3GPP TSG SA #6 **Tdoc TSG SA SP-99584**
Nice, FRANCE
15th - 17th December 1999

Source: **TSG SA WG3**

Subject: **R99 CRs to 33.102**
Agenda item: 5.3.3

This document contains CRs to 33.102 version 3.2.0 agreed by SA WG3 to be presented to SA#6 for approval.

CR	REV	CAT	SUBJECT	WG_DOC
022	1	C	Refinement of Enhanced User Identity Confidentiality	S3-99459
025		C	Length of KSI	S3-99389
026	1	B	Mobile IP security	S3-99541
027	1	C	Clarification of re-authentication during PS connections	S3-99552
030			Handling of the MS UEA and UIA capability information	S3-99409
032		F	Removal of network-wide encryption mechanism form	S3-99543
033		C	Distribution of authentication data within one serving	S3-99544
034		C	Interoperation and intersystem handover/change between	S3-99545
035		C	Authentication and key agreement	S3-99538
036		C	Sequence number management	S3-99539
037	1	C	Authentication and key agreement	S3-99548
038		C	Clarification on system architecture	S3-99528
039		D	Updated definitions and abbreviations	S3-99529
040		B	An authentication failure report mechanism from SN to HE	S3-99536
041		B	UIA and UEA identifications	S3-99520

TSG SA WG3 #8, **S3-99389**

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 025 Current Version: V3.2.0

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

For submission to TSG: SA#6 — for approval: X; for information: (blank)

list TSG meeting no. here ↑ *(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: USIM X ME X UTRAN Core Network X

(at least one should be marked with an X)

Source: S3 **Date:** 16-11-99

Subject: Refinement of key set identifier (KSI) specification to reach alignment with CKSN.

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: The length of KSI is changed to reach alignment with CKSN in GSM. In addition, it is specified that KSI can have seven values with '111' being used by the mobile station to indicate that a valid key set is not available for use.

Clauses affected: Section 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:

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.~~It is stored together with the cipher and integrity keys in the MS and in the network~~.

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. The~~e~~is ~~key set identifier~~ is used to allow ~~key~~ re-use of the cipher key CK and integrity key IK during subsequent connections~~ set-ups~~. ~~The KSI is used to verify whether the MS and the SN are to use the same cipher key and integrity key.~~

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 set is not available for use. The value of ‘111’ in the other direction from network to mobile station is reserved.

3GPP TSG SA WG3 Meeting 8, Sophia Antipolis, France, 16th – 19th November 1999 **S3-99409**

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 30 Current Version: V3.2.0

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

For submission to TSG SA#6 for approval X for information

list TSG meeting no. here ↑ *(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: USIM [ ] ME [X] UTRAN [X] Core Network [X]

(at least one should be marked with an X)

Source:	S3
Date:	1999-11-15
Subject:	Handling of the MS UEA and UIA capability information
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:

Since both the ciphering and integrity protection is UTRAN functionality, then also the MS UEA and UIA capability information must be handled by UTRAN. At start of ciphering and integrity protection, the CN shall be able to indicate towards UTRAN the allowed algorithms for the MS. The UTRAN then selects an appropriate algorithm, taking into account the MS ciphering and integrity protection capabilities.

Consequently the MS UEA and UIA capability information is not handled on CN level.

Clauses affected: Sections 6.4.5

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:

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.

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

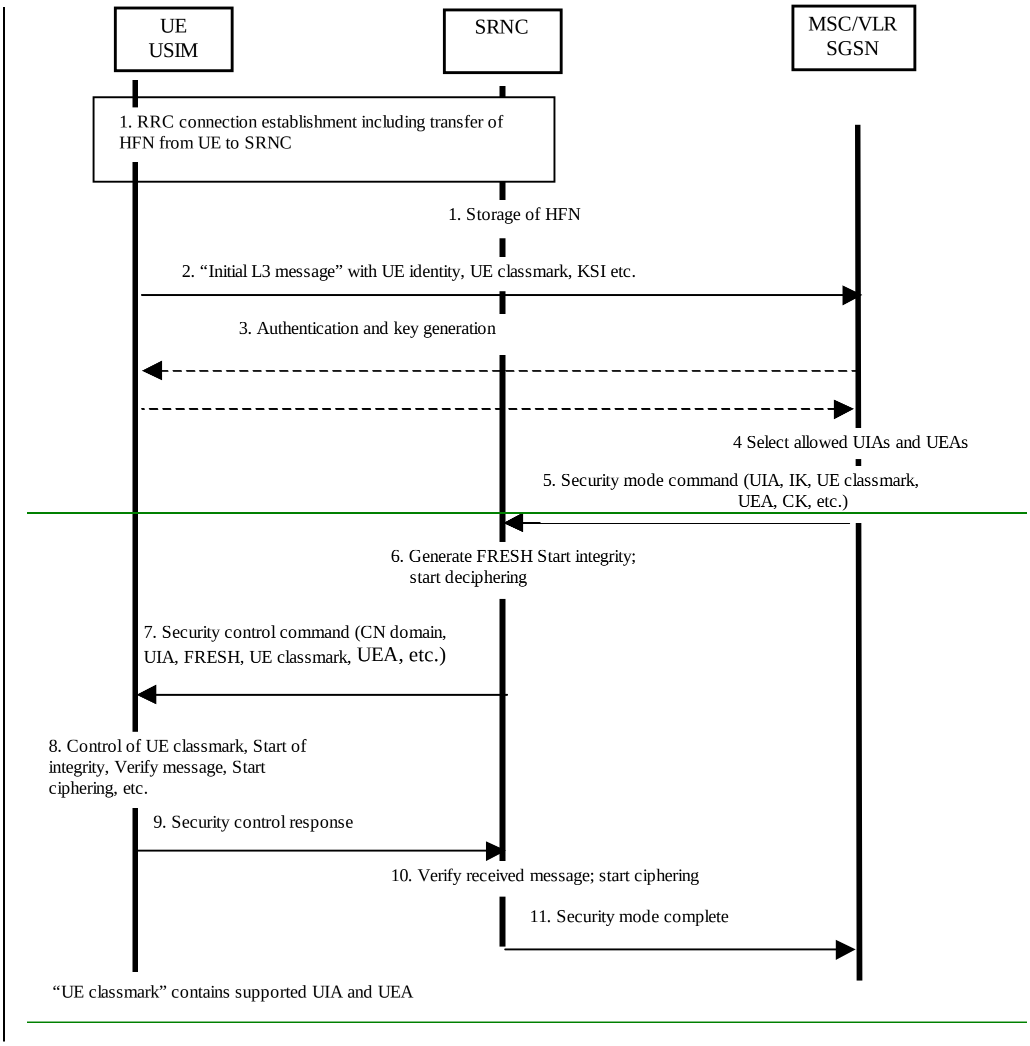
6.4.4 Cipher key and integrity key identification

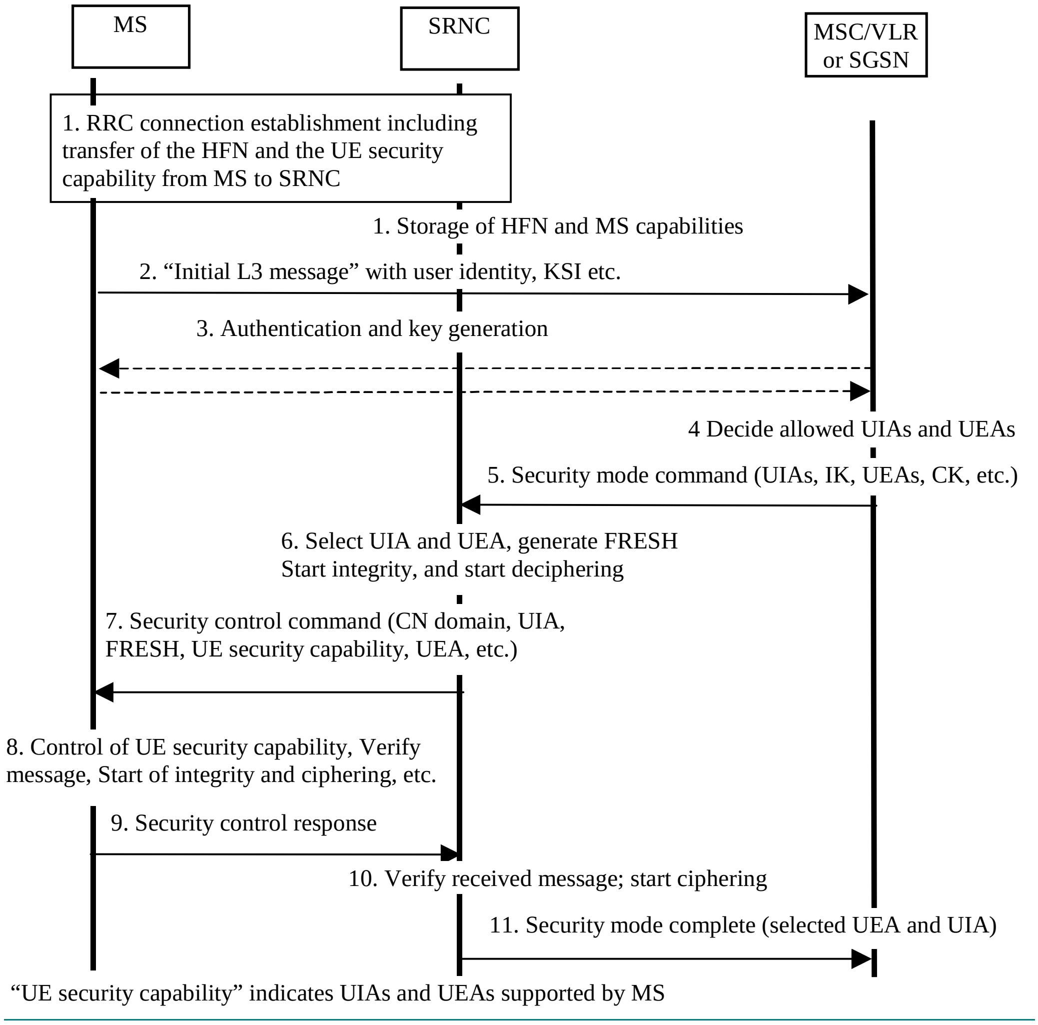
The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. It is stored together with the cipher and integrity keys in the MS and in the network.

The key set identifier is used to allow key re-use during subsequent connection set-ups. The KSI is used to verify whether the MS and the SN are to use the same cipher key and integrity key.

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





Note 1: The network must have the "UE security capability" information~~, which is part of the "UE Classmark",~~ before the integrity protection can start, i.e. the "UE security capability~~Classmark~~" must be sent to the network in an unprotected message. Returning the "UE security capability~~Classmark~~" later on to the ~~UE~~ MS in a protected message will give ~~UE~~ the MS the possibility to verify that it was the correct "UE security capability~~Classmark~~" that reached the network.
This latter point, as well as the RRC interwork described below, is yet to be agreed in RAN WG2.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from ~~UE~~ MS to RNC of the "UE security capability" and the hyperframe number to be used as part of one of the input parameters for the integrity algorithm and for the ciphering algorithm. The COUNT-I parameter (together with COUNT which is used for ciphering) is stored in the SRNC.

2. The ~~UE~~ MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the relevant CN domain. This message contains relevant MM information e.g. the KSI. ~~and the UE classmark IE, which includes information on the UIA(s) and UEA(s) supported by the UE.~~ The KSI (Key Set Identifier) is the number allocated by the CN at the last authentication for this CN domain.

3. Authentication of the user and generation of new security keys (IK and CK) may be performed. A new KSI will then also be allocated.

4. The CN node determines which UIAs and UEAs that are allowed to be used.

5. The CN initiates integrity (and possible also ciphering) by sending the RANAP message Security Mode Command to SRNC. This message contains a list of allowed UIAs and the IK to be used. It may also

contain the allowed UEAs and the CK to be used. ~~This message contains also the UE classmark IE to be sent transparently to the UE.~~

6. The SRNC decides which algorithms to use by selecting, from the list of allowed algorithms, the first UEA and the first UIA that both the MS and SRNC supports. ~~it supports from the list.~~The SRNC generates a random value FRESH and initiates the downlink integrity protection. If SRNC supports no UIA algorithms in the list, it sends a SECURITY MODE REJECT message to CN.

7. The SRNC generates the RRC message Security control command. The message includes the ~~UE classmark Ie~~"UEsecurity capability", the UIA and FRESH to be used and possibly also the UEA to be used. Additional information (start of ciphering) may also be included. Since we have two CNs with an IK each, the network must indicate which IK to use. This is obtained by including a CN type indicator information in "Security control command". Before sending this message to the ~~UE~~MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security control command message, the ~~UE~~ MS controls that the ~~UE classmark IE~~"UE security capability" received is equal to the ~~UE classmark IE~~"UE security capability" sent in the initial message. The UE computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The ~~UE~~ MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the ~~UE~~ MS compiles the RRC message Security control command response and generates the MAC-I for this message. If any control is not successful, a SECURITY CONTROL REJECT message is sent from the ~~UE~~ MS.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the CN node ends the procedure.

The Security mode command to ~~UE~~ MS starts the downlink integrity protection, i.e. also all following downlink messages sent to the ~~UE~~ MS are integrity protected and possibly ciphered. The Security mode command response from ~~UE~~ MS starts the uplink integrity protection and possible ciphering, i.e. also all following messages sent from the ~~UE~~ MS are integrity protected and possibly ciphered.

3GPP TSG SA WG3 (Security) meeting #8 **Tdoc S3-99459**

Sophia Antipolis, 16-19 November, 1999

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**	**022 r1**	Current Version:	3.2.0

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

For submision to TSG SA#6 for approval **X** (*only one box should be marked with an X*)
list TSG meeting no. here ↑ for information

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 **X** UTRAN **X** Core Network **X**
(at least one should be marked with an X)

Source:	TSG SA WG3
Date:	1999-11-18
Subject:	Refinement of Enhanced User Identity Confidentiality
3G Work item:	Enhanced User Identity Confidentiality

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: Refinement and clarification of enhanced user identity confidentiality mechanism

Clauses affected: 6.2; Annex B

Other specs affected:			
Other 3G core specifications	X	→ List of CRs:	33.103CR001r1
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.

6.2 Identification by a permanent identity

The mechanism described in here allows the identification of a user on the radio path by means of the permanent user identity (IMUI).

The mechanism should be invoked by the serving network whenever the user cannot be identified by means of a temporary identity. In particular, it should be used when the user registers for the first time in a serving network, or when the serving network cannot retrieve the IMUI from the TMUI by which the user identifies itself on the radio path.

The mechanism is illustrated in Figure 3.

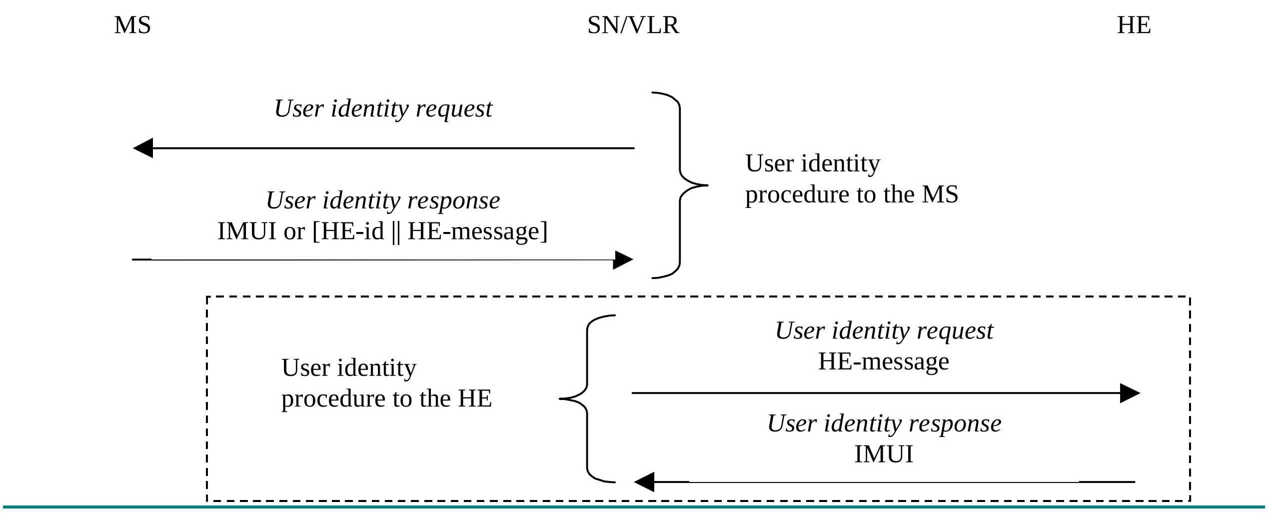


Figure 3: Identification by the permanent identity

The mechanism is initiated by the visited SN/VLR that requests the user to send its permanent identity. According to the user's preferences, his response may contain either 1) the IMUI in cleartext, or 2) the user's HE-identity in cleartext and an HE-message that contains an encrypted IMUI.

~~Note: ~~The term HE-id denotes ~~the 3G equivalent of the information contained in MCC || MNC.~~an expression which is sufficient to route the User identity request message to an appropriate network element of the HE. Annex B contains a proposal to use MCC, MNC and the first three digits of the user's MSIN as routing information to address an HE/HLR.

In case the response contains the IMUI in cleartext, the procedure is ended successfully. This variant represents a breach in the provision of user identity confidentiality.

In case the response contains an encrypted IMUI, the visited SN/VLR forwards the HE message to the user's HE in a request to send the user's IMUI. The user's HE then derives the IMUI from the HE-message and sends the IMUI back to the SN/VLR. Annex B describes an example mechanism that makes use of group keys to encrypt the IMUI.

