

CR-Form-v7
CHANGE REQUEST
⌘ TS 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 Radio Access Network Core Network

Title:	⌘ Introducing the special RAND mechanism
Source:	⌘ Orange, Vodafone
Work item code:	Date: ⌘ 14/11/2003
Category:	⌘ B Release: ⌘ Rel-6 Use <u>one</u> of the following categories: <i>F</i> (correction) <i>A</i> (corresponds to a correction in an earlier release) <i>B</i> (addition of feature), <i>C</i> (functional modification of feature) <i>D</i> (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .
	Use <u>one</u> 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:	⌘ As there is no cryptographic key separation between GSM / GPRS encryption algorithms, it cannot be controlled with which algorithm the ciphering key may be used.
Summary of change:	⌘ Introduces the special RAND mechanism described in [S3-030588] to restrict the ciphering algorithms with which a particular GSM or GPRS ciphering key may be used.
Consequences if not approved:	⌘ There is no mean to restrict the algorithms with which the ciphering key may be used.

Clauses affected:	⌘ 2, 3.3, 6.8.1.2, 6.8.1.4, 6.8.2.2, 6.8.2.2, 6.8.2.4, 6.8.4.1, 6.8.4.2, 6.8.6.1, 6.8.6.2									
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px 5px;">Y</td> <td style="padding: 2px 5px;">N</td> </tr> <tr> <td style="padding: 2px 5px;">X</td> <td style="padding: 2px 5px;"></td> </tr> <tr> <td style="padding: 2px 5px;"></td> <td style="padding: 2px 5px;">X</td> </tr> <tr> <td style="padding: 2px 5px;"></td> <td style="padding: 2px 5px;">X</td> </tr> </table>	Y	N	X			X		X	⌘ Other core specifications ⌘ TS 43.020, TS 24.008, 44.018 ⌘ Test specifications ⌘ O&M Specifications
	Y	N								
	X									
	X									
	X									
Other comments:	⌘									

***** BEGIN SET OF CHANGES *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
 - For a specific reference, subsequent revisions do not apply.
 - For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.
- [1] 3GPP TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".
 - [2] 3GPP TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".
 - [3] 3GPP TR 21.905: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 1999)".
 - [4] 3GPP TS 23.121: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Architecture Requirements for Release 99".
 - [5] 3GPP TS 31.101: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".
 - [6] 3GPP TS 22.022: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".
 - [7] 3GPP TS 23.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM application toolkit; Stage 2".
 - [8] ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".
 - [9] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".
 - [10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".
 - [11] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".
 - [12] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".
 - [13] 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data".
 - [14] 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data".

- [15] 3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".
- [16] 3GPP TS 22.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM Application Toolkit; Stage 1".
- [17] 3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RRC Protocol Specification".
- [18] 3GPP TS 25.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; MAC protocol specification".
- [19] 3GPP TS 25.322: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RLC Protocol Specification".
- [20] 3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Characteristics of the USIM Application".
- [21] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".
- [22] 3GPP TS 23.195: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Provision of User Equipment Specific Behaviour Information (UESBI) to network entities".
- [23] [3GPP TS 43.020: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Related Network Functions"](#).

***** END SET OF CHANGES *****

***** BEGIN SET OF CHANGES *****

3.3 Abbreviations

In addition to (and partly in overlap to) the abbreviations included in TR 21.905 [3], 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
EARV	Encryption Algorithm Restriction Variable
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	The message authentication code included in AUTN, computed using f1
MAC	The message authentication code included in AUTN, computed using f1*
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector

RAI	Routing Area Identifier
RAND	Random challenge
SQN	Sequence number
SQN _{HE}	Individual sequence number for each user maintained in the HLR/AuC
SQN _{MS}	The highest sequence number the USIM has accepted
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Identity Module
VLR	Visitor Location Register
XRES	Expected Response

***** END SET OF CHANGES *****

***** BEGIN SET OF CHANGES *****

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 a ME capable of UMTS AKA and also the 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 a ME not capable of UMTS AKA. 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 operate within a ME not capable of UMTS AKA, the USIM may support the SIM-ME interface as defined in GSM 11.11, and support GSM AKA which provides the corresponding GSM functionality for calculating SRES and Kc based on the authentication key K and the 3G authentication algorithm implemented in the USIM. Due to the fact that the UMTS 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 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 in a mixed network architecture.

