Technical Specification Group Services and System Aspects
Meeting #25, Palm Springs, USA

TSGS#25(04)0627

Source: **SA WG3**

Title: **2 CRs to 33.102: Correction to mis-implementation of CR175: Rel4- definition (Rel-5 and Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs were provided by MCC in response to the LS in SP-040491, which highlighted the mis-implementation of CR175 in 2002. These corrective CRs are now presented to TSG SA for approval.

The originally approved CR175 is added to this contribution for information only.

TSG SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Work item
SP-040627	33.102	187	-	Rel-5	Correction to mis-implementation of CR175: Rel4- definition	F	5.4.0	- (MCC input)	SEC1
SP-040627	33.102	188	-	Rel-6	Correction to mis-implementation of CR175: Rel4- definition	F	6.1.0	- (MCC input)	SEC1

Technical Specification Group Services and System Aspects **TSGS#25(04)0627.a**

Meeting #25, Palm Springs, USA

CR-Form-v7

CHANGE REQUEST

⌘ **33.102 CR 187** ⌘ **rev - ** ⌘ Current version: **5.4.0** ⌘

*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: ⌘ Correction to mis-implementation of CR175: Rel4- definition

Source: ⌘ SA WG3 (MCC)

Work item code: ⌘ SEC1 ***Date:*** ⌘ 08/08/2004

Category: ⌘ **F** ***Release:*** ⌘ Rel-5

Use one of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘ The change from **Rel-4** to **Rel4-** was missed in the implementation of CR175 and has lead to a mis-understanding in T WG3 (see LS in SP-040491)

Summary of change: ⌘ Replace **Rel-4** by **Rel4-** in section 6.8.1.4. Correct definition in section 3.1.

Consequences if not approved: ⌘ Specification will not provide intended allowance for Rel-99 ME with no UTRAN capabilities to support the USIM-ME interface.

Clauses affected: ⌘ 3.1, 6.8.1.4

Other specs affected: ⌘

Y	N		
	N	Other core specifications	⌘
	N	Test specifications	
	N	O&M Specifications	

Other comments: ⌘ This was intended to be added in 2002 by approved CR 175 but was mistakenly not implemented.

**** FIRST CHANGE ****

3 Definitions, symbols abbreviations and conventions

3.1 Definitions

In addition to the definitions included in TR 21.905 [3] and TS 22.101 [21], for the purposes of the present document, the following definitions apply:

NOTE: 'User' and 'Subscriber' have been defined in TR 21.905 [3]. 'User Equipment', 'USIM', 'SIM' and 'IC Card' have been defined in TS 22.201 [21].

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

UMTS Entity authentication and key agreement: Entity authentication according to this specification.

GSM Entity authentication and key agreement: The entity Authentication and Key Agreement procedure to provide authentication of a SIM to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in GSM 03.20.

User: Within the context of this specification a user is either a UMTS subscriber (Section 6.8.1) or a GSM Subscriber (Section 6.8.2) or a physical person as defined in TR 21.905[3] (Section 5.3 and 5.5).

UMTS subscriber: a Mobile Equipment with a UICC inserted and activated USIM-application.

GSM subscriber: a Mobile Equipment with a SIM inserted or a Mobile Equipment with a UICC inserted and activated SIM-application.

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI. One is still in a UMTS security context, if the keys CK/IK are converted into Kc to work with a GSM BSS.

GSM security context: a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

Quintet, UMTS authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

Triplet, GSM authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

Authentication vector: either a quintet or a triplet.

Temporary authentication data: either UMTS or GSM security context data or UMTS or GSM authentication vectors.

R98-: Refers to a network node or ME that conforms to R97 or R98 specifications.

R99+: Refers to a network node or ME that conforms to R99 or later specifications.

Rel4- ME: Refers to a ME that conforms to Rel-4 or R99 specifications.

Rel5+ ME: Refers to a ME that conforms to Rel-5 or later specifications.

ME capable of UMTS AKA: either a ~~Rel-4~~ Rel4- ME that does support USIM-ME interface or a ~~Rel-5+~~ Rel5+ ME.

ME not capable of UMTS AKA: a ~~Rel-4~~ Rel4- ME that does not support USIM-ME interface or a R98- ME.

**** NEXT CHANGE ****

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~~ Rel4- 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.

