Technical Specification Group Services and System Aspects Meeting #4, Miami, USA, 21-23 June 1999 ***TSG SA#4(99)308***

TSG SA WG3 #4, London, 16-18 June 1999 **S3-99203**

Subject: Change requests to 3G TS 33.102
Source: TSG SA WG3
Document for: Approval

The following CRs to 3G TS 33.102 V3.0.0 are presented to SA#4 for approval:

CR	REV	SUBJECT	CAT	Date of CR	SOURCE	STC_MEET	STC_DOC
001		Mechanism for data integrity of signalling messages	C	990618	S3	4	S3-99203
002		Description of layer on which ciphering takes place	C	990618	S3	4	S3-99203
003		Conditions on use of authentication information	C	990618	S3	4	S3-99203
004		Modified re-synchronisation procedure for AKA protocol	C	990618	S3	4	S3-99203
005		Sequence number management scheme protecting against USIM lockout	C	990618	S3	4	S3-99203
006		Criteria for Replacing the Authentication “Working Assumption”	C	990618	S3	4	S3-99203
007		Functional modification of Network domain security mechanisms	C	990618	S3	4	S3-99203
008		Cipher key lifetime	C	990618	S3	4	S3-99203
009		Mechanism for user domain security	C	990618	S3	4	S3-99203
010		Replacement of incorrect diagrams	F	990618	S3	4	S3-99203
011		Precision of the status of annex B	C	990618	S3	4	S3-99203

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 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**	**010**	Current Version:	3.0.0

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

For submision to TSG SA#4 *list TSG meeting no. here ↑* for approval **X** for information *(only one box should be marked with an X)*

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

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

Source: SA WG3 **Date:** 99-06-18

Subject: Replacement of incorrect diagrams

3G Work item: DTS/TSGS-0333102U

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: Due to conversion errors between word processor versions, figures 2, 5, 7, 9 and 10 need to be replaced with the appropriate diagrams.

Clauses affected: 6.1.2, 6.3.2, 6.3.3, 6.3.4, 6.3.5

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: Diagrams have been retrieved from the previous SA WG3 version 0.1.4 which was converted for presentation as version 2.0.0 at TSG-SA#3.

help.doc

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

6.1.2 TMUI reallocation procedure

The purpose of the mechanism described in this subsection is to allocate a new TMUI/LAI pair to a user by which he may subsequently be identified on the radio access link.

The procedure should be performed after the initiation of ciphering. The ciphering of communication over the radio path is specified in clause 6.6.

The allocation of a temporary identity is illustrated in Figure 2.

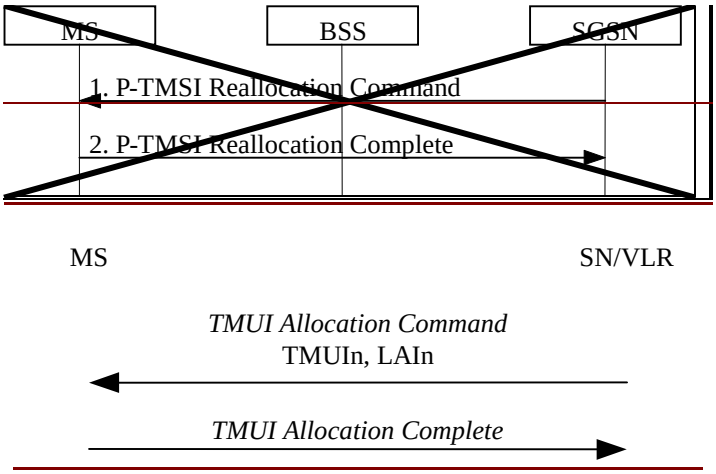


Figure 2: TMUI Allocation

The allocation of a temporary identity is initiated by the VLR.

The VLR generates a new temporary identity (TMUIn) and stores the association of TMUIn and the permanent identity IMUI in its database. The TMUI should be unpredictable. The VLR then sends the TMUIn and (if necessary) the new location area identity LAIn to the user.

Upon receipt the user stores TMUIn and automatically removes the association with any previously allocated TMUI. The user sends an acknowledgement back to the VLR.

Upon receipt of the acknowledgement the VLR removes the association with the old temporary identity TMUIo and the IMUI (if there was any) from its database.

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.

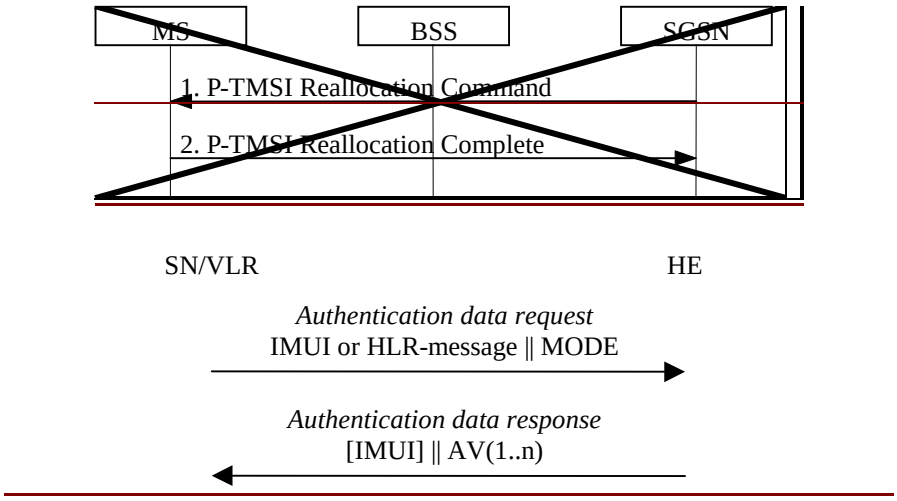


Figure 5: Distribution of authentication data from HE to SN/VLR

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

The *authentication data request* shall include a user identity and a parameter MODE that indicates whether the requesting node is a PS node or a CS node. 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).

…

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.

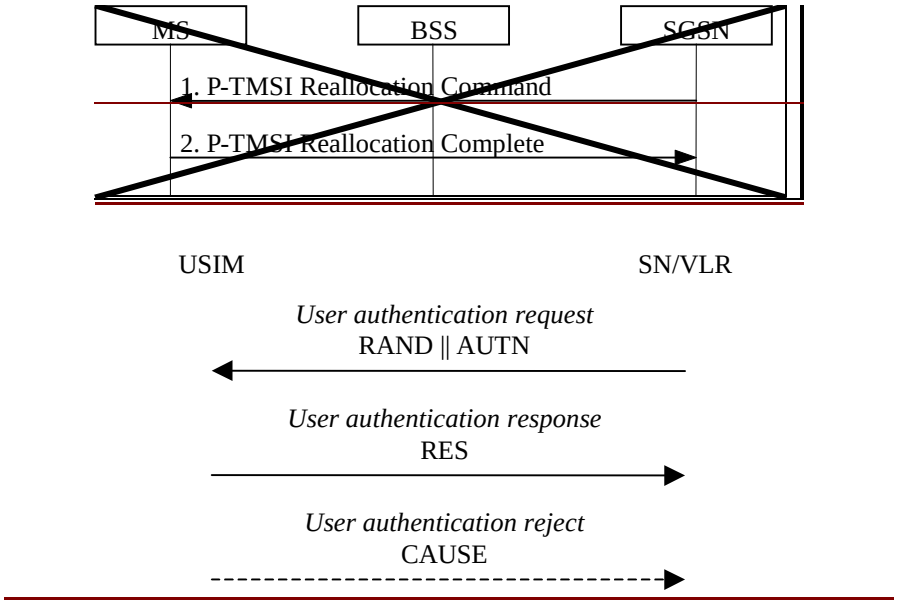


Figure 7: Authentication and key establishment

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.

…

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 9.

The procedure is initiated by the visited VLR and illustrated in the following figure:

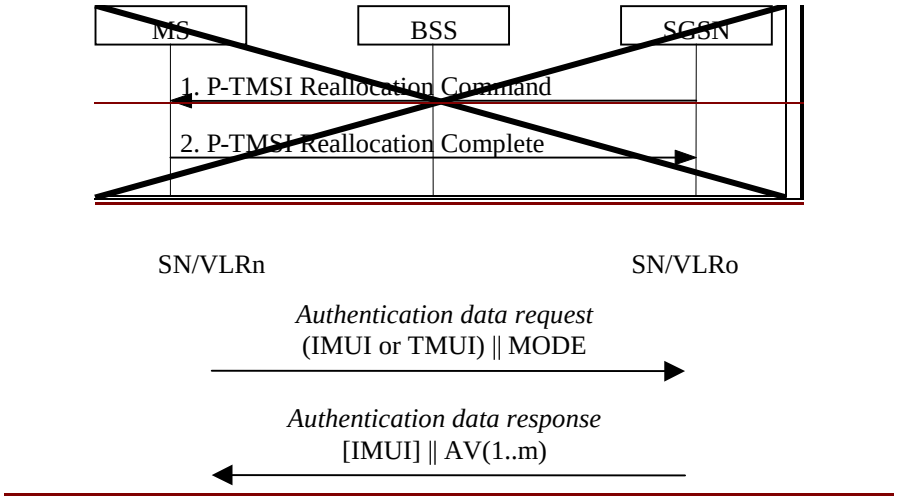


Figure 9: Distribution of authentication data between SN/VLR

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. In addition, the SN/VLRn indicates whether it is a CS or PS node.