Annex B (Informative): Enhanced user identity confidentiality

This mechanism allows the identification of a user on the radio access by means of the permanent user identity encrypted by means of a group key. The mechanism described here can be used in combination with the mechanism described in 6.2 to provide user identity confidentiality in the event that the user not known by means of a temporary identity in the serving network.

The mechanism assumes that the user belongs to a user group with group identity GI. Associated to the user group is a secret group key GK_{GI} which is shared between all members of the user group and the user's HE/HLR, and securely stored in the USIM and in the HE/HLR.

The mechanism is illustrated in Figure B.1.

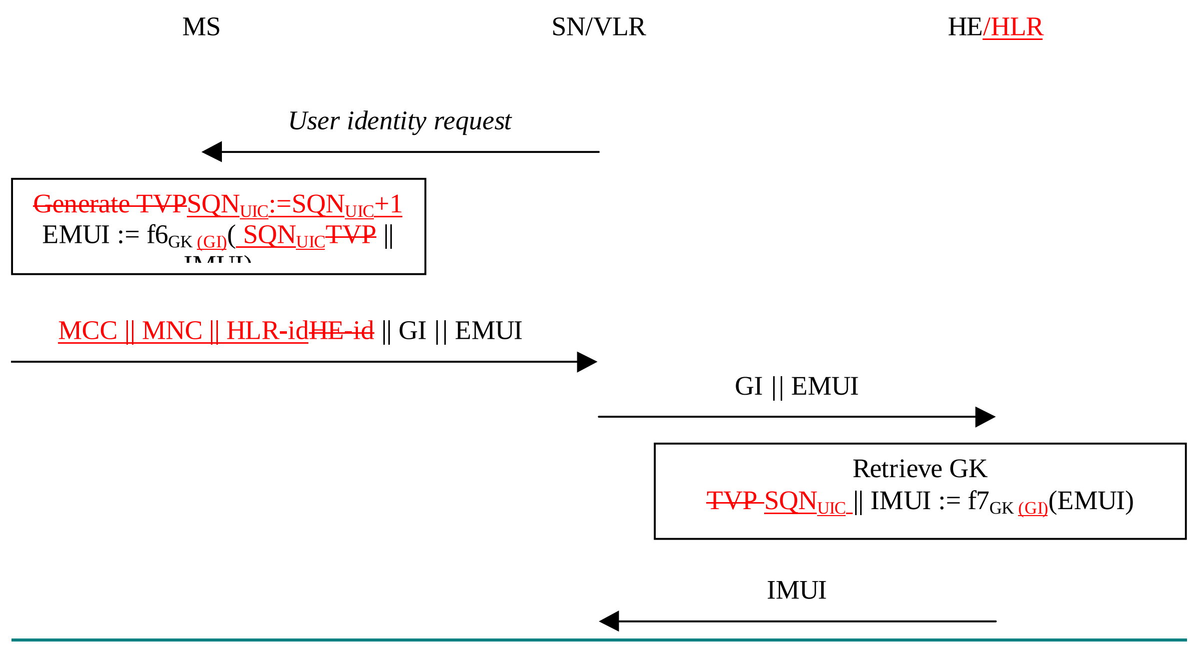


Figure B.1: Identification by means of the IMUI encrypted by means of a group key

The user identity procedure is initiated by the visited SN/VLR. The visited SN/VLR requests the user to send its permanent user identity.

Upon receipt the user increments SQN_{UIC}~~generates~~ as a time variant parameter TVP. The user encrypts SQN_{UIC} ~~the time variant parameter TVP~~ and the IMUI with enciphering algorithm f6 and his group key GK_{GI}. The SQN_{UIC}~~TVP~~ prevents traceability attacks. The user sends a response to the SN/VLR that includes MCC||MNC||HLR-id and the first three digits of the user's MSIN and identifies an HLR within the core network.~~the HE identity, the group identity GI and the encrypted mobile user identity (EMUI).~~

Note: Alternatives are:

- to define a single network element within each HE which performs all de~~en~~cryption related to EMUI or
- that all gateways ;MSCs are able to decrypt EMUI and route the message to the correct HLR.

Upon receipt of that response the SN/VLR should resolve the user's HE/HLR address from MCC||MNC||HLR-id ~~HE-identity~~ and forwards the group identity GI and the user's EMUI to the user's HE/HLR.

Upon receipt the HE/HLR retrieves the group key GK_{GI} associated with the group identity GI. The HE/HLR then decrypts EMUI with the deciphering algorithm f7 ($f7 = f6^{-1}$) and the group key GK and retrieves SQN_{UIC}~~TVP~~ and IMUI. SQN_{UIC} is no longer used. The HE/HLR ~~then~~ sends the IMUI in a response to the visited SN/VLR.

3GPP/SMG Meeting TSG SA WG3#9
Helsinki,Finland, 99-12-07/09

***Document* S3-99520**
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**	**041**	Current Version:	3.2.0

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

For submission to:		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: S3   **Date:** 1999-12-03

Subject: UIA and UEA identifications

Work item: Security

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

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

Release:

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

Reason for change:
a) Clarification needed regarding the UIA and UEA identifications.
b) Inclusion of "No encryption" as one option in the list of UEAs. This to be in line with chapter 6.4.2 in 33.102 where following text can be found:
" 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."

Clauses affected: 6.5.3, 6.6.3

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.

6.5.3 UIA identification

Each UIA will be assigned a 4-bit identifier.

Table1 - UIA identification

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

Note: For R99, only the value 0000_2 (UIA1) is applicable. All other UIA identification values, given in the table above, shall be seen as examples.

6.6.3 UEA identification

Each UEA will be assigned a 4-bit identifier.

Table 2 – UEA identification

Information Element	Length	Value	Remark
UEA Number	4	0000_2	~~Standard UMTS Encryption Algorithm, UEA1~~Value used to indicate “No encryption”
		0001_2	Standard UMTS Encryption Algorithm, ~~UEA2~~UEA1
		0010_2	Standard UMTS Encryption Algorithm, ~~UEA3~~UEA2
		0011_2 to 0111_2	Reserved for future expansion
		$1xxx_2$	Proprietary UMTS Algorithms

Note: For R99, only the values 0000_2 (“No encryption”) and 0001_2 (UEA1) are applicable. All other UEA identification values, given in the table above, shall be seen as examples.

3GPP/SMG Meeting TSG SA WG3#9
Helsinki,Finland, 99-12-07/09

Document S3-99528
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 38 Current Version: 3.2.0

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

For submission to: SA#6 — for approval [X] — for information [ ] — strategic [ ] — Non-strategic [ ] *(for SMG use only)*

list expected approval meeting # here ↑

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 [ ]
(at least one should be marked with an X)

Source: S3 **Date:** 1999-12-08

Subject: Clarification on system architecture

Work item: Security

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

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

Release:

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

Reason for change: The UMTS system architecture with respect to the PS and CS domains is introduced in order to clarify access security procedures and mechanisms

Clauses affected: 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.

4 Overview of the security architecture

Figure 1 gives an overview of the complete 3G security architecture.

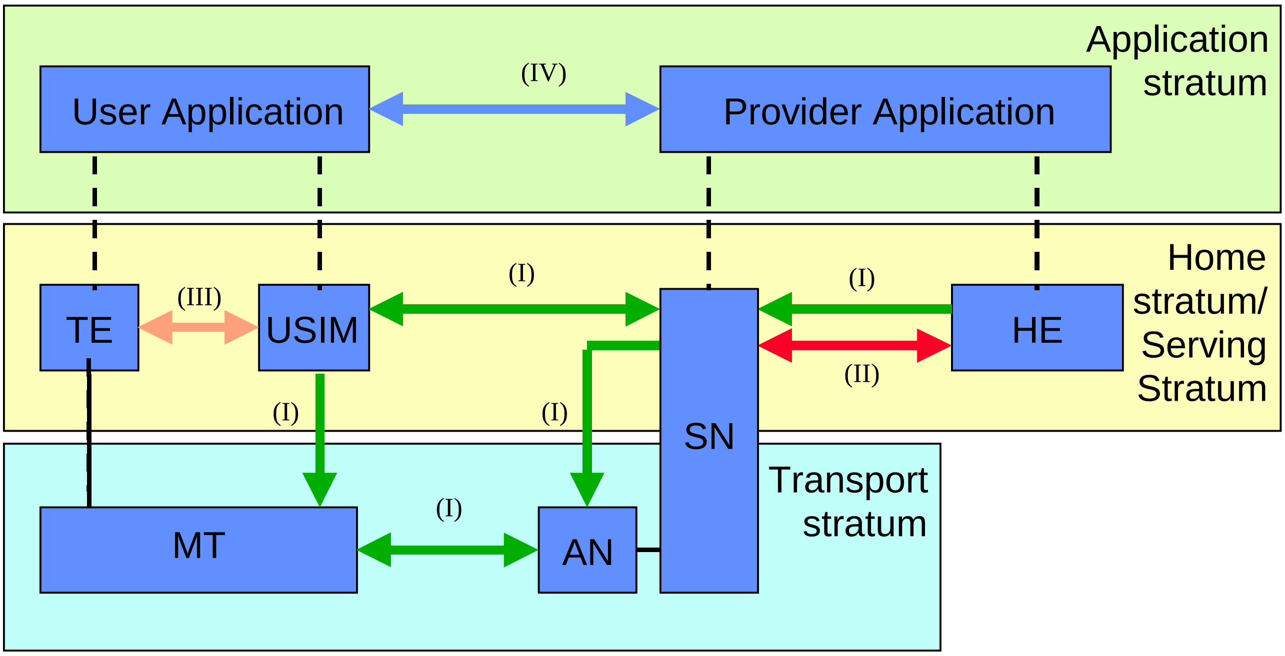


Figure 1 : Overview of the security architecture

Five security feature groups are defined. Each of these feature groups meets certain threats, accomplishes certain security objectives:

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security (III):** the set of security features that secure access to mobile stations
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security features is in operation or not and whether the use and provision of services should depend on the security feature.

Figure 2 gives an overview of the UE registration and connection principles within UMTS with a CS service domain and a PS service domain. As in GSM/GPRS, user (temporary) identification, authentication and key agreement will take place independently in each service domain. User plane traffic will be ciphered using the cipher key agreed for the corresponding service domain while control plane data will be ciphered and integrity protected using the cipher and integrity keys from either one of the service domains. ~~in which the most resent authentication and key agreement took place,~~ In clause 6 the detailed procedures are defined and when not otherwise stated they are used in both service domains.

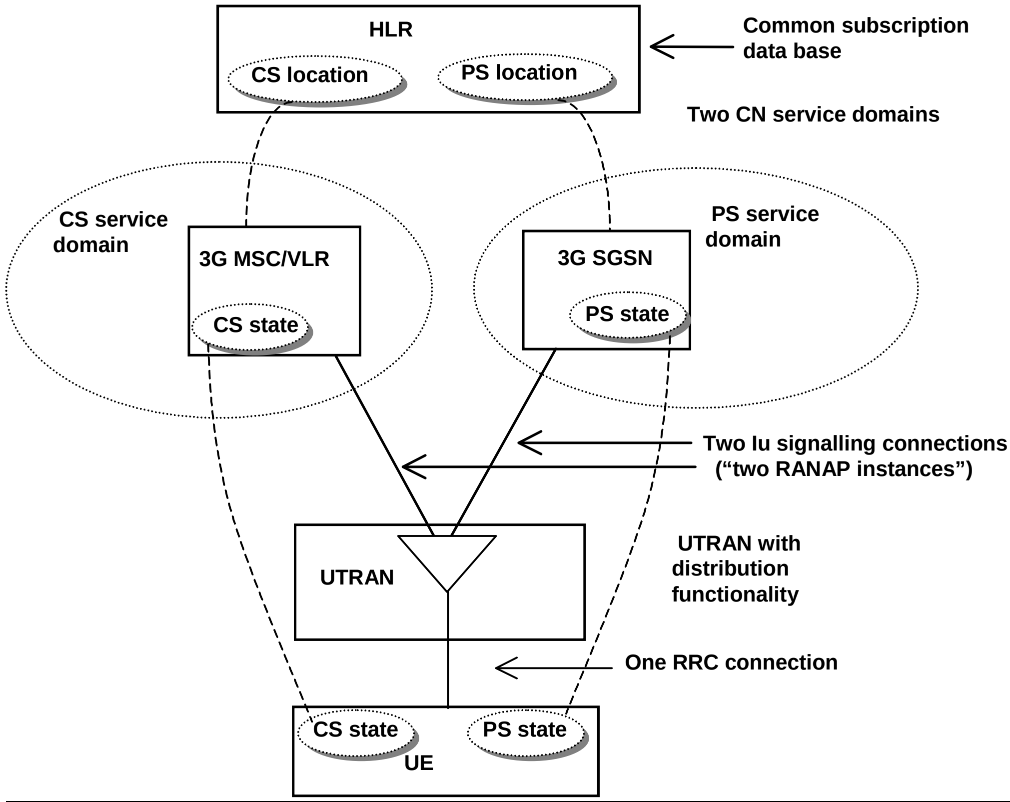


Figure 2: Overview of the UE registration and connection principles within UMTS for the separate CN architecture case when the CN consists of both a CS service domain with evolved MSC/VLR, 3G_MSC/VLR, as the main serving node and an PS service domain with evolved SGSN/GGSN, 3G_SGSN and 3G GGSN, as the main serving nodes, (Extract from RS23.121 – Figure 4-8**)**

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 39 Current Version: 3.2.0

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

For submission to:
list expected approval meeting # here ↑

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

Source: S3 **Date:** 1999-12-03

Subject: Updated definitions and abbreviations

Work item: Security

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

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

Release:

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

Reason for change: Need for additonal definitions and abbreviations chapters.

Clauses affected: 3.1, 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.

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

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

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

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

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

USIM – User Services Identity Module. In a security context, this module is responsible for performing UMTS subscriber and network authentication and key agreement. It should also be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network.

SIM – GSM Subscriber Identity Module. In a security context, this module is responsible for performing GSM subscriber authentication and key agreement. This module is **not** capable of handling UMTS authentication nor storing UMTS style keys.

UMTS Entity a~~A~~uthentication and key agreement:~~:~~ Entity authentication according to this specification.

GSM Entity ~~A~~authentication and key agreement: Entity authentication according to TS ETSI GSM 03.20

User access module: either a USIM or a SIM

Mobile station, user: the combination of user equipment and a user access module.

UMTS subscriber: a mobile station that consists of user equipment with a USIM inserted.

GSM subscriber: a mobile station that consists of user equipment with a SIM inserted.

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends “UMTS security context data” is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI.

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

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

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

Authentication vector: either a quintet or a triplet.

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

~~…. Next Change ….~~

3.3 Abbreviations

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

~~3GMS~~	~~Third Generation Mobile Communication System~~
AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
$D_{SK(X)}$(data)	Decryption of "data" with Secret Key of X used for signing
$E_{KSXY(i)}$(data)	Encryption of "data" with Symmetric Session Key #i for sending data from X to Y
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption
~~SIM~~	~~GSM Subscriber Identity Module~~
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
~~IMUI~~IMSI	International Mobile ~~User~~ Subscriber Identity
IV	Initialisation Vector
KAC_X	Key Administration ~~Center~~ Centre of Network X
KS_{XY}(i)	Symmetric Session Key #i for sending data from X to Y
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAP	Mobile Application Part
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
MS	Mobile Station
MSC	Mobile Services Switching Centre
MT	Mobile Termination
NE_X	Network Element of Network X
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
RND_X	Unpredictable Random Value generated by X
~~SEQ~~SQN	Sequence number
SQN_{UIC}	Sequence number user for enhanced user identity confidentiality
SQN_{HE}	Sequence number counter maintained in the HLR/AuC
SQN_{MS}	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TE	Terminal Equipment
Text1	Optional Data Field
Text2	Optional Data Field
Text3	Public Key algorithm identifier and Public Key Version Number (eventually included in Public Key Certificate)
~~TMUI~~TMSI	Temporary Mobile ~~User~~ Subscriber Identity
TTP	Trusted Third Party
~~TVP~~	~~Time Variant Parameter~~
UE	User equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
~~UN~~	~~User Name~~
USIM	User Services Identity Module
VLR	~~Visited~~ Visitor Location Register
X	Network Identifier

XRES	Expected Response
~~XUR~~	~~Expected User Response~~
Y	Network Identifier

3GPP TSG SA WG 3 (Security) meeting #9 S3-99536
Helsinki, 7—9 December 1999.

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 40 Current Version: V3.2.0

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

For submission to TSG SA#6 for approval [X] for information [ ] *(only one box should be marked with an X)*

list TSG meeting no. here ↑

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 [ ] ME [ ] UTRAN [ ] Core Network [X]
(at least one should be marked with an X)

Source: S3 **Date:** 09-12-99

Subject: An authentication failure report mechanism from SN to HE

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: This CR proposes to add a mechanism for reporting authentications failures from the SN to the HE.

Clauses affected: Section 6.3

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 Authentication and key agreement

6.3.1 General

The mechanism described here achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the AuC in the user's HE. In addition the USIM and the HE keep track of counters SQN_{MS} and SQN_{HE} respectively to support network authentication.

The method was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication derived from the ISO standard ISO/IEC 9798-4 (section 5.1.1).

An overview of the mechanism is shown in figure 4.

