Technical Specification Group Services and System Aspects **TSGS#7(00)0112**

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

Source: **SA WG3**

Title: **Miscellaneous CRs to 33.102**

Document for: **Approval**

Agenda Item: **5.3.3**

CRs to 33.102

Introduction:

This document contains 23 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
S3-000043	33.102	043		R99	Clarification on cipher key and integrity key lifetime lifetime	C	3.3.1	
S3-000044	33.102	044		R99	local Authenication and connection establishment	D	3.3.1	
S3-000051	33.102	048		R99	Clarification on the reuse of Avs	C	3.3.1	
S3-000076	33.102	049		R99	Authentication failure reporting	F	3.3.1	
S3-000101	33.102	050		R99	Refinement of Cipher key and integrity key lifetime	F	3.3.1	agreed by e-mail
S3-000159	33.102	051	1	R99	Conversion function c3 at USIM	F	3.3.1	
S3-000160	33.102	052	1	R99	Trigger points of AFR during AKA	F	3.3.1	
S3-000163	33.102	053	1	R99	Removal of EUIC from 'Authentication Data Request' procedure	F	3.3.1	
S3-000161	33.102	054	1	R99	Clarification of the scope	F	3.3.1	
S3-000115	33.102	055		R99	SQN Generation Requirements	F	3.3.1	
S3-000162	33.102	056	1	R99	Identification of temporary identities	F	3.3.1	
S3-000117	33.102	057		R99	Cipher key and integrity key selection	F	3.3.1	
S3-000167	33.102	058	1	R99	Clarification on ciphering and integrity mode setting	F	3.3.1	
S3-000119	33.102	059		R99	Clarification on when integrity protection is started	F	3.3.1	
S3-000168	33.102	061	1	R99	Unsuccessful integrity check	F	3.3.1	
S3-000176	33.102	062	1	R99	Clarification on signalling messages to be integrity protected	F	3.3.1	
S3-000177	33.102	063	1	R99	Clarification of the HFN handling	F	3.3.1	
S3-000178	33.102	071	1	R99	Use of default IK at emergency call with no (U)SIM or when authentication has failed	F	3.3.1	Agreed by e-mail
S3-000148	33.102	072		R99	Clarification on ciphering and integrity protection at intersystem handover	F	3.3.1	
S3-000108	33.102	074		R99	Clarification about CK and IK which are transmitted in clear over the Iu-interface	B	3.3.1	Agreed by e-mail
S3-000193	33.102	076		R99	Cipher key and integrity key lifetime	F	3.3.1	Agreed by e-mail
S3-000194	33.102	077		R99	Cipher key and integrity key setting	F	3.3.1	Agreed by e-mail
S3-000214	33.102	079	1	R99	Local Authenication and connection establishment	C	3.3.1	Agreed by e-mail

3GPP TSG SA WG3 (Security) meeting #10
Antwerpen, 19-21 January, 2000

***Document* S3-000043**
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	043	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		ME	X	UTRAN / Radio	X	Core Network	X

Source: SA WG3 **Date:** 2000-01-17

Subject: Clarification on cipher key and integrity key lifetime

Work item: Release 99

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: Clarification needed on how the USIM shall trigger the generation of new security keys.

Clauses affected: 6.4.3, 6.4.4

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.

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the highest value of the hyperframe number (the current value of COUNT) of the bearers that were protected in that RRC connection is stored in the USIM. When the next RRC connection is established that value is read from the USIM and incremented by one.

The USIM shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out. When this maximum value is reached the cipher key and integrity key stored on USIM shall be deleted.

This mechanism will ensure that a cipher/integrity key set cannot be reused more times than the limit set by the operator.

6.4.4 Cipher key and integrity key identification

The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. The key set identifier is allocated by the network and sent with the authentication request message to the mobile station where it is stored together with the calculated cipher key CK and integrity key IK.

The purpose of the key set identifier is to make it possible for the network to identify the cipher key CK and integrity key IK which is stored in the mobile station without invoking the authentication procedure. This is used to allow re-use of the cipher key CK and integrity key IK during subsequent connection set-ups.

The key set identifier is three bits. Seven values are used to identify the key set. A value of "111" is used by the mobile station to indicate that a valid key is not available for use. At deletion of the cipher key and integrity key, the KSI is set to “111”. The value '111' in the other direction from network to mobile station is reserved.

3GPP TSG SA WG 3 (Security) meeting #10 **S3-000044**
Antwerpen, 19—21 January, 2000.

3G 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 044 Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG SA #7 for approval **X** *(only one box should*
list TSG meeting no. here ↑ for information *be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: USIM **X** ME UTRAN Core Network
(at least one should be marked with an X)

Source: SA WG3 **Date:** 2000-Jan-17

Subject: Local Authenication and connection establishment

3G Work item: Security

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

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	X

Reason for change: Clarification needed on :
Local Authentication, Cipher and integrity key setting and
Cipher and integrity key identification

Clauses affected: 6.4, 6.4.1 and 6.4.4

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other 2G 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.

6.4 Local authentication and connection establishment

Local authentication is obtained by integrity protection functionality.

6.4.1 Cipher key and integrity key setting

~~Mutual key setting is the procedure that allows the MS and the RNC to agree on the key IK used to compute message authentication codes using algorithm UIA.~~ Authentication and key setting ~~is~~ are triggered by the authentication procedure and described in 6.3. Authentication and key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. P-TMSI, TM~~U~~SI or IM~~U~~SI) is known by the ~~SN/~~VLR/SGSN. The CK and~~key~~ IK ~~is~~are stored in the ~~SN/~~VLR/SGSN and transferred to the RNC when ~~it is~~ needed. The CK and ~~key~~ IK for the CS domain are ~~is~~ stored ~~i~~on the USIM ~~until it is~~ and updated at the next authentication from this domain. The CK and IK for the PS domain are stored on the USIM and updated at the next authentication from this domain.

If an authentication procedure is performed during a data transfer in the PS mode, the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the UE as part of the security mode negotiation (see 6.4.5) that follows the authentication procedure.

6.4.4 Cipher key and integrity key identification

The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. The key set identifier is allocated by the network and sent with the authentication request message to the mobile station where it is stored together with the calculated cipher key CK and integrity key IK. KSI in UMTS corresponds to CKSN in GSM. The USIM stores one KSI/CKSN for the PS domain key set and one KSI/CKSN for the CS domain key set.

The purpose of the key set identifier is to make it possible for the network to identify the cipher key CK and integrity key IK which ~~is~~are stored in the mobile station without invoking the authentication procedure. This is used to allow re-use of the cipher key CK and integrity key IK during subsequent connection set-ups.

KSI and CKSN have the same format. The key set identifier is three bits. Seven values are used to identify the key set. A value of "111" is used by the mobile station to indicate that a valid key is not available for use. The value '111' in the other direction from network to mobile station is reserved.

3G 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** **048** Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG: SA #7 *list TSG meeting no. here ↑*
for approval: **X**
for information:
(only one box should be marked with an X)

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM **X** ME **X** UTRAN ☐ Core Network **X**

Source: SA WG3 **Date:** 2000-Jan-17

Subject: Clarification on the reuse of AVs

3G Work item: Security

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

F	Correction	**X**
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Reason for change: Agreed text including “Conditions on the use of authentication information by the VLR/SGSN” has been omitted in latest version of 33.102 (refer to CR 37, Tdoc S3-99548).
This text has been included again and has also been modified to clarify that UMTS AVs (quintuplets) cannot be reused. GSM AVs (triplets) can be reused as per GSM.

Clauses affected: 6.3.3

Other specs affected:

Other 3G core specifications	☐	→ List of CRs:
Other 2G 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 Authentication and key agreement

The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the MS. During the authentication, the user verifies the freshness of the authentication vector that is used.

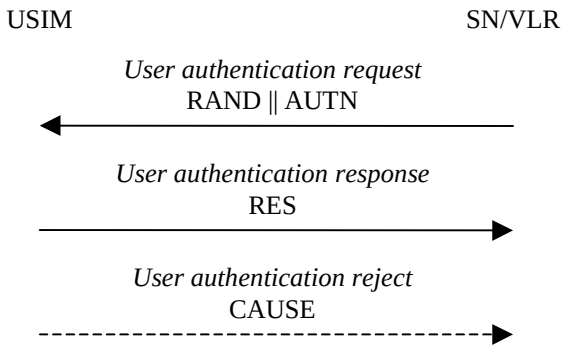


Figure 8: Authentication and key establishment

The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR database. The VLR/SGSN sends to the user the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.

Upon receipt the user proceeds as shown in Figure 9.

