3GPP TSG SA WG 3 (Security) meeting #11
Mainz, 22—24 February, 2000

Document **S3-000208 (Rev. of S3-000126)**
e.g. for 3GPP use the format TP-99xxx or for SMG, use the format P-99-xxx

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**	**047rx**	Current Version:	3.3.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	SA #7	for approval	X	strategic	*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [X]
(at least one should be marked with an X)

Source: Ericsson **Date:** 2000-03-03

Subject: Interoperation and intersystem handover/change between UTRAN and GSM BSS

Work item: Security

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

F	Correction		
A	Corresponds to a correction in an earlier release		
B	Addition of feature		
C	Functional modification of feature	X	
D	Editorial modification		

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change:

Scenarios for authentication and intersystem handover/change are described in greater detail in order to clarify the existing section. Major modifications include:

a) General:
- Terms 'MSC/VLR or SGSN' and 'quintet' replaced by 'VLR/SGSN' and 'quintuplets' respectively.
- Conversion function c3 (CK, IK → Kc) located only at USIM.

b) Chapter 6.8.1.3: Key freshness provided to UMTS subs even under GSM BSS
c) Chapter 6.8.1.5: UISM vs UICC (UICC abbreviation in section 3.3).
d) Chapter 6.8.2.2: Handling of GSM subscribers by R99+ HLR/AuC.
e) Chapter 6.8.3 and 6.8.4: Key derivation at anchor MSC/VLR.
f) Chapter 6.8.3.1: Inclusion of handover case c)
g) Chapter 6.8.7.2: New intersystem change from GSM BSS to UTRAN (USIM).

Clauses affected: 3.3, 6.8

Other specs affected:

Other 3G core specifications		→ List of CRs:	
Other GSM 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:

help.doc

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

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
$D_{SK(X)}$(data)	Decryption of "data" with Secret Key of X used for signing
$E_{KSXY(i)}$(data)	Encryption of "data" with Symmetric Session Key #i for sending data from X to Y
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
IV	Initialisation Vector
KAC_X	Key Administration Centre of Network X
KS_{XY}(i)	Symmetric Session Key #i for sending data from X to Y
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAP	Mobile Application Part
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
MS	Mobile Station
MSC	Mobile Services Switching Centre
MT	Mobile Termination
NE_X	Network Element of Network X
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
RND_X	Unpredictable Random Value generated by X
SQN	Sequence number
SQN_{UIC}	Sequence number user for enhanced user identity confidentiality
SQN_{HE}	Sequence number counter maintained in the HLR/AuC
SQN_{MS}	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TE	Terminal Equipment
Text1	Optional Data Field
Text2	Optional Data Field
Text3	Public Key algorithm identifier and Public Key Version Number (eventually included in Public Key Certificate)
TMSI	Temporary Mobile Subscriber Identity
TTP	Trusted Third Party
UE	User equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Identity Module

VLR	Visitor Location Register
X	Network Identifier
XRES	Expected Response
Y	Network Identifier

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:

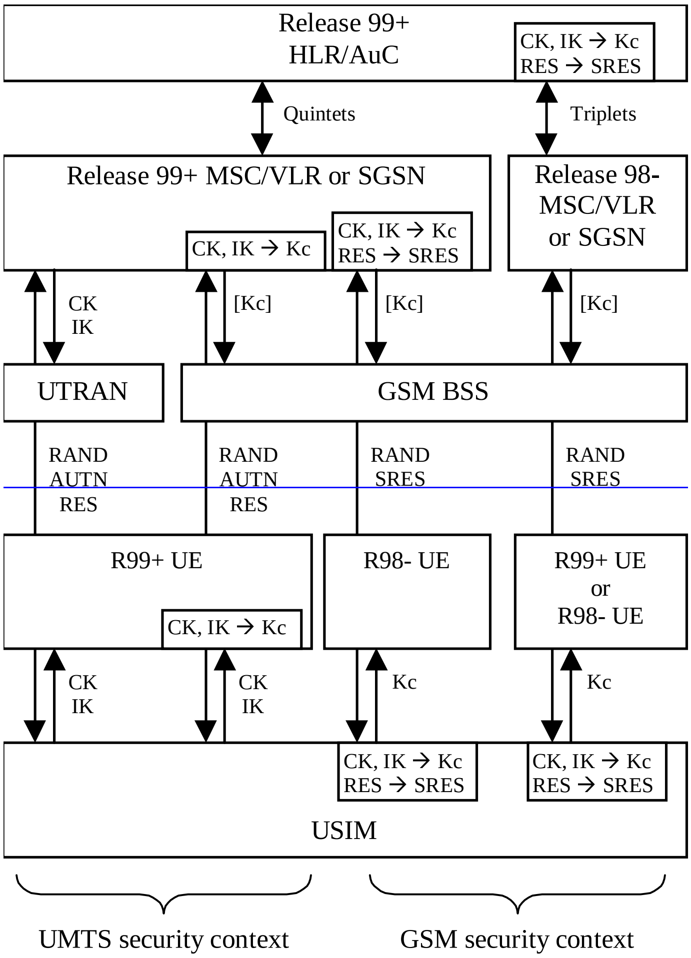
- UMTS AKA shall be applied when the user is attached to a UTRAN.
- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has R99+ UE and also the ~~MSC/VLR or SGSN~~VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and 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. A R98- VLR/SGSN uses the stored Kc and RES and a R99+ VLR/SGSN derives the SRES from RES and Kc from CK, IK.

  Note*: To support R98- UE the UICC may contain a GSM SIM application which provides the corresponding GSM functionality for calculating SRES and Kc based on the 3G authentication key K and the 3G authentication algorithm implemented in the USIM. Due to the fact that the 3G authentication algorithm only computes CK/IK and RES, conversion of CK/IK to Kc shall be achieved by using the conversion function c3, and conversion of RES to SRES by c2.

- 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.


Release 99+
HLR/AuC
CK, IK → Kc
RES → SRES
Quintets
Triplets
Release 99+ MSC/VLR or SGSN
CK, IK → Kc
CK, IK → Kc
RES → SRES
Release 98-
MSC/VLR
or SGSN
CK
IK
[Kc]
[Kc]
[Kc]
UTRAN
GSM BSS
RAND
AUTN
RES
RAND
AUTN
RES
RAND
SRES
RAND
SRES
R99+ UE
CK, IK → Kc
R98- UE
R99+ UE
or
R98- UE
CK
IK
CK
IK
Kc
Kc
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
USIM
UMTS security context
GSM security context