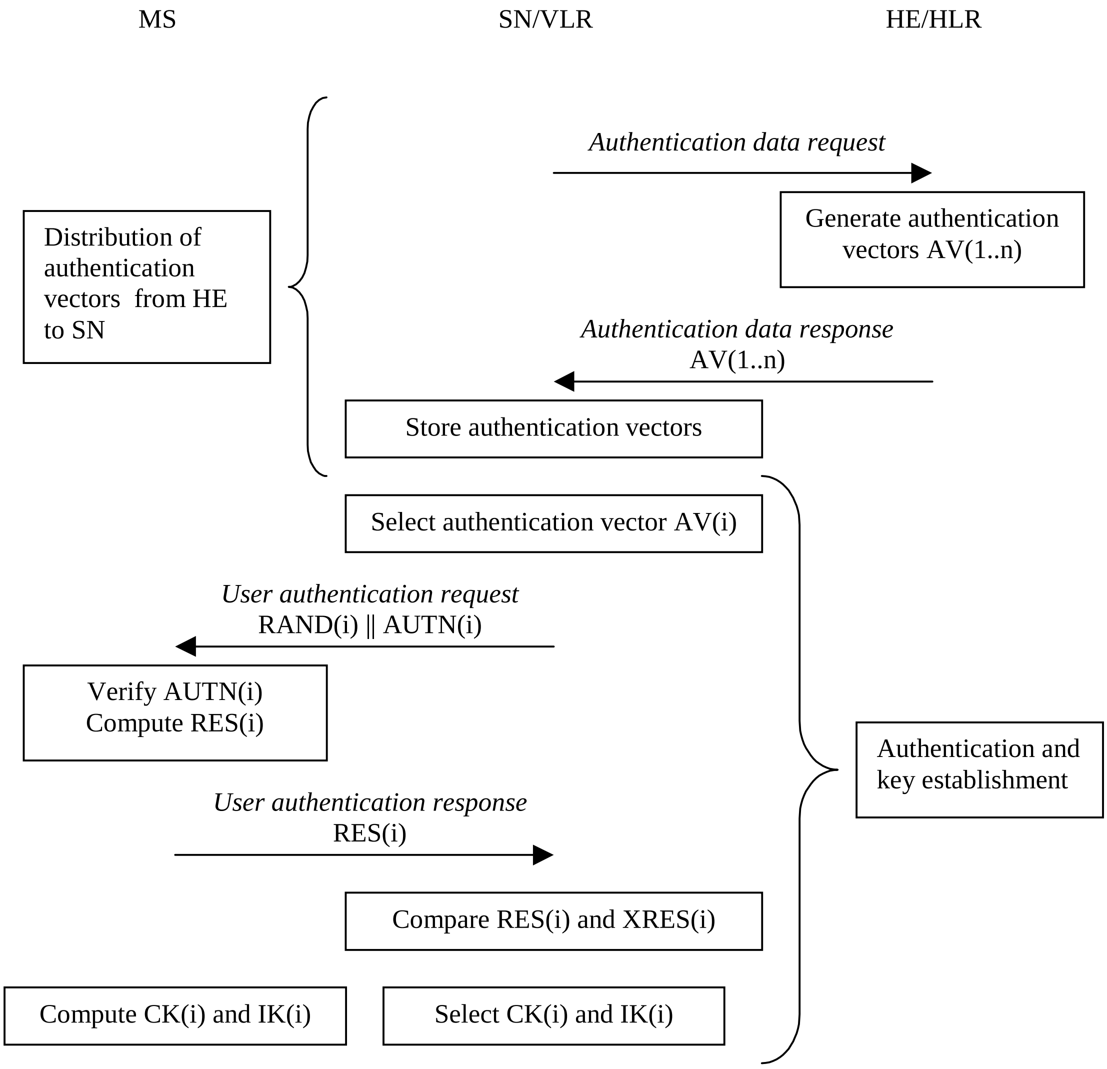


Figure 4: Authentication and key agreement

Upon receipt of a request from the SN/VLR, the HE/AuC sends an ordered array of *n* authentication vectors (the equivalent of a GSM "triplet") to the SN/VLR. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the SN/VLR and the USIM.

When the SN/VLR initiates an authentication and key agreement, it selects the next authentication vector from the array and sends the parameters RAND and AUTN to the user. The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the SN/VLR. The USIM also computes CK and IK. The SN/VLR compares the received RES with XRES. If they match the SN/VLR considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the SN/VLR to the entities which perform ciphering and integrity functions.

SN/VLRs can offer secure service even when HE/AuC links are unavailable by allowing them to use previously derived cipher and integrity keys for a user so that a secure connection can still be set up without the need for an authentication and key agreement. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signalling messages (see 6.4).

The authenticating parties shall be the AuC of the user's HE (HE/AuC) and the USIM in the user's mobile station. The mechanism consists of the following procedures:

A procedure to distribute authentication information from the HE/AuC to the SN/VLR. This procedure is described in 6.3.2. The SN/VLR is assumed to be trusted by the user's HE to handle authentication information securely. It is also assumed that the intra-system links between the SN/VLR to the HE/AuC are adequately secure. Mechanisms to secure these links are described in clause 7. It is further assumed that the user trusts the HE.

A procedure to mutually authenticate and establish new cipher and integrity keys between the SN/VLR and the MS. This procedure is described in 6.3.3.

A procedure to distribute authentication data from a previously visited VLR to the newly visited VLR. This procedure is described in 6.3.4. It is also assumed that the links between SN/VLRs are adequately secure. Mechanisms to secure these links are described in clause 7.

6.3.2 Distribution of authentication data from HE to SN

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

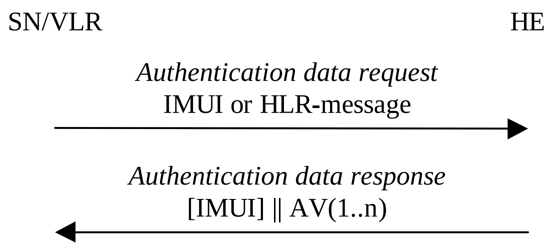


Figure 5: Distribution of authentication data from HE to SN/VLR

The SN/VLR 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 SN/VLR 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 SN/VLR, 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 SN/VLR that contains an ordered array of n authentication vectors AV(1..n).

Figure 6 shows the generation of an authentication vector AV by the HE/AuC.

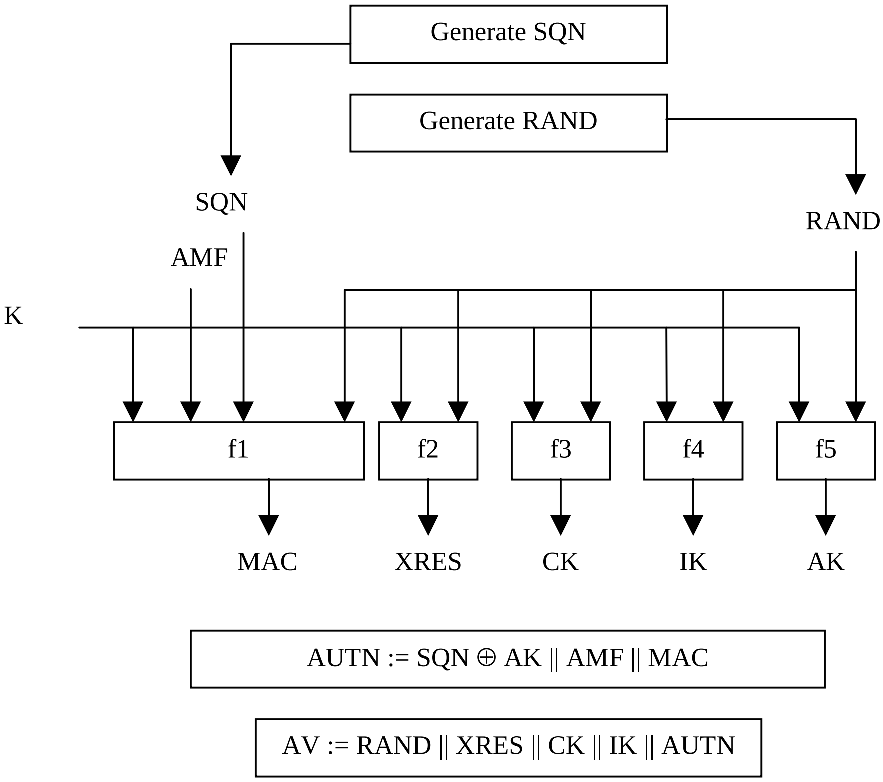


Figure 6: Generation of an authentication vector

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}

To generate a fresh sequence number, the counter is incremented and subsequently the SQN is set to the new counter value.

Note 1: The HE has some flexibility in the management of sequence numbers. Annex C and Annex F.3 contain alternative methods for the generation and verification of sequence numbers.

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.

Finally the authentication token AUTN = SQN ⊕ 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.

Note 1: The need for f5 to use a long-term key different from K is ffs.

Note 2: The requirements on f3, f4 and f5 are ffs.

Note 3: It is also ffs in how far the functions f1, ..., f5 need to differ and how they may be suitably combined.

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 SN/VLR and the MS. During the authentication, the user verifies the freshness of the authentication vector that is used.

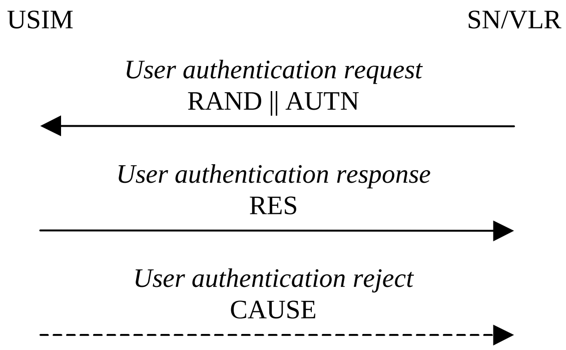


Figure 7: Authentication and key establishment

The SN/VLR invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR database. The SN/VLR 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 8.

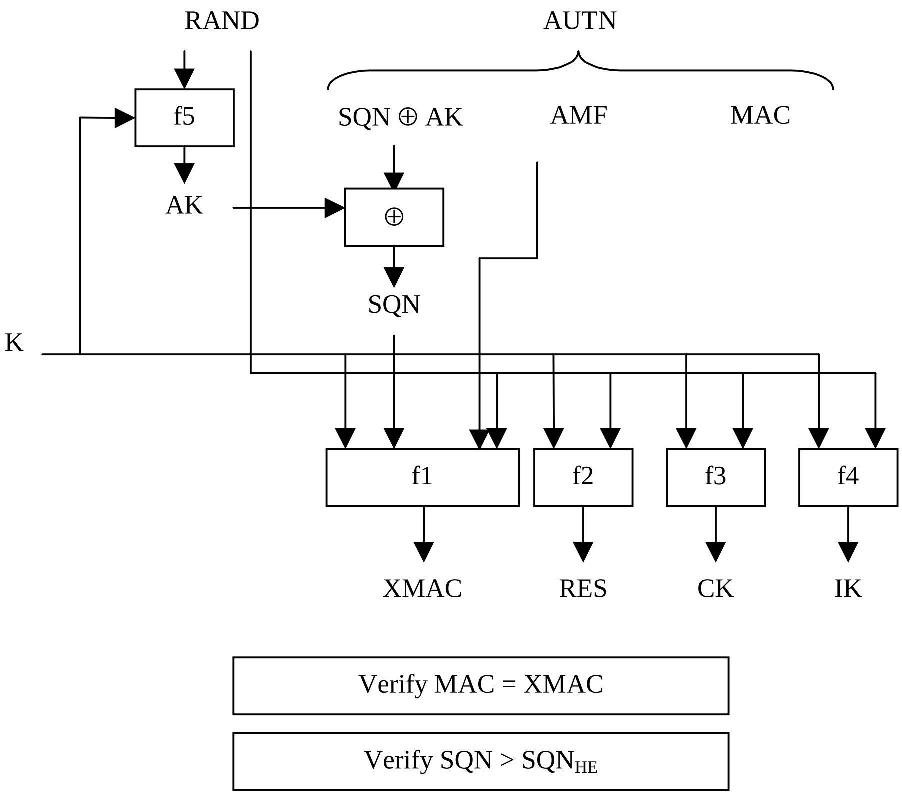


Figure 8: User authentication function in the USIM

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 SN/VLR with an indication of the cause and the user abandons the procedure.

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

The USIM keeps track of a counter: SQN_{MS}.

To verify that the sequence number SQN is in the correct range, the USIM compares SQN with SQN_{MS}. If SQN > SQN_{MS} the MS considers the sequence number to be in the correct range and subsequently sets SQN_{MS} to SQN.

Note: The MS and the HE have some flexibility in the management of sequence numbers. Annex C and Annex F.3 contain alternative methods for the generation and verification of sequence numbers.

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

The *synchronisation failure* message contains the parameter $RAND_{MS}$ || *AUTS.*
Here $RAND_{MS}$ is the random value stored on the MS which was received in user authentication request causing the last update of SQN_{MS} .
It is $AUTS = Conc(SQN_{MS}) \| MACS$.
$Conc(SQN_{MS}) = SQN_{MS} \oplus f5_K(RAND_{MS})$ is the concealed value of the counter SQN_{MS} in the MS, and.
$MACS = f1^*_K(SQN_{MS} \| RAND \| AMF)$ 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 9:

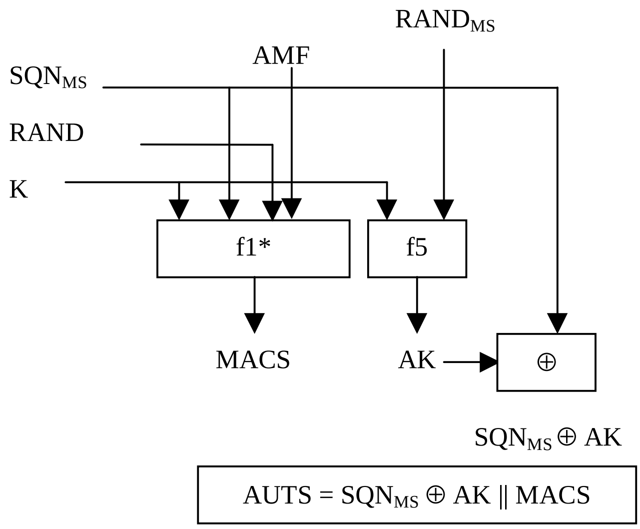


Figure 9: Construction of the parameter AUTS

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 SN/VLR. 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 SN/VLR 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 SN/VLR 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 SN/VLR: Using the procedures described in subsections 6.3.1, 6.3.2 and 6.3.4, authentication vectors will have to be used in the specific order in which they were generated, otherwise the user will reject the authentication attempt. The SN/VLR shall use an authentication vector 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 authentication vectors cannot be reused. When a user changes from one VLR to another one and the new VLR requests remaining authentication vectors from the old VLR (cf. subsection 6.3.4) then the old VLR shall not retain any copies of these authentication vectors. When a VLR receives a “cancel location” request for a certain user it shall delete all authentication vectors relating to that user. When a VLR receives a location update request from a user and the VLR notices that authentication vectors relating to that user are still stored in the VLR it will delete this information and request fresh authentication vectors from the HE/AuC.

Different rules may apply when one of the alternative schemes for sequence number handling described in Annex C or Annex F.3 are applied. This is true in particular when the schemes based on windows or lists described in Annexes C.3 and C.4 are applied.

6.3.3.1 Cipher key selection

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

6.3.3.1.1 User plane

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

6.3.3.1.2 Control plane

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

6.3.4 Distribution of authentication vectors between VLRs

The purpose of this procedure is to provide a newly visited VLR with unused authentication vectors from a previously visited VLR.

The procedure is shown in Figure 10.

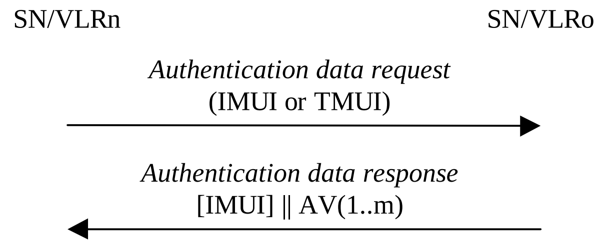


Figure 10: Distribution of authentication data between SN/VLR

The procedure is invoked by the newly visited SN/VLRn after a *location update request* sent by the user. Typically the user identifies himself using a temporary user identity TMUIo and the location area identity LAIo of a location area under the jurisdiction of SN/VLRo. In that case this procedure is integrated with the procedure described in 6.1.4.

Upon receipt of the request the VLRo verifies whether it has any unused authentication vectors of the appropriate mode in its database and if so, sends the unused authentication vectors to VLRn. The previously visited VLRo shall then delete these authentication vectors from its database.

Upon receipt the VLRn stores the received authentication vectors.

If VLRo indicates that it has no authentication vectors or the VLRo cannot be contacted, VLRn should request new authentication vectors from the user's HE using the procedure described in 6.3.2.

6.3.5 Re-synchronisation procedure

An SN/VLR may send two types of *authentication data requests* to the HE/AuC, the (regular) one described in subsection 6.3.2 and one used in case of synchronisation failures, described in this subsection.

Upon receiving a *synchronisation failure* message from the user, the SN/VLR sends an *authentication data request* with a "*synchronisation failure indication*" to the HE/AuC, together with the parameters

- *RAND* sent to the MS in the preceding user authentication request and
- $RAND_{MS}$ || *AUTS* received by the SN/VLR in the response to that request, as described in subsection 6.3.3.

An SN/VLR will not react to unsolicited " synchronisation failure indication" messages from the MS.

The SN/VLR does not send new user authentication requests to the user before having received the response to its authentication data request from the HE/AuC (or before it is timed out).

When the HE/AuC receives an *authentication data request* with a "*synchronisation failure indication*" it acts as follows: The HE/AuC verifies *AUTS* by computing $f5_K(RAND_{MS})$, retrieving SQN_{MS} from Conc(SQN_{MS}) and verifying *MACS* (cf. subsection 6.3.3.). If the verification is successful, but SQN_{MS} is such that SQN_{HE} is not in the correct range then the HE/AuC resets the value of the counter SQN_{HE} to SQN_{MS}.
Otherwise, the HE/AuC leaves SQN_{HE} unchanged.

In all cases the HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the SN/VLR. If the counter SQN_{HE} was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting SQN_{HE}. In order to reduce the real-time computation burden on the HE/AuC, the HE/AuC may also send only a single authentication vector in the latter case.