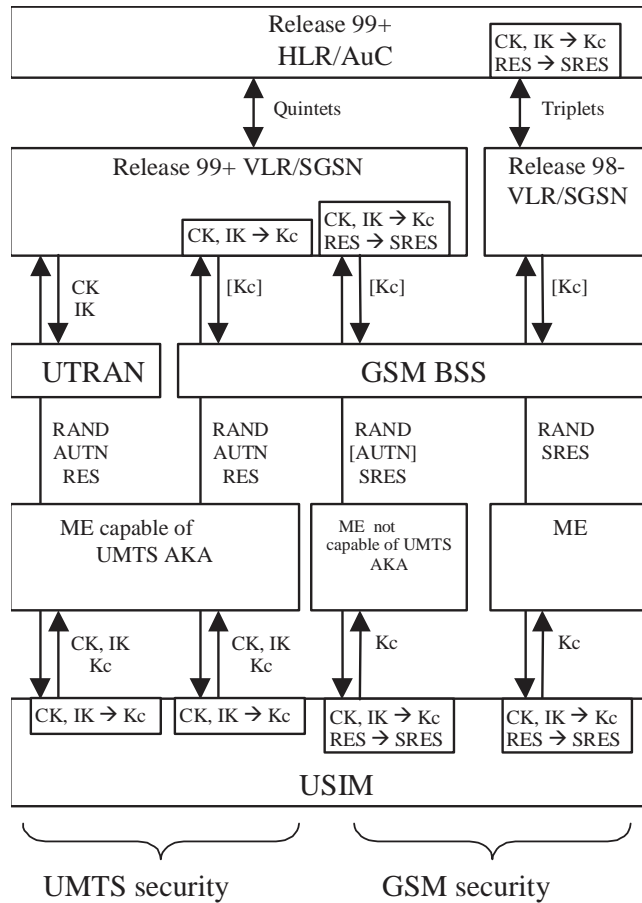


Figure 18: Authentication and key agreement of UMTS subscribers

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 and integrity are always applied in the RNC, and the UMTS cipher/integrity keys CK and IK are always sent to the RNC.

6.8.1.2 R99+ HLR/AuC

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

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

- $c1: RAND_{[GSM]} = RAND$
- $c2: SRES_{[GSM]} = XRES^*_1 \text{ xor } XRES^*_2 \text{ xor } XRES^*_3 \text{ xor } XRES^*_4$
- $c3: Kc_{[GSM]} = CK_1 \text{ xor } CK_2 \text{ xor } IK_1 \text{ xor } IK_2$

whereby XRES* is 16 octets long and $XRES^* = XRES$ if XRES is 16 octets long and $XRES^* = XRES \parallel 0\dots0$ if XRES is shorter than 16 octets, $XRES^*_i$ are all 4 octets long and $XRES^* = XRES^*_1 \parallel XRES^*_2 \parallel XRES^*_3 \parallel XRES^*_4$, CK_i and IK_i are both 64 bits long and $CK = CK_1 \parallel CK_2$ and $IK = IK_1 \parallel IK_2$

A RAND generated by an HLR/AuC for subscribers that may roam into GSM may include an Encryption Algorithms Restriction Vector (EARV) according to the specifications in TS 43.020 [23].

6.8.1.3 R99+ VLR/SGSN

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

UMTS subscriber with R99+ ME

When the user has R99+ ME, the VLR/SGSN shall send the ME a UMTS authentication challenge (i.e. RAND and AUTN) using a quintet that is either:

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

Note: Originally all quintets are provided by the HLR/AuC.

When the ME is capable of the USIM-ME interface, then UMTS AKA is performed and the VLR/SGSN receives the UMTS response RES.

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 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+ ME independently of the radio access network.

When the ME is not capable of the USIM-ME interface, then GSM AKA is performed and the VLR/SGSN receives the GSM response SRES.

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.

The R99+ VLR/SGSN shall reject authentication if SRES is received in response of a UMTS challenge (RAND, AUTN) over an Iu-Interface.

The R99+ VLR/SGSN shall accept authentication if a valid SRES is received in response of a UMTS challenge (RAND, AUTN) over A or Gb-Interface. This will happen in case a UICC is inserted in a ME that is not capable of UMTS AKA and is attached to a GSM BSS. In this case the R99+ VLR/SGSN uses function c2 to convert RES (from the quintet) to SRES to verify the received SRES.