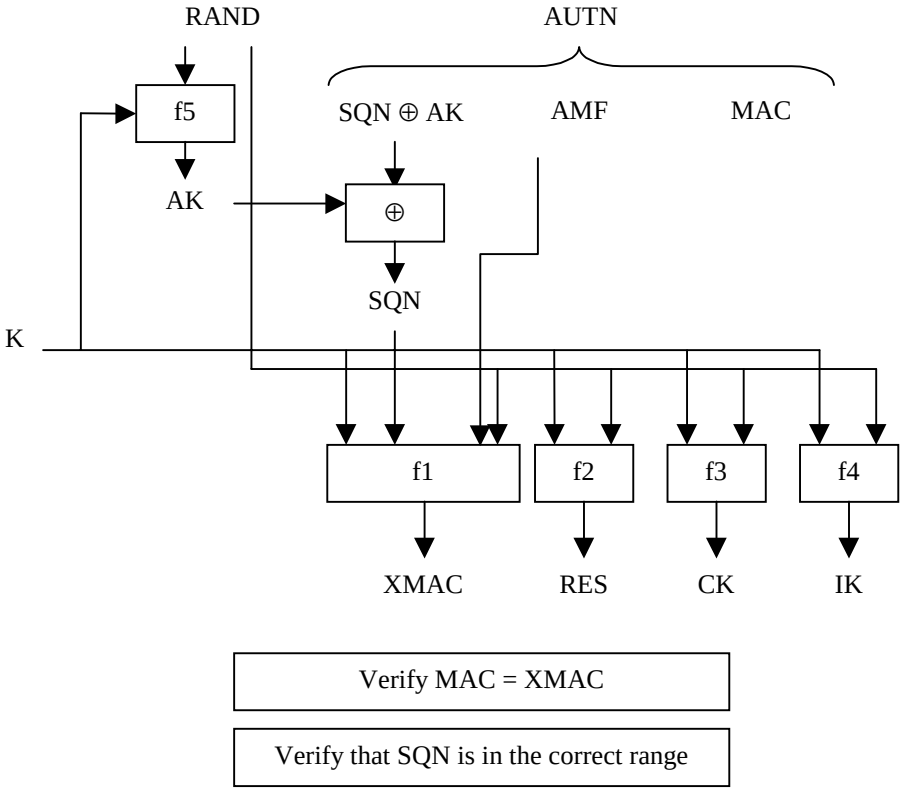


Figure 9: User authentication function in the USIM

Upon receipt of RAND and AUTN the user first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Next the user computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends *user authentication reject* back to the VLR/SGSN with an indication of the cause and the user abandons the procedure.

Next the USIM verifies that the received sequence number SQN is in the correct range.

If the user considers the sequence number to be not in the correct range, he sends *synchronisation failure* back to the VLR/SGSN including an appropriate parameter, and abandons the procedure.

The synchronisation failure message contains the parameter AUTS. It is AUTS = Conc(SQN_{MS}) || MACS. Conc(SQN_{MS}) = $SQN_{MS} \oplus f5_K$(MACS) is the concealed value of the counter SEQ_{MS} in the MS, and MACS = $f1^*_K$(SEQ_{MS} || RAND || AMF) where RAND is the random value received in the current user authentication request. f1* is a message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa.

The AMF used to calculate MACS assumes a dummy value of all zeros so that it does not need to be transmitted in the clear in the re-synch message.

The construction of the parameter AUTS in shown in the following Figure 10:

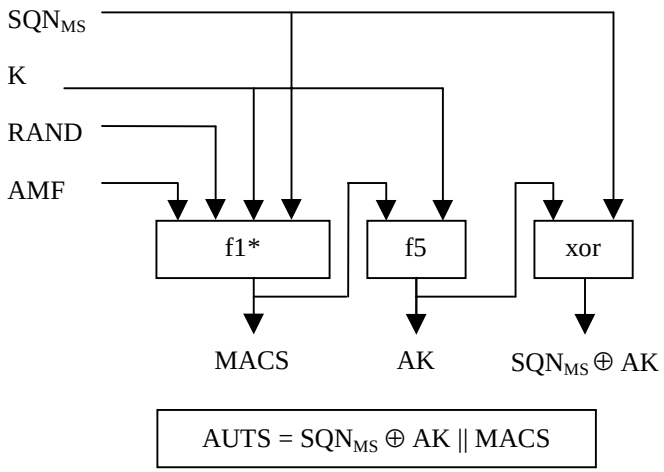


Figure 10: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range however, the user computes RES = $f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the VLR/SGSN. Finally the user computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND. The MS stores RAND for re-synchronisation purposes.

Upon receipt of *user authentication response* the VLR/SGSN compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The VLR/SGSN also selects the appropriate cipher key CK and integrity key IK from the selected authentication vector.

Conditions on the use of authentication information by the VLR/SGSN: The **VLR/SGSN** shall use a UMTS authentication vector (i.e. a quintuplet) only once and, hence, shall send out each user authentication request *RAND* || *AUTN* only once no matter whether the authentication attempt was successful or not. A consequence is that UMTS authentication vectors (quintuplets) cannot be reused.

Technical Specification Group Services and System Aspects Meeting #7, ***S3-000076***

TSG SA WG3 #10, Antwerp 19-21 January 2000

DRAFT 3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

TS 33.102 **CR** **049** Current Version: V3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG SA#7 *list TSG meeting no. here ↑* for approval [X] for information [ ] *(only one box should be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM [ ] ME [ ] UTRAN [ ] Core Network [X]

Source: SA WG3 **Date:** 2000-01-21

Subject: Authentication failure reporting

3G Work item: Security

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

F	Correction	X
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Reason for change: The *Authentication Failure Report* from the SGSN/VLR does not need to be acknowledged by the HLR and consequently the acknowledge should be removed.

Clauses affected: 6.3.6

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other 2G 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: This CR is the result of a request from N2 to consider removing the acknowledge part of the *Authentication Failure Report* mechanism.

6.3.6 Reporting authentication failures from the SGSN/VLR to the HLR

The purpose of this procedure is to provide a mechanism for reporting authentication failures from the serving environment back to the home environment.

The procedure is shown in Figure 13.

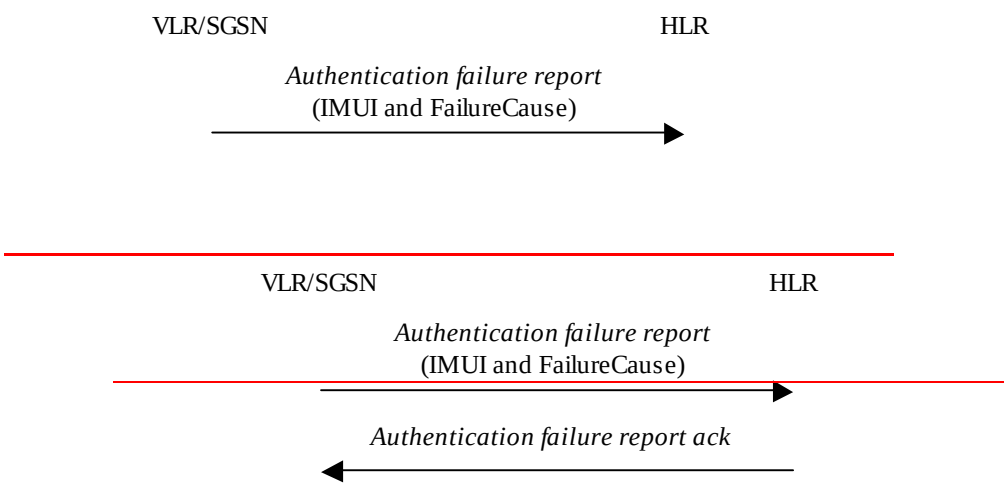


Figure 13: Reporting authentication failure from VLR/SGSN to HLR

The procedure is invoked by the serving network VLR/SGSN when the authentication procedure fails. The *authentication failure report* shall contain the subscriber identity and a failure cause code. The possible failure causes are either that the network signature was wrong or that the user response was wrong.

~~When the home environment receives the *authentication failure report* it shall respond by an acknowledge back to the serving network.~~ The HE may decide to cancel the location of the user after receiving an *authentication failure report*.

3G 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**	**050**	Current Version:	3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG	SA #7	for approval	**X**	*(only one box should*
list TSG meeting no. here ↑		for information		*be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)*	USIM	**X**	ME	**X**	UTRAN		Core Network	

Source:	SA WG3 **Date:** 2000-Feb-09
Subject:	Refinement of Cipher key and integrity key lifetime
3G Work item:	Security

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

F	Correction	**X**
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Reason for change: Generation of a new access link key set shall be triggered by UE instead of USIM

Clauses affected: 6.4.3

Other specs affected:

Other 3G core specifications		→ List of CRs:	31.102
Other 2G 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.

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the highest value of the hyperframe number (the current value of COUNT) of the bearers that were protected in that RRC connection is stored in the USIM. When the next RRC connection is established that value is read from the USIM and incremented by one.

The ~~USIM~~ UE shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out.

This mechanism will ensure that a cipher/integrity key set cannot be reused more times than the limit set by the operator.

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

Document S3-000159
(Rev.of S3-000111)
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	051r1	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 [ ]

Source: S3 **Date:** 2000-02-23

Subject: Conversion function c3 at USIM

Work item: Security

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

F	Correction	X	**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			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:

Conversion function c3 (CK, IK → Kc) is located at USIM only. USIM shall derive Kc using c3 in order to provide it to a R99 UE for UMTS-GSM interoperability purposes.

The terms 'user' and 'MS' have been replaced by 'USIM' where applicable.

