS to UTRAN

6.8.54.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with R99+ UE 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 new 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(second) MSC/VLR that controls the new RNC. The initial MSC/VLR remains the anchor point for throughout the service.

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

6.8.4.26.8.5.2 GSM security context

A GSM security context in GSM BSS can be either:

- Established for a UMTS subscribers

  GSM security context for a UMTS subscriber is established in case the user has a R98- UE, where handover to UTRAN is not possible, or the VLR/SGSN is R98 , where handover to UTRAN implies a change to a R99+ VLR/SGSN.

  As result, in case of handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR sends the stored GSM cipher key Kc to the new MSC/VLR controlling the new RNC. That MSC/VLR derives UMTS cipher/integrity keys CK and IK which are then forwarded to the new RNC. The initial MSC/VLR remains the anchor point for throughout the service.

  It should be noticed that the provided GSM cipher key Kc has been originally derived by the R99+ HLR from the UMTS CK and IK. In order to allow handover for UMTS subscriber with a established GSM security context implies a new derivation of the UMTS CK and IK from the provided GSM cipher key Kc.

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

  This handover case implies a security level reduction for UMTS subscriber during the current call.

- Established for a GSM subscribers

Handover from GSM BSS to UTRAN for GSM subscriber is only possible with R99+ UE.

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 new RNC.

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

At the user side, in either case, the UE 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.

For UMTS subscriber the handover from a GSM BSS to a UTRAN results in the exceptional situation that a UMTS subscriber with a R99+ UE has a GSM security context while attached to a UTRAN. UMTS AKA should be performed as soon as possible to establish a UMTS security context.

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

6.8.65.1 UMTS security context

At the network side, three cases are distinguished:

a) In case of a handover 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 a handover 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 a handover 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 case a) or b), the UE derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and applies it.

In case c), the handover makes that the UMTS security context between the user and the serving network domain is lost. The UE needs to be aware of that. The UE then deletes the UMTS cipher/integrity keys CK and IK and stores the derived GSM cipher key Kc.

6.8.65.2 GSM security context

At the network side, two cases are distinguished:

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

b) In case of a handover 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 UE applies the GSM cipher key Kc that is stored.

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

6.8.76.1 UMTS security context

At the network side, two cases are distinguished:

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

b) In case of a handover 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 new 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 new RNC.

At the user side, in both cases, the UE applies the stored UMTS cipher/integrity keys CK and IK.

6.8.76.2 GSM security context

At the network side, two cases are distinguished:

a) In case of a handover 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 new RNC.

b) In case of a handover to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the new 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 new RNC.

At the user side, in both cases, the UE 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.