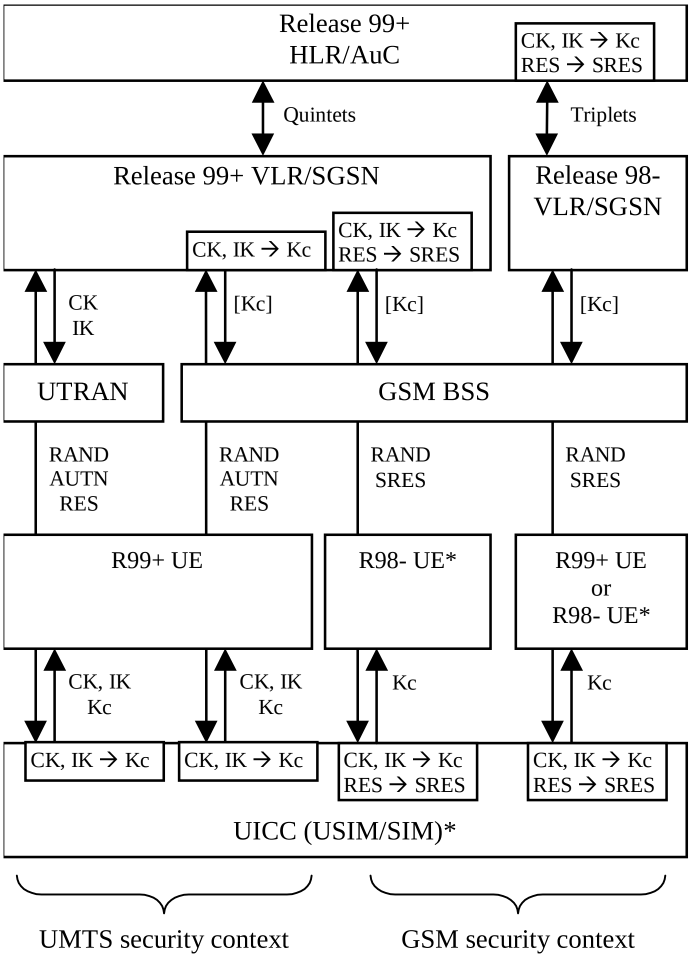


Figure 18: Authentication and key agreement of UMTS subscribers

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 and integrity ~~is~~ are 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~~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: $Kc_{[GSM]} = CK_1 \text{ xor } CK_2 \text{ xor } IK_1 \text{ xor } IK_2$

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

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~~quintuplet 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~~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~~VLR/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~~VLR/SGSN from a ~~quintet~~quintuplet 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~~VLR/SGSN, or

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

Note that for a UMTS subscriber, all triplets are derived from ~~quintet~~quintuplets, be it in the HLR/AuC or in an ~~MSC/VLR or SGSN~~VLR/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 VLR/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 cannot be provided to UMTS subscriber with R98- UE.

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~~Participation in 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 inpassed to the UE. The UE shall also receive a GSM cipher key Kc derived at 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 UICC (USIM/SIM)

The UICC shall support UMTS AKA (UICC shall contain USIM application) and may support GSM AKA (UICC may contain a SIM application). Support of GSM AKA is required to allow access to GSM-BSS with a R98- VLR/SGSN and/or with a R98- UE.

When the UE provides the UICC 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 UICC shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The UICC shall store CK and IK as current security context data. The UICC 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 R99+ UE. In case the verification of AUTN is not successful, the UICC shall respond with an appropriate error indication to the R99+ UE.

When the UE provides the UICC 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 UICC first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM UICC then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The USIM UICC then stores the GSM cipher key Kc and sends the GSM user response SRES and the GSM cipher key Kc to the UE.

