Technical Specification Group Services and System Aspects **TSGS#7(00)0077**

Meeting #7, Madrid, Spain, 15-17 March 2000

Source: **SA WG3**

Title: **CRs to 33.102**

Document for: **Approval**

Agenda Item: **5.3.3**

CRs to 33.102

Introduction:

This document contains 4 CRs to **33.102** for Release 1999 which are submitted to SA#7 for approval.

SA WG3 TD	Spec	CR	Rev	Phase	Subject	Cat	Current Version	Comments
S3-000208	33.102	047	2	R99	Interoperation and intersystem handover/change between UTRAN and GSM BSS	C	3.3.1	Agreed by e-mail 10/03/00
S3-000212	33.102	064	2	R99	Distribution and Use of Authentication Data between VLRs/SGSNs	F	3.3.1	Agreed by e-mail 10/03/00
S3-000220	33.102	066	1	R99	Ciphering	C	3.3.1	Agreed by e-mail 10/03/00
S3-000221	33.102	067	1	R99	Data integrity	C	3.3.1	Agreed by e-mail 10/03/00

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**	**047r2**	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: *(at least one should be marked with an X)* (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [X]

Source: SA WG3 **Date:** 2000-03-10

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:

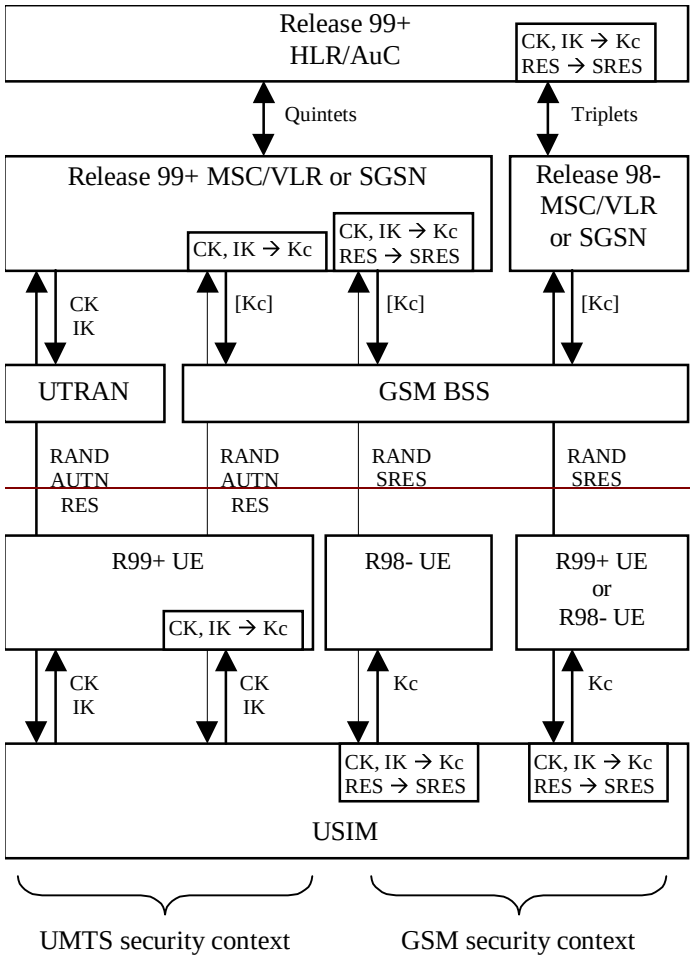
- UMTS AKA shall be applied when the user is attached to a UTRAN.
- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has R99+ UE and also the ~~MSC/VLR or SGSN~~VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and 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
Release 98-
MSC/VLR
or SGSN
CK, IK → Kc
CK, IK → Kc
RES → SRES
CK
IK
[Kc]
[Kc]
[Kc]
UTRAN
GSM BSS
RAND
AUTN
RES
RAND
AUTN
RES
RAND
SRES
RAND
SRES
R99+ UE
R98- UE
R99+ UE
or
R98- UE
CK, IK → Kc
CK
IK
CK
IK
Kc
Kc
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
USIM
UMTS security context
GSM security context