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

The purpose of this procedure is to re-synchronise a counter in the HLR/AuC with a counter in the USIM. The procedure may be invoked by the HLR/AuC in the event of:

- a database failure in the HLR/AuC whereby the value of the counter $SQN_{HE/MODE}$ is lost;
- a message coming from the SN/VLR saying that the user could verify the data integrity of AUTN sent by the SN/VLR, but that he rejected AUTN because $SQN \leq SQN_{MS/MODE}$. In normal operations this should not happen. This may point to a replay of AUTN || RAND, but may also be caused because the counter value in the HLR/AuC is accidentally set to a lower value than is required.

The re-synchronisation procedure is described in Figure 10:

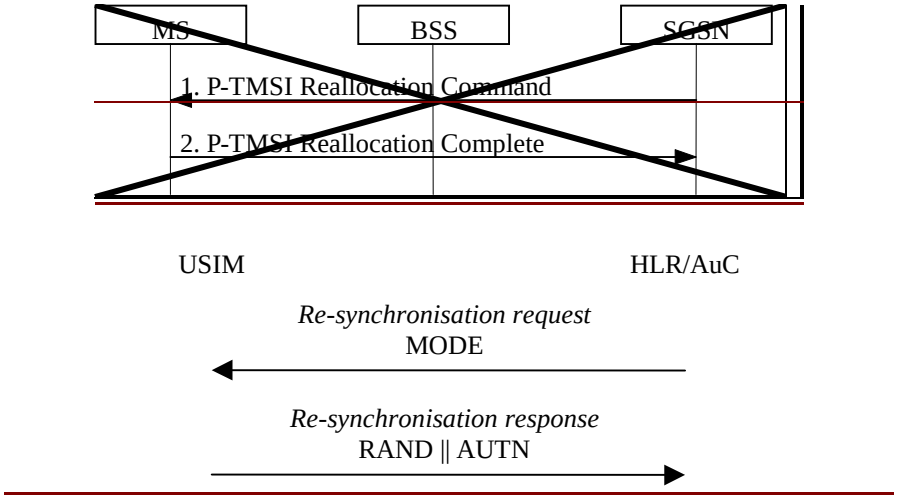


Figure 10: Re-synchronisation of the counter in the HLR/AuC

The HLR/AuC initiates the re-synchronisation procedure by sending a *re-synchronisation request* to the user that includes the appropriate mode.

Upon receipt of the request the USIM sends a *re-synchronisation response* back to the HLR/AuC that includes a RAND and AUTN pair with $SQN = SQN_{MS/MODE}$. The USIM has several ways to produce RAND || AUTN. Either it stores and returns the latest received RAND || AUTN pair, or it only stores the received RAND and re-computes AUTN, or it generates a RAND and computes the corresponding AUTN. AUTN is computed as described in 6.3.2.

Upon the receipt of the *re-synchronisation response* the HLR/AuC verifies the data integrity of AUTN as described in 6.3.3. Only if the received SQN is greater than $SQN_{HE/MODE}$, then $SQN_{HE/MODE}$ is set to SQN.

Technical Specification Group Services and System Aspects ***TSG SA#4(99)___***
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **S3-99203**

Subject: Change requests to 3G TS 33.102
Source: TSG SA WG3
Document for: Approval

The following CRs to 3G TS 33.102 V3.0.0 are presented to SA#4 for approval:

CR	REV	SUBJECT	CAT	Date of CR	SOURCE	STC_MEET	STC_DOC
001		Mechanism for data integrity of signalling messages	C	990618	S3	4	S3-99203
002		Description of layer on which ciphering takes place	C	990618	S3	4	S3-99203
003		Conditions on use of authentication information	C	990618	S3	4	S3-99203
004		Modified re-synchronisation procedure for AKA protocol	C	990618	S3	4	S3-99203
005		Sequence number management scheme protecting against USIM lockout	C	990618	S3	4	S3-99203
006		Criteria for Replacing the Authentication “Working Assumption”	C	990618	S3	4	S3-99203
007		Functional modification of Network domain security mechanisms	C	990618	S3	4	S3-99203
008		Cipher key lifetime	C	990618	S3	4	S3-99203
009		Mechanism for user domain security	C	990618	S3	4	S3-99203
010		Replacement of incorrect diagrams	F	990618	S3	4	S3-99203
011		Precision of the status of annex B	C	990618	S3	4	S3-99203

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex A of S3-99203**

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	001	Current Version:	3.0.0

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

For submision to TSG SA#4 *list TSG meeting no. here ↑* for approval **X** for information *(only one box should be marked with an X)*

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

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

Source: 3GPP TSG SA WG 3 **Date:** 1999-06-18

Subject: Mechanism for data integrity of signalling messages

3G Work item: DTS/TSGS-0333102U

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: Progress of work on the mechanism.

Clauses affected: 6.4

Other specs affected:

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

Other comments:

help.doc

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

6.4 Data integrity of signalling elements

6.4.1 General

Some RRC, MM and CC signalling information elements are considered sensitive and must be integrity protected. An integrity function shall be applied on certain signalling information elements transmitted between the MS and the SN.

~~The UMTS Integrity Algorithm (UIA) shall be implemented in the USIM and in the RNC.~~

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

At least ~~The~~ the following signalling elements sent by the MS to the RNC should be protected:

- ~~—~~The MS capabilities, including authentication mechanism, ciphering algorithm and message authentication function capabilities.
- ~~—~~The security mode accept/reject message.
- ~~—~~The called party number in a mobile originated call.
- ~~—~~Periodic message authentication messages.
- Various location updates, e.g. cell updates and URA updates.

At least ~~The~~ the following signalling elements sent by the RNC to the MS should be protected:

- The security mode command, including whether ciphering is enabled or not and the ciphering and integrity algorithm to be used.
- Periodic message authentication messages.

~~Note: The point at which integrity protection is applied in the UTRAN architecture is for further study. At this stage we assume that integrity protection is applied at the RNC but may be applied at the MSC/VLR.~~

6.4.2 Integrity algorithm

The UMTS Integrity Algorithm (UIA) shall be implemented in the MS and in the RNC.

Figure 1 illustrates the use of the UIA to authenticate the data integrity of a signalling message.

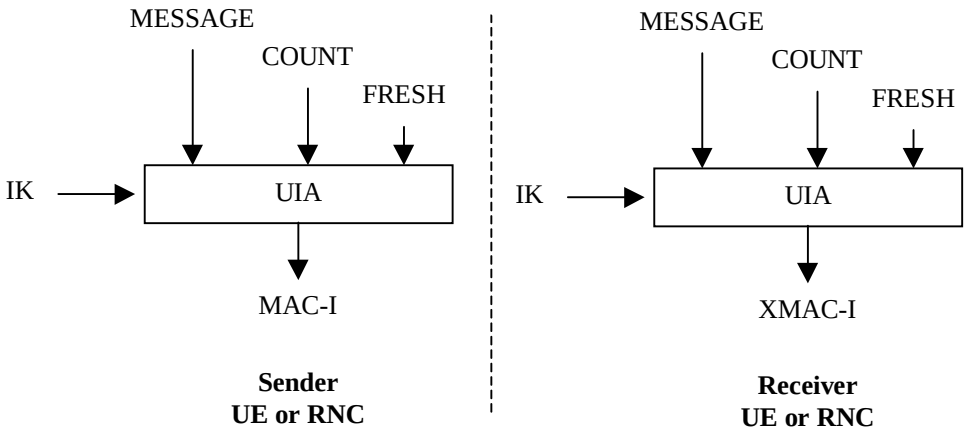


Figure 1: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), a time dependent input (COUNT), a random value generated by the network side (FRESH) and the signalling data (MESSAGE). Based on these input parameters the user computes message authentication code for data integrity (MAC-I) using the UMTS Integrity Algorithm (UIA). The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the

message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I.

The input parameter COUNT protects against replay during a connection. It is a value incremented at both sides of the radio access link every 10 ms layer 1 frame. Its initial value is sent by the user to the network at connection set-up. The user stores the last used COUNT value from the previous connection and increments it by one. In this way the user is assured that no COUNT value is re-used (by the network) with the same integrity key.

The input parameter FRESH protects network against replay of signalling messages by the user. At connection set-up the network generates a random value FRESH and sends it to the user. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is.

6.4.~~2~~3 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 6.3. Key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. TMUI or IMUI) is known by the SN/VLR. The key IK is stored in the SN/VLR and transferred to the RNC when it is needed. The key IK is stored in the USIM until it is updated at the next authentication.

