

6.8 Interoperation and handover between UMTS and GSM

6.8.1 Authentication and key agreement of UMTS subscribers

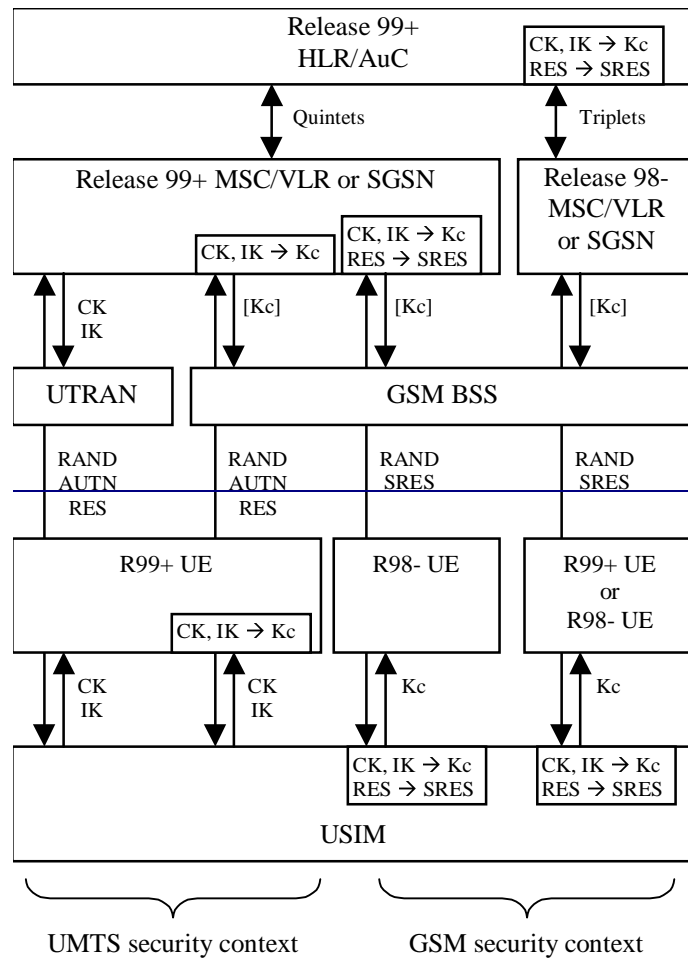
6.8.1.1 General

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/VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK, by the VLR/SGSN on the network side and by the USIM on the 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.~~
- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the VLR/SGSN is R98-. In this case, the USIM derives the GSM user response SRES and the GSM cipher key Kc from the UMTS user response RES and the UMTS cipher/integrity keys CK, IK.

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/VLR/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.



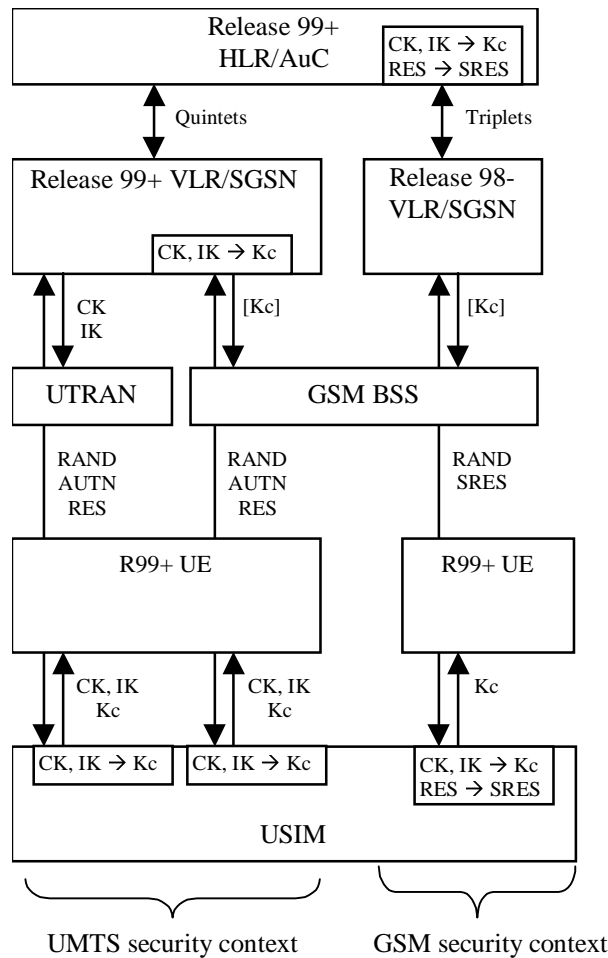


Figure 18: Authentication and key agreement of UMTS subscribers

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 K_c is not sent to the GSM BSS.