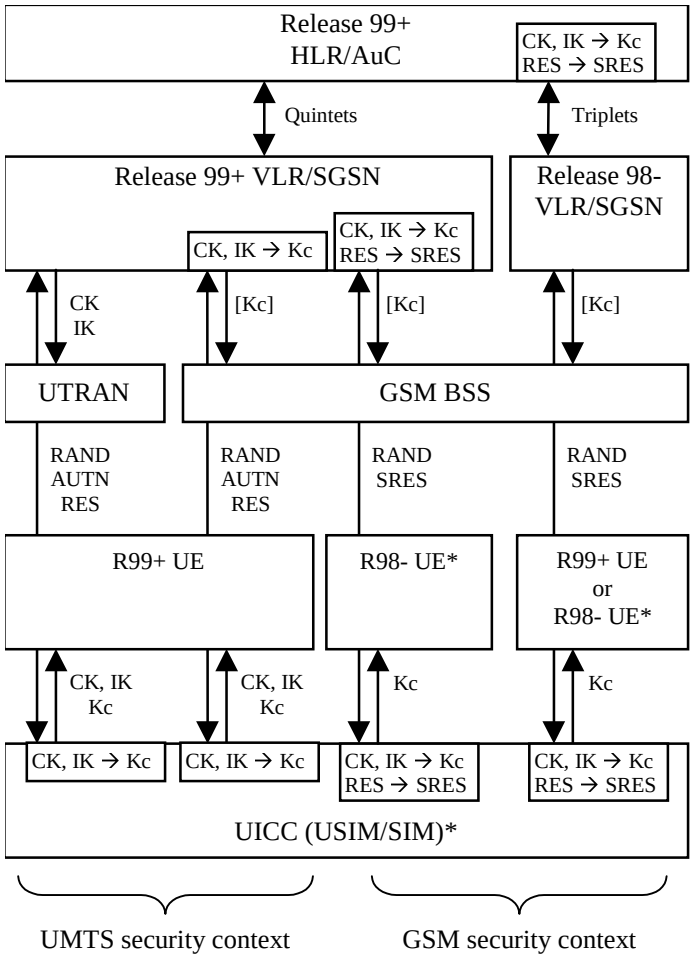


Figure 18: Authentication and key agreement of UMTS subscribers

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

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

6.8.1.3 R99+ ~~MSC/VLR or SGSN~~VLR/SGSN

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 in~~passed 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

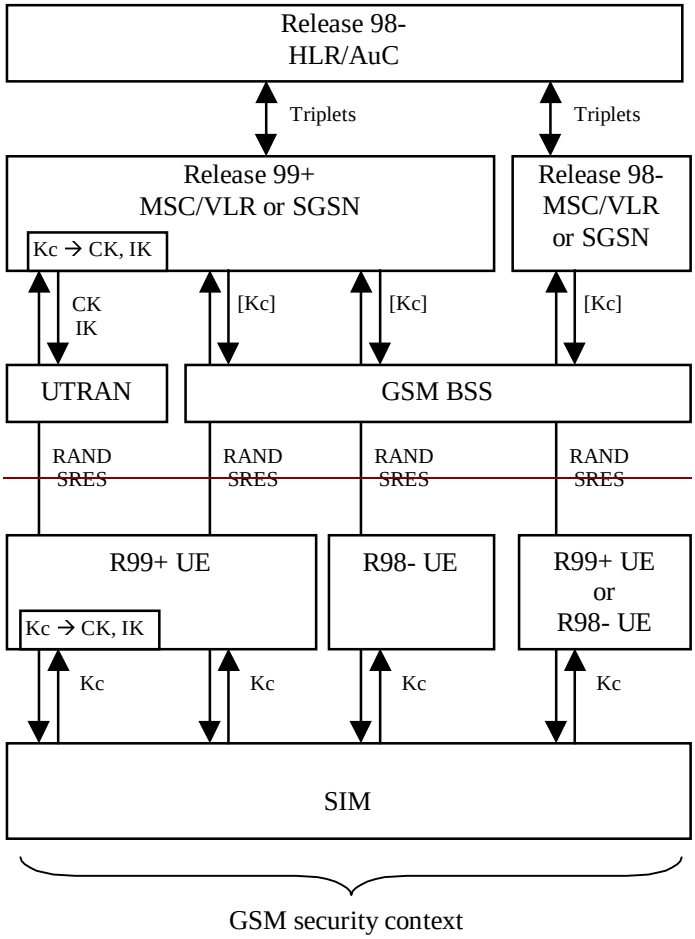
6.8.2.1 General

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 SGSN~~VLR/SGSN belongs. The user needs to separately establish a security context with each serving network domain.