**** END OF CHANGES ****

Technical Specification Group Services and System Aspects **_TSGS#25(04)0627.b_**

Meeting #25, Palm Springs, USA

CR-Form-v7

CHANGE REQUEST

⌘	**33.102**	**CR**	**188**	⌘**rev**	**-**	⌘	Current version:	**6.1.0**	⌘

*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:	⌘	Correction to mis-implementation of CR175: Rel4- definition			
Source:	⌘	SA WG3 (MCC)			
Work item code:	⌘	SEC1	***Date:***	⌘	08/08/2004
Category:	⌘	**A**	***Release:***	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The change from **Rel-4** to **Rel4-** was missed in the implementation of CR175 and has lead to a mis-understanding in T WG3 (see LS in SP-040491)
Summary of change:	⌘	Replace **Rel-4** by **Rel4-** in section 6.8.1.4. Correct definition in section 3.1.
Consequences if not approved:	⌘	Specification will not provide intended allowance for Rel-99 ME with no UTRAN capabilities to support the USIM-ME interface.

Clauses affected:	⌘	3.1, 6.8.1.4				
		Y	**N**			
Other specs affected:	⌘		**N**	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘	This was intended to be added in 2002 by approved CR 175 but was mistakenly not implemented.				

**** FIRST CHANGE ****

3 Definitions, symbols abbreviations and conventions

3.1 Definitions

3 Definitions, symbols abbreviations and conventions

3.1 Definitions

In addition to the definitions included in TR 21.905 [3] and TS 22.101 [21], for the purposes of the present document, the following definitions apply:

NOTE: 'User' and 'Subscriber' have been defined in TR 21.905 [3]. 'User Equipment', 'USIM', 'SIM' and 'IC Card' have been defined in TS 22.201 [21].

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

UMTS Entity authentication and key agreement: Entity authentication according to this specification.

GSM Entity authentication and key agreement: The entity Authentication and Key Agreement procedure to provide authentication of a SIM to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in GSM 03.20.

User: Within the context of this specification a user is either a UMTS subscriber (Section 6.8.1) or a GSM Subscriber (Section 6.8.2) or a physical person as defined in TR 21.905[3] (Section 5.3 and 5.5).

UMTS subscriber: a Mobile Equipment with a UICC inserted and activated USIM-application.

GSM subscriber: a Mobile Equipment with a SIM inserted or a Mobile Equipment with a UICC inserted and activated SIM-application.

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI. One is still in a UMTS security context, if the keys CK/IK are converted into Kc to work with a GSM BSS.

GSM security context: a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

Quintet, UMTS authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

Triplet, GSM authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

Authentication vector: either a quintet or a triplet.

Temporary authentication data: either UMTS or GSM security context data or UMTS or GSM authentication vectors.

R98-: Refers to a network node or ME that conforms to R97 or R98 specifications.

R99+: Refers to a network node or ME that conforms to R99 or later specifications.

Rel4- ME: Refers to a ME that conforms to Rel-4 or R99 specifications.

Rel5+ ME: Refers to a ME that conforms to Rel-5 or later specifications.

ME capable of UMTS AKA: either a ~~Rel-4 –~~Rel4- ME that does support USIM-ME interface or a ~~Rel-5+~~ Rel5+ ME.

ME not capable of UMTS AKA: a ~~Rel-4 –~~Rel4- ME that does not support USIM-ME interface or a R98- ME.

**** NEXT CHANGE ****

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~~ Rel4- 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.

**** END OF CHANGES ****

3GPP TSG SA WG3 Security ó S3#26 S3-020591

19 - 22 November 2002, Oxford, UK

CR-Form-v7

CHANGE REQUEST

⌘	**TS 33.102**	**CR**	**175**	⌘ **rev**	**-** ⌘	Current version: **5.0.0** ⌘

*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:	⌘	USIM support in GERAN only terminals		
Source:	⌘	SA WG3		
Work item code:	⌘	SEC1	***Date:*** ⌘	6/11/2002
Category:	⌘	**F**	***Release:*** ⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	To bring TS 33.102 in line with TS 22.101 V5.7.0 on the support of USIM in GERAN only terminals for Rel-5 or later. SP-020051 is the approved CR for TS 22.101 Rel-5 : It says that GERAN only terminals shall support the USIM. This is a change with respect to Rel-4 requirements where GERAN only terminals may support the USIM. The interworking clause of TS 33.102 did not yet reflect the Rel-5 requirements.
Summary of change:	⌘	TS 33.102 is updated to remove ambiguity in interpretation in interworking scenarios and to adapt conflicting requirements.
Consequences if not approved:	⌘	TS 33.102 will be inconsistent with specification TS 22.101.

Clauses affected:	⌘	3.1; 6.8.1; 6.8.4; 6.8.5; 6.8.7			
		Y	**N**		
Other specs affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

******* first change *******

3.1 Definitions

In addition to the definitions included in TR 21.905 [3] and TS 22.101 [21], for the purposes of the present document, the following definitions apply:

NOTE: 'User' and 'Subscriber' have been defined in TR 21.905 [3]. 'User Equipment', 'USIM', 'SIM' and 'IC Card' have been defined in TS 22.201 [21].

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

UMTS Entity authentication and key agreement: Entity authentication according to this specification.