Clauses affected: 6.3.3

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 Authentication and key agreement

The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the ~~MS~~USIM. During the authentication, the ~~user~~ USIM verifies the freshness of the authentication vector that is used.

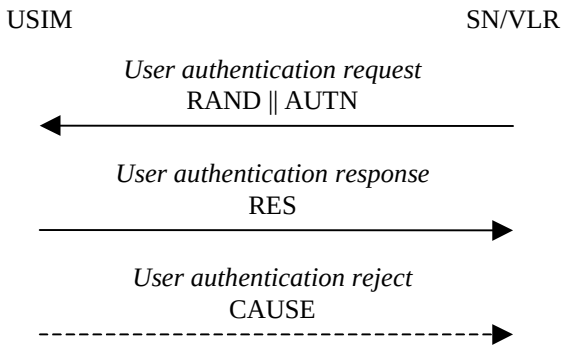


Figure 8: Authentication and key establishment

The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR database. The VLR/SGSN sends to the ~~user~~ USIM the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.

Upon receipt the user proceeds as shown in Figure 9.

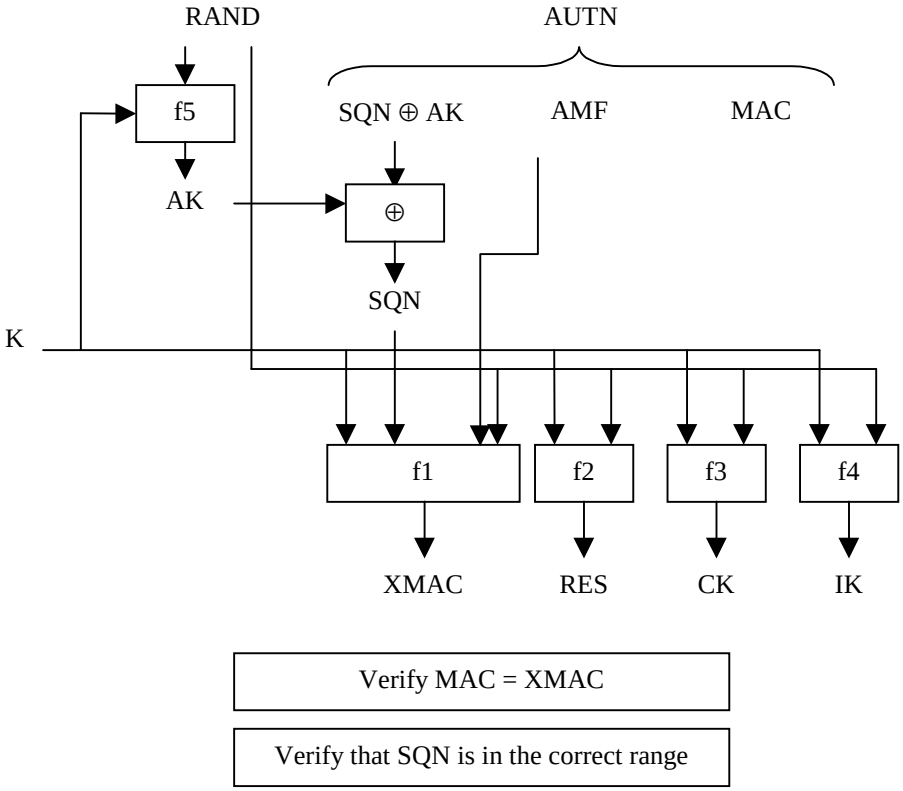


Figure 9: User authentication function in the USIM

Upon receipt of RAND and AUTN the ~~user~~ USIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Next the ~~user~~ USIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends *user authentication reject* back to the VLR/SGSN with an indication of the cause and the user abandons the procedure.

Next the USIM verifies that the received sequence number SQN is in the correct range.

If the ~~user~~ USIM considers the sequence number to be not in the correct range, ~~he~~ it sends *synchronisation failure* back to the VLR/SGSN including an appropriate parameter, and abandons the procedure.

The synchronisation failure message contains the parameter AUTS. It is AUTS = Conc(SQN_{MS}) || MACS. Conc(SQN_{MS}) = $SQN_{MS} \oplus f5_K$(MACS) is the concealed value of the counter SEQ_{MS} in the MS, and MACS = $f1^*_K$(SEQ_{MS} || RAND || AMF) where RAND is the random value received in the current user authentication request. f1* is a message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa.

The AMF used to calculate MACS assumes a dummy value of all zeros so that it does not need to be transmitted in the clear in the re-synch message.

The construction of the parameter AUTS in shown in the following Figure 10:

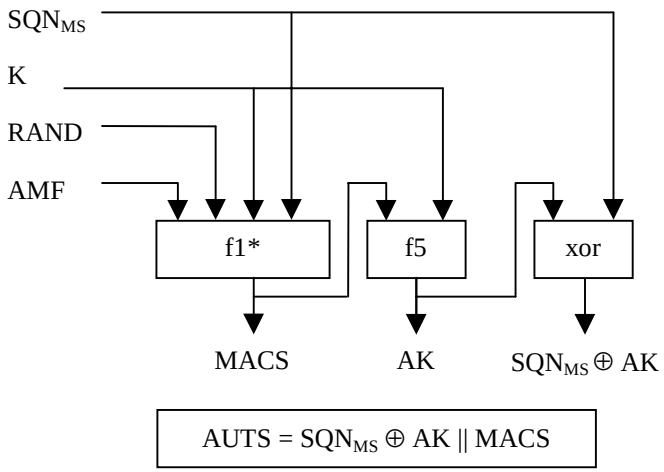


Figure 10: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range however, the ~~user~~ USIM computes RES = $f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the VLR/SGSN. Finally the ~~user~~ USIM computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND. If the USIM also supports GSM AKA, it shall derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3. UMTS keys are sent to the MS along with the derived GSM key for UMTS-GSM interoperability purposes. USIM shall store original CK, IK until the next successful execution of AKA. The ~~MS~~ USIM also stores RAND until completion of current AKA, for re-synchronisation purposes.

Upon receipt of *user authentication response* the VLR/SGSN compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The VLR/SGSN also selects the appropriate cipher key CK and integrity key IK from the selected authentication vector.

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

Document S3-000160
(Rev. of S3-000112)
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	052r1	Current Version:	3.3.1

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

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

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

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

Source: S3 **Date:** 2000-02-23

Subject: Trigger points of AFR during AKA

Work item: Security

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

F	Correction	X	**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			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:
Points where Authentication Failure report mechanism towards HLR is triggered are specified within the AKA procedure.

Term 'SN/VLR' has been replaced by 'VLR/SGSN'.

Clauses affected: 6.3.3

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 Authentication and key agreement

The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the MS. During the authentication, the user verifies the freshness of the authentication vector that is used.

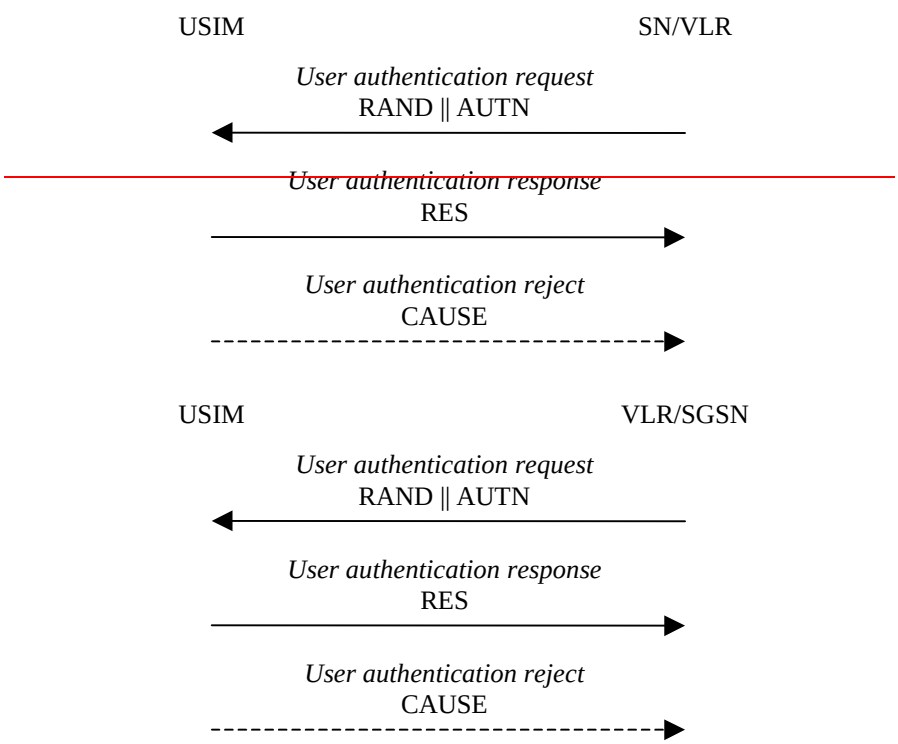


Figure 8: Authentication and key establishment

The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR/SGSN database. The VLR/SGSN sends to the user the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.