UMTS subscriber with R98- ME

When the user has R98- ME, the R99+ VLR/SGSN sends the ME a GSM authentication challenge using a triplet that is either:

- a) derived by means of the conversion functions c2 and c3 in the R99+ VLR/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+ VLR/SGSN, or
- b) provided as a triplet by the previously visited VLR/SGSN.

NOTE: R99+ VLR/SGSN will always provide quintets for UMTS subscribers.

NOTE: For a UMTS subscriber, all triplets are derived from quintets, be it in the HLR/AuC or in an 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.

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- ME.

6.8.1.4 R99+ ME

Release 99+ ME that has UTRAN radio capability shall support the USIM-ME interface as specified in TS 31.102 [20].

Rel-4 ME that has no UTRAN radio capabilities may support the USIM-ME interface as specified in TS 31.102 [20].

Rel5+ ME that has no UTRAN radio capabilities shall support the USIM-ME interface as specified in TS 31.102 [20].

A ME capable of UMTS AKA with a USIM active and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA.

A ME capable of UMTS AKA with a USIM active and attached to a GSM BSS shall participate in UMTS AKA and may participate in GSM AKA. Participation in GSM AKA is required to allow registration in a R98- VLR/SGSN.

A ME that not capable of UMTS AKA with a USIM active can only participate in GSM AKA.

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 passed to the ME. If the USIM supports conversion function c3 and/or GSM AKA, the ME shall also receive a GSM cipher key Kc derived 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 ME.

[An ME that has GSM radio capabilities shall be able to process RAND values which include an Encryption Algorithms Restriction Vector \(EARV\) according to the specifications in TS 43.020 \[23\].](#)

6.8.1.5 USIM

The USIM shall support UMTS AKA and may support backwards compatibility with the GSM system, which consists of:

- Feature 1: GSM cipher key derivation (conversion function c3) to access GSM BSS attached to a R99+ VLR/SGSN using a dual-mode R99+ ME;
- Feature 2: GSM AKA to access the GSM BSS attached to a R98- VLR/SGSN or when using ME not capable of UMTS AKA;
- Feature 3: SIM-ME interface (GSM 11.11) to operate within ME not capable of UMTS AKA.

When the ME provides the USIM with RAND and AUTN, UMTS AKA shall be executed. If 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 as current security context data. If the USIM supports access to GSM cipher key derivation (feature 1), 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 ME. In case the verification of AUTN is not successful, the USIM shall respond with an appropriate error indication to the ME.

When the ME provides the USIM with only RAND, and the USIM supports GSM AKA (Feature 2), GSM AKA shall be executed. 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 key Kc as the current security context and sends the GSM user response SRES and the GSM cipher key Kc to the ME.

In case the USIM does not support GSM cipher key derivation (Feature 1) or GSM AKA (Feature 2), the ME shall be informed. An ME with a USIM that does not support GSM cipher key derivation (Feature 1) shall not perform the GSM cipher key derivation (conversion function c3) in the ME and therefore cannot operate in any GSM BSS with 64-bit key ciphering enabled. An ME with a USIM that does not support GSM AKA (Feature 2) cannot operate under a R98-

VLR/SGSN. A USIM that does not support GSM AKA (Feature 2) cannot work within a ME that is not capable of UMTS AKA.

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 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 ME and the VLR/SGSN, both R99+ entities.