Whenever the SN/VLR receives a new batch of authentication vectors from the HE/AuC in an authentication data response it deletes the old ones for that user in the VLR.

The user may now be authenticated based on a new authentication vector from the HE/AuC.
Optionally, in order to minimise extra effort by the HE/AuC, in an authentication data request with synchronisation failure indication the SN/VLR may also send the concealed sequence number Conc(SQN_{SN}) corresponding to the last authentication vector received which the SN/VLR has in storage, i.e. it may send Conc(SQN_{SN}) = $RAND_{SN} \| SQN_{SN} \oplus f5_K(RAND_{MS})$.

On receipt the HE/AuC retrieves SQN_{SN} from Conc(SQN_{SN}). If the counter in the HE/AuC did not have to be reset and if $SQN_{SN} = SQN_{HE}$ the HE/AuC informs the SN/VLR accordingly and does not send fresh authentication vectors. (In this way, a synchronisation failure does not cause the HE/AuC to produce extra authentication vectors when they are not needed.)

Figure 11 shows how re-synchronisation is achieved by combining a *user authentication request* answered by a *synchronisation failure* message (as described in subclause 6.3.3) with an *authentication data request* with *synchronisation failure* indication answered by an *authentication data response* (as described in this subclause).

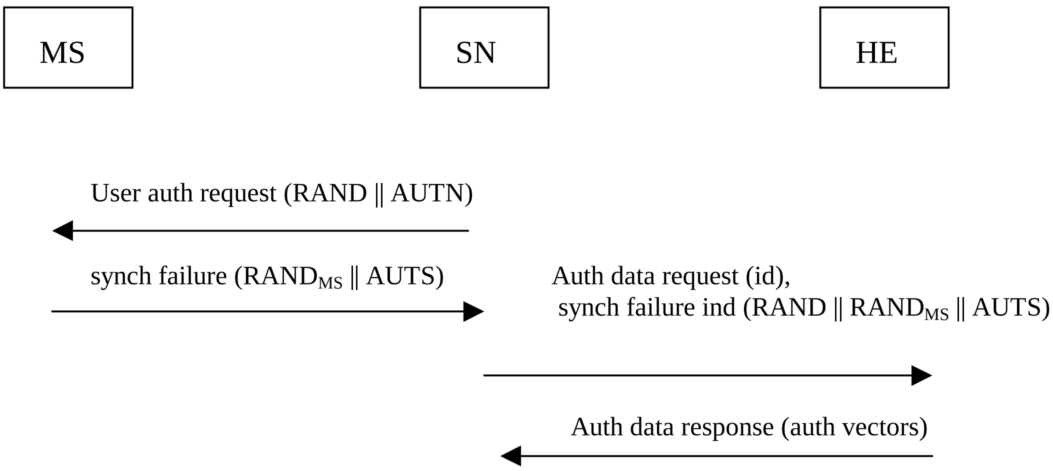


Figure 11: Re-synchronisation procedure

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 12.

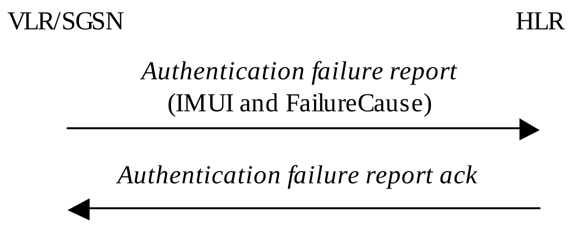


Figure 12: Reporting authentication failure from VLR/SGSN to HLR

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*.

6.3.7~~6~~ Length of sequence numbers

Sequence numbers shall be sufficiently long so that they cannot wrap around during the lifetime of the system. Consequently, in normal operations neither SQN_{MS} nor SQN_{HE} can wrap around during the lifetime of a USIM.

Note 1: If the counters would derive sequence numbers from time (see Annex C), then a 32-bit counter that is derived from the number of seconds that have elapsed since January 1, 2000 would only wrap around in the year 2136. So a length of 32-bits for the sequence numbers and counters should be sufficient. For individual incremental counters, a smaller range of sequence numbers should be sufficient, as authentication and key agreement is expected to occur far less frequently than once every second. Shorter lengths would however exclude the use of time-derived sequence numbers.

Note 2: Sequence numbers for CS and PS operation are expected to have the same length.

6.3.8~~7~~ Support for window and list mechanisms

In Annex C.3 and Annex C.4 respectively, the window and list mechanisms for sequence number management in the USIM are described. If one of these mechanisms is employed in the USIM and if there is no need to conceal sequence numbers then the MS shall send information on the current value of the lowest entry SQN_{LO} in the window or list to the SN/VLR at every location update. Sequence numbers which do not need to be concealed may be generated according to Annex C.2 or Annex C.6.

When the SN/VLR authenticates a user for the first time after receiving a new value SQN_{LO} from the MS then the SN/VLR checks whether the sequence number of the authentication vector it wants to use is greater than SQN_{LO}. The SN/VLR uses the AV only if this is the case. Otherwise, the AV is discarded. If all AVs have to be discarded the SN/VLR requests new ones from the HE/AuC.

3GPP TSG SA WG 3 (Security) meeting #9 S3-99538
Helsinki, 7—9 December 1999.

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 35 Current Version: V3.2.0

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

For submission to TSG SA#6 for approval X for information *(only one box should be marked with an X)*

list TSG meeting no. here ↑

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 X
(at least one should be marked with an X)

Source: S3 **Date:** 1999-Dec-09

Subject: Authentication and key agreement

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: Remove option no longer needed, add parameter to be managed

Clauses affected: Annex F

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.

Annex F (Informative): Example uses of AMF

F.1 Support multiple authentication algorithms and keys

A mechanism to support the use of multiple authentication and key agreement algorithms is useful for disaster recovery purposes. AMF may be used to indicate the algorithm and key used to generate a particular authentication vector.

The USIM keeps track of the authentication algorithm and key identifier and updates it according to the ~~received~~ value received in an accepted network authentication token.

~~.~~

F.2 Changing ~~the size of windows and~~ list~~s~~ parameters

This mechanisms is used in conjunction with the ~~window and~~ list mechanism~~s~~ described in Annex~~es~~ C.2~~3 and C.4~~.

Parameters which may be used to manage a list are the number of entries in a list (the list size) and an upper limit on the admissible difference SEQ_{MS} - SEQ between the highest batch number SEQ_{MS} in the list and an accepted batch number SEQ. A mechanism to change ~~the window and list size~~these parameters dynamically is useful since the optimum ~~window and list size~~for these parameters may change over time. AMF is used to indicate the maximum admissible ~~window or~~ list size or maximum admissible difference SEQ_{MS} - SEQ to be used by the user when verifying the authentication token and deciding whether it is still accepted.

The USIM keeps track of the maximum admissible list size and maximum admissible difference SEQ_{MS} - SEQ ~~the window or list size~~ and updates ~~it~~ them according to the ~~received~~ value received in an accepted network authentication token providing that $SEQ > SEQ_{MS}$. ~~SQN > SQN_{MS}.~~

~~F.3 Handling authentication vectors from separate CS/PS domains using a MODE parameter~~

~~A mechanism to distinguish authentication vectors from different CS/PS domains is useful so that separate CS/PS nodes can simultaneously and independently support mobility management for the user. AMF is used to indicate the domain associated with a particular authentication vector. Using this mechanism two counters are required for each domain in both the USIM and the AuC.~~

> ~~Note: If a single counter was used, the following problem occurs: Suppose that a CS node orders SQNs 1–5, and uses SQN 1 and then a PS node orders SQNs 6–10 and uses 6. At this point the CS node may need to use SQN 2, but cannot since the SQN will be rejected and must order new authentication vectors, with SQNs 11–15, and authenticates with SQN 11. Maintaining separate counters for CS and PS domains provide a solution for this problem.~~

~~An alternative to the use of the MODE parameter is the use of the window or list mechanism described in Annexes C3. and C.4.~~

F.3 Setting threshold values to restrict the life time~~s~~ of cipher and integrity keys

According to section 6.4.3, the USIM contains a mechanism to limit the amount of data that is protected by an access link key set. The AMF field may be used by the operator to set or adjust this limit in the USIM. For instance, there could be two threshold values and the AMF field instructs the USIM to switch between them.

The USIM keeps track of the limit to the key set life time and updates it according to the value received in an accepted network authentication token.

3GPP TSG SA WG 3 (Security) meeting #9 S3-99539
Helsinki, 7—9 December, 1999.

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 36 Current Version: V3.2.0

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

For submission to TSG SA#6 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 X
(at least one should be marked with an X)

Source: S3 **Date:** 1999-Dec-09

Subject: Sequence number management

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: The current version 3.2.0 of TS 33.102 contains several options for sequence number management. Some of these options are deleted as they are not needed, others are slightly enhanced.

Clauses affected: Annex C

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.

Annex C (Informative): Management of sequence numbers

This annex is devoted to the management of sequence numbers for the authentication and key agreement protocol.

~~C.1 A mechanism using two individual counters on each side~~

~~This is the mechanism included in the main body of this specification.~~

~~C.2 A mechanism using a global counter in the HE and two counters in the MS~~

~~In this mechanism the HLR/AuC keeps track of time, while the USIM keeps track of a counters for PS mode $SQN_{MS/PS}$ and a counter for CS mode $SQN_{MS/CS}$.~~

~~The HLR/AuC may for instance use as a sequence number the number of seconds t that have elapsed since the start of the year 2000 (GMT). Then, a 32-bit sequence number will suffice for 136 years of operation. When an array of n authentication vectors is generated, the values t, t+1, …, t+n-1 could be used.~~

~~At the user end, SQN is treated as in the mechanism described under C.1.~~

~~Note 1: When using a time-value to generate sequence numbers it may not be necessary to conceal the sequence number to avoid user identification.~~

~~Note 2: The re-synchronisation procedure is not required in this case, as time can be recovered from any source.~~

~~C.3 A mechanism using one individual counter in the HE and a window in the USIM~~

~~In this mechanism the sequence numbers are generated as in the mechanism described in C.1. However, the USIM verifies the freshness differently. In addition to the highest sequence number SQN_{MS} it has accepted, it keeps track of which values in a window [SQN_{MS} – w, SQN_{MS}) it has already accepted... If a sequence number is received that is higher than SQN_{MS} – w and has not been accepted before, it is accepted and the window is updated accordingly.~~

~~Using this mechanism, it is not required that a previously visited SN/VLR deletes the unused authentication vectors when a user de-registers from the serving network. Retaining the authentication vectors for use when the user returns later may be more efficient as regards signalling when a user abroad switches a lot between two serving networks.~~

~~Note: When a VLR uses fresh authentication vectors obtained during a previous visit of the user, the USIM can reject them although they have not been used before (because w is finite). Rejection of a sequence number can therefore occur in normal operation, i.e., it is not necessarily caused by (malicious) replay or a database failure.~~

~~C.4 A mechanism using a (partly) global counter in the HE and a list in the USIM~~

~~In this mechanism the sequence numbers are generated with one of the mechanisms described in C.2 and in C.6. However, the USIM verifies the freshness differently. Instead of keeping track of the highest sequence number SQN_{MS} only, it keeps track of an ordered list of the b highest values it has accepted,. If a sequence number is received that is lower than or equal to the lowest value SQN_{LO} in that list, it is rejected. If however, a sequence number is received that is higher than the lowest entry in the list, but is not in the list it is accepted and included in the list. The lowest value SQN_{LO} in the list is then deleted.~~

~~Using this mechanism, it is not required that a previously visited SN/VLR deletes the unused authentication vectors when a user de-registers from the serving network. Retaining the authentication vectors for use when the user returns later may be more efficient as regards signalling when a user abroad switches a lot between two serving networks.~~

> ~~Note: When a VLR uses fresh authentication vectors obtained during a previous visit of the user, the USIM can reject them although they have not been used before (because b is finite). Rejection of a sequence number can therefore occur in normal operation, i.e., it is not necessarily caused by (malicious) replay or a database failure.~~

~~C.5 A mechanism using two individual counters on each side offering protection against wrap around of counters~~

~~The basic idea of the alternative sequence number handling is that the MS will not accept arbitrary jumps in sequence numbers. The sequence number *SQN* is accepted by the MS if and only if the following holds for some Δ:~~

~~$SQN > SQN_{MS}$ (as for alternative C.1) and $SQN - SQN_{MS} < \Delta$.~~

~~This means that SQN_{MS} can reach its maximum value only after a minimum of $SQNmax/\Delta$ successful authentications have taken place.~~

~~Conditions on Δ :~~

~~(1) Δ shall be sufficiently large so that the MS will not receive any SQN with $SQN - SQN_{MS} \geq \Delta$ if the HE/AuC functions correctly.~~

~~(2) $SQNmax / \Delta$ shall be sufficiently large to prevent that SQN_{MS} ever reaches $SQNmax$ during the lifetime of the USIM.~~

~~C.6 A generalised scheme for sequence number management~~

~~This section describes the use of generalised sequence numbers which have an individual and a global component.~~

~~(1)The sequence number consists of two concatenated parts $SQN = SQN1 \| SQN2$. $SQN1$ represents the most significant bits of SQN, and $SQN2$ represents the least significant bits of SQN.~~

~~(2)There are counters SQN_{MS} and SQN_{HE} in the MS and the HE respectively. Both parts of SQN are stored by these counters. SQN_{HE} is an individual counter, i.e. there is one per user.~~

~~(3)There is a global counter, e.g. a universal clock with an appropriate time granularity (e.g. seconds elapsed since the start of the system). For short we call the value of this global counter at any one time GLC. If GLC is taken from a universal clock it is computed mod 2^n where n is the length of GLC and of SQN2 in bits.~~

~~(4)When the HE needs a new sequence number SQN to create a new authentication vector, HE retrieves the (user-specific) value of $SQN_{HE} = SQN1_{HE} \| SQN2_{HE}$ from the database. If $SQN2_{HE} < GLC$ then HE sets $SQN = SQN1_{HE} \| GLC$. If $SQN2_{HE} \geq GLC$ then HE sets $SQN = (SQN1_{HE} + 1) \| GLC$.~~
~~Then SQN_{HE} is reset to SQN.~~

~~(5)The sequence number SQN is accepted by the USIM if and only if $SQN > SQN_{MS}$ holds.~~

~~(6)If the mechanism described in Annex C.4 (lists of sequence numbers in the USIM) is used and if SQN_{LO} denotes the lowest sequence number in the list then (5) becomes:~~

~~The sequence number SQN is now accepted by the USIM if and only if $SQN > SQN_{LO}$ holds and SQN is not in the list.~~

~~(7)If the mechanism described in Annex C.5 (protection against counter wrap-around) is employed then (5) becomes:~~

~~The sequence number SQN is now accepted by the USIM if and only if $SQN > SQN_{MS}$ and $SQN - SQN_{MS} < \Delta$ hold.~~

~~(8)If both the mechanisms described in Annexes C.4 and C.5 are employed and if SQN_{HI} denotes the highest sequence number in the list then (5) becomes:~~

~~The sequence number SQN is now accepted by the USIM if and only if $SQN > SQN_{LO}$ and $SQN - SQN_{HI} < \Delta$ hold and SQN is not in the list.~~

~~When parameters are appropriately chosen then this use of sequence numbers is compatible with the re-synchronisation procedure described in section 6.3.5 and the protection against wrap around of counters described in Annex C.5, and it is not required to conceal this type of sequence numbers.~~

C.1 Generation of sequence numbers in the Authentication Centre

According to section 6.3 of this specification, authentication vectors are generated in the authentication centre (AuC) using sequence numbers. This section specifies how these sequence numbers are generated. It is taken into account that authentication vectors may be generated and sent by the AuC in batches such that all authentication vectors in one batch are sent to the same SN/VLR.

(1) In its binary representation, the sequence number consists of two concatenated parts $SQN = SEQ \| IND$. *SEQ* is the batch number, and *IND* is an index numbering the authentication vectors within one batch. *SEQ* in its turn consists of two concatenated parts $SEQ = SEQ1 \| SEQ2$. *SEQ1* represents the most significant bits of *SEQ*, and *SEQ2* represents the least significant bits of *SEQ*. *IND* represents the least significant bits of *SQN*.
If the concept of batches is not supported then *IND* is void and $SQN = SEQ$.

(2) There is a counter SEQ_{HE} in the HE. $SEQ = SEQ1 \| SEQ2$ is stored by this counter. SEQ_{HE} is an individual counter, i.e. there is one per user.

(3) There is a global counter, e.g. a clock giving universal time. For short we call the value of this global counter at any one time *GLC*. If *GLC* is taken from a clock it is computed mod p, where $p = 2^n$ and ~~where~~ n is the length of *GLC* and of *SEQ2* in bits.

(4) If *GLC* is taken from a clock then there is a number $D > 0$ such that the following holds:
(i) the time interval between two consecutive increases of the clock (the clock unit) shall be chosen such that, for each user, at most *D* batches are generated at the AuC during any *D* clock units;
(ii) the clock rate shall be significantly higher than the average rate at which batches are generated for any user;
(iii) $D << 2^n$.

(5) When the HE needs new sequence numbers *SQN* to create a new batch of authentication vectors, HE retrieves the (user-specific) value of $SEQ_{HE} = SEQ1_{HE} \| SEQ2_{HE}$ from the database.
(i) If $SEQ2_{HE} < GLC < SEQ2_{HE} + p - D + 1$ then HE sets $SEQ = SEQ1_{HE} \| GLC$;
(ii) if $GLC \le SEQ2_{HE} \le GLC+D-1$ or $SEQ2_{HE} + p - D + 1 \le GLC$ then HE sets $SEQ = SEQ_{HE} + 1$;
(iii) if $GLC+D-1 < SEQ2_{HE}$ then HE sets $SEQ = (SEQ1_{HE} + 1) \| GLC$.
(iv) The i-th authentication vector in the batch receives the sequence number $SQN = SEQ \| i$.
(v) After the generation of the first authentication vector in the batch has been completed SEQ_{HE} is reset to *SEQ*.