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

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


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

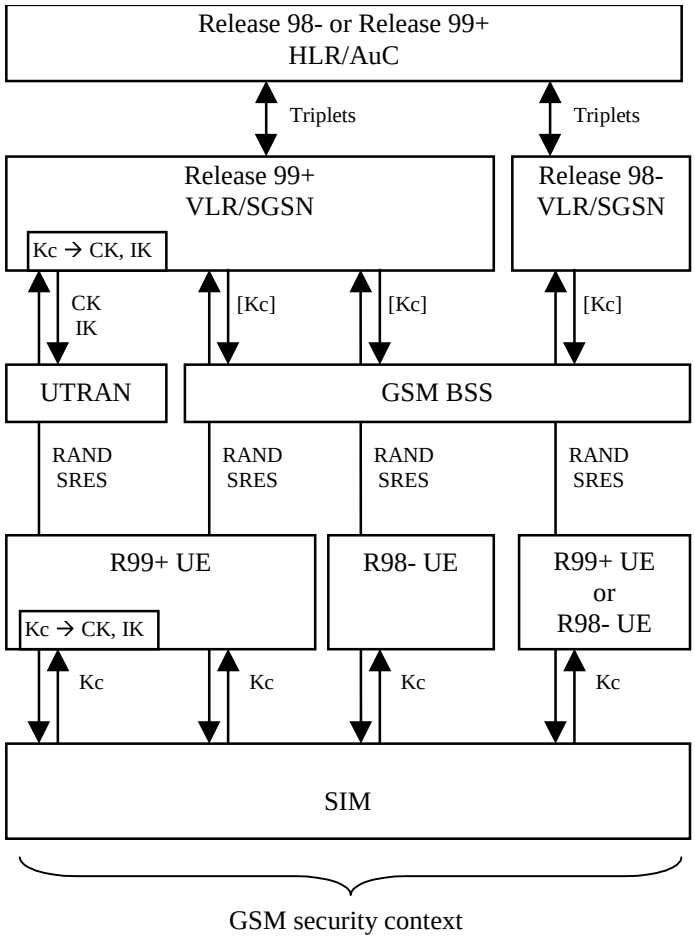


Figure 19: Authentication and key agreement for GSM subscribers

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: $CK_{[UMTS]} = 0\ldots0 \parallel Kc$;

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

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

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

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

6.8.2.~~43~~ R99+ UE

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

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

When the user is attached to a UTRAN, R99+ UE shall derive the UMTS cipher/integrity keys CK~~k~~ 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, three~~two~~ 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 ~~an~~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 ~~(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 derive~~d~~s ~~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.

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

S3-000212
Document **(Rev. of S3-000209)**
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**	**064r2**	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 *list expected approval meeting # here ↑*

for approval [X]
for information [ ]

strategic [ ]
non-strategic [ ]
(for SMG use only)

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

Source: SA WG3 **Date:** 2000-03-10

Subject: Distribution and Use of Authentication Data between VLRs/SGSNs

Work item: Security

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

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

Release:

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

Reason for change:

This CR specifies the conditions for the distribution of authentication data (unused AVs and/or current security context data) between VLRs/SGSNs (of the same or different releases) and use of such information at VLRn/SGSNn.

A new chapter under section 6.8 ('Interoperation and handover between UMTS and GSM') is inserted: Chapter 6.8.3 'Distribution of Authentication Data between VLRs/SGSNs'.

Clauses affected: 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:

Mind that this new chapter does not intend to subsitute current chapter 6.8.3. in 33.102 3.3.1. ("Intersystem HO for CS services – from UTRAN to GSM BSS"), it shall be inserted before it instead.


help.doc

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

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 (quintuplets 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 UE release (R'99 UE ←→ R'98 UE) 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 UE (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 quintuplets 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- UE.

In all other cases, R99+ VLR/SGSN shall request fresh AVs (either triplets or quintuplets) to HE. In the event, the R99+ VLR/SGSN receives quintuplets, 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).