GSM Entity authentication and key agreement: The entity Authentication and Key Agreement procedure to provide authentication of a SIM to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in GSM 03.20.

User: Within the context of this specification a user is either a UMTS subscriber (Section 6.8.1) or a GSM Subscriber (Section 6.8.2) or a physical person as defined in TR 21.905[3] (Section 5.3 and 5.5).

UMTS subscriber: a Mobile Equipment with a UICC inserted and activated USIM-application.

GSM subscriber: a Mobile Equipment with a SIM inserted or a Mobile Equipment with a UICC inserted and activated SIM-application.

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI. One is still in a UMTS security context, if the keys CK/IK are converted into Kc to work with a GSM BSS.

GSM security context: a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

Quintet, UMTS authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

Triplet, GSM authentication vector: temporary authentication and key agreement data that enables an VLR/SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

Authentication vector: either a quintet or a triplet.

Temporary authentication data: either UMTS or GSM security context data or UMTS or GSM authentication vectors.

R98-: Refers to a network node or ME that conforms to R97 or R98 specifications.

R99+: Refers to a network node or ME that conforms to R99 or later specifications.

Rel4- ME: Refers to a ME that conforms to Rel4 or R99 specifications.

Rel5+ ME: Refers to a ME that conforms to Rel5 or later specifications.

~~R99+~~ **ME capable of UMTS AKA**: ~~either a R99+ UMTS only ME, a R99+ GSM/UMTS ME, or a R99+ GSM only~~Either a Rel4- ME that does support USIM-ME interface or a Rel5+ ME.

~~R99+~~ **ME not capable of UMTS AKA**: ~~a R99+ GSM only~~ A Rel4- ME that does not support USIM-ME interface or a R98- ME.

********* next change ******

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:

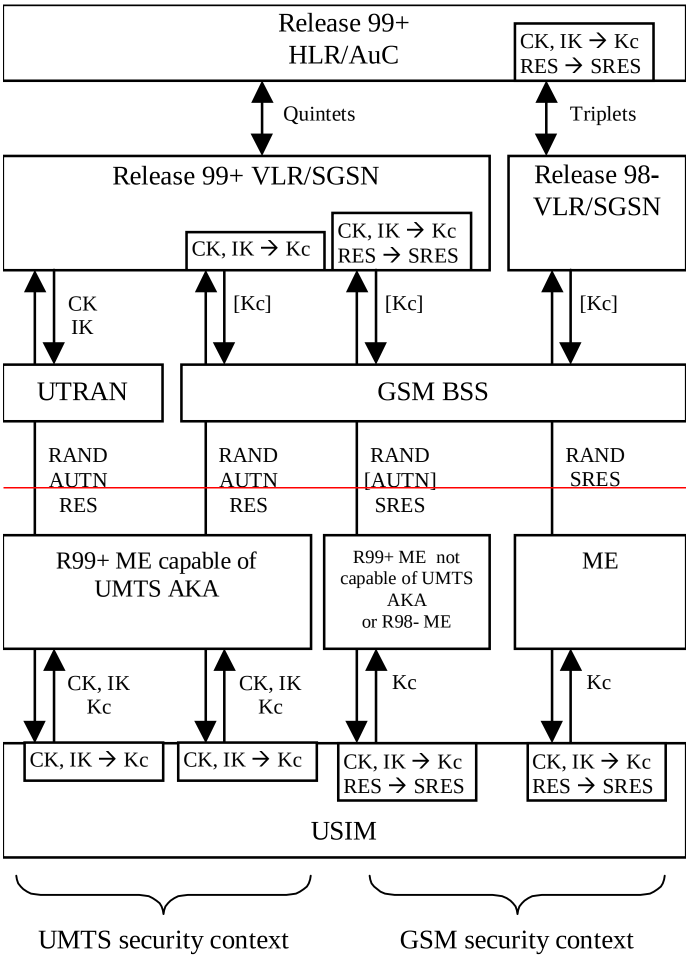
- UMTS AKA shall be applied when the user is attached to a UTRAN.
- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has a ~~R99+~~ ME capable of UMTS AKA and also the VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys 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~~R99+~~ ME not capable of UMTS AKA~~ or R98- ME or R98- ME~~. 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 ~~R99+~~ ME not capable of UMTS AKA~~ or R98- ME~~, 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.