Notes

1. The clock unit and the value *D* have to be chosen with care so that condition (4)(i) is satisfied for every user at all times. Otherwise, user identity confidentiality may be compromised. When the parameters are chosen appropriately sequence numbers for a particular user do not reveal significant information about the user's identity. In particular, *IND* is to be sufficiently short so that no unacceptably long contiguous strings of sequence numbers are generated. If authentication vectors for the CS and the PS domains are not separated by other means it is recommended to choose $D > 1$ as requests from the two different domains may arrive completely independently.

2. The use of *IND* is only for the benefit of the USIM (see note 4 in Annex C.2). When *D* is chosen sufficiently large then several authentication vectors can be generated at the same time by (5)(ii) even when *IND* is not present.

C.2 Handling of sequence numbers in the USIM

This section assumes that sequence numbers are generated according to Annex C.1. If the concept of batches is not supported then batch numbers and sequence numbers coincide and the parameter *IND* is not used.

The USIM keeps track of an ordered **list** of the *b* highest batch number values it has accepted. In addition, for each batch number *SEQ* in the list, the USIM stores the highest *IND* value *IND(SEQ)* it has accepted associated with that batch number. Let SEQ_{LO} denote the lowest and SEQ_{MS} denote the highest batch number in the list.

Protection against wrap around of counter in the USIM

The USIM will not accept arbitrary jumps in batch numbers, but only increases by a value of at most Δ.

Conditions on the choice of Δ :
(1) Δ shall be sufficiently large so that the MS will not receive any batch number *SEQ* with $SEQ - SEQ_{MS} \geq \Delta$ if the HE/AuC functions correctly.
(2) In order to prevent that SEQ_{MS} ever reaches the maximum batch number value *SEQmax* during the lifetime of the USIM the minimum number of steps *SEQmax* /Δ required to reach *SEQmax* shall be sufficiently large.

Acceptance rule

When a user authentication request arrives the USIM checks whether the sequence number is acceptable. The sequence number *SQN = SEQ || IND* is accepted by the USIM if and only if (i) and either (ii) or (iii) hold:
(i) $SEQ - SEQ_{MS} < \Delta$;
(ii) *SEQ* is in the list and *IND > IND(SEQ)* ;
(iii) *SEQ* is not in the list and $SEQ > SEQ_{LO}$.

The USIM shall also be able to put a limit *L* on the difference between SEQ_{MS} and an accepted batch number *SEQ*. If such a limit is applied then, in addition to the above conditions, the sequence number shall only be accepted by the USIM if $SEQ_{MS} - SEQ < L$.

List update

After a sequence number *SQN = SEQ || IND* received in a user authentication request has been accepted by the USIM the USIM proceeds as follows:
(i) Case 1: the batch number *SEQ* is not in the list.
Then the list entry corresponding to SEQ_{LO} is deleted, *SEQ* is included in the list, *IND(SEQ)* is set to *IND* and SEQ_{LO} and SEQ_{MS} are updated;
(ii) Case 2: the batch number *SEQ* is in the list.
Then *IND(SEQ)* is set to *IND*.
If a sequence number received in a user authentication request is rejected the list remains unaltered.

Notes

1. Using the above list mechanism, it is not required that a previously visited SN/VLR deletes the unused authentication vectors when a user de-registers from the serving network. Retaining the authentication vectors for use when the user returns later may be more efficient as regards signalling when a user abroad switches a lot between two serving networks.

2. The list mechanism may also be used to avoid unjustified rejection of user authentication requests when authentication vectors in two SN/VLRs from different mobility management domains (circuit and packet) are used in an interleaving fashion.

3. When a VLR uses fresh authentication vectors obtained during a previous visit of the user, the USIM can reject them although they have not been used before (because the list size *b* and the limit *L* are finite). Rejection of a sequence number can therefore occur in normal operation, i.e., it is not necessarily caused by (malicious) replay or a database failure.

4. The mechanism presented in this section allows the USIM to exploit knowledge about which authentication vectors belong to the same batch. It may be assumed that authentication vectors in the same batch are always used in the correct order as they are handled by the same SN/VLR. Consequently, only one sequence number per batch has to be stored.

5. With the exception of SEQ_{MS} , the batch numbers in the list need not be stored in full length if a limit L on the difference between SEQ_{MS} and an accepted batch number is applied and if those entries in the list which would cause the limit L to be exceeded are removed from the list after a new sequence number has been accepted.

6. Condition (2) on Δ means that SEQ_{MS} can reach its maximum value only after a minimum of $SEQmax / \Delta$ successful authentications have taken place.

7. There is a dependency of the choice of Δ and the size n of global counter GLC in Annex C.1: Δ shall be chosen larger than 2^n.

TSG SA WG3 #8, Sophia Antipolis, 16—19 November, 1999 **S3-99541**

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** **026 r1** Current Version: V3.2.0

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

For submission to TSG ___ *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 [ ]

Source:	S3
Date:	16-11-99
Subject:	Mobile IP security
3G Work item:	Security Architecture

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 clause for IP (including Mobile IP) security in 33.102 has so far been marked as for further study. It is important to make clear that the MIP introduction in 3G has no influence on the 3G security architecture. The proposed text for clause 8.3 introduces the notion of mutual independence between 3G security and Mobile IP security.

Clauses affected: Clause 8

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:

8.3 ~~IP security.~~Mobile IP security

~~[ffs]~~The introduction of Mobile IP functionality for end users in 3G has no influence on the security architecture for 3G.

Mobile IP terminals may be equipped with security functionality independent of the 3G network access security in order to allow security functions outside the 3G network.

3G networks, supporting Mobile IP services, should support its inherent security functionality.

On the other hand, 3G network access security architecture can not be influenced or reduced by the Mobile IP option.

The Mobile IP security functionality must thus be separate from the 3G network access security and it is developed in an other forum, IETF.

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 032 Current Version: 3.2.0

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

For submission to TSG SA #6 for approval X
list TSG meeting no. here ↑ 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: USIM [ ] ME [ ] UTRAN [ ] Core Network [ ]
(at least one should be marked with an X)

Source: TSG SA WG 3 **Date:** 1999-Dec-09

Subject: Removal of duplicate description of network-wide encryption mechanism

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 mechanism has been copied in the section on access link security but not deleted from the section on application security.

Clauses affected: 8.2

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.

8.2 Void

~~Network-wide user traffic confidentiality~~

~~8.2.1 Introduction~~

~~Subclause 6.6 specifies how signalling information, user identity and user traffic information may be confidentiality protected by providing a protected mode of transmission on dedicated channels between the UE and the RNC. Network-wide confidentiality is an extension of this security feature which provides a protected mode of transmission on user traffic channels across the entire network. This gives users assurance that their traffic is protected against eavesdropping on every link within the network, i.e. not just the particularly vulnerable radio links in the access network, but also on the fixed links within the core network.~~

~~If network-wide confidentiality of user traffic is provided then access link confidentiality of user traffic between UE and RNC shall be replaced with the network-wide service. Access link confidentiality of signalling information and user identity between UE and RNC shall be applied regardless of whether or not the network-wide user traffic confidentiality service is applied.~~

~~Note: The exact architectural placement of the network-wide encryption function is for further study. This may have an impact on whether network-wide encryption replaces or supplements access link encryption.~~

~~A lawful interception interface may be implemented according to TS33.107 regardless of whether or not network-wide confidentiality is applied by the network. It shall be possible to remove any network-wide confidentiality protection within the core network to provide access to plaintext user traffic at the lawful interception interface.~~

~~Network-wide confidentiality shall be provided by protecting transmissions on user traffic channels using a synchronous stream cipher. This involves the specification of a standard method for ciphering user traffic on a network-wide basis (clause 8.2.2) and a standard method for managing the ciphering key required at the end points of the protected channel (clause 8.2.3).~~

~~8.2.2 Ciphering method~~

~~The network-wide encryption algorithm shall be a synchronous stream cipher. It shall be possible to use the same algorithm UEA for access link encryption and network-wide encryption.~~

~~The network-wide synchronous stream cipher shall contain a key stream generator which shall have two inputs: the network-wide cipher key (ECK) and an initialisation value (IV). The plaintext shall be encrypted using the key stream by applying an exclusive-or operation to the plaintext on a bit per bit basis to generate the ciphertext. The decryption operation shall involve applying the same key stream to the ciphertext to recover the plaintext.~~

~~Synchronisation of the key stream shall be achieved using the initialisation value. Synchronisation information shall be available at both end points of the communication and shall be used to maintain alignment of the key stream. Protection against replay of user traffic shall be achieved through the use of a time variable initialisation vector combined with a time variable cipher key.~~

~~Note: The stream cipher does not protect against bit toggling so other mechanisms must be used if this type of integrity protection is required on user traffic.~~

~~For encryption of voice traffic then Transcoder Free Operation (TFO) shall be used between the two end points such that the structure and ordering of the transmitted data shall be maintained with the same boundary conditions at each end of the link.~~

~~Note: In the initial phases of 3GPP, transcoder free operation may only be possible for user traffic channels which terminate within the same serving network. Furthermore, TFO may only be possible if the entire communication path is within the same serving network. Thus, in non optimal routing cases where the tromboning effect occurs, TFO may not be available, even if the traffic channel terminates within the same serving network.~~

~~For encryption of data traffic a transparent data service shall be used between the two end points such that the structure and ordering of transmitted data shall be maintained with the same boundary conditions at each end of the link.~~

~~To satisfy lawful interception requirements it must be possible to decrypt network-wide encrypted traffic within the core network to provide access to plaintext user traffic. Thus decryption facilities (and the network-wide cipher key) shall be available in the core network for lawful interception reasons. If transcoder free operation is used on voice traffic channels, transcoders shall be available in the core network for lawful interception reasons whether or not network-wide encryption is provided.~~

~~For further study:~~

- ~~Specification of encryption synchronisation mechanism;~~
- ~~Adaptation of TFO voice traffic channels for network-wide confidentiality;~~
- ~~Adaptation of data traffic channels for network-wide confidentiality;~~

- ~~The ability to terminate network-wide encryption at network gateways for inter-network user traffic channels;~~
- ~~The ability to handle multiparty calls, explicit call transfer and other supplementary services;~~
- ~~Network-wide encryption control – algorithm selection, mode selection, user control~~

~~8.2.3 Key management~~

~~Signalling links within the network shall be protected on a link-by-link basis. In particular, the UE to RNC signalling links shall be protected using access link keys (see clause 6) and core network signalling links shall be protected using network security domain keys (see clause 7). If network-wide encryption is provided across serving network boundaries (which requires that inter-network TFO is available) then the signalling links requiring protection will cross network boundaries.~~

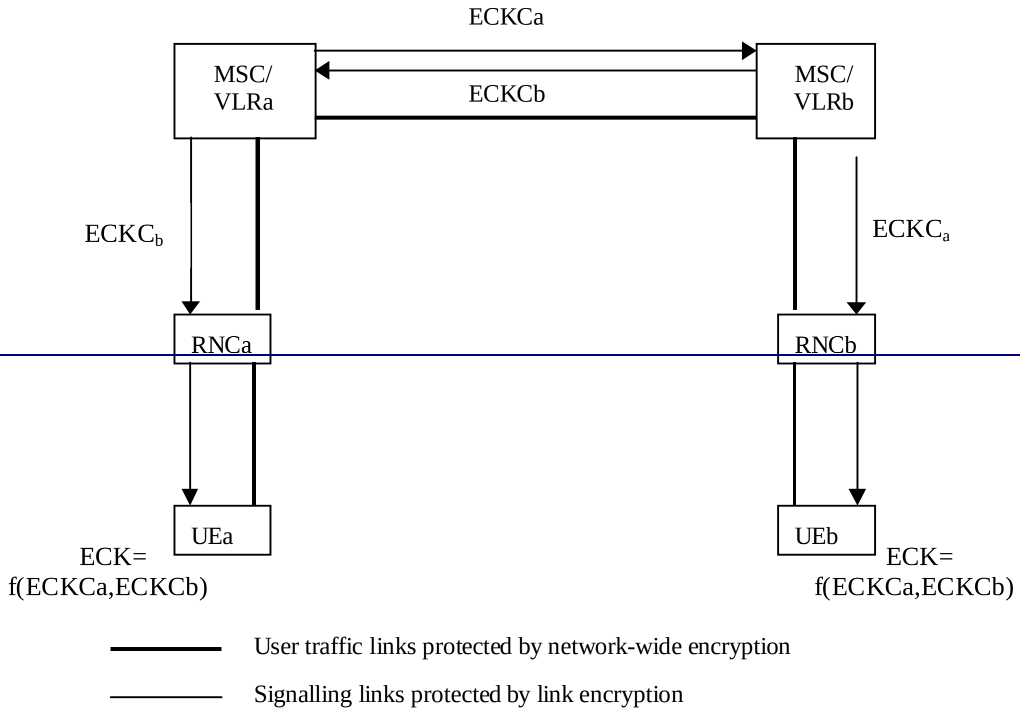
~~Note: If network-wide encryption is provided across serving network boundaries then the two serving networks may not be roaming partners yet they still must be able to protect inter-network signalling by establishing appropriate keys.~~

~~The key management scheme for network-wide encryption involves establishing a network-wide cipher key between the end points of the traffic channel. It should not be possible to obtain this key by eavesdropping on any transmission links within the network.~~

~~Note: However, it is be possible to obtain the network-wide key by compromising certain nodes within the network (e.g. nodes where link encryption terminates).~~

~~To satisfy lawful interception requirements it shall be possible to decrypt network-wide encrypted traffic within the core network to provide access to plaintext user traffic. Thus, the network-wide cipher key (and decryption facilities) shall be available in the core network for lawful interception reasons.~~

~~The key management scheme is illustrated in the diagram below.~~



~~**Figure 17: Key management scheme for network-wide encryption**~~

~~In addition to the access link cipher and integrity keys, the USIM and the MSC/VLR shall also establish a network-wide cipher key component ECKC as part of the authentication and key agreement procedure (clause 6.3). This key component will be used to generate the network-wide cipher key ECK.~~

~~As part of establishing a network-wide encrypted connection, MSC/VLRa and MSC/VLRb shall exchange network-wide cipher keys components for UEa and UEb. MSC/VLRa passes ECKCb to UEa, while MSC/VLRb passes ECKCa to UEb. At each end the access link key is transmitted to the UE over signalling channels which are protected using the access link cipher keys CK. When each UE has received the other party's network-wide cipher key component, the network-wide cipher key ECK shall be calculated as a function of ECKCa and ECKCb.~~

~~The key management scheme satisfies the lawful interception requirement since ECK can be generated by MSC/VLRa or MSC/VLRb and then used by decryption facilities in the core network to provide plaintext user traffic at the lawful interception interface.~~

~~For further study:~~

- ~~Specification of mechanism to exchange network-wide cipher key components.~~

- ~~The ability to terminate network-wide cipher key management at network gateways for inter-network user traffic channels.~~

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 033 Current Version: 3.2.0

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

For submission to TSG SA #6 — for approval: X — for information: (blank)
list TSG meeting no. here ↑ *(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: USIM [X] ME [X] UTRAN [ ] Core Network [X]
(at least one should be marked with an X)

Source: S3 **Date:** 1999-Dec-09

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

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: All scenarios for authentication and intersystem handover/change are described in greater detail in order to clarify the existing section.

Clauses affected: 6.8

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.

6.8 Interoperation and handover between UMTS and GSM

6.8.1 Authentication and key agreement of UMTS subscribers

6.8.1.1 General

For UMTS subscribers,

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

The execution of the UMTS (resp. GSM) AKA results in the establishment of a UMTS (resp. GSM) security context between the user and the serving network domain to which the MSC/VLR or SGSN belongs. The user needs to separately establish a security context with each serving network domain.

Figure 1 shows the different scenarios that can occur with UMTS subscribers using either R98- or R99+ UE in a mixed network architecture.

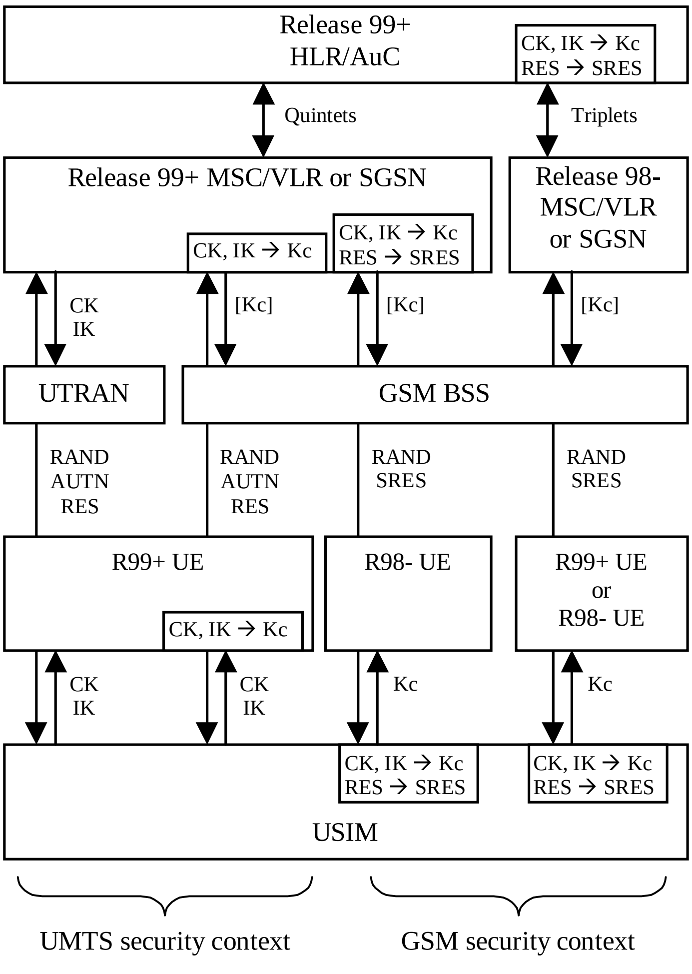


Figure 1: Authentication and key agreement of UMTS subscribers

Note that the UMTS parameters RAND, AUTN and RES are sent transparently through the UTRAN or GSM BSS and that the GSM parameters RAND and SRES are sent transparently through the GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering is always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

6.8.1.2 R99+ HLR/AuC

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

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

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

b) c2: $SRES_{[GSM]} = XRES_1$ [xor $XRES_2$ [xor $XRES_3$ [xor $XRES_4$]]]

c) c3: $Kc_{[GSM]} = CK_1$ xor CK_2 xor IK_1 xor IK_2

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

6.8.1.3 R99+ MSC/VLR or SGSN

UMTS subscriber with R99+ UE

When the user has R99+ UE, UMTS AKA shall be performed using a quintet that is either a) retrieved from the local database, b) provided by the HLR/AuC, or c) provided by the previously visited R99+ MSC/VLR or SGSN. Note that originally all quintets are provided by the HLR/AuC.

UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are stored in the MSC/VLR or SGSN.

When the user is attached to a UTRAN, the UMTS cipher/integrity keys are sent to the RNC, where the cipher/integrity algorithms are allocated.

When the user is attached to a GSM BSS, UMTS AKA is followed by the derivation of the GSM cipher key from the UMTS cipher/integrity keys. When the user receives service from an MSC/VLR, the derived cipher key Kc is then sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the derived cipher key Kc is applied in the SGSN itself.

UMTS subscriber with R98- UE

When the user has R98- UE, the R99+ MSC/VLR or SGSN shall perform GSM AKA using a triplet that is either

a) derived by means of the conversion functions c2 and c3 in the R99+ MSC/VLR or SGSN from a quintet that is i) retrieved from the local database, ii) provided by the HLR/AuC, or iii) provided by the previously visited R99+ MSC/VLR or SGSN, or

b) provided as a triplet by the previously visited MSC/VLR or SGSN.

Note that all triplets are derived from quintets, be it in the HLR/AuC or in an MSC/VLR or SGSN.

This results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the MSC/VLR or SGSN.

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

6.8.1.4 R99+ UE

R99+ UE with a USIM inserted and attached to a UTRAN shall only support UMTS AKA and shall not support GSM AKA.

R99+ UE with a USIM inserted and attached to a GSM BSS shall support UMTS AKA and may support GSM AKA. Support of GSM AKA is required to allow registration in a R98- MSC/VLR or SGSN.

The execution of UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys

CK and IK and the key set identifier KSI are stored in the UE.

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

When the user is attached to a GSM BSS and the user participates in UMTS AKA, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK using conversion function c3.

6.8.1.5 USIM

The USIM shall support UMTS AKA. When the UE provides the USIM with RAND and AUTN and the verification of AUTN is successful, the USIM shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK.

The USIM may support GSM AKA. In that case, when the UE provides the USIM with RAND, the USIM first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The USIM then sends the GSM user response SRES and the GSM cipher key Kc to the UE.

In case the USIM does not support GSM AKA, the USIM responds with an appropriate message to the R99+ UE. USIM that do not support GSM AKA cannot operate in R98- UE.

6.8.2 Authentication and key agreement for GSM subscribers

6.8.2.1 General

For GSM subscribers, GSM AKA shall always be used.

The execution of the GSM AKA results in the establishment of a GSM security context between the user and the serving network domain to which the MSC/VLR or SGSN belongs. The user needs to separately establish a security context with each serving network domain.

When in a UTRAN, the UMTS cipher/integrity keys CK and IK are derived from the GSM cipher key Kc.

Figure 2 shows the different scenarios that can occur with GSM subscribers using either R98- or R99+ UE in a mixed network architecture.

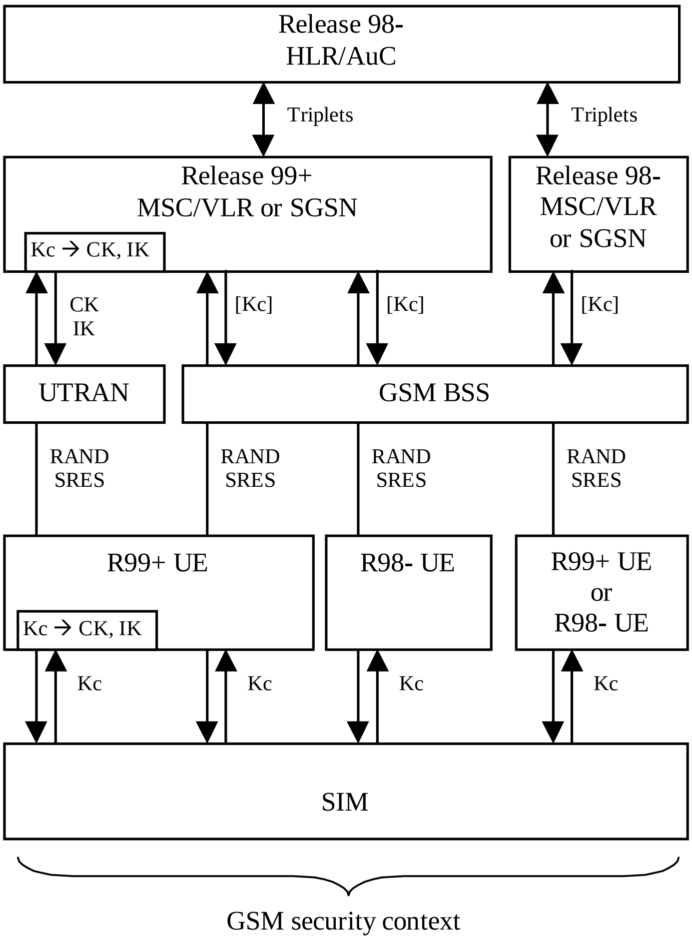


Figure 2: Authentication and key agreement for GSM subscribers

Note that the GSM parameters RAND and RES are sent transparently through the UTRAN or GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering is always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

6.8.2.2 R99+ MSC/VLR or SGSN

The R99+ MSC/VLR or SGSN shall perform GSM AKA using a triplet that is either a) retrieved from the local database, b) provided by the HLR/AuC, or c) provided by the previously visited MSC/VLR or SGSN. Note that all triplets are originally provided by the R98- HLR/AuC.

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

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

a) c4: $CK_{[UMTS]} = 0\ldots0 \,||\, Kc$;

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

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

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

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

6.8.2.3 R99+ UE

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

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

When the user is attached to a UTRAN, R99+ UE shall derive the UMTS cipher/integrity keys Ck and IK from the GSM cipher key Kc using the conversion functions c4 and c5.

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

6.8.3.1 UMTS security context

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

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.

6.8.4.2 GSM 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, UMTS cipher/integrity keys CK and IK are derived from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sent to the new RNC.

b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR sends the stored GSM cipher key Kc to the (second) MSC/VLR controlling the new RNC. That MSC/VLR derives UMTS cipher/integrity keys CK and IK which are then forwarded to the new RNC. The initial MSC/VLR remains the anchor point for throughout the service.

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

6.8.5 Intersystem change for PS Services – from UTRAN to GSM BSS

6.8.5.1 UMTS security context

At the network side, three cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same SGSN, the SGSN derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and applies it.

b) In case of a handover to a GSM BSS controlled by another R99+ SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the new SGSN. The new SGSN stores the keys, derives the GSM cipher key Kc and applies the latter. The new SGSN becomes the new anchor point for the service.

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

At the user side, in case a) or b), 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 it.

In case c), the handover makes that the UMTS security context between the user and the serving network domain is lost. The UE needs to be aware of that. The UE then deletes the UMTS cipher/integrity keys CK and IK and stores the derived GSM cipher key Kc.

6.8.5.2 GSM security context

At the network side, two cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same SGSN, the SGSN starts to apply the stored GSM cipher key Kc.

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

At the user side, in both cases, the UE applies the GSM cipher key Kc that is stored.

6.8.6 Intersystem change for PS services – from GSM BSS to UTRAN

6.8.6.1 UMTS security context

At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same SGSN, 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 SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the (new) SGSN controlling the new RNC. The new SGSN becomes the new anchor point for the service. The new SGSN then stores the UMTS cipher/integrity keys CK and IK and sends them to the new RNC.

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

6.8.6.2 GSM security context

At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same SGSN, the SGSN derives UMTS cipher/integrity keys

CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sends them to the new RNC.

b) In case of a handover to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the new RNC. The new SGSN becomes the new anchor point for the service. The new SGSN stores the GSM cipher key Kc and derives the UMTS cipher/integrity keys CK and IK which are then forwarded to the new RNC.

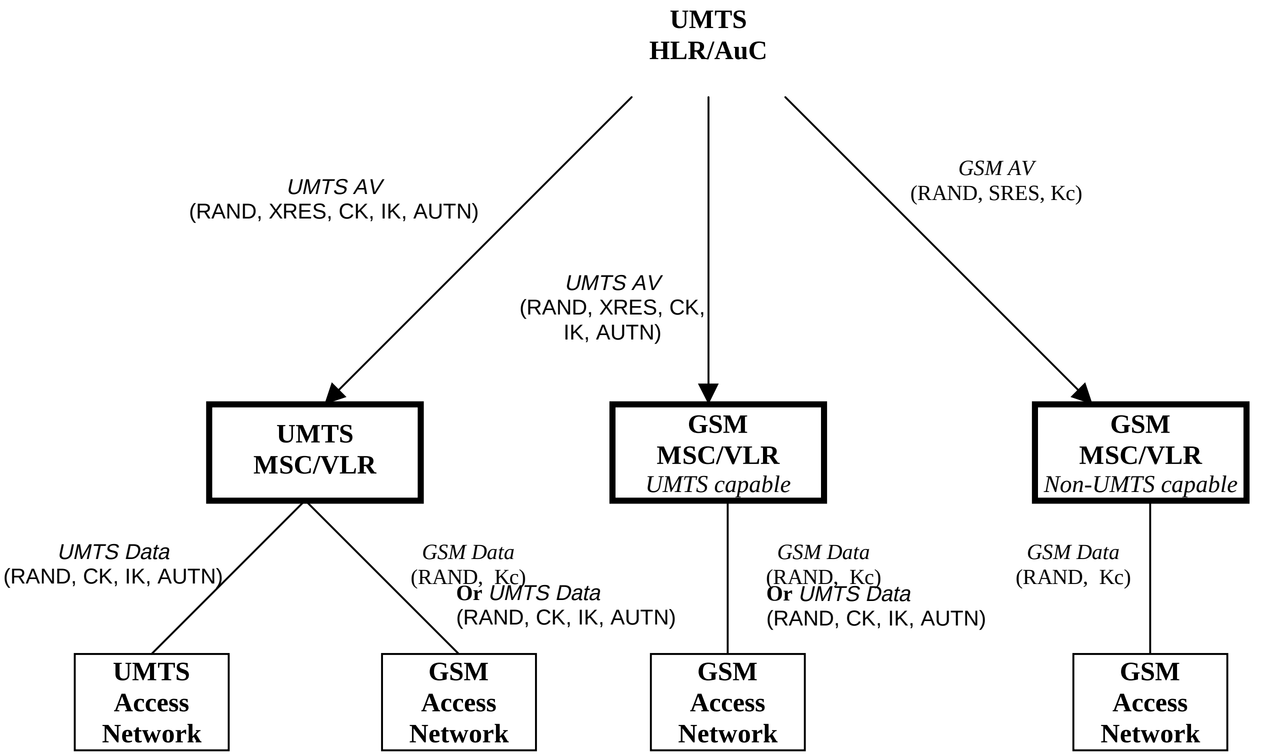
At the user side, in both cases, the UE derives the UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and applies them.

~~Note: The description below is mainly based on CS domain procedures. It will be extended to also completely describe PS procedures.~~

~~6.8.1 Interoperability for UMTS users~~

~~A general principle in designing the security interoperation between 3G and 2G networks has been that a UMTS user (i.e. a user with a USIM issued by a R99 HLR/AuC) shall get UMTS level of security whenever possible.~~

~~The mechanism described here achieves intersystem operability between UMTS and GSM networks allowing secure interoperation between both networks for UMTS users (USIM). The following figure illustrates the different scenarios of interoperability for UMTS users:~~



~~Figure 14: Interoperability for UMTS Users~~

~~The UMTS authentication parameters are generated by the UMTS HLR/AuC and USIM by use of the home operator specified algorithms for this purpose.~~

~~Upon receipt of an *authentication data request* from a UMTS SN/VLR or a UMTS capable GSM SN/VLR , the HLR/AuC sends an ordered array of *n* UMTS authentication vectors (quintuples) to the SN/VLR.~~

~~If the UMTS MSC/VLR is able to handle GSM radio access network, the MSC/VLR shall be able to derive a GSM authentication vector from the received UMTS vector, by means of the standardised conversion functions defined below, in order to provide the GSM security parameters to the GSM radio access network. Whether GSM Data or UMTS Data is used depends on the terminal capabilities.~~

~~Upon receipt of an *authentication data request* from a non-UMTS capable GSM SN/VLR, the HLR/AuC shall derive the GSM authentication vectors from the UMTS vectors, by means of the standardised conversion functions defined below. Then, the HLR/AuC sends an *authentication response* back to the SN/VLR that contains an ordered array of *n* GSM authentication vectors (triples). The HLR/AuC may have pre-computed GSM authentication vectors or may derive them on demand from the UMTS authentication vectors.~~

~~On the mobile side, the USIM shall derive the GSM authentication parameters from the UMTS authentication parameters by means of the standardised conversion functions, when the MS is located in the GSM radio access network.~~

~~The previous procedures are also applicable to the corresponding PS network and so as to the corresponding SGSN entity.~~

~~Subsequently the following entities shall implement the standardised conversion functions for generating GSM authentication vectors (triplets) from UMTS authentication vectors (quintuplets):~~

- ~~UMTS HLR/AuC~~
- ~~UMTS MSC/VLR~~
- ~~UMTS SGSN~~
- ~~UMTS capable GSM MSC/VLR~~
- ~~UMTS capable GSM SGSN~~
- ~~USIM~~

~~Interoperability with non-UMTS capable GSM entities is achieved by use of the standardised conversion functions implemented in the HLR/AuC. The handover case is described in section 6.6.4.2.~~

~~The following conversion functions shall be computed for generating the GSM authentication parameters:~~

- ~~**Generation of GSM RAND**~~

~~f: ($RAND_U$) -> $RAND_G$;~~ $\cancel{RAND_G = RAND_U}$

- ~~**Generation of GSM SRES**~~

~~f: (XRES) -> SRES;~~ $\cancel{SRES = XRES_1 \oplus XRES_2 \oplus XRES_3 \oplus XRES_4}$

~~*whereby* $XRES = XRES_1 \,||\, XRES_2 \,||\, XRES_3 \,||\, XRES_4$*; and with* $XRES_n$ *32 bits each. If any of* $XRES_n$ *is not used, it is assumed zeros.*~~

- ~~**Generation of GSM Kc**~~

~~f: (CK, IK) -> Kc;~~ $\cancel{Kc = CK_1 \oplus CK_2 \oplus IK_1 \oplus IK_2}$

~~*whereby* CK_1 *(resp.* IK_1*) is the first half and* CK_2 *(resp.* IK_2*) is the second half of CK (resp. IK)*~~

~~The GSM authentication vector is generated using the UMTS authentication parameters. Consequently, the generated triplet depends on the UMTS authentication algorithms and inputs parameters for these algorithms, all this information under the control of the HE, being the algorithms operator specific.~~

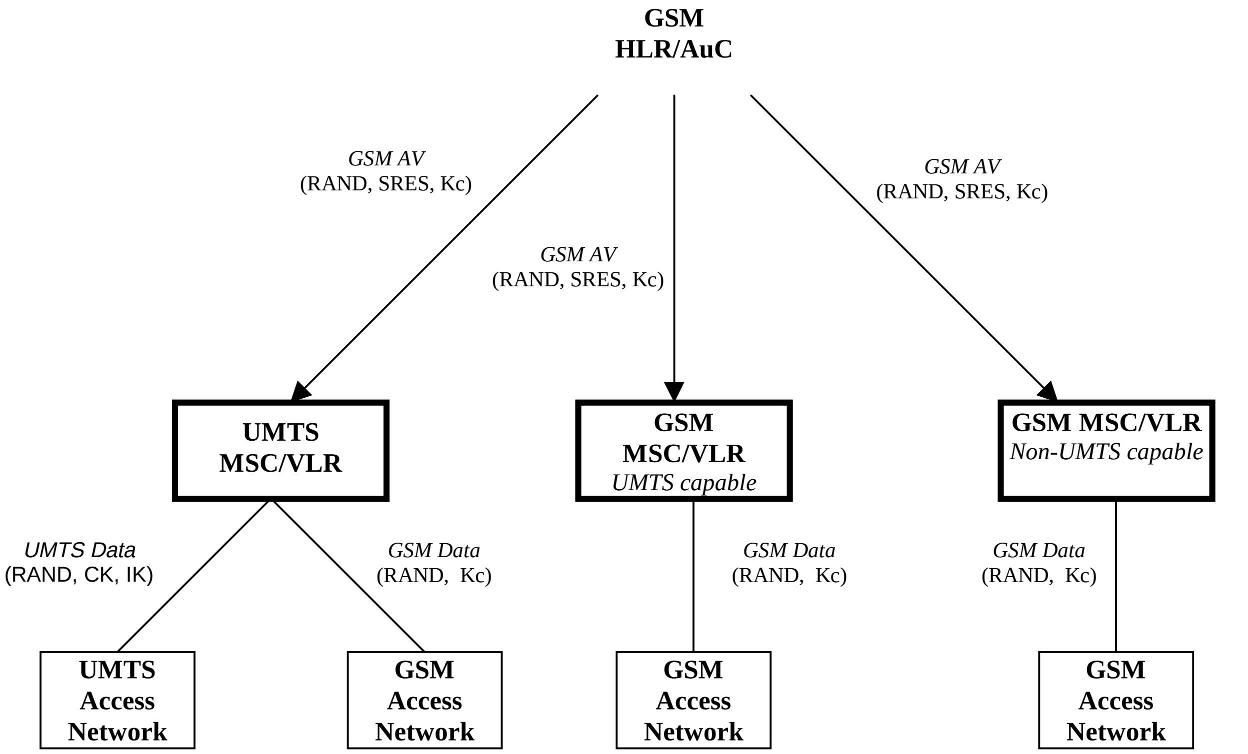
~~The GSM authentication and key generating algorithms are specified as follows:~~