3GPP TSG SA 3 meeting #12
Stockholm, Sweden, 11-14 April 2000

***Document* S3-000220**
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	66r1	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 #8	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: *(at least one should be marked with an X)*	(U)SIM	X	ME	X	UTRAN / Radio	X	Core Network	

Source: SA WG3 **Date:** 24-03-10

Subject: Ciphering

Work item: Security

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

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Clause 6.6 on ciphering is updated with the description that was in TS 33.105 and in TS 25.301. The description in 6.3.3.1 on the selection of a cipher key for user data and signalling data is moved to 6.6.5. In 6.6.4 more detail is added on how the HFN is initialised by means of the parameter START and synchronisation is maintained throughout the connection.

Clauses affected: 6.3.3.1, 6.6

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.

6.3.3.1 Cipher key selection

Because of the separate mobility management for CS and PS services, the USIM establishes cipher keys with both the CS and the PS core network service domains. The conditions on the use of these cipher keys in the user and control planes are given below.

6.3.3.1.1 User plane

The CS user data connections are ciphered with the cipher key CK_{CS} established between the user and the 3G CS core network service domain and identified in the security mode setting procedure. The PS user data connections are ciphered with the cipher key CK_{PS} established between the user and the 3G PS core network service domain and identified in the security mode setting procedure.

6.3.3.1.2 Control plane

When a security mode setting procedure is performed, the cipher/integrity key set by this procedure is applied to the signalling plane, what ever core network service domain is specified in the procedure. This may require that the cipher/integrity key of an (already ciphered/integrity protected) ongoing signalling connection is changed. This change should be completed within five seconds.

6.6 Access link data confidentiality

6.6.1 General

User data and some signalling information elements are considered sensitive and must be confidentiality protected. To ensure identity confidentiality (see ~~clause~~ 6.1), the ~~Temporary~~ temporary ~~Mobile User~~ user ~~Identity~~ identity (P-)TMSI must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it. ~~The confidentiality of user traffic concerns the information transmitted on traffic channels.~~

These needs for a protected mode of transmission are fulfilled by a confidentiality function which is applied on dedicated channels between the ~~MS~~ UE and the RNC.

6.6.2 Layer of ciphering

The ciphering function is performed either in the RLC sub-layer or in the MAC sub-layer, according to the following rules:

- If a logical channel is expected to be supported on a common transport channel and has to be ciphered, it shall use UM RLC mode and ciphering is performed at the RLC sub-layer.
- If a logical channel is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-layer.
- If a logical channel is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).

Ciphering when applied is performed in the S-RNC and the UE and the context needed for ciphering (CK, HFN, etc.) is only known in S-RNC and the UE.

~~6.6.2 Ciphering algorithm~~

6.6.3 Ciphering method

~~Algorithm UEA is implemented in both the MS and the RNC.~~ Figure 6.6.1 illustrates the use of the ciphering algorithm f8 to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the ciphertext. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the ciphertext.