Upon receipt the user proceeds as shown in Figure 9.

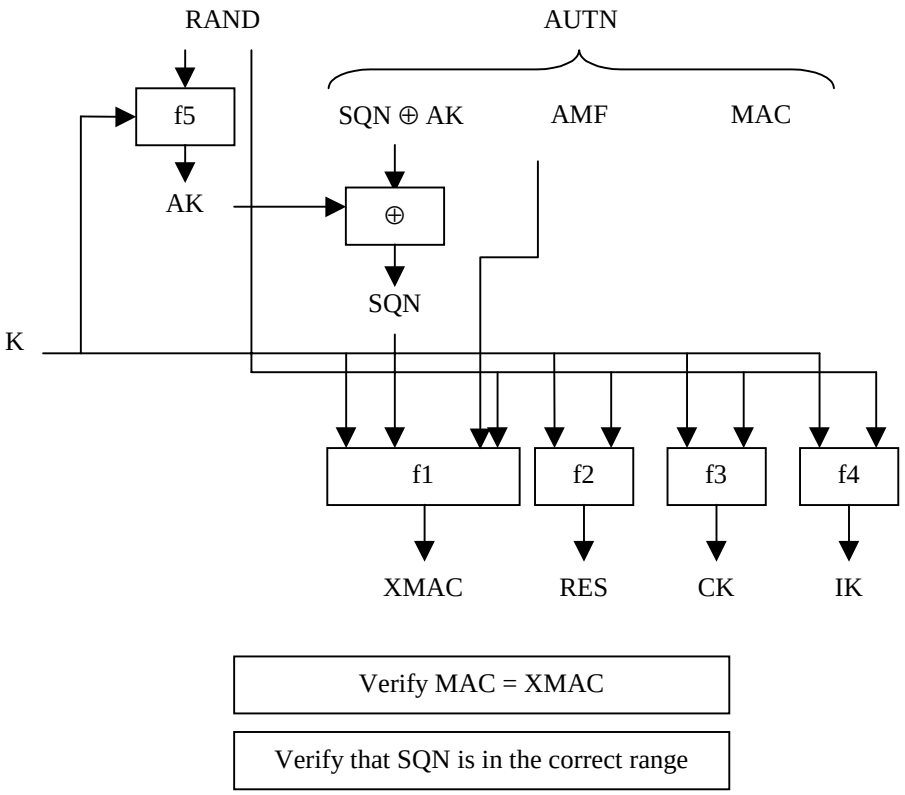


Figure 9: User authentication function in the USIM

Upon receipt of RAND and AUTN the user first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Next the user computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends *user authentication reject* back to the VLR/SGSN with an indication of the cause and the user abandons the procedure. In this case, VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR as specified in section 6.3.6. VLR/SGSN may also decide to initiate a new identification and authentication procedure towards the user.

Next the USIM verifies that the received sequence number SQN is in the correct range.

If the user considers the sequence number to be not in the correct range, he sends *synchronisation failure* back to the VLR/SGSN including an appropriate parameter, and abandons the procedure.

The synchronisation failure message contains the parameter AUTS. It is AUTS = Conc(SQN_{MS}) || MACS. Conc(SQN_{MS}) = SQN_{MS} ⊕ $f5_K$(MACS) is the concealed value of the counter SEQ_{MS} in the MS, and MACS = $f1^*_K$(SEQ_{MS} || RAND || AMF) where RAND is the random value received in the current user authentication request. f1* is a message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa.

The AMF used to calculate MACS assumes a dummy value of all zeros so that it does not need to be transmitted in the clear in the re-synch message.

The construction of the parameter AUTS in shown in the following Figure 10:

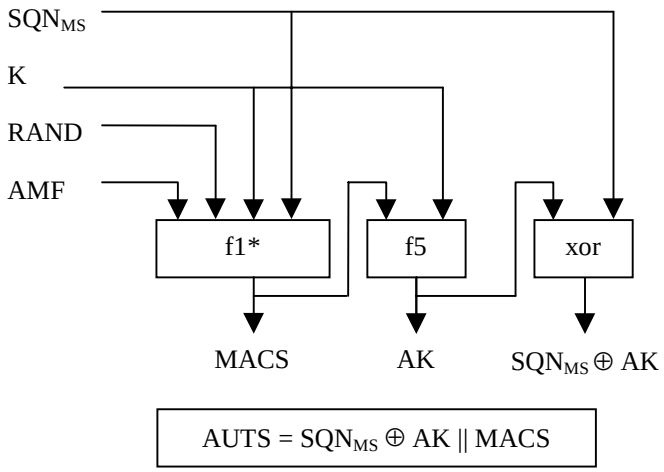


Figure 10: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range however, the user computes RES = $f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the VLR/SGSN. Finally the user computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND. The MS stores RAND for re-synchronisation purposes.

Upon receipt of *user authentication response* the VLR/SGSN compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The VLR/SGSN also selects the appropriate cipher key CK and integrity key IK from the selected authentication vector. If XRES and RES are different, VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR as specified in section 6.3.6. VLR/SGSN may also decide to initiate a new identification and authentication procedure towards the user.

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

Document S3-000163 (Rev. of S3-000113)
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	053r1	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: S3 **Date:** 2000-02-23

Subject: Removal of EUIC from 'Authentication Data Request' procedure.

Work item: Security

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

F	Correction	[X]	**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	[ ]		Release 98	[ ]
D	Editorial modification	[ ]		Release 99	[X]
				Release 00	[ ]

Reason for change:

Decryption of EMSI will only be performed within a "User Identity Request Procedure" described in chapter 6.2 of TS 33.102 (MAP_SEND_IMSI operation will be used for this purpose). The rest of operations will have to wait until decryption of EMSI is performed.

The use of EMSI ('*HLR message*') is therefore removed from 'Authentication Data Request' procedure. IMSI is also removed from 'Authentication data response'.

The terms "SN/VLR" and "IMUI" have been replaced by "VLR/SGSN" and "IMSI" respectively.

Clauses affected: 6.3.2

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.

6.3.2 Distribution of authentication data from HE to SN

The purpose of this procedure is to provide the VLR/SGSN with an array of fresh authentication vectors from the user's HE to perform a number of user authentications.

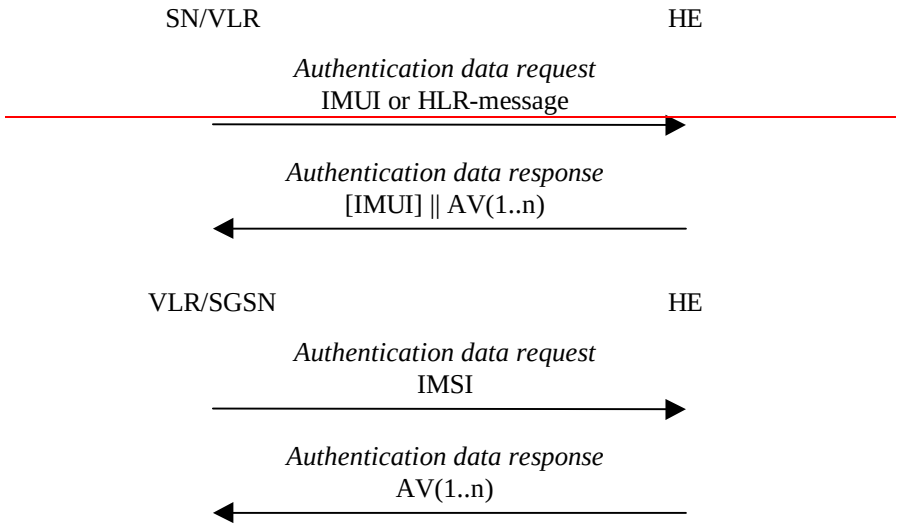


Figure 6: Distribution of authentication data from HE to VLR/SGSN

The VLR/SGSN invokes the procedures by requesting authentication vectors to the HE/AuC.

The *authentication data request* shall include ~~a user~~ the IMSI~~identity. If the user is known in the VLR/SGSN by means of the IMUI, the *authentication data request* shall include the IMUI. However, if the user is identified by means of an encrypted permanent identity (see 6.2), the HLR message from which the HE can derive the IMUI is included instead. In that case, this procedure and the procedure *user identity request to the HLR* are integrated.~~

Upon the receipt of the *authentication data request* from the VLR/SGSN, the HE may have pre-computed the required number of authentication vectors and retrieve them from the HLR database or may compute them on demand. The HE/AuC sends an authentication response back to the VLR/SGSN that contains an ordered array of n authentication vectors AV(1..n).

Figure 7 shows the generation of an authentication vector AV by the HE/AuC.