~~***A3***: $RAND_G$ -> SRES;~~ $\cancel{SRES = f(f2_K(RAND_U))}$

~~***A8***: $RAND_G$ -> Kc;~~ $\cancel{Kc = f(f3_K(RAND_U), f4_K(RAND_U))}$

~~6.8.2 Interoperability for GSM users~~

~~The mechanism described here achieves intersystem operability between UMTS and GSM networks allowing secure interoperation between both networks for GSM users (SIM). The following figure illustrates the different scenarios of interoperability for 2G users:~~



~~Figure 15: Interoperability for GSM Users~~

~~The GSM authentication parameters are generated by the GSM HLR/AuC and the SIM by use of the home operator specified algorithms for this purpose.~~

~~Upon receipt of an *authentication data request* from any SN/VLR (UMTS or GSM), the HLR/AuC sends an ordered array of *n* GSM authentication vectors (triplets) to the SN/VLR.~~

~~If the UMTS MSC/VLR is able to handle UMTS radio access network, the MSC/VLR shall be able to derive a UMTS authentication vector from the received GSM authentication vector, by means of the standardised conversion functions defined below, in order to provide the UMTS security parameters to the UMTS radio access network.~~

~~On the mobile side, the UE shall derive the UMTS authentication parameters from the GSM authentication parameters generated by the SIM by means of the standardised conversion functions, when the MS is located in the UMTS radio access network.~~

~~The previous procedures are also applicable to the corresponding PS network and so as to the corresponding SGSN entity.~~

~~Subsequently the following entities shall implement the standardised conversion functions for generating UMTS authentication parameters from GSM authentication vectors (triplets):~~

- ~~UMTS MSC/VLR~~

- ~~UMTS SGSN~~

- ~~UE~~

~~The following conversion functions shall be computed for generating the UMTS authentication parameters:~~

- ~~**Generation of UMTS RAND**~~

~~f: ($RAND_G$) -> $RAND_U$;~~ ~~$RAND_U = RAND_G$~~

- ~~**Generation of UMTS XRES**~~

~~f: (SRES) -> XRES;~~ ~~*XRES = SRES*~~

~~**• Generation of UMTS CK**~~

~~f: (Kc) -> CK;~~ ~~*CK = 0..0 || Kc*~~

~~**• Generation of UMTS IK**~~

~~f: (Kc) -> IK;~~ ~~*IK = Kc || Kc*~~

~~**• Generation of UMTS AUTN**~~

~~The authentication token AUTN is not used for GSM users.~~

~~The UMTS authentication vector is generated using the GSM authentication parameters. Consequently, the generated quintuplet depends on the GSM authentication algorithms and inputs parameters for these algorithms, all this information under the control of the HE, being the algorithms operator specific.~~

~~A GSM user should receive the security level provided by the home network. The effective encryption key length used in UMTS radio access network is the GSM Kc length, provided by the HE; Integrity protection is provided by using the GSM encryption key; and the AUTN parameter is not used.~~

~~The UMTS authentication and key generating algorithms are specified as follows:~~

~~f_2: $RAND_u$ -> XRES;~~ ~~*XRES =A3($RAND_G$)*~~

~~f_3: $RAND_u$ -> CK;~~ ~~*CK = 0..0 || A8($RAND_G$)*~~

~~f_4: $RAND_u$ -> IK;~~ ~~*IK = A8($RAND_G$) || A8($RAND_G$)*~~

~~*f*: ($RAND_u$, SEQ, AK, MAC) -> AUTN;~~ ~~*Parameter not used*~~

3GPP TSG SA WG 3 (Security) meeting #9 **S3-99545**
Helsinki, 7—9 December, 1999.

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**	**034**	Current Version:	3.2.0

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

For submision to TSG	SA #6	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 [ ] ME [ ] UTRAN [ ] Core Network [X]
(at least one should be marked with an X)

Source:	TSG SA WG 3	**Date:**	1999-Dec-9
Subject:	Distribution of authentication data within one serving network domain		
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: The modification allows that the user is authenticated using local authentication after a location/routing area update in a new MSC/VLR or SGSN. The use of that options lowers the number of quintets that are used by avoiding authentication and key establishment when there is no reason for from a security viewpoint. The secure reduction of the number of authentication and key agreement protocol runs results in a reduced amount of required signalling and Authentication Centre activity.

Clauses affected: 6.3.4

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: The changes bring TS 33.102 in line with TS 23.060, especially section 6.8.1.2, that describes the information elements sent from one SGSN to another SGSN on an intersystem change for PS services.

help.doc

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

6.3.4 Distribution of IMSI and temporary authentication data within one serving network domain

The purpose of this procedure is to provide a newly visited MSC/VLR or SGSN with temporary authentication data from a previously visited MSC/VLR or SGSN within the same serving network domain.

The procedure is shown in Figure 10.

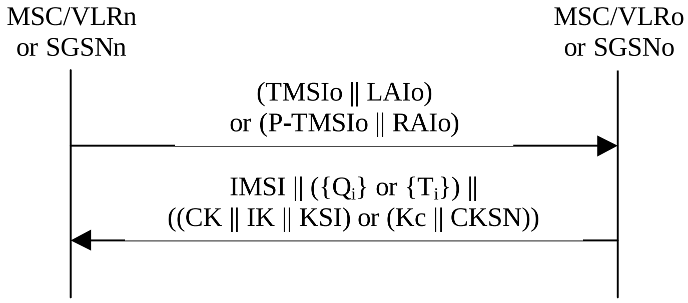


Figure 10: Distribution of IMSI and temporary authentication data within one serving network domain

The procedure shall be invoked by the newly visited MSC/VLRn (resp. SGSNn) after the receipt of a location update request (resp. routing area update request) from the user wherein the user is identified by means of a temporary user identity TMSIo (resp. P-TMSIo) and the location area identity LAIo (resp. routing area identity RAIo) under the jurisdiction of a previously visited MSC/VLRo or SGSNo that belongs to the same serving network domain as the newly visited MSC/VLRn or SGSNn.

The protocol steps are as follows:

a) The MSC/VLRn (resp. SGSNn) sends a *user identity request* to the MSC/VLRo (or SGSNo), this message contains TMSIo and LAIo (resp. P-TMSIo and RAIo).

b) The MSC/VLRo (resp. SGSNo) searches the user data in the database.

If the user is found, the MSC/VLRo (resp. SGSNo) shall send a *user identity response* back that

i) shall include the IMSI,

ii) may include a number of unused authentication vectors (quintets or triplets) and

iii) may include the current security context data: CK, IK and KSI (UMTS) or Kc and CKSN (GSM).

The MSC/VLRo or SGSNo subsequently deletes the authentication vectors which have been sent and the data elements on the current security context.

If the user cannot be identified the MSC/VLRo or SGSNo shall send a *user identity response* indicating that the user identity cannot be retrieved.

c) If the MSC/VLRn or SGSNn receives a *user identity response* with an IMSI, it creates an entry and stores any authentication vectors and any data on the current security context that may be included.

If the MSC/VLRn or SGSNn receives a *user identity response* indicating that the user could not be identified, it shall initiate the user identification procedure described in 6.2.

3GPP TSG SA WG 3 (Security) meeting #9 S3-99548
Helsinki, 7—9 December 1999

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 37r1 Current Version: V3.2.0

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

For submission to TSG SA#6 for approval X for information

list TSG meeting no. here ↑ *(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: USIM X ME UTRAN Core Network X
(at least one should be marked with an X)

Source: S3 **Date:** 1999-Dec-09

Subject: Authentication and key agreement

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: Include requirements on sequence number handling, remove description of any particular method of sequence number handling, improve efficiency of re-synchronisation procedure, correct notation

Clauses affected: Section 6.3

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: The value of the number x = 50 in requirement e) in section 6.3.2 shall be used pending further studies.

help.doc

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

6.3 Authentication and key agreement

6.3.1 General

The mechanism described here achieves mutual authentication by the user and the network showing knowledge of a secret key K which is shared between and available only to the USIM and the AuC in the user's HE. In addition the USIM and the HE keep track of counters SEQ_{MS} ~~SQN_{MS}~~ and SEQ_{HE} ~~SQN_{HE}~~ respectively to support network authentication.

The method was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication derived from the ISO standard ISO/IEC 9798-4 (section 5.1.1).

An overview of the mechanism is shown in figure 4.

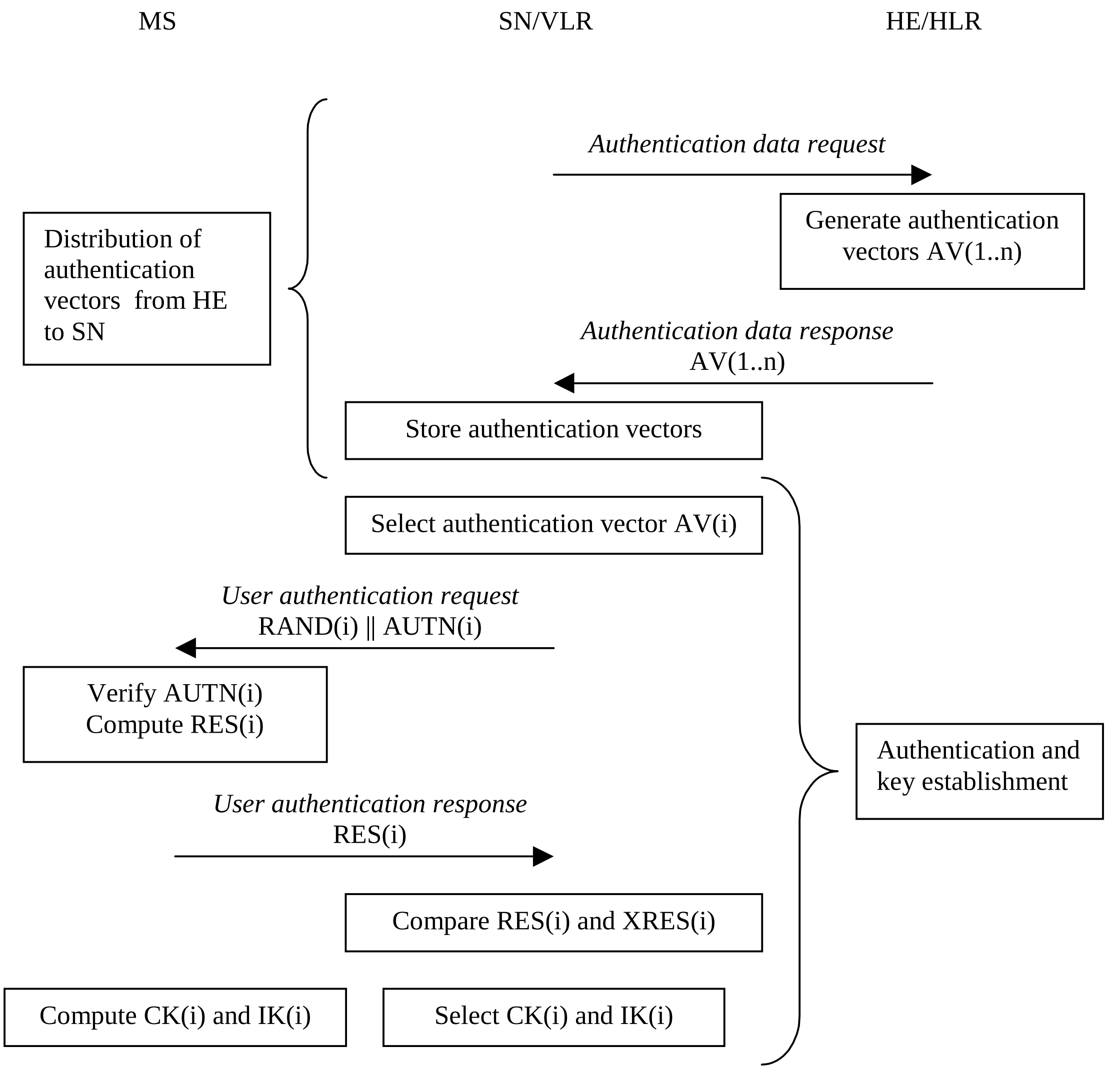


Figure 4: Authentication and key agreement

Upon receipt of a request from the ~~SN/VLR~~VLR/SGSN, the HE/AuC sends an ordered array of *n* authentication vectors (the equivalent of a GSM "triplet") to the ~~SN/VLR~~VLR/SGSN. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the ~~SN/VLR~~VLR/SGSN and the USIM.

When the ~~SN/VLR~~VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the array and sends the parameters RAND and AUTN to the user. The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the ~~SN/VLR~~VLR/SGSN. The USIM also computes CK and IK. The ~~SN/VLR~~VLR/SGSN compares the received RES with XRES. If they match the ~~SN/VLR~~VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the ~~SN/VLR~~VLR/SGSN to the entities which perform ciphering and integrity functions.

~~SN/VLR~~VLR/SGSNs can offer secure service even when HE/AuC links are unavailable by allowing them to use previously derived cipher and integrity keys for a user so that a secure connection can still be set up without the need for an authentication and key agreement. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signalling messages (see 6.4).

The authenticating parties shall be the AuC of the user's HE (HE/AuC) and the USIM in the user's mobile station. The mechanism consists of the following procedures:

A procedure to distribute authentication information from the HE/AuC to the ~~SN/VLR~~VLR/SGSN. This procedure is described in 6.3.2. The ~~SN/VLR~~VLR/SGSN is assumed to be trusted by the user's HE to handle authentication information securely. It is also assumed that the intra-system links between the ~~SN/VLR~~VLR/SGSN to the HE/AuC are adequately secure. Mechanisms to secure these links are described in clause 7. It is further assumed that the user trusts the HE.

A procedure to mutually authenticate and establish new cipher and integrity keys between the ~~SN/VLR~~VLR/SGSN and the MS. This procedure is described in 6.3.3.

A procedure to distribute authentication data from a previously visited ~~VLR~~VLR/SGSN to the newly visited ~~VLR~~VLR/SGSN. This procedure is described in 6.3.4. It is also assumed that the links between ~~SN/VLR~~VLR/SGSNs are adequately secure. Mechanisms to secure these links are described in clause 7.

6.3.2 Distribution of authentication data from HE to SN

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

SN/VLR HE

Authentication data request
IMUI or HLR-message
→

Authentication data response
[IMUI] || AV(1..n)
←

Figure 5: Distribution of authentication data from HE to ~~SN/VLR~~VLR/SGSN

The ~~SN/VLR~~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 ~~SN/VLR~~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 ~~SN/VLR~~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 ~~SN/VLR~~VLR/SGSN that contains an ordered array of n authentication vectors AV(1..n).

Figure 6 shows the generation of an authentication vector AV by the HE/AuC.

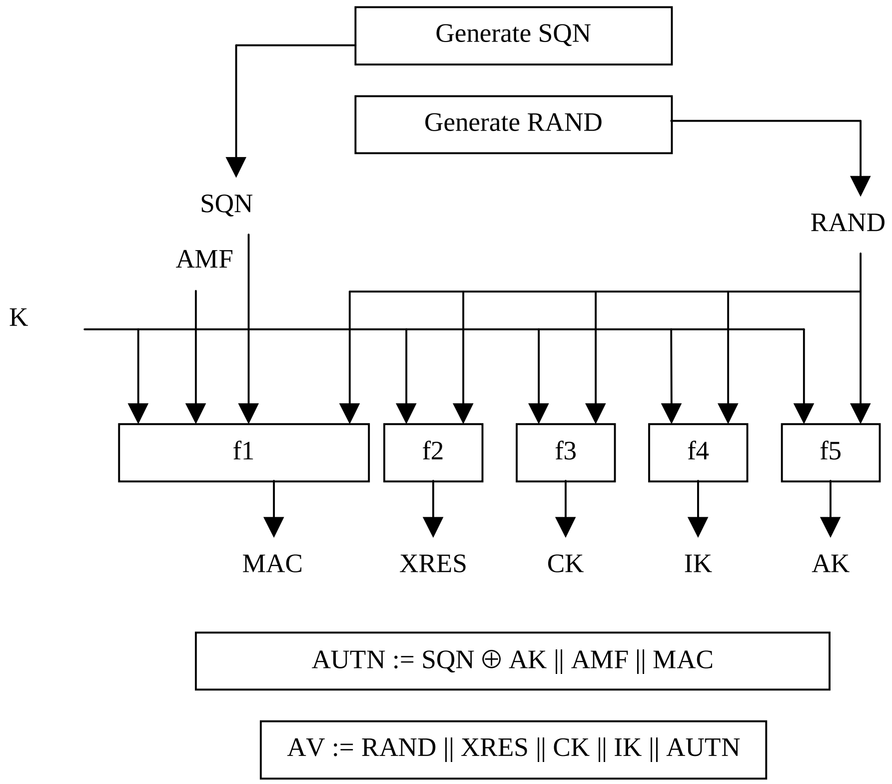


Figure 6: Generation of an authentication vector

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~~:~~ SEQ_{HE}~~SQN_{HE}~~.