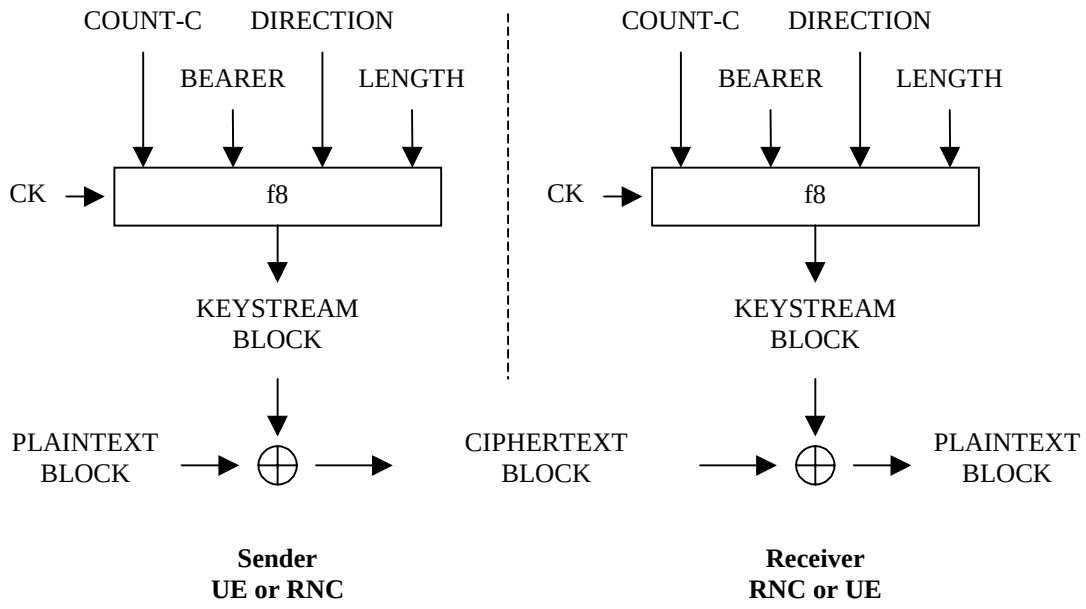


Figure 6.6.1: Ciphering of user and signalling data transmitted over the radio access link

The input parameters to the algorithm are the cipher key CK, a time dependent input COUNT-C, the bearer identity BEARER, the direction of transmission DIRECTION and the length of the keystream required LENGTH. Based on these input parameters the algorithm generates the output keystream block KEYSTREAM which is used to encrypt the input plaintext block PLAINTEXT to produce the output ciphertext block CIPHERTEXT.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

~~On the RNC side the description below assumes that one algorithm UEA is implemented for each dedicated physical channel [not yet decided]. The data flow on dedicated channels is ciphered by a bit per bit or stream cipher generated by an algorithm UEA.~~

6.6.4 Input parameters to the cipher algorithm

6.6.4.1 COUNT-C

The ciphering sequence number COUNT-C is 32 bits long.

There is one COUNT-C value per logical RLC AM channel, one per logical RLC UM channel and one for all logical channels using the transparent RLC mode (and mapped onto DCH).

COUNT-C is composed of two parts: a "short" sequence number and a "long" sequence number. The update of COUNT-C depends on the transmission mode as described below (see Figure 6.6.2):

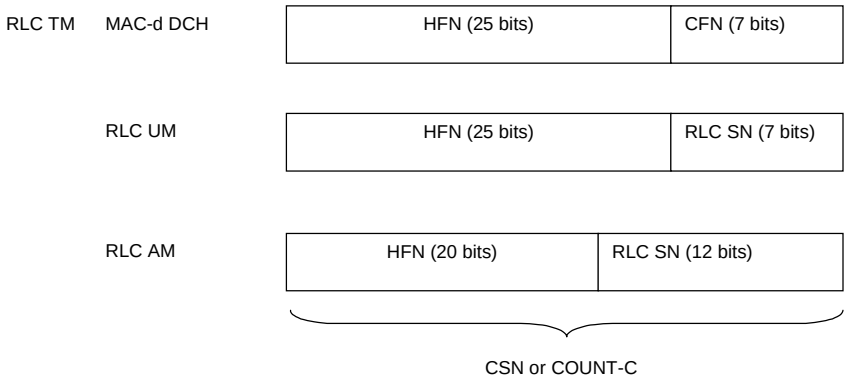


Figure 6.6.2: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 7-bit ciphering frame number CFN of the UEFN. It is independently maintained in the UE MAC entity and the SRNC MAC-d entity. The "long" sequence number is the 25-bit MAC HFN which is incremented at each CFN cycle. The ciphering sequence number CSN or COUNT-C is identical to the UEFN.

- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 25-bit RLC HFN which is incremented at each RLC SN cycle.

- For RLC AM mode, the "short" sequence number is the 12-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 20-bit RLC HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is transmitted from UE to RNC in *RRC connection establishment*. The UE and the RNC then initialise the X most significant bits of the RLC HFN and MAC HFN to START; the remaining LSB of the RLC HFN and MAC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel.

Editor's note: The value of X still needs to be decided.

Editor's note: The description of how START is managed in the UE needs to be added.

6.6.4.2 CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. Which cipher key to use for a particular logical channel is described in 6.6.6.