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

Note that a USIM is not able to operate in a R98- UE.

6.8.1.2 R99+ HLR/AuC

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

Upon receipt of an *authentication data request* from a R98- MSC/VLR or SGSN/VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send triplets, derived from quintet/quintuplets 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/VLR/SGSN~~

UMTS subscriber with R99+ UE

~~When the user has R99+ UE, A R99+ VLR/SGSN shall execute~~ UMTS AKA ~~shall be performed~~ using a ~~quintet~~quintuplet that is either

- a) ~~a)~~ retrieved from the local database,
- b) ~~b)~~ provided by the HLR/AuC, or
- c) ~~e)~~ provided by the previously visited R99+ ~~MSC/VLR or SGSN/VLR/SGSN~~.

Note that originally all ~~quintet~~quintuplets 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/VLR/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 is always provided to UMTS subscribers with R99+ UE independently of the radio access network.

~~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 e2 and e3 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 MSC/VLR or SGSN.~~

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

6.8.1.4 R99+ UE

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

R99+ UE with a USIM inserted and attached to a GSM BSS shall ~~support~~ participate in UMTS AKA and may ~~support~~ participate in GSM AKA. Support of GSM AKA is required to allow registration in a R98- ~~MSC/VLR or SGSN/VLR/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~~passed to the UE. The UE shall also receive a derived GSM cipher key Kc at the USIM.

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 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 access to GSM-BSS with a R98- VLR/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. The USIM shall store CK and IK. The USIM shall also derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3 and send the derived Kc to the UE. In case the verification of AUTN is not successful, the USIM shall respond with an appropriate error indication to the 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 stores the GSM cipher Kc and sends the GSM user response SRES and the GSM cipher key Kc to the UE.

~~In case the USIM does not support GSM AKA (conversion function c3 is not available to derive Kc and pass it to the UE), the UE shall be informed. USIM responds with an appropriate message to the R99+ UE. A USIM that do not support GSM AKA cannot operate under a R98- VLR/SGSN. in R98- UE.~~

6.8.2 Authentication and key agreement for GSM subscribers

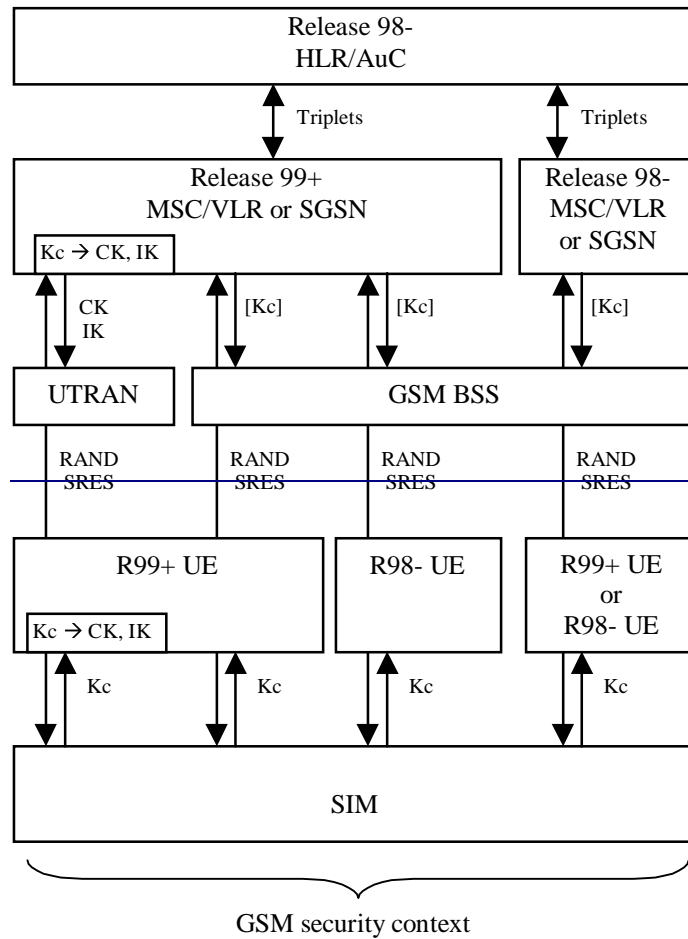
6.8.2.1 General

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/VLR/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 VLR/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.