6.4.~~3~~4 Key set identifier

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.~~4~~5 Integrity key lifetime

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

Each time an RRC connection is released the highest value of the hyperframe number 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.

~~Operators shall decide on the value of this number of calls, and write this parameter on the USIM. The USIM shall have a counter that counts the number of times the integrity key is used and~~ The USIM shall trigger the generation of a new ~~integrity key~~ access link key set (a cipher key and an integrity key) if the counter reaches ~~the~~ a maximum value set by the operator and stored in the USIM[1] at the next RRC connection request message sent out. This mechanism will ensure that an integrity key and cipher key cannot be reused more times than the limit set by the operator.

~~Note: The decision on when a key needs to be updated may depend on a number of factors, including the time since the last key update, the amount of data protected using that key, and the cost/value of the services protected through the use of that key. Unfortunately they cannot be easily measured by the USIM, so it is suggested that the number of calls made using the key should be measured instead. Some concern exists whether this is a good enough measure. Should also the (periodic) in-call authentication messages be counted, such that long calls weigh more than short calls? Should also the authentications based on a shared integrity key be counted, invoked for other purposes than for calls?~~

[1] *Which message should be chosen as a parameter? Using this would register call attempts as well as calls...*

6.4.5 UIA numbering

Table ~~Error! Style not defined..Error! Bookmark not defined.~~1 - UIA numbering

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

6.4.6 UIA negotiation

Not more than [n] versions of the UIA algorithm will be defined.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM classmark which version of the UIA algorithm the ~~USIM~~ MS supports. This message itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving classmark the latter must be stored in the RNC and the integrity of the classmark with the newly generated IK and this value is transmitted to the RNC after the authentication procedure is complete.

~~Note: This message itself must be integrity protected itself which effectively means that there must be at least one UIA algorithm in common, otherwise the connection is released.~~

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

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

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

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

6.4.7 Integrity protection procedures

~~Note: The integrity protection procedures are for further study.~~

Integrity protection is performed by appending a message authentication code (MAC-I) to the message that is to be integrity protected. The MS can append the MAC-I to signalling messages as soon as it has received a connection specific FRESH value from the RNC.

If the value of HFN_{MS} is larger or equal to the maximum value stored in the USIM, the MS indicates to the network in the RRC connection set-up that it is required to initialize a new authentication and key agreement.

Note: The precise set-up of data integrity is for further study.

6.4.7.1 Handover

Note: It is expected that in case of inter-operator handover a handover agreement exists that covers all charging aspects. Agreements on cipher key transportation/re-use shall also be included.

1) Intra-system:

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

2) Inter-system/ (between 2G and other 3G mobile radio systems and UMTS):

The following functionality has to be provided.

2G and other 3G mobile radio systems → UMTS

The UMTS network entered by the user handing over from other systems will enable integrity protection. This will involve setting the integrity protection key. There are two options:

a) Establishing the integrity protection key (with UMTS key formats) using the UMTS authentication and key agreement mechanism.

b) Deriving of integrity protection key (with UMTS key formats) from the existing cipher key (e.g. GSM formats).

Note 1: One of the two possibilities a), b) has to be chosen and agreed!

Note 2: A third option may be that a user at handover to the UMTS network returns to a previously visited UMTS network, with which he still shares a cipher and integrity key (e.g., because he was handed over from that UMTS network to the 2G or other 3G mobile radio system previously, during the same call). M

UMTS → other systems

The integrity protection key has to be deleted securely.

Note: Rather than deleting the integrity key, the UMTS network may store the integrity key securely for use in case the user would return to the UMTS network in a second handover.

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex B of S3-99203**

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** **002** Current Version: 3.0.0

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

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

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

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

Source: SA3 **Date:**

Subject: Description of layer on which ciphering takes place

3G Work item: UTRAN 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: Description of the layer on which ciphering takes place is inserted following agreement on this with RAN2.

Clauses affected: New clause 6.6.9.3

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.

6.6.9 Ciphering procedures

6.6.9.1 Starting of the ciphering and deciphering processes

The MS and the RNC must co-ordinate the instants at which the enciphering and deciphering processes start.

This procedure takes place under the control of the network some time after the completion of the authentication procedure (if any), or after the key CK has been made available at the RNC.

No information elements for which protection is needed must be sent before the ciphering and deciphering processes are operating.

The transition from clear text mode to ciphered mode proceeds as follows: deciphering starts in the RNC, which sends in clear text to the MS a specific message, here called "Start cipher". Both the enciphering and deciphering start on the MS side after the message "Start cipher" has been correctly received by the MS. Finally, enciphering on the RNC side starts as soon as a frame or a message from the MS has been correctly deciphered at the RNC.

[diagram to be added]

6.6.9.2 Synchronisation

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

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

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

[diagram to be added]

6.6.9.3 Layer for ciphering

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

6.6.9.43 Handover

Note: It is expected that in case of inter-operator handover a handover agreement exists that covers all charging aspects. Agreements on cipher key transportation/re-use shall also be included.

1) Intra-system

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

2) Inter-system

The following functionality has to be provided.

2G and other 3G mobile communications systems → UMTS

The UMTS network entered by the user handing over will enable integrity protection. This will involve setting the integrity protection key. There are two options:

a) Establishing the cipher key CK (with UMTS key format) using the UMTS authentication and key agreement mechanism.

b) Deriving of cipher key (with UMTS key formats) from the existing cipher key (e.g. GSM formats).

UMTS → 2G and other 3G mobile communications systems

a) Establishing the system specific security key (e.g. in case of GSM: cipher key Kc with GSM key format) using the system specific key agreement mechanisms.

b) Deriving the system specific security keys (e.g. in case of GSM: cipher key K_C with GSM key format) from the UMTS cipher key.

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex C of S3-99203**

TSG SA WG3 #4, London, 16-18 June 1999-06-16

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** **003** Current Version: V3.0.0

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

For submission to TSG SA#4 *list TSG meeting no. here* ↑ for approval [X] for information [ ] *(only one box should be marked with an X)*

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

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

Source: Siemens AG **Date:** 99-06-18

Subject: Conditions on use of authentication 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: Authentication information needs to be handled by the SN/VLR according to certain rules. These rules are not clearly described in the current version of 33.102 and are therefore added for clarification.

Clauses affected: 6.3.3

Other specs affected:

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

Other comments:

help.doc

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

6.3.3 Authentication and key agreement

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

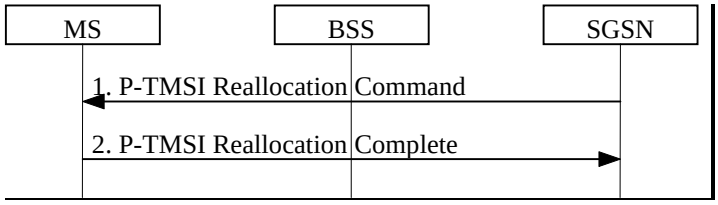


Figure 1: Authentication and key establishment

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 2.

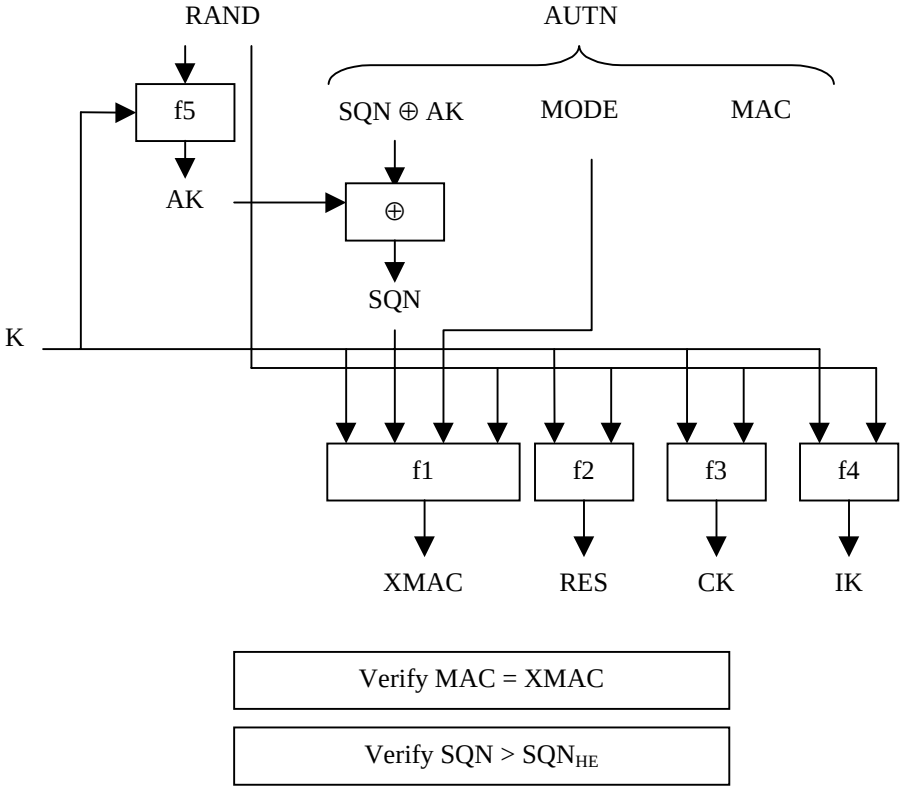


Figure 2: User authentication function in the USIM

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 || MODE) 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 the freshness of the received sequence number SQN.