For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the UE. CK is sent from the USIM to the UE upon request of the UE. The USIM shall send CK under the condition that 1) a valid CK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The UE shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of the quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) security mode command. The VLR or SGSN shall assure that CK is updated at least once every 24 hours.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.

6.6.4.3 BEARER

The logical channel identifier BEARER is 4 bits long.

There is one BEARER parameter per logical channel associated with the same user and multiplexed on a single 10ms physical layer frame. The logical channel identifier is input to avoid that for different keystream an identical set of input parameter values is used.

6.6.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the an identical set of input parameter values.

6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

The length indicator determines the length of the required keystream block. LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it. ~~The UEA shall produce one output as a sequence of keystream bits referred to as a Key Stream Segment (KSS). A KSS of length n shall be produced to encrypt a given segment of plaintext of length n. The bits of KSS are labelled KSS(0), …KSS(n-1), where KSS(0) is the first bit output from the generator. The bits in the KSS shall be used to encrypt or decrypt the data.~~

6.6.5 Cipher key selection

There is one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user.

The logical channels for CS user data are ciphered with CK_{CS}.

The logical channels for PS user data are ciphered with CK_{PS}.

Signalling data (for both CS an PS services) is sent over common logical channels. These logical channels are ciphered by the CK of the service domain for which the most recent security mode negotiation took place. This may require that the cipher key of an (already ciphered) ongoing signalling connection is changed, when a new RRC connection establishment occurs, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.

6.6.~~3~~6 UEA identification

Each UEA will be assigned a 4-bit identifier. Currently the following values have been defined:

"0000_2" : UEA0, no encryption.

"0001_2" : UEA1, Kasumi.

The remaining values are not defined.

~~Table 2 – UEA identification~~

~~Information Element~~	~~Length~~	~~Value~~	~~Remark~~
~~UEA Number~~	~~4~~	~~0000_2~~	~~Standard UMTS Encryption Algorithm, UEA1~~
		~~0001_2~~	~~Standard UMTS Encryption Algorithm, UEA2~~
		~~0010_2~~	~~Standard UMTS Encryption Algorithm, UEA3~~
		~~0011_2 to 0111_2~~	~~Reserved for future expansion~~
		~~$1xxx_2$~~	~~Proprietary UMTS Algorithms~~

~~6.6.4 Synchronisation of ciphering~~

~~The enciphering stream at one end and the deciphering stream at the other end must be synchronised, for the enciphering bit stream and the deciphering bit streams to coincide.~~

~~Synchronisation is guarantied by driving UEA by an explicit time variable, COUNT, derived from an appropriate frame number available at the MS and at the RNC.~~

~~The diagram below summarises the implementation indications listed above, with only one enciphering/deciphering procedure represented (the second one for deciphering/enciphering is symmetrical).~~

~~6.6.4.1 Layer for ciphering~~

~~The layer on which ciphering takes place depends on the Layer 2 mode of the data. Data transmitted on logical channels using a non-transparent RLC mode (either Acknowledged Mode or Unacknowledged Mode) is ciphered in the RLC sub-~~

~~layer of Layer 2. Data transmitted on a logical channel using the transparent RLC mode is ciphered at the MAC sub-layer of Layer 2.~~

~~6.6.4.2 Intra-system handover~~

~~When a handover occurs, the CK and IK are transmitted within the system infrastructure from the old RNC to the new one to enable the communication to proceed, and the synchronisation procedure is resumed. The keys CK and IK remain unchanged at handover.~~

3GPP TSG SA 3 meeting #12
Stockholm, Sweden, 11-14 April 2000

***Document* S3-000221**
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**	**067r1**	Current Version:	3.2.0

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

For submission to: SA #8 *list expected approval meeting # here ↑*	for approval	X	strategic		*(for SMG use only)*
	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: *(at least one should be marked with an X)*	(U)SIM	X	ME	X	UTRAN / Radio	X	Core Network	

Source: SA WG3 **Date:** 10/03/00

Subject: Data integrity

Work item: Security

Category: *(only one category shall be marked with an X)*			**Release:**	
F	Correction		Phase 2	
A	Corresponds to a correction in an earlier release		Release 96	
B	Addition of feature		Release 97	
C	Functional modification of feature	X	Release 98	
D	Editorial modification		Release 99	X
			Release 00	

Reason for change: Detail is added to the description of the integrity protection mechanism: the layer of integrity protection is identified and the input values are discussed.