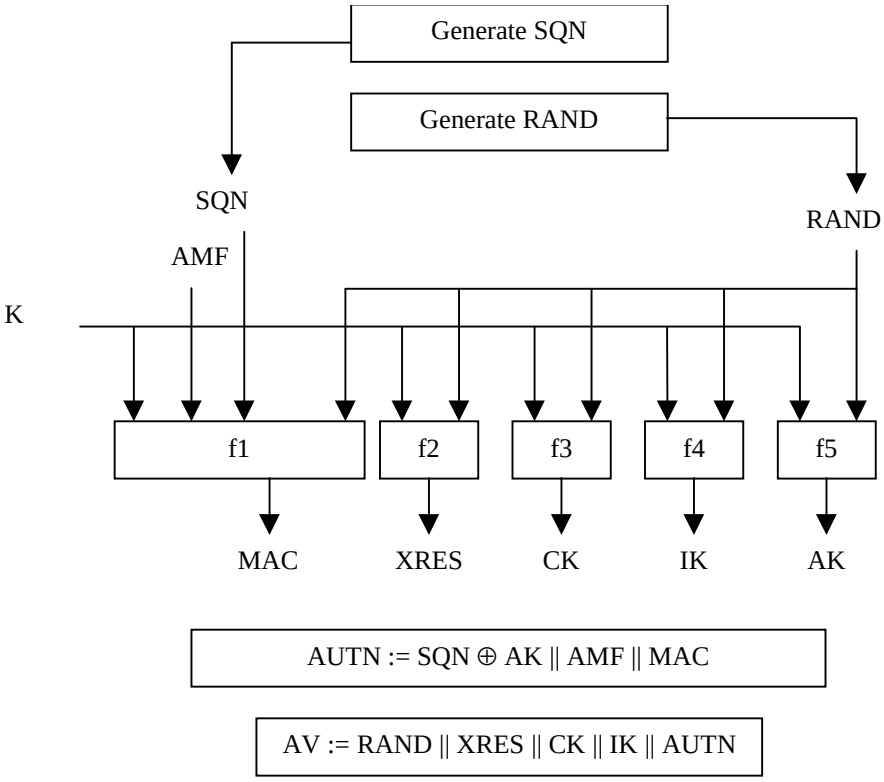


Figure 7: Generation of authentication vectors

The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND.

For each user the HE/AuC keeps track of a counter: SQN_{HE}

The HE has some flexibility in the management of sequence numbers, but some requirements need to be fulfilled by the mechanism used:

a) The generation mechanism shall allow a re-synchronisation procedure in the HE described in section 6.3.5

b) The SQN should be generated in such way that it does not expose the identity and location of the user.

c) In case the SQN may expose the identity and location of the user, the AK may be used as an anonymity key to conceal it.

d) The generation mechanism shall allow protection against wrap around the counter in the USIM.
A method how to achieve this is given in informative Annex C.2.

The mechanisms for verifying the freshness of sequence numbers in the USIM shall to some extent allow the out-of-order use of sequence numbers. This is to ensure that the authentication failure rate due to synchronisation failures is sufficiently low. This requires the capability of the USIM to store information on past successful authentication events (e.g. sequence numbers or relevant parts thereof). The mechanism shall ensure that a sequence number can still be accepted if it is among the last x = 50 sequence numbers generated. This shall not preclude that a sequence number is rejected for other reasons such as a limit on the age for time-based sequence numbers.
The same minimum number x needs to be used across the systems to guarantee that the synchronisation failure rate is sufficiently low under various usage scenarios, in particular simultaneous registration in the CS- and the PS-service domains, user movement between VLRs/SGSNs which do not exchange authentication information, super-charged networks.

The use of SEQ_{HE} ~~HE~~ is specific to the method of generation sequence numbers. A method is specified in Annex C.1 how to generate a fresh sequence number. A method is specified in Annex C.2 how to verify the freshness of a sequence number.

An authentication and key management field AMF is included in the authentication token of each authentication vector. Example uses of this field are included in Annex F.

Subsequently the following values are computed:

- a message authentication code MAC = $f1_K$(SQN || RAND || AMF) where f1 is a message authentication function;
- an expected response XRES = $f2_K$ (RAND) where f2 is a (possibly truncated) message authentication function;
- a cipher key CK = $f3_K$ (RAND) where f3 is a key generating function;
- an integrity key IK = $f4_K$ (RAND) where f4 is a key generating function;
- an anonymity key AK = $f5_K$ (RAND) where f5 is a key generating function or $f5 \equiv 0$.

Finally the authentication token AUTN = SQN $\oplus$ AK || AMF || MAC is constructed.

Here, AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only. If no concealment is needed then $f5 \equiv 0$.

3G 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** **054r1** Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG: SA #7 *list TSG meeting no. here ↑*

for approval **X**

for information

(only one box should be marked with an X)

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM **X** ME **X** UTRAN **X** Core Network **X**

Source: S3 **Date:** 2000-Feb-23

Subject: Scope

3G Work item: Security

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

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	**X**

Reason for change: Clarification of the scope of 33.102 needed w.r.t GSM interoperability.

Clauses affected: 1

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other 2G 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.

1 Scope

This specification defines the security architecture, i.e., the security features and the security mechanisms, for the third generation mobile telecommunication system.

A security feature is a service capabilityies that meets one or several security requirements. The complete set of security features address the security requirements as they are defined in "3G Security: Threats and Requirements" (21.133 [1]). A security mechanism is an element that is used to realise a security feature. All security features and security requirements taken together form the security architecture.

An example of a security feature is user data confidentiality. A security mechanism that may be used to implement that feature is a stream cipher using a derived cipher key.

This specification defines 3G security procedures performed within 3G capable networks (R99+), i.e intra-UMTS and UMTS-GSM. As an example, UMTS authentication is applicable to UMTS radio access as well as GSM radio access provided that the serving network node and the subscriber are UMTS capable. Interoperability with non-UMTS capable networks (R98-) is also covered.

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

Document **S3-000115**
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**	**055**	Current Version:	3.3.1

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

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

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

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

Source: Ericsson **Date:** 2000-02-16

Subject: SQN Generation Requirements

Work item: Security

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

F	Correction	X	**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			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:

Requirements b) and c) for generation of SQN numbers are contradictory.

SQNs may always be concealed using current requirement c) (independantly of how SQN were generated). Therefore, it is proposed to delete requirement b).

It has been also clarified that when there is no need to conceal SQN, then AK=0.

Clauses affected: 6.3.2

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.

6.3.2 Distribution of authentication data from HE to SN

The purpose of this procedure is to provide the VLR/SGSN with an array of fresh authentication vectors from the user's HE to perform a number of user authentications.

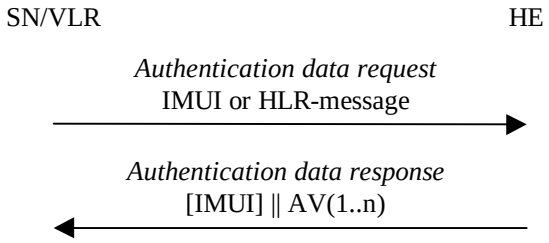


Figure 6: Distribution of authentication data from HE to VLR/SGSN

The VLR/SGSN invokes the procedures by requesting authentication vectors to the HE/AuC.

The *authentication data request* shall include a user identity. If the user is known in the VLR/SGSN by means of the IMUI, the *authentication data request* shall include the IMUI. However, if the user is identified by means of an encrypted permanent identity (see 6.2), the HLR-message from which the HE can derive the IMUI is included instead. In that case, this procedure and the procedure *user identity request to the HLR* are integrated.

Upon the receipt of the *authentication data request* from the VLR/SGSN, the HE may have pre-computed the required number of authentication vectors and retrieve them from the HLR database or may compute them on demand. The HE/AuC sends an authentication response back to the VLR/SGSN that contains an ordered array of n authentication vectors AV(1..n).

Figure 7 shows the generation of an authentication vector AV by the HE/AuC.

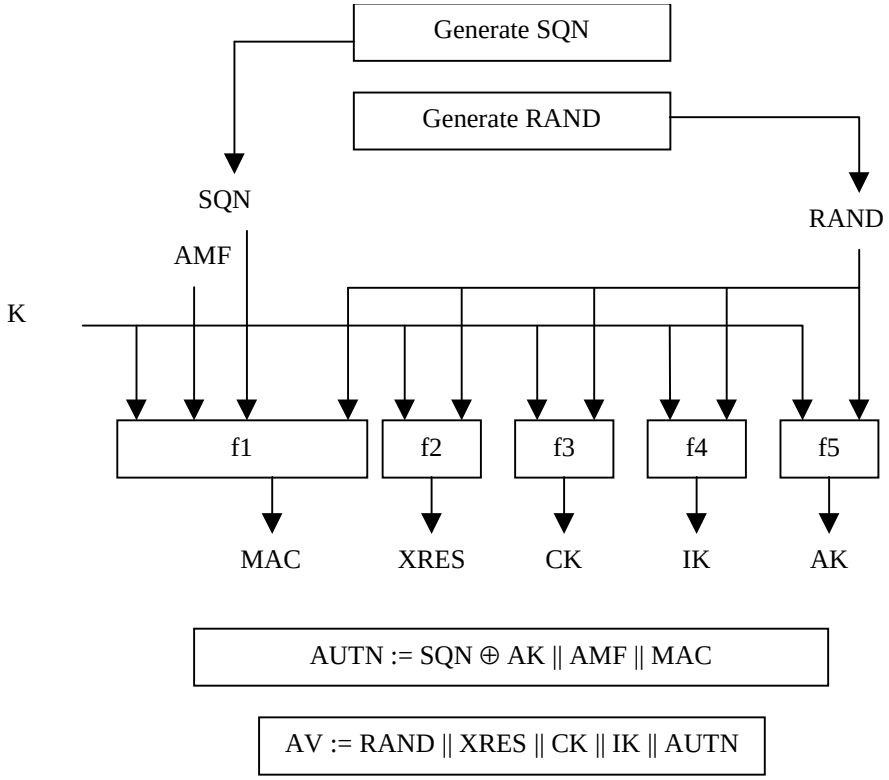


Figure 7: Generation of authentication vectors

The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND.