For each mode the USIM keeps track of one counter: $SQN_{MS/CS}$ for authentications initiated by the CS CN nodes, and $SQN_{MS/PS}$ for authentications initiated by the PS CN nodes.

To verify the freshness of the sequence number SQN, the USIM compares SQN with $SQN_{MS/MODE}$. If SQN > $SQN_{MS/MODE}$ the MS considers the sequence number as fresh and subsequently sets $SQN_{MS/MODE}$ to SQN.

Note: The HE has some flexibility in the management of sequence numbers. Annex C contains alternative method for the generation and verification of sequence numbers.

If the user considers the sequence numbers not fresh, he sends *user authentication reject* back to the SN/VLR with an indication of the cause and the user abandons the procedure.

If the sequence number is consider fresh 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.

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 is applied. This is true in particular when the schemes based on windows or lists described in Annexes C.3 and C.4 are applied.

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex D of S3-99203**

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** **004** Current Version: V3.0.0

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

For submission to TSG SA#4 *list TSG meeting no. here ↑* for approval [X] for information [ ] *(only one box should be marked with an X)*

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

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

Source: TSG SA WG3 **Date:** 99-06-18

Subject: Modified re-synchronisation procedure for AKA protocol

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 procedure for re-synchronisation of sequence numbers in TS 33.102 V3.0.0 takes more messages than necessary and introduces a new MAP-procedure which can be avoided. Furthermore, the proposed changes provide freshness guarantees for the re-synchronisation message.

Clauses affected: 6.3.3, 6.3.5

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:


help.doc

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

6.3 Authentication and key agreement

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.

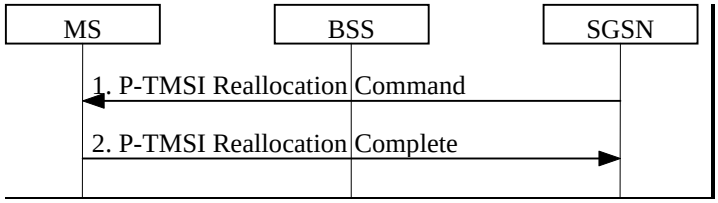


Figure 1: Authentication and key establishment

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 2.

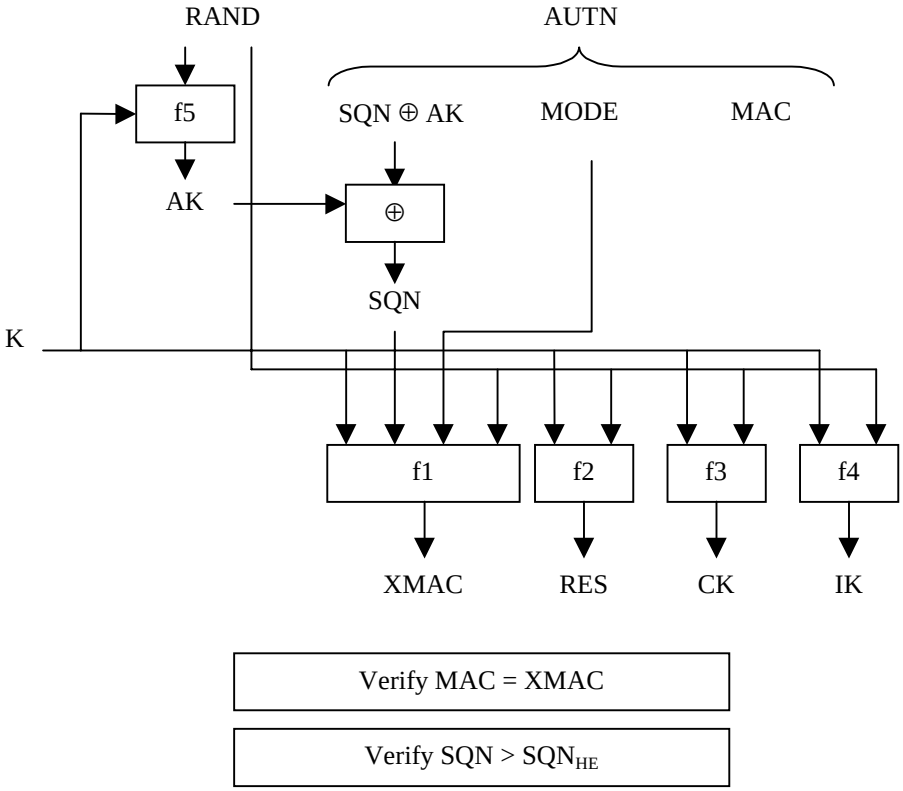


Figure 2: User authentication function in the USIM

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 || MODE) 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 ~~the freshness of~~that the received sequence number SQN is in the correct range.

For each mode the USIM keeps track of one counter: $SQN_{MS/CS}$ for authentications initiated by the CS CN nodes, and $SQN_{MS/PS}$ for authentications initiated by the PS CN nodes.

To verify ~~the freshness of~~that the sequence number SQN is in the correct range, the USIM compares SQN with $SQN_{MS/MODE}$. If SQN > $SQN_{MS/MODE}$ the MS considers the sequence number ~~as fresh~~to be in the correct range and subsequently sets $SQN_{MS/MODE}$ to SQN.

~~Note: The HE has some flexibility in the management of sequence numbers. Annex C contains alternative method for the generation and verification of sequence numbers.~~

~~If the user considers the sequence numbers not fresh, he sends *user authentication reject* back to the SN/VLR with an indication of the cause and the user abandons the procedure.~~

Note: The MS and the HE have some some flexibility in the management of sequence numbers. Annex C contains 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.
$MACS = f1^*_K(SQN_{MS} \| RAND \| MODE)$ 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 construction of the parameter AUTS in shown in the following figure xxx:

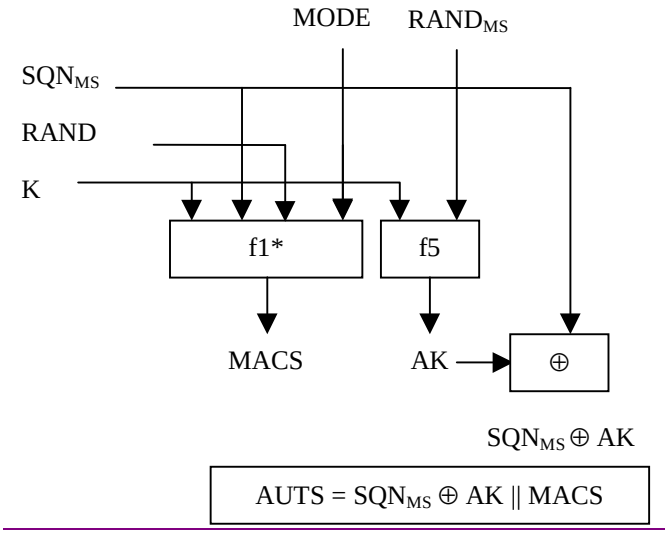


Figure xxx: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range ~~fresh~~ 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.

6.3.5 Re-synchronisation procedure

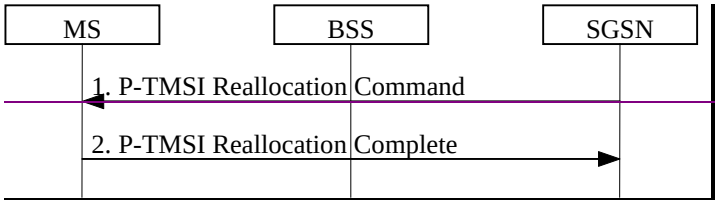
The purpose of this procedure is to re-synchronise a counter in the HLR/AuC with a counter in the USIM.

~~The procedure may be invoked by the HLR/AuC in the event of:~~

~~- a database failure in the HLR/AuC whereby the value of the counter $SQN_{HE/MODE}$ is lost;~~

~~- a message coming from the SN/VLR saying that the user could verify the data integrity of AUTN sent by the SN/VLR, but that he rejected AUTN because $SQN \leq SQN_{MS/MODE}$. In normal operations this should not happen. This may point to a replay of AUTN || RAND, but may also be caused because the counter value in the HLR/AuC is accidentally set to a lower value than is required.~~

~~The re-synchronisation procedure is described in Figure 3:~~



~~Figure 3: Re-synchronisation of the counter in the HLR/AuC~~

~~The HLR/AuC initiates the re-synchronisation procedure by sending a *re-synchronisation request* to the user that includes the appropriate mode.~~

~~Upon receipt of the request the USIM sends a *re-synchronisation response* back to the HLR/AuC that includes a RAND and AUTN pair with $SQN = SQN_{MS/MODE}$. The USIM has several ways to produce RAND || AUTN. Either it stores and returns the latest received RAND || AUTN pair, or it only stores the received RAND and re-computes AUTN, or it generates a RAND and computes the corresponding AUTN. AUTN is computed as described in 6.3.2.~~

~~Upon the receipt of the *re-synchronisation response* the HLR/AuC verifies the data integrity of AUTN as described in 6.3.3. Only if the received SQN is greater than $SQN_{HE/MODE}$, then $SQN_{HE/MODE}$ is set to SQN.~~

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($SQN_{SN/MODE}$). 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 10 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).