Clauses affected: 6.5

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.

6.5 Access link data integrity

6.5.1 General

Most RRC, MM and CC signalling information elements are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the ~~MS~~ UE and the ~~SN~~RNC.

~~The UMTS Integrity Algorithm (UIA) shall be used with an Integrity Key (IK) to compute a message authentication code for a given message.~~

All signalling messages except the following ones shall be integrity protected:

- Notification
- Paging Type 1
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete
- RRC Connection Reject
- All System Information messages.

6.5.2 Layer of integrity protection

The UIA shall be implemented in the UE and in the RNC.

Integrity protection shall be apply at the RRC layer.

~~6.5.2~~6.5.3 ~~Integrity algorithm~~Data integrity protection method

~~The UIA shall be implemented in the UE and in the RNC.~~

Figure 6.5.1 illustrates the use of the ~~UIA~~ integrity algorithm f9 to authenticate the data integrity of a signalling message.

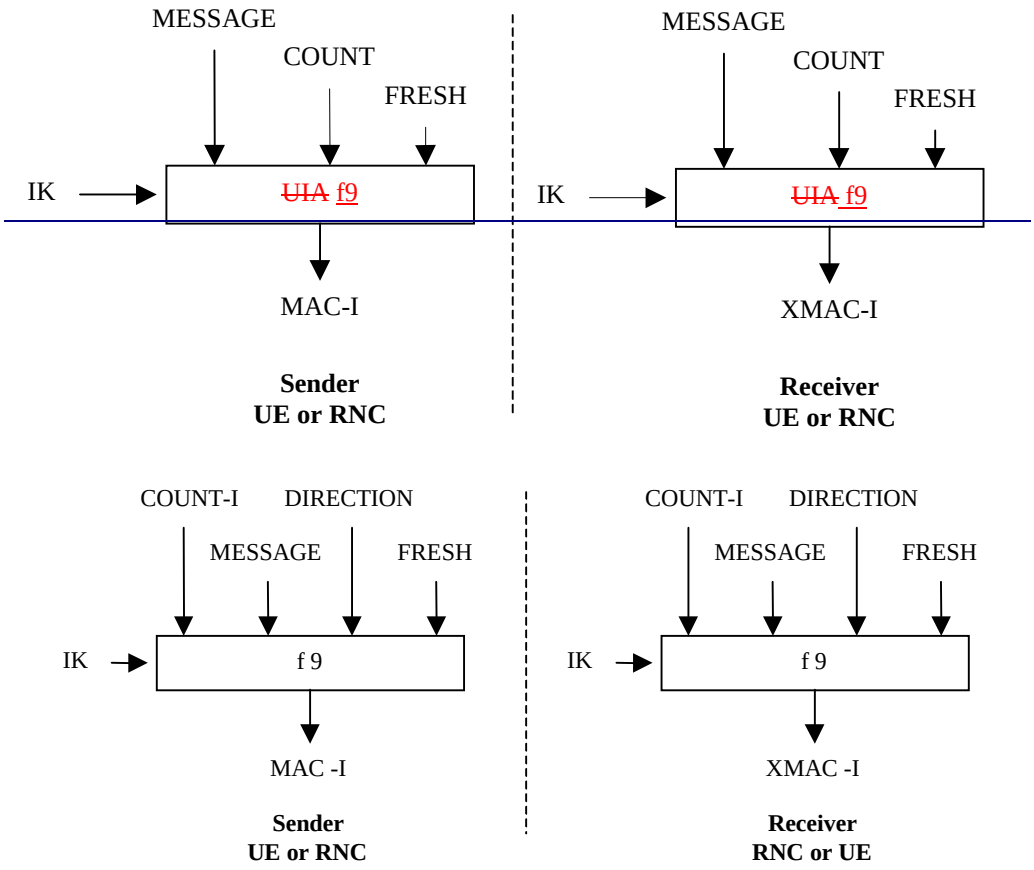


Figure 6.5.1: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the ~~Integrity Key~~ integrity key ~~(~~IK~~)~~, ~~a time dependent input~~the integrity sequence number ~~(~~COUNT-I~~)~~, a random value generated by the network side ~~(~~FRESH~~)~~, the direction bit ~~(~~DIRECTION~~)~~ and the signalling data ~~(~~MESSAGE~~)~~. Based on these input parameters the user computes message authentication code for data integrity ~~(~~MAC-I~~)~~ using the ~~UMTS Integrity Algorithm (UIA)~~integrity algorithm f9. The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I.