For each user the HE/AuC keeps track of a counter: SQN_{HE}

The HE has some flexibility in the management of sequence numbers, but some requirements need to be fulfilled by the mechanism used:

a) The generation mechanism shall allow a re-synchronisation procedure in the HE described in section 6.3.5

~~b) The SQN should be generated in such way that it does not expose the identity and location of the user.~~

b~~c~~) In case the SQN ~~may~~ expose<u>s</u> the identity and location of the user, the AK may be used as an anonymity key to conceal it.

c~~d~~) The generation mechanism shall allow protection against wrap around the counter in the USIM. A method how to achieve this is given in informative Annex C.2.

The mechanisms for verifying the freshness of sequence numbers in the USIM shall to some extent allow the out-of-order use of sequence numbers. This is to ensure that the authentication failure rate due to synchronisation failures is sufficiently low. This requires the capability of the USIM to store information on past successful authentication events (e.g. sequence numbers or relevant parts thereof). The mechanism shall ensure that a sequence number can still be accepted if it is among the last x = 50 sequence numbers generated. This shall not preclude that a sequence number is rejected for other reasons such as a limit on the age for time-based sequence numbers.
The same minimum number x needs to be used across the systems to guarantee that the synchronisation failure rate is sufficiently low under various usage scenarios, in particular simultaneous registration in the CS- and the PS-service domains, user movement between VLRs/SGSNs which do not exchange authentication information, super-charged networks.

The use of SEQHE is specific to the method of generation sequence numbers. A method is specified in Annex C.1 how to generate a fresh sequence number. A method is specified in Annex C.2 how to verify the freshness of a sequence number.

An authentication and key management field AMF is included in the authentication token of each authentication vector. Example uses of this field are included in Annex F.

Subsequently the following values are computed:

- a message authentication code MAC = $f1_K$(SQN || RAND || AMF) where f1 is a message authentication function;
- an expected response XRES = $f2_K$ (RAND) where f2 is a (possibly truncated) message authentication function;
- a cipher key CK = $f3_K$ (RAND) where f3 is a key generating function;
- an integrity key IK = $f4_K$ (RAND) where f4 is a key generating function;
- an anonymity key AK = $f5_K$ (RAND) where f5 is a key generating function or $f5 \equiv 0$.

Finally the authentication token AUTN = SQN $\oplus$ AK || AMF || MAC is constructed.

Here, AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only. If no concealment is needed then $f5 \equiv 0$ <u>(AK = 0)</u>.

3G 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** **056r1** Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG: SA #7 *list TSG meeting no. here ↑*
for approval **X**
for information
(only one box should be marked with an X)

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM **X** ME **X** UTRAN **X** Core Network **X**

Source: S3 **Date:** 2000-Feb-23

Subject: Identification of temporary identities

3G Work item: Security

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

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	**X**

Reason for change: Clarification of the relation to GSM 03.20 and GSM 23.060 for identification of temporary identities.
Terminology clean-up.

Clauses affected: 2.1; 6.1.1

Other specs affected:

Other 3G core specifications		→ List of CRs:
Other 2G 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.

2.1 Normative references

[1] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3G TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] UMTS 33.21, version 2.0.0: "Security requirements".

[4] UMTS 33.22, version 1.0.0: "Security features".

[5] UMTS 33.23, version 0.2.0: "Security architecture".

[6] Proposed UMTS Authentication Mechanism based on a Temporary Authentication Key.

[7] TTC Work Items for IMT-2000 – System Aspects.

[8] Annex 8 of "Requirements and Objectives for 3G Mobile Services and systems" – "Security Design Principles".

[9] ETSI GSM 09.02 Version 4.18.0: Mobile Application Part (MAP) Specification.

[10] ISO/IEC 11770-3: *Key Management – Mechanisms using Asymmetric Techniques*.

[11] ETSI SAGE: Specification of the BEANO encryption algorithm, Dec. 1995 (confidential).

[12] ETSI SMG10 WPB: SS7 Signalling Protocols Threat Analysis , Input Document AP 99-28 to SMG10 Meeting#28, Stockholm, Sweden.

[13] 3G TS 33.105: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Cryptographic Algorithm Requirements".

[xx] 3G TS 23.060: "3rd Generation Partnership Project; Technical Specification Group and System Aspects; Digital cellular telecomunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

6.1 Identification by temporary identities

6.1.1 General

This mechanism allows the identification of a user on the radio access link by means of a temporary mobile ~~user~~ subscriber identity (TMS~~U~~I/P-TMSI). A TMS~~U~~I/P-TMSI has local significance only in the location area or routing area in which the user is registered. Outside that area it should be ~~a~~ accompanied by an appropriate Location Area Identification (LAI) or Routing Area Identification (RAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR/SGSN) in which the user is registered.

The TMS~~U~~I/P-TMSI, when available, is normally used to identify the user on the radio access path, for instance in paging requests, location update requests, attach requests, service requests, connection re-establishment requests and detach requests.

The procedures and mechanisms are described in GSM 03.20 and TS 23.060. The following subchapters contain a summary of this feature.

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000117**
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	057	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:	TSG 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	X	Core Network	X

Source:	Ericsson	**Date:**	2000-02-17

Subject:	Cipher key and integrity key selection

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		Release 98	
D	Editorial modification	X	Release 99	X
			Release 00	

Reason for change:	Editorial changes in the section 6.3.3.1

Clauses affected:	6.3.3.1, 6.3.3.1.2

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 and integrity key selection

Because of the separate mobility management for CS and PS services, the USIM establishes a separate cipher/integrity keys set with ~~both~~ each of 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 established cipher/integrity key set of the core network service domain that is specified by this procedure is applied to the common 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.

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000167**
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	058r1	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: TSG SA #7	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑	for information		non-strategic		

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

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

Source: Ericsson **Date:** 2000-02-17

Subject: Clarification on ciphering and integrity mode setting

Work item: Security

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

F	Correction	[X]	**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	[ ]		Release 98	[ ]
D	Editorial modification	[ ]		Release 99	[X]
				Release 00	[ ]

Reason for change: Due to the use of a common MS-RNC connection for both CN domains, the two CN domains must have the same preferences and requirements regarding ciphering and integrity mode.
Editorial changes in the section 6.4.2

Clauses affected: 6.4.2

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.

6.4.2 Ciphering ~~key~~ and integrity mode negotiation

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM Classmark which cipher and integrity algorithms the MS supports. This ~~message~~ information itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving the MS/USIM Classmark ~~the cipher and it~~this information must be stored in the RNC. ~~and the~~The data integrity of the classmark is performed, during the security mode set-up procedure ~~with~~ by use of the ~~newly last~~ most recently generated IK (see section 6.4.5).~~and this value is transmitted to the RNC after the authentication procedure is complete~~.

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the SN have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the SN have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UIA algorithm for use on that connection.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UEA algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.

2) If the MS and the network have at least one version of the UEA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection.

3) If the MS and the network have no versions of the UEA algorithm in common and the user (respectively the user's HE) and the SN are willing to use an unciphered connection, then an unciphered connection shall be used.

Because of the separate mobility management for CS and PS services, one CN domain may, independent of the other CN, establish a connection to one and the same MS. Change of ciphering and integrity mode (algorithms) at establishment of a second MS to CN connection shall not be permitted. The preferences and special requirements for the ciphering and integrity mode setting shall be common for ~~the~~ both domains. (e.g. the order of preference of the algorithms).

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000119**
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	059	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:	TSG 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		ME	X	UTRAN / Radio	X	Core Network	X

Source: Ericsson **Date:** 2000-02-17

Subject: Clarification on when integrity protection is started

Work item: Security

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

F	Correction	X	**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			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change:
A clarification is needed on when integrity protection is started and what procedures that are allowed without integrity protection.
The integrity protection is started after that the RRC connection has been established and the network and MS has agreed upon the key(s) to be used. This implies e.g. that the initial L3 message (including e.g. the MS identity) that is sent to the CN can not be integrity protected.

Clauses affected: 6.4.5

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.

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. ~~This procedure is mandatory.~~ It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and MSC/VLR respective SGSN. The three exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.

- If there is no MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), i.e. in the case of deactivation indication sent from the MS followed by connection release.

- If the only MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.