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

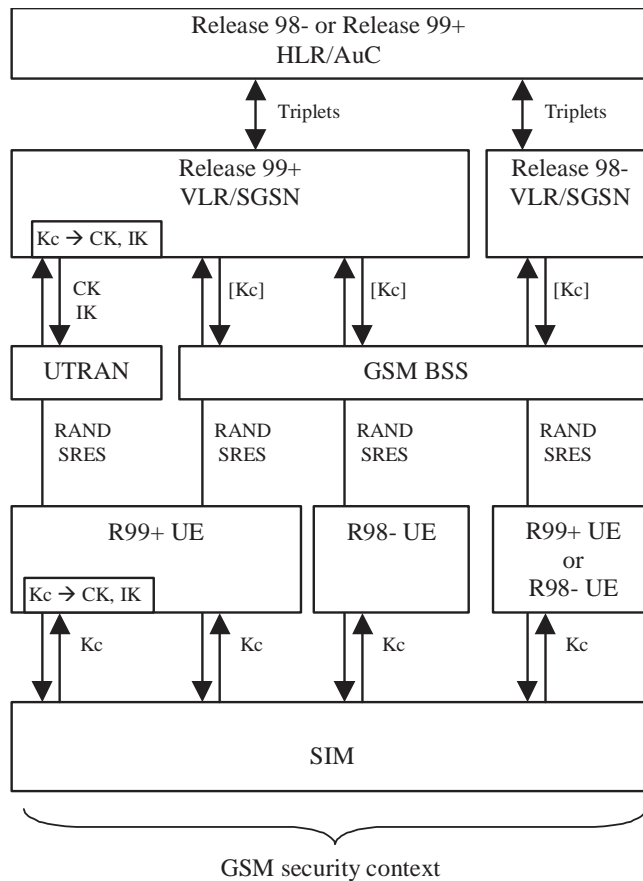


Figure 19: Authentication and key agreement for GSM subscribers

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.

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.

[A RAND generated by an HLR/AuC for subscribers that may roam into GSM may include an Encryption Algorithms Restriction Vector \(EARV\) according to the specifications in TS 43.020 \[23\].](#)

6.8.2.3 VLR/SGSN

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

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

NOTE: All triplets are originally provided by the HLR/AuC.

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

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

- a) c4: $CK_{[UMTS]} = K_c \parallel K_c$;
- b) c5: $IK_{[UMTS]} = K_{c1} \text{ xor } K_{c2} \parallel K_c \parallel K_{c1} \text{ xor } K_{c2}$;

whereby in c5, K_{c_i} are both 32 bits long and $K_c = K_{c1} \parallel K_{c2}$.

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

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

6.8.2.4 R99+ ME

R99+ ME 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 K_c and the cipher key sequence number CKSN are stored in the ME.

When the user is attached to a UTRAN, R99+ ME shall derive the UMTS cipher/integrity keys CK and IK from the GSM cipher key K_c using the conversion functions c4 and c5. The ME shall handle the $START_{CS}$ and $START_{PS}$ as described in section 6.4.8 with the exception that the START values shall be stored in non-volatile memory on the ME rather than on the GSM SIM. If a different SIM is inserted then the ME shall delete the GSM cipher keys for the PS and CS domain (K_c), the derived UMTS cipher/integrity keys (CK and IK) for the PS and CS domain, and reset the START values to zero. The ME shall then trigger a new authentication and key agreement at the next connection establishment by indicating to the network that no valid keys are available for use using the procedure described in section 6.4.4.

When the user is attached to a UTRAN, a R99+ ME with a SIM inserted shall use a default value of all ones for maximum value of $START_{CS}$ or $START_{PS}$. The ME shall handle the maximum value of $START_{CS}$ or $START_{PS}$ as described in section 6.4.3 with the exception that the maximum value of $START_{CS}$ or $START_{PS}$ is stored on the ME rather than on the GSM SIM.

[An ME that has GSM radio capabilities shall be able to process RAND values which include an Encryption Algorithms Restriction Vector \(EARV\) according to the specifications in TS 43.020 \[23\].](#)

6.8.3 Distribution and use of authentication data between VLRs/SGSNs

The distribution of authentication data (unused authentication vectors and/or current security context data) between

R99+ VLRs/SGSNs of the same service network domain is performed according to chapter 6.3.4. The following four cases are distinguished related to the distribution of authentication data between VLRs/SGSNs (of the same or different releases). Conditions for the distribution of such data and for its use when received at VLRn/SGSNn are indicated for each case:

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

UMTS and GSM authentication vectors can be distributed between R99+ VLRs/SGSNs. Note that originally all authentication vectors (quintets for UMTS subscribers and triplets for GSM subscribers) are provided by the HLR/AuC.

Current security context data can be distributed between R99+ VLRs/SGSNs. VLRn/SGSNn shall not use current security context data received from VLRo/SGSNo to authenticate the subscriber using local authentication in the following cases:

- i) Security context to be established at VLRn/SGSNn requires a different set of keys than the one currently in use at VLRo/SGSNo. This change of security context is caused by a change of ME release (R'99 ME \leftrightarrow R'98 ME) when the user registers at VLRn/SGSNn.
- ii) Authentication data from VLRo includes Kc+CKSN but no unused AVs and the subscriber has a R'99 ME (under GSM BSS or UTRAN). In this situation, VLRn have no indication of whether the subscriber is GSM or UMTS and it is not able to decide whether Kc received can be used (in case the subscriber were a GSM subscriber).