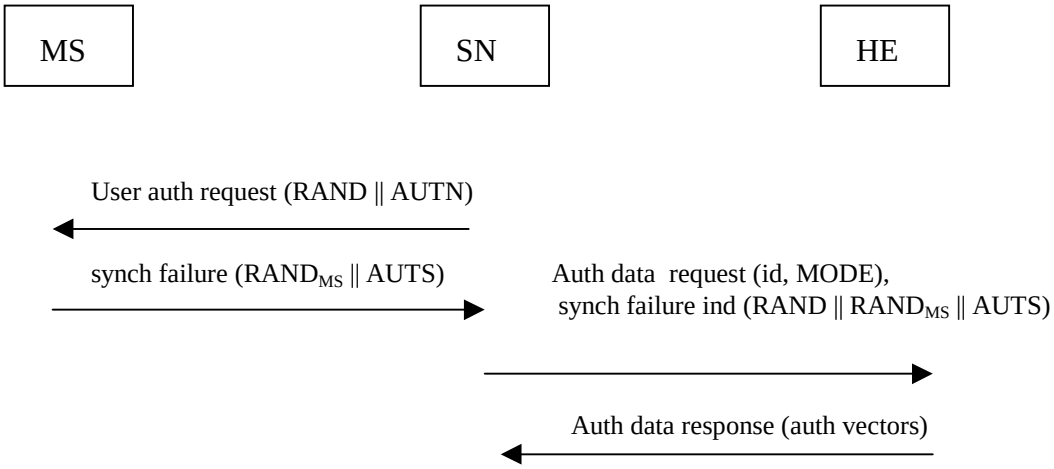


Figure xxx: Re-synchronisation procedure

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex E of S3-99203**

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** **Xxx** Current Version: V3.0.0

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

For submission to TSG SA#4 *list TSG meeting no. here ↑* for approval [X] for information [ ] *(only one box should be marked with an X)*

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

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

Source: TSG SA WG3 **Date:** 99-06-18

Subject: Sequence number management scheme protecting against USIM lockout

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: If a serious breach of security in the Authentication Centre ever occurred it could lead to a denial of service condition called USIM lockout. The new scheme prevents this condition. The CR does not imply anything about the likelihood of such an event.

Clauses affected: Annex C.5 (new)

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.

[new text:]

Annex C:
Management of sequence numbers

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

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.

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex F of S3-99203**

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	006	Current Version:	3.0.0

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

For submission to TSG SA#4 *list TSG meeting no. Here ↑* for approval [X] for information [ ] *(only one box should be marked with an X)*

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

Proposed change affects: *(at least one should be marked with an X)*

USIM	ME	UTRAN	Core Network
[ ]	[ ]	[ ]	[X]

Source: TSG SA WG3 **Date:** 99-06-18

Subject: Criteria for Replacing the Authentication "Working Assumption"

3G Work item:

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: To provide the criteria for replacing the current authentication "working assumption" with the alternate method described in the annex D of TS 33.102

Clauses affected: Annex D of TS 33.102 – new paragraph "D.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.

Annex D: A mechanism for authentication based on a temporary key

D.3 Criteria for replacing the authentication "working assumption"

One of the following conditions should be met before considering replacement of the authentication "working assumption":

- A serious security flaw is discovered with the SQN protocol. A "serious flaw" is a weakness that allows a demonstrable attack on the authentication system, leading to theft of service (fraud), compromise of privacy, or any degradation below the security level of current systems. If the flaw can be easily fixed without changing the fundamental nature of the protocol, there are no grounds for replacement.

- Serious operational difficulties are discovered with the SQN protocol. These are problems implementing the protocol that may be discovered during early development or testing. A "serious operation difficulty" is one that prevents the successful and reliable completion of the protocol. If the problem can be solved with a simple alteration that does not change the fundamental nature of the protocol, there are no grounds for replacement.

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 — Annex G of S3-99203

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**	**007**	Current Version:	3.0.0

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

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

for approval: **X**

for information:

(only one box should be marked with an X)

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

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

Source: 3GPP TSG S3 **Date:** 99-06-18

Subject: Functional modification of Network domain security mechanisms

3G Work item: 3G 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	
C	Functional modification of feature	X
D	Editorial modification	

Reason for change: Functional modification of Core Network Security

Clauses affected: 2.1, 3.3, 7 (complete), Annex E

Other specs affected:

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

Other comments:

help.doc

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

2.1 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

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

– break –

3.3 Abbreviations

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

3GMS	Third Generation Mobile Communication System
AK	Anonymity Key
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
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 toY
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMUI	International Mobile User Identity
IV	Initialisation Vector
KAC_X	Key Administration Center 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
MAC	Message Authentication Code
MAC	The message authentication code included in AUTN, computed using f1
MAP	Mobile Application Part
MS	Mobile Station
MSC	Mobile Services Switching Centre
MT	Mobile Termination
NE_X	Network Element of Network X
PS	Packet Switched
TE	Terminal Equipment
TMUI	Temporary Mobile User Identity
RAND	Random challenge
RND_X	Unpredictable Random Value generated by X
SEQ	Sequence number
SN	Serving Network
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	Temporary Mobile User Identity
TTP	Trusted Third Party
TVP	Time Variant Parameter
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UN	User Name
USIM	User Services Identity Module
VLR	Visited Location Register
X	Network Identifier
XRES	Expected Response
XUR	Expected User Response
Y	Network Identifier

– break –

7 Network domain security mechanisms

~~The authentication and key agreement scheme assumes that authentication information passed between network nodes in appropriate signalling information elements is adequately protected. Also administrative network element commands, e.g. HLR Reset, have to be protected.~~

This subclause describes mechanisms for establishing secure signalling links between network nodes, in particular between SN/VLRs and HE/AuCs. Such procedures may be incorporated into the roaming agreement establishment process.

~~Note: Mechanisms are required to allow all SN-HE pairs to establish a secure signalling connection. These mechanisms could be part of the roaming agreement establishment process between operators. In addition to the usual signalling link establishment and testing, the SN-HE pair could agree on algorithms and keys for protecting signalling links.~~

~~The mechanism described in annex E 'A Proposal for Securing SS7 Based Transmission of Sensitive Data between Network Elements' will be used as a basis for further developments.~~

7.1 Overview of Mechanism

The proposed mechanism consists of three layers.

7.1.1 Layer I

Layer I is a secret key transport mechanism based on an asymmetric crypto-system and is aimed at agreeing on a symmetric session key for each direction of communication between two networks X and Y.

[Note: For secure transmission of sensitive data between elements of one and the same network operator only Layer II and Layer III will be involved. In this case Layer I can be dropped. There will also be only one symmetric key in this case, to be used for communication between network elements of one network operator in both directions.]

The party wishing to send sensitive data initiates the mechanism and chooses the symmetric session key it wishes to use for sending the data to the other party. The other party may choose a symmetric session key of its own, used for sending data in the other direction. The session symmetric keys are protected by asymmetric techniques. They are exchanged between certain elements called the *Key Administration Centres* (KACs) of the network operators X and Y. The format of the Layer I transmissions is based on ISO/IEC 11770-3: *Key Management – Mechanisms using Asymmetric Techniques* [10]. Public Keys may be exchanged between a pair of network operators when setting up their roaming agreement (manual roaming) or they may be distributed by a TTP e.g. in case of automatic roaming.

Note: In the case of manual roaming no general PKI is required.

Note: For the transmission of the messages, no special assumptions regarding the transport protocol are made, a possible example would be IP.

7.1.2 Layer II

In Layer II the agreed symmetric keys for sending and receiving data are distributed by the KACs in each network to the relevant network elements. For example, an AuC will normally send sensitive authentication data to VLRs belonging to other networks and will therefore get a session key from its KAC. Layer II is carried out entirely inside one operator's network. It is clear that the distribution of the symmetric keys to the network elements must be carried out in a secure way, as not to compromise the whole system. Therefore, in Annex E a mechanism for distributing the keys, which very similar to that of Layer I, is proposed for Layer II.

7.1.3 Layer III

Layer III uses the distributed symmetric keys for securely exchanging sensitive data between the network elements of one operator (internal use) or different operators (external use) by means of a symmetric encryption algorithm. A block cipher (e.g. BEANO, which has been developed by ETSI SAGE [11]) shall be used for this

purpose, as defined in 3G TS 33.105. The encrypted (resp. authenticity/integrity-protected) messages will be transported via the MAP protocol.