Release 99+
HLR/AuC
CK, IK → Kc
RES → SRES
Quintets
Triplets
Release 99+ VLR/SGSN
CK, IK → Kc
CK, IK → Kc
RES → SRES
Release 98-
VLR/SGSN
CK
IK
[Kc]
[Kc]
[Kc]
UTRAN
GSM BSS
RAND
AUTN
RES
RAND
AUTN
RES
RAND
[AUTN]
SRES
RAND
SRES
R99+ ME capable of
UMTS AKA
R99+ ME not capable of UMTS AKA or R98- ME
ME
CK, IK
Kc
CK, IK
Kc
Kc
Kc
CK, IK → Kc
CK, IK → Kc
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
USIM
UMTS security context
GSM security context

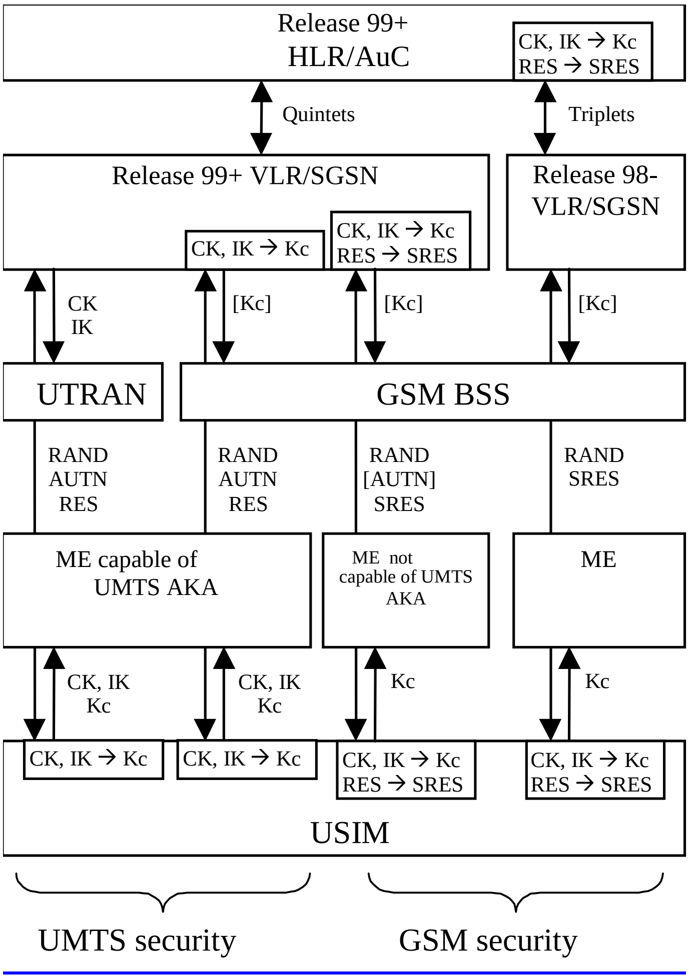


Figure 18: Authentication and key agreement of UMTS subscribers

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 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+ 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:

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

b) c2: $SRES_{[GSM]} = XRES*_1 \text{ xor } XRES*_2 \text{ xor } XRES*_3 \text{ xor } XRES*_4$

c) 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 || 0...0 if XRES is shorter than 16 octets, $XRES*_i$ are all 4 octets long and $XRES* = XRES*_1 \| XRES*_2 \| XRES*_3 \| XRES*_4$, 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+ 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 ~~R99+~~ 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 theVLR/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 ~~R99+~~ 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 ~~R99+~~ 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].

Rel4-~~ease 99+~~ 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 ~~R99+~~ ME capable of UMTS AKA with a USIM active~~inserted~~ and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA.

A ~~R99+~~ ME capable of UMTS AKA with a USIM active~~inserted~~ 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 ~~A R99+~~ ME that ~~does not support the USIM-ME interface (~~not capable of UMTS AKA~~)~~ with a USIM active~~inserted~~ 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.

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 ~~R99+~~ ME not capable of UMTS AKA~~ or R98- ME~~;

Feature 3: SIM-ME interface (GSM 11.11) to operate within~~ R98- ME or R99+~~ 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~~ R99+~~ ME. In case the verification of AUTN is not successful, the USIM shall respond with an appropriate error indication to the~~ R99+~~ 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~~ R99+~~ ME shall be informed. A USIM that does not support GSM cipher key derivation (Feature 1) cannot operate in any GSM

BSS. A USIM that does not support GSM AKA (Feature 2) cannot operate under a R98- VLR/SGSN or in a both ~~R99+~~ ME that is not capable of UMTS AKA.~~and in R98- ME.~~

********* next change ******

6.8.4 Intersystem handover for CS Services ñ 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 ~~R99+~~ 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 during the last UMTS AKA procedure.

6.8.4.2 GSM security context

A GSM security context in UTRAN is only established for 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.

********* next change ******

6.8.5 Intersystem handover for CS Services ñ 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 ~~R99+~~ 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.

********* next change ******

6.8.7 Intersystem change for PS services ñ 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 ~~R99+~~ 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 ~~R98- ME or R99+~~ 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 over-written with a new CK, IK pair due to the new AKA.