In these two cases, received current security context data shall be discarded and a new AKA procedure shall be performed.

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

Only triplets can be distributed between R98- VLRs/SGSNs. Note that originally for GSM subscribers, triplets are generated by HLR/AuC and for UMTS subscribers, they are derived from UMTS authentication vectors by R99+ HLR/AuC. UMTS AKA is not supported and only GSM security context can be established by a R98- VLR/SGSN.

R98- VLRs are not prepared to distribute current security context data.

Since only GSM security context can be established under R98- SGSNs, security context data can be distributed and used between R98- SGSNs.

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

R99+ VLR/SGSN can distribute to a new R98- VLR/SGSN triplets originally provided by HLR/AuC for GSM subscribers or can derive triplets from stored quintets originally provided by R99+ HLR/AuC for UMTS subscribers. Note that R98- VLR/SGSN can only establish GSM security context.

R99+ VLRs shall not distribute current security context data to R98- VLRs.

Since R98- SGSNs are only prepared to handle GSM security context data, R99+ SGSNs shall only distribute GSM security context data (Kc, CKSN) to R98- SGSNs.

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

In order to not establish a GSM security context for a UMTS subscriber, triplets provided by a R98- VLR/SGSN can only be used by a R99+ VLR/SGSN to establish a GSM security context under GSM-BSS with a R98- ME.

In all other cases, R99+ VLR/SGSN shall request fresh AVs (either triplets or quintets) to HE. In the event, the R99+ VLR/SGSN receives quintets, it shall discard the triplets provided by the R98- VLR/SGSN.

R98- VLRs are not prepared to distribute current security context data.

R98- SGSNs can distribute GSM security context data only. The use of this information at R99+ SGSNn shall be performed according to the conditions stated in a).

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 (using the conversion function c3) and sends Kc to the target BSC (which forwards it to the BTS).
- b) In case of a handover to a GSM BSS controlled by other R98- MSC/VLR, the initial MSC/VLR derives the GSM cipher key from the stored UMTS cipher/integrity keys (using the conversion function c3) and sends it to the target BSC via the new MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.
- c) In case of a handover to a GSM BSS controlled by another R99+ MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new MSC/VLR. The initial MSC/VLR also derives Kc and sends it to the new MSC/VLR. The new MSC/VLR store the keys and sends the received GSM cipher key Kc to the target BSC (which forwards it to the BTS). The initial MSC/VLR remains the anchor point throughout the service.

At the user side, in either case, the ME applies the derived GSM cipher key Kc received from the USIM and the Encryption Algorithms Restriction Vector (EARV) derived from RAND according to TS 43.020 [23] 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 to the target BSC (which forwards it to the BTS).
- b) In case of a handover to a GSM BSS controlled by another MSC/VLR (R99+ or R98-), the initial MSC/VLR sends the stored GSM cipher key Kc to the BSC via the new MSC/VLR controlling the target BSC. The initial MSC/VLR remains the anchor point throughout the service.

If the non-anchor MSC/VLR is R99+, then the anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the UMTS cipher/integrity keys CK and IK. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.

At the user side, in either case, the ME applies the stored GSM cipher key Kc and the Encryption Algorithms Restriction Vector (EARV) derived from RAND according to TS 43.020 [23].

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

If ciphering has been started when an intersystem handover occurs from GSM BSS to UTRAN, the necessary information (e.g. CK, IK, START value information, supported/allowed UMTS algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old GSM

BSS to the new RNC, and to continue the communication in ciphered mode. The GSM BSS requests the MS to send the UMTS capability information, which includes information on the START values and UMTS security capabilities of the MS. The intersystem handover will imply a change of ciphering algorithm from a GSM A5 to a UEA. The target UMTS RNC includes the selected UMTS ciphering mode in the handover to UTRAN command message sent to the MS via the GSM BSS.

The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed. The Serving RNC will do this by initiating the RRC security mode control procedure when the first RRC message (i.e. the Handover to UTRAN complete message) has been received from the MS. The UE security capability information, that has been sent from MS to RNC via the GSM radio access and the system infrastructure before the actual handover execution, will then be included in the RRC Security mode command message sent to MS and then verified by the MS (i.e. verified that it is equal to the UE security capability information stored in the MS).