7.1.4 General Overview

Figure 1 provides an overview of the whole mechanism. Note that the messages are not fully specified in this figure. Rather, only the "essential" parts of the messages are given. More details on the format of the messages in the single layers will be provided in subsequent chapters.

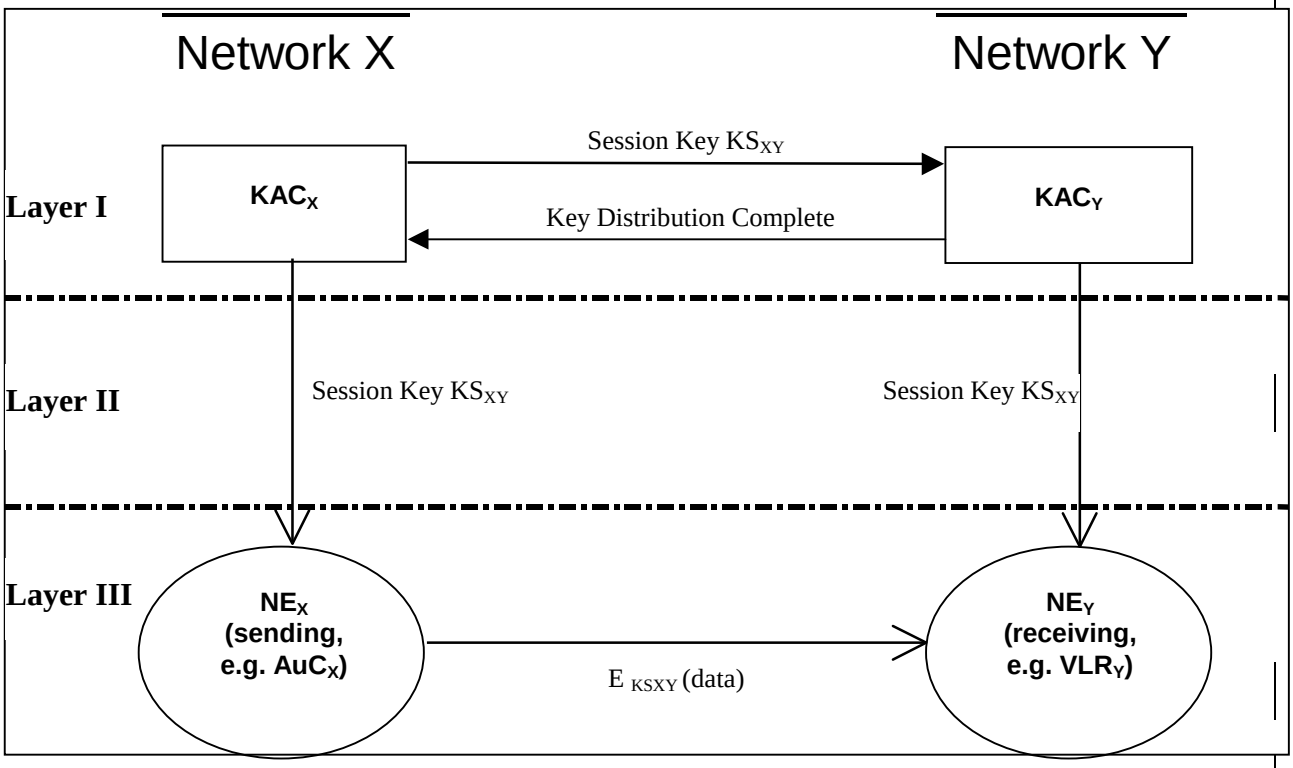


Figure 11: Overview of Proposed Mechanism

E_{KSXY}(data) denotes encryption of data by a symmetric algorithm using the session key from network X to network Y. (If the data are sent inside one operator's network, X = Y).

7.2 Layer I Message Format

Layer I describes the communication between two newly defined network entities of different networks, the so-called Key Administration Centres (KACs).

[Note: We do not make any assumptions about the protocols to be used for this communications, although IP might be the most likely candidate.

7.2.1 Properties and Tasks of Key Administration Centres

There is only one KAC per network operator. KACs perform the following tasks:

- Generation and storage of its own asymmetric key pairs (different key pairs used for signing/verifying and encrypting/decrypting, cf. 7.2.2)
- Storage of public keys of KACs of other network operators
- Generation and storage of symmetric session keys for sending sensitive information to network entities of other networks

- Reception and storage of symmetric session keys for receiving sensitive information from network entities of other networks
- Secure distribution of symmetric session keys to network entities in the same network

Due to these sensitive tasks, a KAC has to be physically secured.

7.2.2 Transport of Session Keys

The transport of session keys in Layer I is based on asymmetric cryptographic techniques (cf. [10]).

[Note: Public key certificates shall be included in Text3 if required.]

In order to establish a symmetric session key with version no. i to be used for sending data from X to Y, the KAC_X sends a message containing the following data to the KAC_Y:

$$E_{PK(Y)}\{X||Y||i||KS_{XY}(i)||RND_X||Text1||D_{SK(X)}(Hash(X||Y||i||KS_{XY}(i)||RND_X||Text1))||Text2\}||Text3$$

The reasons for this message format are as follows:

- Encrypting the message with the public key used for encrypting of the receiving network Y provides message confidentiality, while decrypting the message body with the private key used for signing of the sending network X provides message integrity and authenticity.
- X includes RND_X to make sure that the message contents contains some random data before signing.

[Note: The hash function used shall be collision-resistant and have the one-way property.]

The symmetric session keys $KS_{XY}(i)$ should be periodically updated by this process, thereby moving on to $KS_{XY}(i+1)$. For each new session key KS_{XY} i is incremented by one.

After having successfully decrypted the key transport message and having verified the digital signature of the sending network, including the hash value, and having checked the received i the receiving network starts Layer II activities.

If anything goes wrong, e.g. computing the hash value of $X||Y||i||KS_{XY}(i)||RND_X||Text1$ does not yield the expected result, a RESEND message should be sent by Y to X in the form

$$RESEND||Y||X$$

Y shall reject messages with i smaller or equal than the currently used i.

After having successfully distributed the symmetric session key received by network X to its own network entities, network Y sends to X a Key Distribution Complete Message. This is an indication to KAC_X to start with the distribution of the key to its own entities, which can then start to use the key immediately. The message takes the form

$$KEY\_DIST\_COMPLETE||Y||X||i||RND_Y||D_{SK(Y)}(Hash(KEY\_DIST\_COMPLETE||Y||X||i||RND_Y)$$

where i indicates the distributed key and RND_Y is a random number generated by Y. The digital signature is appended for integrity and authenticity purposes. Y includes RND_Y to make sure that the message contents determined by X will be modified before signing.

7.3 Layer II Message Format

It shall be stressed here once again that the distribution of the symmetric session keys, which has to be performed in Layer II, must be done securely. For a detailed proposal which is based on the asymmetric key transport mechanism of Layer I, see Annex E.

In order to ensure that no network element starts enciphering with a key that not all potentially corresponding network elements have received yet, the following approach is suggested:
The distribution of the session keys KS_{XY} in network X having initiated the Layer I message exchange should not begin before the Key Distribution Complete Message from the receiving network Y has been received by KAC_X in Layer I. As soon as a network element of X has received a session key KS_{XY}, it may start enciphering with this key.
A similar statement holds if the transported session keys are used internally only: In this case, all network elements of X should get the symmetric session keys KS_{XX} for internal use as decryption keys (marked with flag RECEIVED) first; if all network elements of X have acknowledged that they have recovered these keys, the KAC_X sends the same key KS_{XX} again as encryption keys (marked with flag SEND). Again, as soon as a network element of X has received an encryption key (marked with flag SEND), it may start enciphering with this key.

7.4 Layer III Message Format

7.4.1 General Structure of Layer III Messages

Layer III messages are transported via the MAP protocol, that means, they form the payload of a MAP message after the original MAP message header. For Layer III Messages, three levels of protection (or protection modes) are defined providing the following security features:

Protection Mode 0: No Protection
Protection Mode 1: Integrity, Authenticity
Protection Mode 2: Confidentiality, Integrity, Authenticity

Layer III messages consists of a Security Header and the Layer III Message Body that is protected by the symmetric encryption algorithm, using the symmetric session keys that were distributed in layer II. Layer III Messages have the following structure:

Security Header	Layer III Message Body

In all three protection modes, the security header is transmitted in cleartext. It shall comprise the following information:

- Protection Mode
- other security parameters (if required, e.g. IV, Version No. of Key Used, Encryption Algorithm Identifier, Mode of Operation of Encryption Algorithm, etc.)