When the integrity protection shall be started, the only procedures between MS and MSC/VLR respective SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to MSC/VLR or SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and

- Authentication and key agreement

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

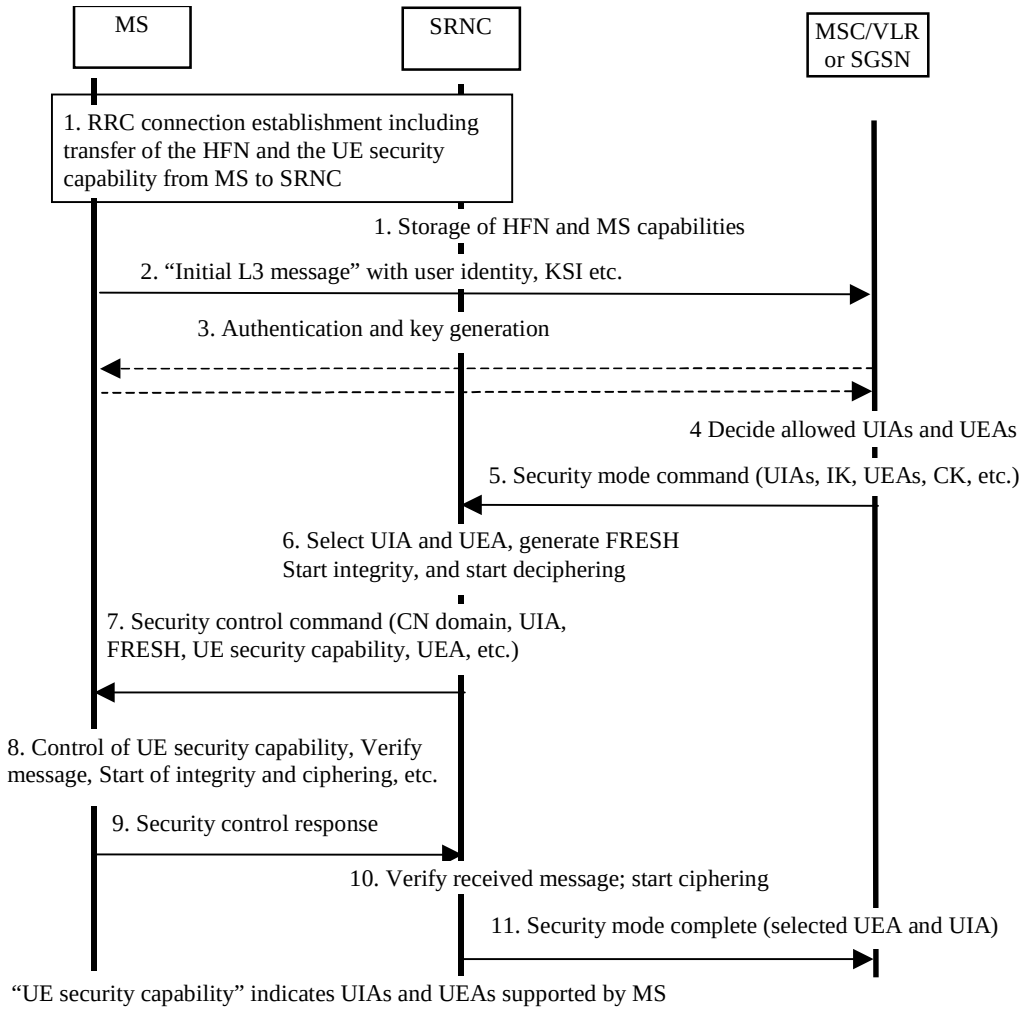


Figure 14: Local authentication and connection set-up

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000168**
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	061r1	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:	TSG 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		ME	X	UTRAN / Radio	X	Core Network	X

Source: Ericsson **Date:** 2000-02-17

Subject: Unsuccessful integrity check

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: At detection of an integrity failure, the concerned message shall be discarded. In both the MS and the SRNC there shall be a supervision of failed integrity checks and if the failure situation persists, the connection shall be dropped.

Clauses affected: 6.4.6

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:	

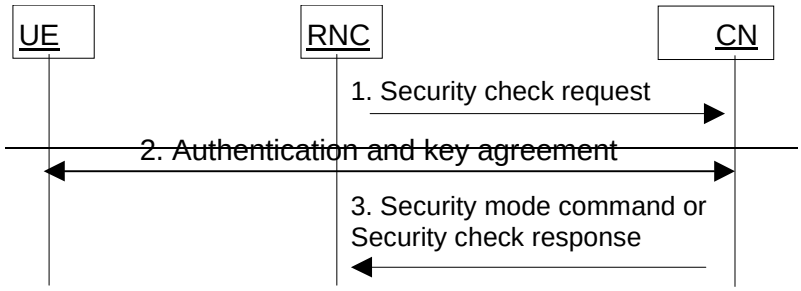
Other comments:

help.doc

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

6.4.6 Signalling procedures in the case of an unsuccessful integrity check

The supervision of failed integrity checks shall be performed both in the MS and the SRNC. In case of failed integrity check (i.e. faulty or missing MAC) is detected after that the integrity protection is started the concerned message shall be discarded. This can happen on the RNC side or on the MS side.~~The following procedure is used by the RNC to request the CN to perform an authentication and to provide a new CK and IK in case of unsuccessful integrity check. This can happen on the RNC side or in the UE side. In the latter case the UE sends a SECURITY CONTROL REJECT message to the RNC.~~



~~Figure 15: Procedures at unsuccessful integrity check~~

~~RNC detects that new security parameters are needed. This may be triggered by (repeated) failure of integrity checks (e.g. COUNT-I went out of synchronisation), or at handover the new RNC does not support an algorithm selected by the old RNC, etc.~~

1. ~~RNC sends a SECURITY CHECK REQUEST message to CN (indicating cause of the request).~~
2. ~~The CN performs the authentication and key agreement procedure.~~
3. ~~If the authentication is successful, the CN sends a Security mode command to RNC. This will restart the ciphering and integrity check with new parameters. If the authentication is not successful, the CN sends a SECURITY CHECK RESPONSE (Cause) to RNC.~~
4. ~~If the failure situation persists, the connection should be dropped.~~

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000176**
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	062r1	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:	TSG 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		ME	X	UTRAN / Radio	X	Core Network	X

Source: Ericsson **Date:** 2000-02-17

Subject: Clarification on signalling messages to be integrity protected

Work item: Security

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

F	Correction	X	**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			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Clarification needed on what messages that shall be integrity protected. The integrity protection is started after that the RRC connection has been established and the network and MS has agreed upon the key(s) to be used. After that the integrity protection is started then all dedicated MS-network control signalling messages are integrity protected.

Clauses affected: 6.5.1

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~~control signalling information elements that are sent between the MS and the network are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the MS and the SN.

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

After the RRC connection establishment and execution of the security mode set-up procedure, all dedicated MS <–> network control signalling messages (e.g. RRC, MM, CC, GMM, and SM messages) shall be integrity protected.~~-~~ The Mobility Management layer in the MS supervises that the integrity protection is started (see ~~6.5.4~~ section 6.4.5)

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

~~- Notification~~

- Paging Type 1
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete
- RRC Connection Reject
- ~~All~~ System Information ~~messages~~ (broadcasted information).

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000177**
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	063r1	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:	TSG 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	X	Core Network	X

Source:	Ericsson		**Date:**	2000-02-17	
Subject:	Clarification of the HFN handling				
Work item:	Security				
Category: *(only one category shall be marked with an X)*	F Correction	X	**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			Release 98	
	D Editorial modification			Release 99	X
				Release 00	

Reason for change:	A reset of the HFN is performed at start using new generated security keys. Editorial changes (e.g. COUNT-I introduced in the figure 16)
Clauses affected:	6.5.2

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.

6.5.2 Integrity algorithm

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

Figure 16 illustrates the use of the UIA to authenticate the data integrity of a signalling message.

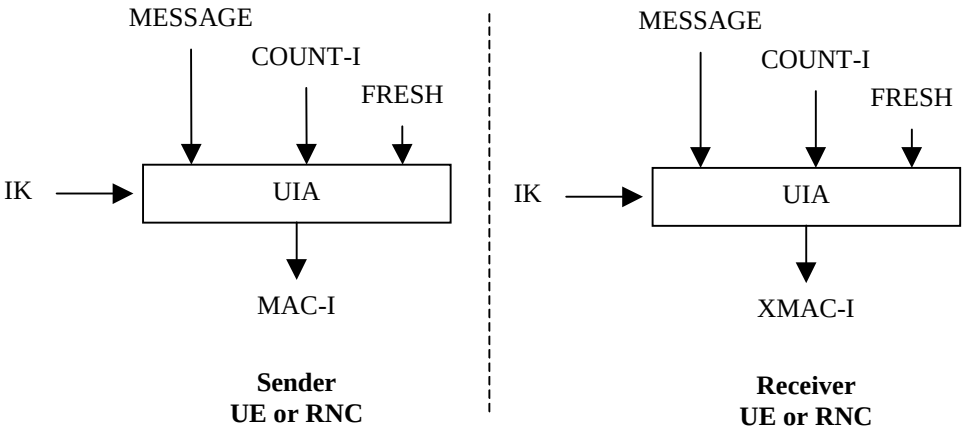


Figure 16: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), a time dependent input (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). 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.