6.5.4 Input parameters to the integrity algorithm

6.5.4.1 COUNT-I

The integrity sequence number COUNT-I is 32 bits long.

There is one COUNT-I value per logical signalling channel.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number is the 4-bit RRC sequence number RRC SN that is available in each RRC PDU. The "long" sequence number is the 28-bit RRC hyperframe number RRC HFN which is incremented at each RRC SN cycle.

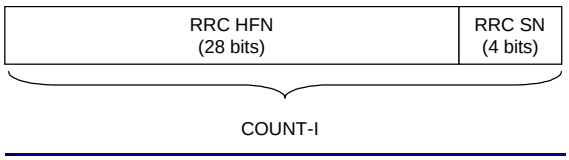


Figure 6.5.2: The structure of COUNT-I

The hyperframe number RRC HFN is initialised by means of the parameter START, which is transmitted from UE to RNC during *RRC connection establishment*. The UE and the RNC then initialise the X most significant bits of the RRC

HFN to START; the remaining (28-X) LSB of the RRC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel used for signalling.

Editor's note: The value of X still needs to be added.

Editor's note: The description of how START is managed in the UE needs to be added.

6.5.4.2 IK

The integrity key IK is 128 bits long.

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user. Which integrity key to use for a particular connection is described in 6.5.6.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the UE. IK is sent from the USIM to the UE upon request of the UE. The USIM shall send IK under the condition that 1) a valid IK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The UE shall delete IK from memory after power-off as well as after removal of the USIM.

IK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of a quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) *security mode command*. The MSC/VLR or SGSN shall assure that the IK is updated at least once every 24 hours.

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

~~The input parameter COUNT-I protects against replay during a connection. It is a value incremented by one for each integrity protected message. COUNT-I consists of two parts: the Hyperframe Number (HFN) as the most significant part, and an RRC Sequence Number as the least significant part. The initial value of the hyperframe number is sent by the user to the network at connection set-up. The user stores the greatest used hyperframe number from the previous connection and increments it by one (see 6.4.5xxx). In this way the user is assured that no COUNT-I value is re-used (by the network) with the same integrity key.~~

6.5.4.3 FRESH

The network-side nonce FRESH is 32 bits long.

There is one FRESH parameter value per user. The input parameter FRESH protects the network against replay of signalling messages by the user. At connection set-up the ~~network~~ RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is.

At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it in a new *security mode command* to the user.

6.5.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the integrity algorithm used to compute the message authentication codes would use an identical set of input parameter values for the up-link and for the down-link messages.

6.5.4.5 MESSAGE

The signalling message itself.

6.5.5 Integrity key selection

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user.

The data integrity of logical channels for user data is not protected.

Signalling data for services delivered by either of both service domains is sent over common logical (signalling) channels. These logical channels are data integrity protected by the IK of the service domain for which the most recent security mode negotiation took place. This may require that the integrity key of an (already integrity protected) ongoing signalling connection has to be changed, when a new RRC connection is established (with another service domain), or when a security mode negotiation follow a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.

6.5.~~3~~6 UIA identification

Each UMTS Integrity Algorithm (UIA) will be assigned a 4-bit identifier. Currently the following values have been defined:

"0001_2" : UIA1, Kasumi.

The remaining values are not defined.

~~Table1 - UIA identifiation~~

~~Information Element~~	~~Length~~	~~Value~~	~~Remark~~
~~UIA Number~~	~~4~~	~~0000_2~~	~~Standard UMTS Integrity Algorithm, UIA1~~
		~~0001_2~~	~~Standard UMTS Integrity Algorithm, UIA2~~
		~~0010_2~~	~~Standard UMTS Integrity Algorithm, UIA3~~
		~~0011_2 to 0111_2~~	~~Reserved for future expansion~~
		~~$1xxx_2$~~	~~Proprietary UMTS Algorithms~~