Both parts of the Layer III messages, security header and message body, will become part of the "new" MAP message body. Therefore, the complete "new" MAP messages take the following form in this proposal:

MAP Message Header	MAP Message Body

	Layer III Message

MAP Message Header	Security Header	Layer III Message Body

Like the security header, the MAP message header is transmitted in cleartext. In protection mode 2 providing confidentiality, the Layer III Message Body is essentially the encrypted "old" MAP message body. For integrity and authenticity, an encrypted hash calculated on the MAP message header, security header and the "old" MAP message body in cleartext is included in the Layer III Message Body in protection modes 1 and 2. In protection

mode 0 no protection is offered, therefore the Layer III Message Body is identical to the "old" MAP message body in cleartext in this case.

In the following subchapters, the contents of the Layer III Message Body for the different protection modes will be specified in greater detail.

7.4.2 Format of Layer III Message Body

7.4.2.1 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the Layer III message body in protection mode 0 is identical to the original MAP message body in cleartext.

7.4.2.2 Protection Mode 1

The message body of Layer III messages in protection mode 1 takes the following form:

Cleartext‖TVP‖$E_{KSXY(i)}$(*Hash*(MAP Header‖Security Header‖Cleartext‖TVP))

where "Cleartext" is the message body of the original MAP message in cleartext.

Authentication of origin is achieved by encrypting the hash value of the cleartext, since only a network element knowing $KS_{XY}(i)$ can encrypt in this way. Message integrity and validation is achieved by hashing and encrypting the cleartext.

[Note: The case X=Y, i.e. only one key for sending and receiving, corresponds to internal use inside network X.]

Note that protection mode 1 is compatible to the present MAP protocol, since everything appended to the cleartext may be ignored by a receiver incapable of decrypting.

7.4.2.3 Protection Mode 2

The Layer III Message Body in protection mode 2 takes the following form:

$E_{KSXY(i)}$(Cleartext‖TVP‖*Hash*(MAP Header‖Security Header‖Cleartext‖TVP))

where "Cleartext" is the original MAP message in cleartext.

Message confidentiality is achieved by encrypting with the session key. This also provides for authentication of origin, since only a network element knowing KSXY(i) can encrypt in this way. Message integrity and validation is achieved by hashing the cleartext. TVP is a random number that avoids traceability.

[Note1: There is need for replay protection of Layer III messages; this is for further study.
By making use of a TVP as timestamp (perhaps derived from an overall present master time) this could be achieved.]

[Note2: In protection mode 2, the original MAP message body will be encrypted in order to achieve confidentiality. For integrity and authenticity, an encrypted hash calculated on the MAP message header and body in cleartext (i.e. the original MAP message) is appended to the messages in protection mode 1 and 2. All protection modes need a security header to be added.
When implementing these changes, care has to be taken that the maximum length of a MAP message (approx. 250 byte) is not exceeded by the protected MAP messages of Layer III, otherwise substantial changes to the underlying SS7 protocol levels (TCAP and SCCP) would have to be made.]

7.5 Mapping of MAP Messages and Modes of Protection

The network operator should be able to assign the mode of protection to each MAP message in order to adapt the level of protection according to its own security policy. Guidance may be obtained from the SS7 Signalling Protocols Threat Analysis [12].

– break –

Annex E: A Proposal for Layer II Message Format

E.1 Introduction

In Layer II symmetric session keys (to encrypt/decrypt data before sending/after receiving) are distributed by the KACs in each network to the relevant network elements. For example, an AuC_X will normally send sensitive authentication data to VLR_Y and will therefore get a session KS_{XY} key from its KAC_X. Layer II is carried out entirely inside one operator's network.
However, in order to achieve a more consistent overall scheme, in this annex it is suggested to use for Layer II the same mechanism for distributing the keys as in Layer I. This requires the KACs of the different networks to generate and distribute asymmetric key pairs for the network elements of that network. These key-pairs will then be used to transfer the symmetric session keys in the same way as in Layer I.
The public and private key pairs needed for the network entities should be distributed to the entities in a secure way, which is in principle an operation & maintenance task. One way to do this is to distribute the key pairs, along with the necessary crypto-software, to the network entities in the form of chipcards, which can also carry out the necessary computations. Therefore, all that has to be added to the present network entities are chipcard readers with a standardised interface. Thus, on adoption of this proposal, in addition to their present tasks, the network entities would have to:

- Store the symmetric session keys to encrypt/decrypt data before sending/after receiving to/from network entities of other networks (external) and of their own network (internal)
- Encrypt/decrypt MAP messages according to their Mode of protection (cf. 7.4). The necessary computations may be carried out by a chipcard.

In addition to their tasks listed in 7.2.1 of the main document, the KACs would have to:

- Generate and store asymmetric key pairs for network entities in the same network
- Distribute asymmetric key pairs to network entities in the same network.

E.2 Proposed Layer II Message Format

The Layer II messages themselves take the same form as in 7.2 of the main document, where the 'receiving network Y' has to be replaced by 'receiving network entity NE_X' (or X by NE_Y). Further, the Key Distribution Complete message is not needed in Layer II. However, the distribution of the session keys KS_{XY} in network X having initiated the Layer I message exchange should not begin before the Key Distribution Complete Message from the receiving network Y has been received by the KAC_X in Layer I. As soon as a network element of X has received a session key KS_{XY}, it may start enciphering with this key. A similar statement holds if the transported keys are used internally only: In this case, all network elements of X should get the symmetric session key KS_{XX} to be used internal for encryption (marked as decryption key with flag RECEIVE) first; if all network elements have acknowledged that they have recovered these keys, the KAC_X sends the same key again (marked as encryption key with flag SEND). Again, as soon as a network element has received the session key KS_{XX} (with flag SEND), it may start enciphering with this key.

[Note: As for layer I, no assumptions about the transport protocol are made, although IP might be a good candidate.]

E.2.1 Sending a session key for decryption

In order to transport a symmetric session key (marked with flag RECEIVE) with version no. i to be used to decrypt received data from network elements of network X in NE_Y, the KAC of Y sends a message containing the following data to NE_Y:

$$E_{PK(NEY)}\{X||NE_Y||RECEIVE||i||KS_{XY}(i)||RND_Y||Text1||D_{SK(Y)}(\mathit{Hash}(X||NE_Y||RECEIVE||i||KS_{XY}(i)||RND_Y||Text1))||Text2\}||Text3$$

After having successfully decrypted the key transport message and having verified the digital signature of the sending network including the hash value, the receiving network entity sends an key installed message to its Key Administration Centre KAC_Y. The message takes the form

$KEY\_INSTALLED \| X \| NE_Y \| RND_Y \| i$

This message can only be sent by the receiving network entity, because only this entity can know about RND_Y. If anything goes wrong, e.g. computing the Hash of $X \| NE_Y \| RECEIVE \| i \| KS_{XY}(i) \| RND_Y \| Text1$ does not yield the expected result, a RESEND message should be sent by NE_Y to KAC_Y in the form

$RESEND \| NE_Y$

E.2.32 Sending a session key for encryption

In order to transport a symmetric SEND key with version no. i to be used for sending data from NE_X to network elements of network Y, KAC_X sends a message containing the following data to NE_X:

$E_{PK(NEX)}\{NE_X \| Y \| SEND \| i \| KS_{XY}(i) \| RND_X \| Text1 \| D_{SK(X)}(Hash(NE_X \| Y \| SEND \| i \| KS_{XY}(i) \| RND_X \| Text1)) \| Text2\} \| Text3$

– break –

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex H of S3-99203**

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	008	Current Version:	3.0.0

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

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

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

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

Source: SA3 **Date:** 99-06-18

Subject: Cipher key lifetime

3G Work item: UTRAN 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 sections describing the cipher key lifetime are replaced by a reference to the mechanisms on the integrity key lifetime. This to assure consistency.

Clauses affected: 6.6.6

Other specs affected:

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

Other comments:

help.doc

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

6.6.6 Cipher key lifetime

A mechanism is needed to ensure that a particular cipher key is not used for an unlimited period of time to avoid attacks using compromised keys. Authentication and key agreement which generates new cipher keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. ~~The USIM shall therefore contain a mechanism to limit the number of calls that can be made with a specific cipher key.~~The lifetime of the cipher key is controlled by the mechanism described in 6.4.6.

~~Operators shall decide on the value of this number of calls, and write this parameter on the USIM. The USIM shall have a counter that counts the number of times the cipher key is used and shall trigger the generation of a new cipher key if the counter reaches the maximum value set in the USIM. This mechanism will ensure that an cipher key cannot be reused more times than the limit set by the operator.~~

~~The cipher key lifetime is linked to the integrity key lifetime.~~

~~Note: The decision on when a key needs to be updated may depend on a number of factors, including the time since the last key update, the amount of data protected using that key, and the cost/value of the services protected through the use of that key. Unfortunately they cannot be easily measured by the USIM, so it is suggested that the number of calls made using the key should be measured instead. Some concern exists whether this is a good enough measure. Should also the (periodic) in-call authentication messages be counted, such that long calls weigh more than short calls? Should also the authentications through the use of the shared integrity call be counted?~~

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex I of S3-99203**

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** **009** Current Version: 3.0.0

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

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

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

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

Source: SA3 **Date:** 99-06-18

Subject: Mechanism for user domain security

3G Work item: UTRAN 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: Where 3GPP has no intention to change a security feature already described in another specification, no description of the mechanism should be included in 3G TS 33.102. 3GPP has no intention to change the existing GSM personalisation feature described in GSM 02.22 or the GSM PIN acess mechanism described in GSM 11.11.