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

6.8.2 Authentication and key agreement for GSM subscribers

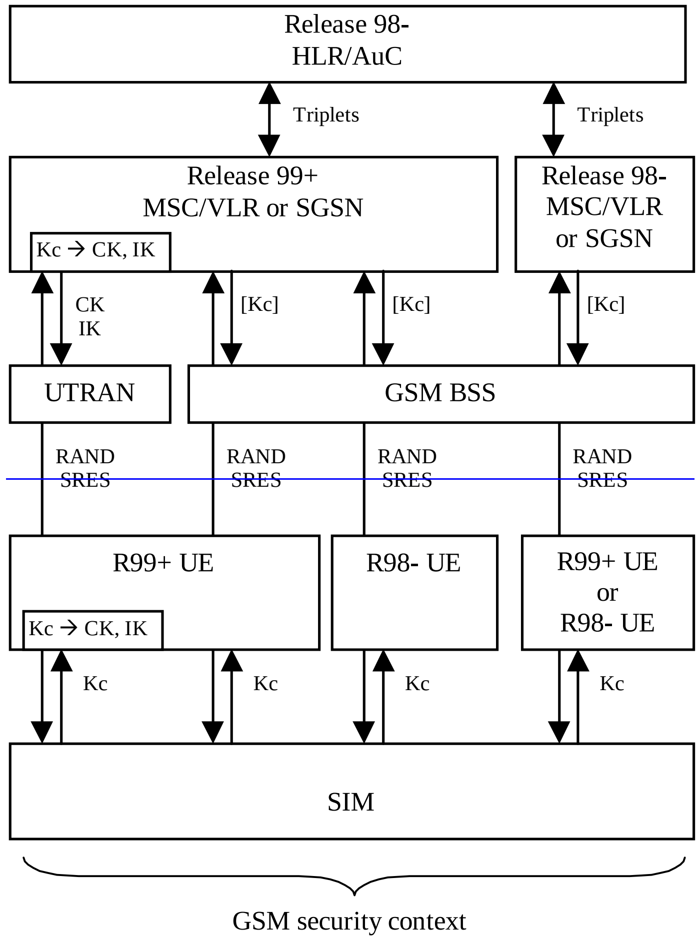
6.8.2.1 General

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 SGSNVLR/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.


Release 98-
HLR/AuC
Triplets
Triplets
Release 99+
MSC/VLR or SGSN
Kc → CK, IK
Release 98-
MSC/VLR
or SGSN
CK
IK
[Kc]
[Kc]
[Kc]
UTRAN
GSM BSS
RAND
SRES
RAND
SRES
RAND
SRES
RAND
SRES
R99+ UE
Kc → CK, IK
R98- UE
R99+ UE
or
R98- UE
Kc
Kc
Kc
Kc
SIM
GSM security context

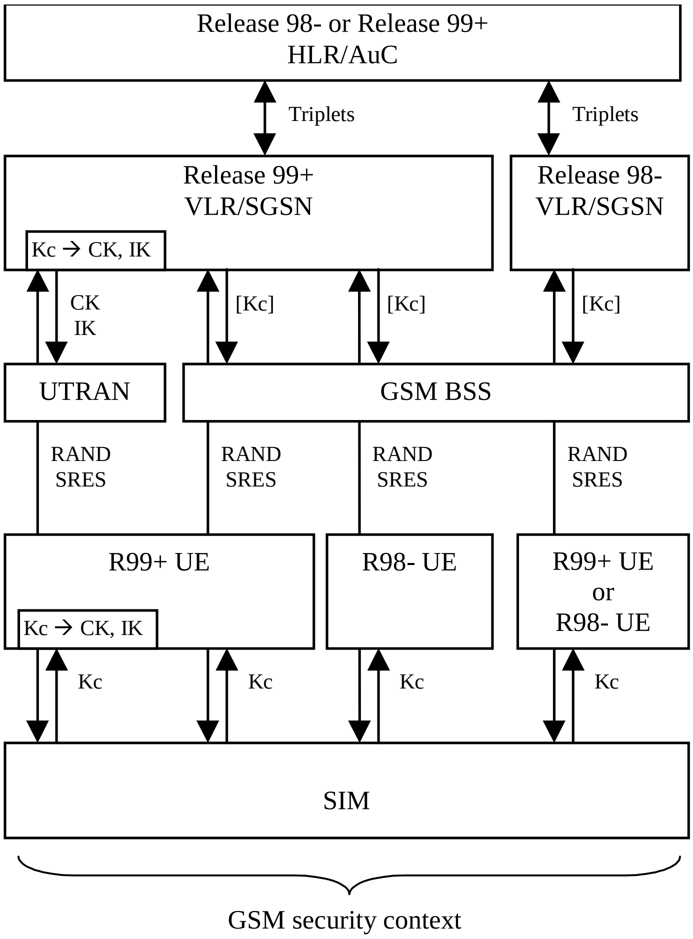


Figure 19: Authentication and key agreement for GSM subscribers

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+ 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.

6.8.2.3~~2~~ 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…0 || Kc;

b) c5: $IK_{[UMTS]}$ = Kc || 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 CKk 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 with a R99+ UE. 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 deriveds 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) 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 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~~ 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 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.~~

6.8.5.2 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 with R99+ UE 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 user has a R98- UE, where intersystem change to UTRAN is not possible, or in case the user has a R99+UE 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 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~~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 ~~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 over-written with a new CK, IK pair due to the new AKA.