6.8.5.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with a ME that is capable of UMTS AKA under GSM BSS controlled by a R99+ VLR/SGSN. At the network side, two cases are distinguished:

- a) In case of a handover to a UTRAN controlled by the same MSC/VLR, the stored UMTS cipher/integrity keys CK and IK are sent to the target RNC.
- b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new RNC via the new MSC/VLR that controls the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

The anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the GSM cipher key Kc. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.

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

6.8.5.2 GSM security context

Handover from GSM BSS to UTRAN with a GSM security context is possible for a GSM subscriber with a R99+ ME or for a UMTS subscriber with a R99+ ME when the initial MSC/VLR is R98-. At the network side, two cases are distinguished:

- a) In case of a handover to a UTRAN controlled by the same MSC/VLR, UMTS cipher/integrity keys CK and IK are derived from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sent to the target RNC. In case of subsequent handover in a non-anchor R99+ MSC/VLR, a GSM cipher key Kc is received for a UMTS subscriber if the anchor MSC/VLR is R98-.
- b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR (R99+ or R98-) sends the stored GSM cipher key Kc to the new MSC/VLR controlling the target RNC. That MSC/VLR derives UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

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

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 (using the conversion function c3) and applies it.
- b) In case of an intersystem change to a GSM BSS controlled by another R99+ SGSN, the initial SGSN sends the

stored UMTS cipher/integrity keys CK and IK to the new SGSN. The new SGSN stores the keys, derives the GSM cipher key Kc and applies the latter. The new SGSN becomes the new anchor point for the service.

- c) In case of an intersystem change to a GSM BSS controlled by a R98- SGSN, the initial SGSN derives the GSM cipher key Kc and sends the GSM cipher key Kc to the new SGSN. The new SGSN stores the GSM cipher key Kc and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in all cases, the ME applies the derived GSM cipher key Kc received from the USIM [and the Encryption Algorithms Restriction Vector \(EARV\) derived from RAND according to TS 43.020 \[23\]](#) during the last UMTS AKA procedure.

6.8.6.2 GSM security context

A GSM security context in UTRAN is only established for GSM subscribers. At the network side, two cases are distinguished:

- a) In case of an intersystem change to a GSM BSS controlled by the same SGSN, the SGSN starts to apply the stored GSM cipher key Kc.
- b) In case of an intersystem change to a GSM BSS controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the BSC. The new SGSN stores the key and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in both cases, the ME applies the GSM cipher key Kc [and the Encryption Algorithms Restriction Vector \(EARV\) derived from RAND according to TS 43.020 \[23\]](#) that ~~is~~are 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 are sent to the target RNC.
- b) In case of an intersystem change to a UTRAN controlled by another SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN then stores the UMTS cipher/integrity keys CK and IK and sends them to the target RNC.

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

6.8.7.2 GSM security context

A GSM security context in GSM BSS can be either:

- **Established for a UMTS subscriber**

A GSM security context for a UMTS subscriber is established in case the user has a ME not capable of UMTS AKA, where intersystem change to UTRAN is not possible, or in case the user has a R99+ ME but the SGSN is R98-, where intersystem change to UTRAN implies a change to a R99+ SGSN.

As result, in case of intersystem change to a UTRAN controlled by another R99+ SGSN, the initial R98- SGSN sends the stored GSM cipher key Kc to the new SGSN controlling the target RNC.

Since the new R99+ SGSN has no indication of whether the subscriber is GSM or UMTS, a R99+ SGSN shall perform a new UMTS AKA when receiving Kc from a R98- SGSN. A UMTS security context using fresh quintets is then established between the R99+ SGSN and the USIM. The new SGSN becomes the new anchor point for the service.

At the user side, new keys shall be agreed during the new UMTS AKA initiated by the R99+ SGSN.

- **Established for a GSM subscriber**

Handover from GSM BSS to UTRAN for GSM subscriber is only possible with R99+ ME. At the network side, three cases are distinguished:

- a) In case of an intersystem change to a UTRAN controlled by the same SGSN, the SGSN derives UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sends them to the target RNC.
- b) In case of an intersystem change from a R99+ SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN stores the GSM cipher key Kc and derives the UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC.
- c) In case of an intersystem change from an R98-SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. To ensure use of UMTS keys for a possible UMTS subscriber (superfluous in this case), a R99+ SGSN will perform a new AKA when a R99+ ME is coming from a R98-SGSN.

At the user side, in all cases, the ME derives the UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and applies them. In case c) these keys will be overwritten with a new CK, IK pair due to the new AKA.

***** **END SET OF CHANGES** *****