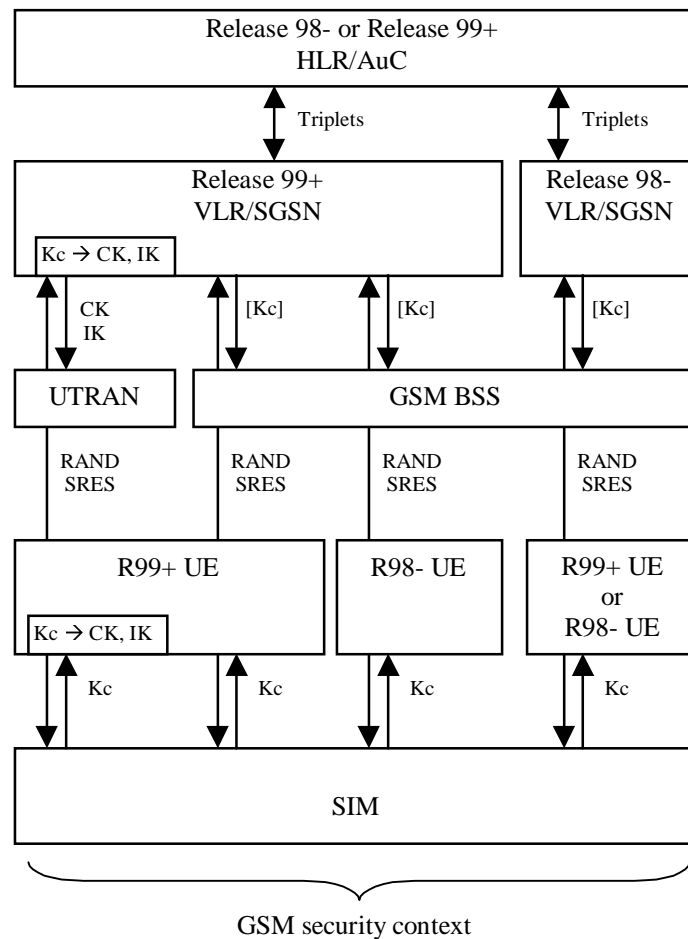


Figure 19: Authentication and key agreement for GSM subscribers

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 and IK are always sent to the RNC.

Note that a SIM can operate in both R99+ and R98- UEs.

6.8.2.2 R99+ HLR/AuC

Upon receipt of an authentication data request for a GSM subscriber, a R99+ HLR/AuC shall send triplets generated as specified in GSM 03.20.

6.8.2.32 R99+ MSC/VLR or SGSN/VLR/SGSN

The R99+ ~~MSC/VLR or SGSN/VLR/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/VLR/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/VLR/SGSN~~.

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

- a) c4: $CK_{[UMTS]} = 0\dots0 \parallel Kc$;
- 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.

6.8.2.43 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 UE.

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

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

6.8.3.1 UMTS security context

A UMTS security context in UTRAN is only established for a UMTS subscriber. At the network side, ~~threetwo~~ 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) b)~~ In case of a handover to a GSM BSS controlled by ~~another~~ 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 ~~(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. 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 UE applies the derived ~~the~~ GSM cipher key Kc received from the USIM during last UMTS AKA procedure. from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and applies Kc.

6.8.3.2 GSM security context

A GSM security context in UTRAN is only established for a GSM subscribers with a R99+ UE. 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(second)~~ 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 UE applies the stored GSM cipher key Kc.

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

6.8.4.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers 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-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(second) MSC/VLR that controls the new 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 UE applies the stored UMTS cipher/integrity keys CK and IK.

6.8.4.2 GSM security context

Handover from GSM BSS to UTRAN with a GSM security context is only possible for a GSM subscriber with a R99+ 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 target 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/new) MSC/VLR controlling the new-target RNC. That MSC/VLR derives UMTS cipher/integrity keys CK and IK which are then forwarded to the new-target 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.

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

6.8.5.1 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 a handover 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 a handover 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 a handover 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 a) or b), the UE ~~derives~~ applies the derived GSM cipher key Kc received from the USIM during last UMTS AKA procedure. ~~from the stored UMTS cipher/integrity keys CK and IK (using the conversion function e3) 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.~~

6.8.5.2 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 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 a handover 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 UE applies the GSM cipher key Kc that is stored.

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

6.8.6.1 UMTS security context

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

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

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

6.8.6.2 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 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 quintuplets 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+ UE. At the network side, ~~two~~ three cases are distinguished:

- a) In case of a handover 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 new target RNC.
- b) In case of a handover 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 new 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 new 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+UE is coming from a R98-SGSN.

At the user side, in both all 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. In case c) these keys will be overwritten with a new CK, IK pair due to the new AKA.