~~To generate a fresh sequence number, the counter is incremented and subsequently the SQN is set to the new counter value.~~

~~Note 1:~~ 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.

e) 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.
~~Such a~~The same minimum number x needs to be ~~defined~~ 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.

.~~Annex C and Annex F.3 contain alternative methods for the generation and verification of sequence numbers.~~

The use of SEQ_{HE} is specific to the method of generating sequence numbers. ~~It~~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 $f5 \equiv 0$.

~~Note 1: The need for f5 to use a long-term key different from K is ffs.~~

~~Note 2: The requirements on f3, f4 and f5 are ffs.~~

~~Note 3: It is also ffs in how far the functions f1, ..., f5 need to differ and how they may be suitably combined.~~

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 ~~SN/VLR~~VLR/SGSN and the MS. During the authentication, the user verifies the freshness of the authentication vector that is used.

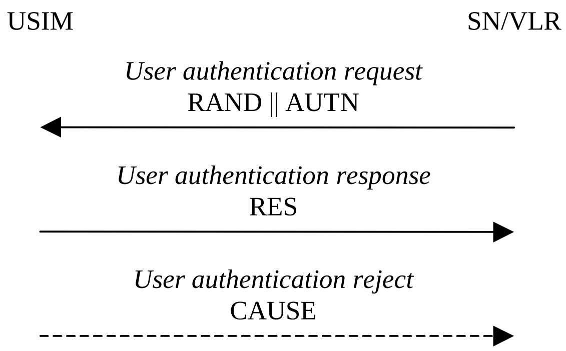


Figure 7: Authentication and key establishment

The ~~SN/VLR~~VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR database. The ~~SN/VLR~~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 8.

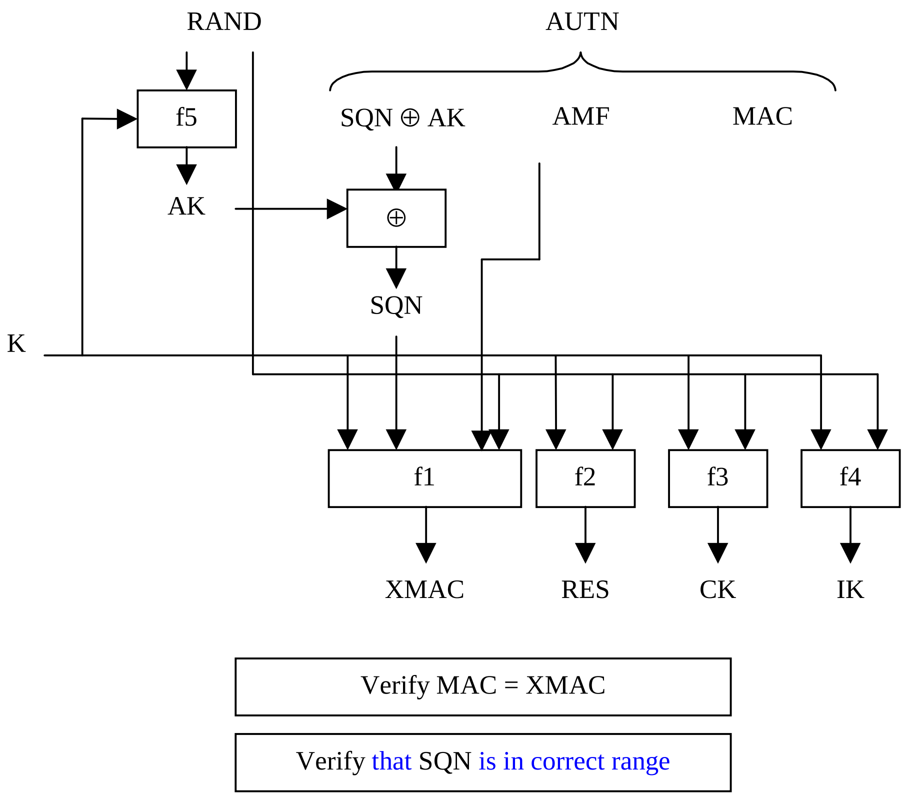


Figure 8: User authentication function in the USIM

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 ~~SN/VLR~~VLR/SGSN with an indication of the cause and the user abandons the procedure.

Next the ~~user~~ USIM verifies that the received sequence number SQN is ~~in the correct range~~fresh. ~~How the USIM does~~

~~this verification is described in Annex C.2.~~

~~The USIM keeps track of a counter: SQN$_{MS}$.~~

~~To verify that the sequence number SQN is in the correct range, the USIM compares SQN with SQN$_{MS}$. If SQN > SQN$_{MS}$ the MS considers the sequence number to be in the correct range and subsequently sets SQN$_{MS}$ to SQN.~~

~~Note: The MS and the HE have some flexibility in the management of sequence numbers. Annex C and Annex F.3 contain alternative methods for the generation and verification of sequence numbers.~~

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

The *synchronisation failure* message contains the parameter ~~*RAND$_{MS}$* ||~~ *AUTS*.
~~Here *RAND$_{MS}$* is the random value stored on the MS which was received in user authentication request causing the last update of *SQN$_{MS}$*.~~
It is *AUTS = Conc(SEQ$_{MS}$* ~~*SQN$_{MS}$*~~*) || MACS.*
Conc(SEQ$_{MS}$ ~~*SQN$_{MS}$*~~*) = SEQ$_{MS}$* ~~*SQN$_{MS}$*~~ *⊕ f5$_K$(*~~*RAND$_{MS}$*~~*MACS)* is the concealed value of the counter *SEQ$_{MS}$* ~~*SQN$_{MS}$*~~ in the MS, and.
MACS = f1$_K$(SEQ$_{MS}$* ~~*SQN$_{MS}$*~~ *|| 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 9:

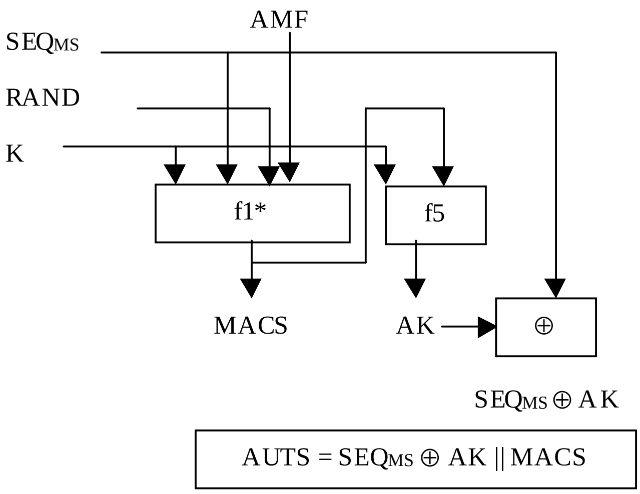


Figure 9: Construction of the parameter AUTS

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 ~~SN/VLR~~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 ~~SN/VLR~~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 ~~SN/VLR~~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 ~~SN/VLR~~VLR/SGSN: ~~Using the procedures described in subsections 6.3.1, 6.3.2 and 6.3.4, authentication vectors will have to be used in the specific order in which they were generated, otherwise the user will reject the authentication attempt.~~ The ~~SN/VLR~~**VLR/SGSN** shall use an authentication vector 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 authentication vectors cannot be reused. ~~When a user changes from one VLR to another one and the new VLR requests remaining authentication vectors from the old VLR (cf. subsection 6.3.4) then the old VLR shall not retain any copies of these authentication vectors. When a VLR receives a "cancel location" request for a certain user it shall delete all authentication vectors relating to that user. When a VLR receives a location update request from a user and the VLR notices that authentication vectors relating to that user are still stored in the VLR it will delete this information and request fresh authentication vectors from the HE/AuC.~~

~~Different rules may apply when one of the alternative schemes for sequence number handling described in Annex C or Annex F.3 are applied. This is true in particular when the schemes based on windows or lists described in Annexes C.3 and C.4 are applied.~~

6.3.3.1 Cipher key selection

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

6.3.3.1.1 User plane

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

6.3.3.1.2 Control plane

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

6.3.4 Distribution of authentication vectors between VLRs

The purpose of this procedure is to provide a newly visited VLR with unused authentication vectors from a previously visited VLR.

The procedure is shown in Figure 10.

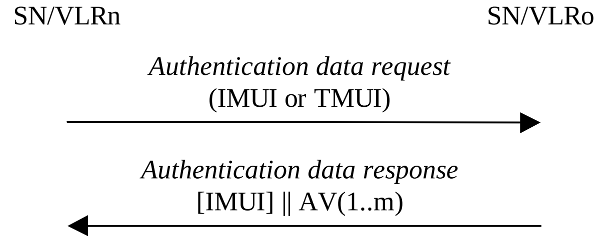


Figure 10: Distribution of authentication data between ~~SN/VLR~~VLR/SGSN

The procedure is invoked by the newly visited ~~SN/VLR~~**VLR/SGSN**n after a *location update request* sent by the user. Typically the user identifies himself using a temporary user identity TMUIo and the location area identity LAIo of a location area under the jurisdiction of ~~SN/VLR~~**VLR/SGSN**o. In that case this procedure is integrated with the procedure described in 6.1.4.

Upon receipt of the request the VLRo verifies whether it has any unused authentication vectors of the appropriate mode in its database and if so, sends the unused authentication vectors to VLRn. The previously visited VLRo shall then delete these authentication vectors from its database.

Upon receipt the VLRn stores the received authentication vectors.

If VLRo indicates that it has no authentication vectors or the VLRo cannot be contacted, VLRn should request new authentication vectors from the user's HE using the procedure described in 6.3.2.

6.3.5 Re-synchronisation procedure

An ~~SN/VLR~~**VLR/SGSN** may send two types of *authentication data requests* to the HE/AuC, the (regular) one described in subsection 6.3.2 and one used in case of synchronisation failures, described in this subsection.

Upon receiving a *synchronisation failure* message from the user, the ~~SN/VLR~~**VLR/SGSN** sends an *authentication data request* with a "*synchronisation failure indication*" to the HE/AuC, together with the parameters

- *RAND* sent to the MS in the preceding user authentication request and
- ~~$RAND_{MS}$ ||~~ *AUTS* received by the ~~SN/VLR~~**VLR/SGSN** in the response to that request, as described in subsection 6.3.3.

An ~~SN/VLR~~**VLR/SGSN** will not react to unsolicited " synchronisation failure indication" messages from the MS.

The ~~SN/VLR~~**VLR/SGSN**VLR/SGSN does not send new user authentication requests to the user before having received the response to its authentication data request from the HE/AuC (or before it is timed out).

When the HE/AuC receives an *authentication data request* with a "*synchronisation failure indication*" it acts as follows:
(1) ~~-~~The HE/AuC retrieves SEQ_{MS} from Conc(SEQ_{MS}) by computing $f5_K$(*MACS*)~~.~~.
(2) The HE/AuC checks if SEQ_{HE} is in the correct range, i.e. if the next sequence number generated SEQ_{HE} using would be accepted by the USIM. ~~$SEQ_{MS} < SEQ_{HE} < SEQ_{MS} + \Delta$ where the parameters SEQ_{MS} , SEQ_{HE} and Δ are defined in Annex C.~~
(3) If SEQ_{HE} is in the correct range then the HE/AuC continues with step (6), otherwise it continues with step (4).
(4) The HE/AuC verifies ~~*AUTS* by computing $f5_K(RAND_{MS})$, retrieving SQN_{MS} from Conc(SQN_{MS}) and verifying~~ *MACS* (cf. subsection 6.3.3.).
(5) If the verification is successful~~, but SQN_{MS} is such that SQN_{HE} is not in the correct range then the~~ the HE/AuC resets the value of the counter SEQ_{HE} ~~SQN_{HE}~~ to SEQ_{MS}~~SQN_{MS}~~.
~~Otherwise, the HE/AuC leaves SQN_{HE} unchanged.~~
(6) ~~In all cases the~~ The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the ~~SN/VLR~~VLR/SGSN.

If the counter SEQ_{HE}~~SQN_{HE}~~ was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting SEQ_{HE}~~SQN_{HE}~~. In order to reduce the real-time computation burden on the HE/AuC, the HE/AuC may also send only a single authentication vector in the latter case.

Whenever the ~~SN/VLR~~VLR/SGSN receives a new batch of authentication vectors from the HE/AuC in an authentication data response to an *authentication data request* with synchronisation failure indication it deletes the old ones for that user in the ~~VLR~~VLR/SGSN.

The user may now be authenticated based on a new authentication vector from the HE/AuC.
~~Optionally, in order to minimise extra effort by the HE/AuC, in an authentication data request with synchronisation failure indication the SN/VLR may also send the concealed sequence number Conc(SQN_{SN}) corresponding to the last authentication vector received which the SN/VLR has in storage, i.e. it may send Conc(SQN_{SN}) = $RAND_{SN}$ || $SQN_{SN} \oplus f5_K(RAND_{MS})$.~~

~~On receipt the HE/AuC retrieves SQN_{SN} from Conc(SQN_{SN}). If the counter in the HE/AuC did not have to be reset and if $SQN_{SN} = SQN_{HE}$ the HE/AuC informs the SN/VLR accordingly and does not send fresh authentication vectors. (In this way, a synchronisation failure does not cause the HE/AuC to produce extra authentication vectors when they are not needed.)~~

Figure 11 shows how re-synchronisation is achieved by combining a *user authentication request* answered by a *synchronisation failure* message (as described in subclause 6.3.3) with an *authentication data request* with *synchronisation failure* indication answered by an *authentication data response (*as described in this subclause*).*

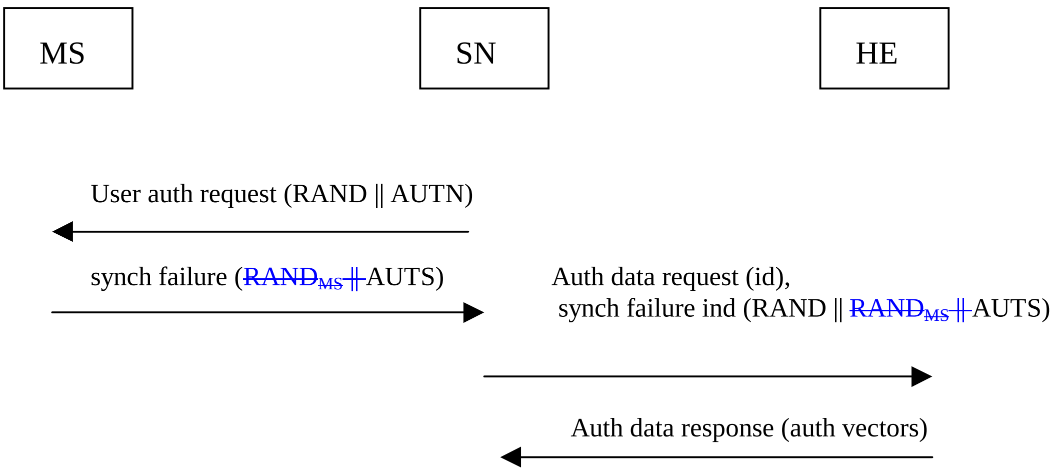


Figure 11: Re-synchronisation procedure

6.3.6 Length of sequence numbers

Sequence numbers ~~shall~~ shall have a length of 6 octets. ~~be sufficiently long so that they cannot wrap around during the lifetime of the system. Consequently, in normal operations neither~~ ~~SQN~~$_{MS}$ ~~nor SQN~~$_{HE}$ ~~can wrap around during the lifetime of a USIM.~~

~~Note 1: If the counters would derive sequence numbers from time (see Annex C), then a 32-bit counter that is derived from the number of seconds that have elapsed since January 1, 2000 would only wrap around in the year 2136. So a length of 32-bits for the sequence numbers and counters should be sufficient. For individual incremental counters, a smaller range of sequence numbers should be sufficient, as authentication and key agreement is expected to occur far less frequently than once every second. Shorter lengths would however exclude the use of time-derived sequence numbers.~~

~~Note 2: Sequence numbers for CS and PS operation are expected to have the same length.~~

~~6.3.7 Support for window and list mechanisms~~

~~In Annex C.3 and Annex C.4 respectively, the window and list mechanisms for sequence number management in the USIM are described. If one of these mechanisms is employed in the USIM and if there is no need to conceal sequence numbers then the MS shall send information on the current value of the lowest entry~~ ~~SQN~~$_{LO}$ ~~in the window or list to the SN/VLR at every location update. Sequence numbers which do not need to be concealed may be generated according to Annex C.2 or Annex C.6.~~

~~When the SN/VLR authenticates a user for the first time after receiving a new value~~ ~~SQN~~$_{LO}$ ~~from the MS then the SN/VLR checks whether the sequence number of the authentication vector it wants to use is greater than~~ ~~SQN~~$_{LO}$~~. The SN/VLR uses the AV only if this is the case. Otherwise, the AV is discarded. If all AVs have to be discarded the SN/VLR requests new ones from the HE/AuC.~~

TSG SA WG3 #8, **S3-99552**

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**	**27r1**	Current Version:	V3.2.0
3G specification number ↑		*↑ CR number as allocated by 3G support team*		

For submission to TSG: SA#6 — *list TSG meeting no. here ↑*

for approval	X	*(only one box should*
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	ME	UTRAN	Core Network
X	X	X	X

Source:	S3	**Date:**	16-11-99
Subject:	Clarification of re-authentication during PS connections.		
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: Re-authentication and key setting should be possible during a PS connection so that the cipher and integrity keys can be updated during long connections. This capability is provided in GPRS. The current text in section 6.4.1 is not very clear on whether this should be supported.

Clauses affected: Section 6.4.1

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:

6.4.1 Authentication and c~~C~~ipher 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. Key setting is triggered by the authentication procedure and described in ~~xxx~~6.3. Authentication and k~~K~~ey 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, the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the UE ~~immediately after~~ as part of the security mode negotiation (see 6.4.5) that follows ~~at the end of~~ the authentication procedure ~~in both the RNC and the UE~~.