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 a 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 (see 6.4.5). The user stores, on the USIM, 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. A reset of the HFN (HFN=0) is performed when the new generated security key set is used for the first time. The user stores one HFN per established security key set.

The input parameter FRESH protects network against replay of signalling messages by the user. At connection set-up the network generates a random value FRESH and sends it to the user. 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.

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000178**
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	071r1	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:	TSG 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		ME	X	UTRAN / Radio	X	Core Network	X

Source: SA WG3 **Date:** 2000-02-16

Subject: Use of default IK at emergency call with no (U)SIM or when authentication has failed

Work item: Security

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

F	Correction	X	**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			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: The handling of emergency call when no USIM is available or when authentication fails. Since integrity protection is mandatory in UMTS it is proposed to use a default IK for emergency calls when there is no (U)SIM available in the UE or when authentication has failed.

Clauses affected: 6.3.3.2 (New clause)

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.

6.3.3.2 Emergency calls

Emergency call is a serving network option that applies to the CS domain and is allowed to be performed even

1. without any (U)SIM present in the UE

2. when user authentication fails (USIM present)

3. when authentication is impossible to perform (USIM present but network failure or invalid USIM)

Since integrity protection is mandatory in UMTS, a default IK is used for emergency calls in the above-mentioned cases and only in these cases. The security mode set-up procedure will then also always be executed during the establishment of an emergency call.

Use of the default IK should be signalled in the security mode command and should only be accepted when an emergency call is made.

Default IK definition: IK[0], IK[1], ….., IK[127], is set to

01000110 11000001 (46C1)

01001110 01011101 (4E5D)

11000000 01001000 (C048)

11010001 01011001 (D159)

11100010 01101010 (E26A)

11110011 01111011 (F37B)

11000000 00010001 (C011)

00001100 10000101 (0C85).

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000148**
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	072	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:	TSG 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		ME	X	UTRAN / Radio	X	Core Network	X

Source: Ericsson **Date:** 2000-02-17

Subject: Clarification on ciphering and integrity protection at intersystem handover

Work item: Security

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

Reason for change: A clarification is needed on that the communication is continued in ciphered mode at intersystem handover.
A clarification is needed on that integrity protection is started at intersystem handover from GSM BSS to UTRAN.

Clauses affected: 6.8.3, 6.8.4

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.

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

If ciphering has been started when an intersystem handover occurs from UTRAN to GSM BSS, the necessary information (e.g. Kc, supported/allowed GSM ciphering algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old RNC to the new GSM BSS, and to continue the communication in ciphered mode.

6.8.3.1 UMTS security context

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 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 BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by another 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 BSC via the (second) MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.

At the user side, in either case, the UE derives the GSM cipher key Kc 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

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 BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by another MSC/VLR, the initial MSC/VLR sends the stored GSM cipher key Kc to the BSC via the (second) MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.

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

If ciphering has been started when an intersystem handover occurs from GSM BSS to UTRAN, the necessary information (e.g. CK, IK, initial HFN 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 integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed.

6.8.4.1 UMTS security context

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 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 (second) MSC/VLR that controls the new RNC. The initial MSC/VLR remains the anchor point for throughout the service.

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

3G 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** **074** Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG: SA #7 *(list TSG meeting no. here ↑)* — for approval **X** — for information — *(only one box should be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM [ ] ME [ ] UTRAN [X] Core Network [X]

Source: SA WG3 **Date:** 2000-Feb-14

Subject: Clarification about CK and IK which are transmitted in clear over the Iu-interface

3G Work item: Security

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

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	X
C	Functional modification of feature	
D	Editorial modification	

Reason for change: The keys CK and IK is transmitted in clear over the Iu-interface. For R99 we merely acknowledge this.

Clauses affected: 7.6

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other 2G 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: This CR does not solve the problem, it just makes it clear that we have identified the problem.

help.doc

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

7.6 Distribution of security parameters to UTRAN

Confidentiality and integrity between the user and the network is handled by the UE/USIM and the RNC.

The security parameters for the confidentiality and integrity algorithms must be distributed from the core network to the RNC over the Iu-interface in a secure manner. The actual mechanism for securing these parameters has not yet been identified.

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000193**
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	076	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:	TSG 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	X	Core Network	X

Source: SA WG3 **Date:** 2000-02-22

Subject: Cipher key and integrity key lifetime

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: It is required to correct a potential weakness in the key lifetime control mechanism so that the authentication and key agreement procedure can be triggered by the UE during a connection if the maximum permitted hyperframe counter value is reached.

Clauses affected: 6.4.3

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.

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the highest value of the hyperframe number (the current value of COUNT) of the bearers that were protected in that RRC connection is stored in the USIM. When the next RRC connection is established that value is read from the USIM and incremented by one.

The USIM shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out or during an RRC connection.

This mechanism will ensure that a cipher/integrity key set cannot be reused ~~more times than~~beyond the limit set by the operator.

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000194**
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	077	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:	TSG 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	X	Core Network	X

Source: SA WG3 **Date:** 2000-02-22

Subject: Cipher key and integrity key setting

Work item: Security

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

F	Correction	X	**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			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: It is required to clarify that after an authentication the new keys are taken into use as part of the security mode control procedure that follows in both the PS and CS domain.

Clauses affected: 6.4.3

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.

6.4.3 Cipher key and integrity key setting

Mutual key setting is the procedure that allows the MS and the RNC to agree on the key IK used to compute message authentication codes using algorithm UIA. Authentication and key setting is triggered by the authentication procedure and described in 6.3. Authentication and key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. TMUI or IMUI) is known by the SN/VLR. The key IK is stored in the SN/VLR and transferred to the RNC when it is needed. The key IK is stored in the USIM until it is updated at the next authentication.

If an authentication procedure is performed during ~~a data transfer in the PS mode~~a connection (PS or CS mode), the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the UE as part of the security mode negotiation (see 6.4.5) that follows the authentication procedure.

3G 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** **079r1** Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG: SA #7 (*list TSG meeting no. here ↑*) — for approval: **X** — for information: (*only one box should be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: (*at least one should be marked with an X*) USIM [ ] ME [X] UTRAN [X] Core Network [ ]

Source: SA 3 **Date:** 2000-Feb-22

Subject: Local Authenication and connection establishment

3G Work item: Security

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

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	X
D	Editorial modification	

Reason for change: A periodic local authentication procedure is added because it provides the RNC and the UE means to verify the amount of data sent during the connection. This is needed in order to prevent intruders from stealing capacity of the network.

Clauses affected: 6.4 (adds new section 6.4.7 "Signalling procedure for periodic local authentication")

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other 2G core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

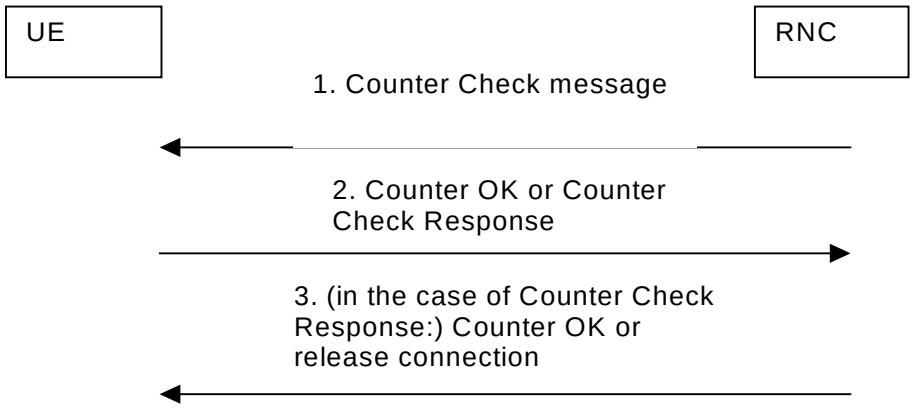
Other comments:

help.doc

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

6.4.7 Signalling procedure for periodic local authentication

The following procedure is used by the RNC to periodically perform a local authentication. At the same time, the amount of data sent during the RRC connection is periodically checked by the RNC and the UE. The procedure should be used for all non-ciphered connections and it may be used also for ciphered connections. The RNC is monitoring the COUNT value associated to each radio bearer. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined by the visited network. All messages in the procedure are integrity protected.



1. When a checking value is reached (e.g. the value in some fixed bit position in the hyperframe number is changed), a Counter Check message is sent by the RNC. The Counter Check message contains the most significant parts of the counter values (which reflect amount of data sent and received) from each active radio bearer.

2. The counter values in the Counter Check message are checked by UE and if they agree with the current status in the UE, a 'Counter OK' message is returned to the RNC. If there is a difference between the counter values in the UE and the values indicated in the Counter Check message, the UE sends a Counter Check response to the RNC. The form of this message is similar to the Counter Check message.

3. In case the RNC receives the 'Counter OK' message the procedure is completed. In case the RNC receives the Counter Check response it compares the counter values indicated in it to counter values in the RNC. If there is no difference or if the difference is acceptable then the RNC completes the procedure by sending the 'Counter OK' message. Otherwise, the connection is released.

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 and the SN.

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.