Clauses affected: 5.3, 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.

5.3 User domain security

5.3.1 User-to-USIM authentication

This feature provides the property that access to the USIM is restricted until the USIM has authenticated the user. Thereby, it is ensured that access to the USIM can be restricted to an authorised user or to a number of authorised users. To accomplish this feature, user and USIM must share a secret (e.g. a PIN) that is stored securely in the USIM. The user gets access to the USIM only if he/she proves knowledge of the secret.

This security feature is implemented by means of the mechanism described in [16].

5.3.2 USIM-Terminal Link

This feature ensures that access to a terminal or other user equipment can be restricted to an authorised USIM. To this end, the USIM and the terminal must share a secret that is stored securely in the USIM and the terminal. If a USIM fails to prove its knowledge of the secret, it will be denied access to the terminal.

This security feature is implemented by means of the mechanism described in [10].

8 VoidUser domain security mechanisms

8.1 User-USIM Authentication

8.1.1 Overview

The User-USIM Authentication (UUA) mechanism provides access control to particular files on the USIM.

Each file in the USIM is under access control. To that extent each file is associated to a user name (UN). Each (UN) has the following attributes:

1) Expected user response (XUR): a value stored in the USIM to verify the responses of the user, as it is described in 8.1.2. This value may be modified by the procedure described in 8.1.5.

2) Activity state: either ENABLED or DISABLED. If enabled, access is granted only when the user has identified himself. The transition between the two states is defined by the procedures described in 8.1.3 and 8.1.4.

3) Block state: either BLOCKED or UNBLOCKED. A UN gets blocked when the number of consecutive failed authentication attempts for that UN reaches a certain threshold. The user name can be unblocked after a successful User-USIM authentication for a UN* that controls access to the Block state of the UN.

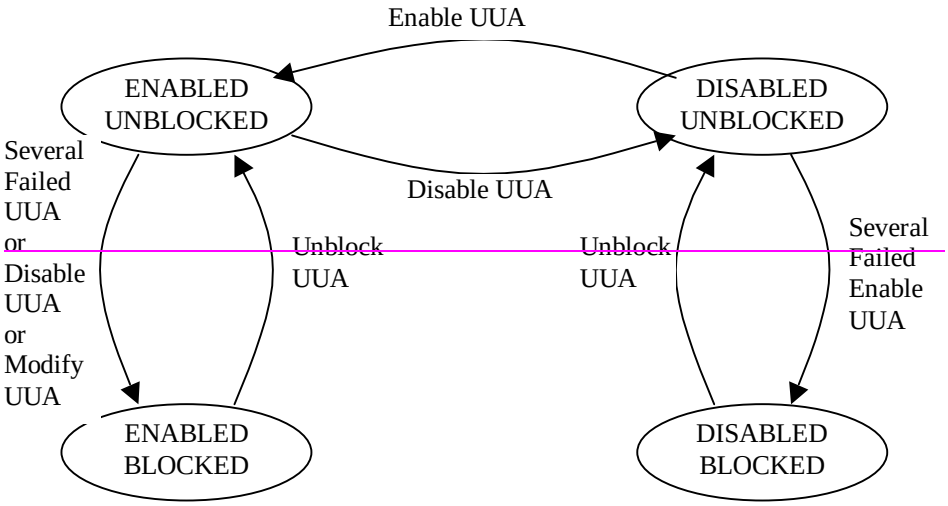


Figure 11: User-USIM Authentication State Model

8.1.2 User-USIM Authentication

This procedure allows the USIM to corroborate the user identity.

The procedure is described in Figure 12.

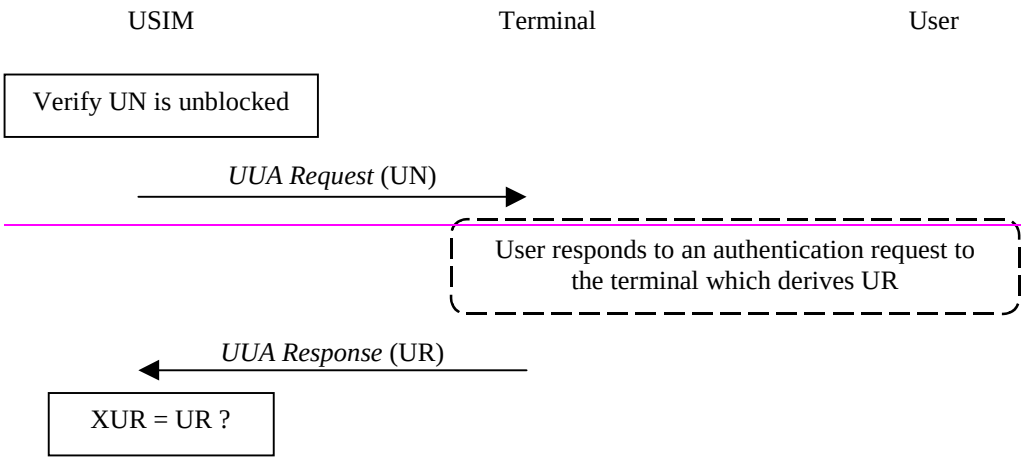


Figure 12: User-USIM Authentication

The procedure is invoked by the USIM when a user attempts to access certain restricted files in the USIM that are associated to a User Name (UN) and User-USIM Authentication for that UN is enabled. Depending on the access rights for the files, access is granted for the execution of a single action or for the duration of a USIM session.

The USIM verifies whether the state of the UN is unblocked. If UN is blocked, the procedure is terminated unsuccessfully, i.e., access to the file is not granted.

If the UN is unblocked, the USIM sends a *UUA request* to the terminal to authenticate the user. This request includes the UN that is associated to the file. The terminal then initiates an authentication procedure with the user. This typically involves a request to the user, a response from the user and may involve some processing to transform the response from the user into a standardised format. The terminal then sends *UUA response* that includes the user response (UR) back to the USIM.

Upon receipt of that message the USIM compares the received UR with the stored XUR associated to the UN. If there is a match, the authentication failure counter for that user name is reset to zero and the procedure is terminated successfully.

Otherwise, the USIM increases the authentication failure counter by one. If that counter reaches a certain threshold value, the USIM will enter blocked mode for that user and refuse to initiate any further User-USIM Authentication procedures. The procedure is ended unsuccessfully, i.e., access to the file is not granted.

8.1.3 Enable User-USIM Authentication for a user name

This procedure is used by the user to enable the User-USIM Authentication procedure.

The procedure is described in Figure 13.

The procedure is initiated by the user who enters a request to enable User-USIM Authentication for a particular UN. The terminal forwards that request to the USIM. Upon receipt of the request the USIM verifies whether the user state is set to DISABLED. If this is not the case the procedure is abandoned unsuccessfully.

The USIM then invokes the User-USIM Authentication procedure described in 8.1.2. If this procedure is ended successfully, the state of UUA for the user is set to ENABLED.

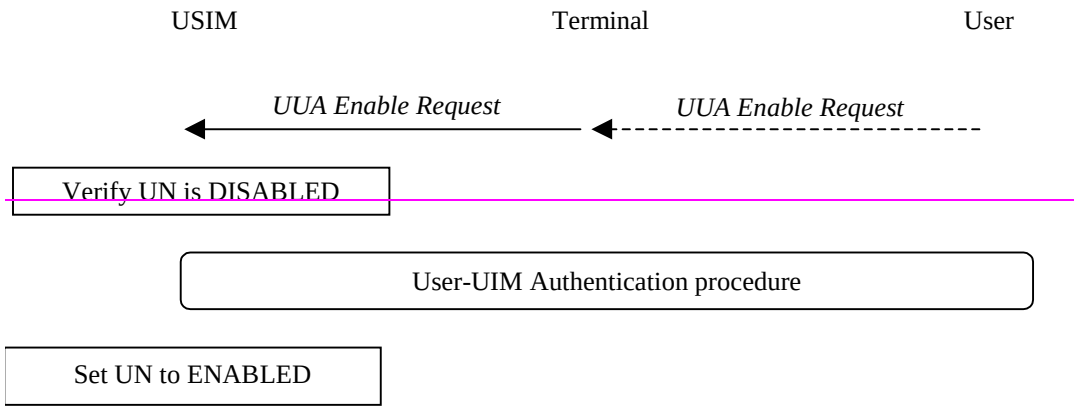


Figure 13: Enable User-USIM Authentication

8.1.4 Disable User-USIM Authentication

This procedure is used by the user to disable the User-USIM Authentication procedure.

The procedure is described in Figure 14.

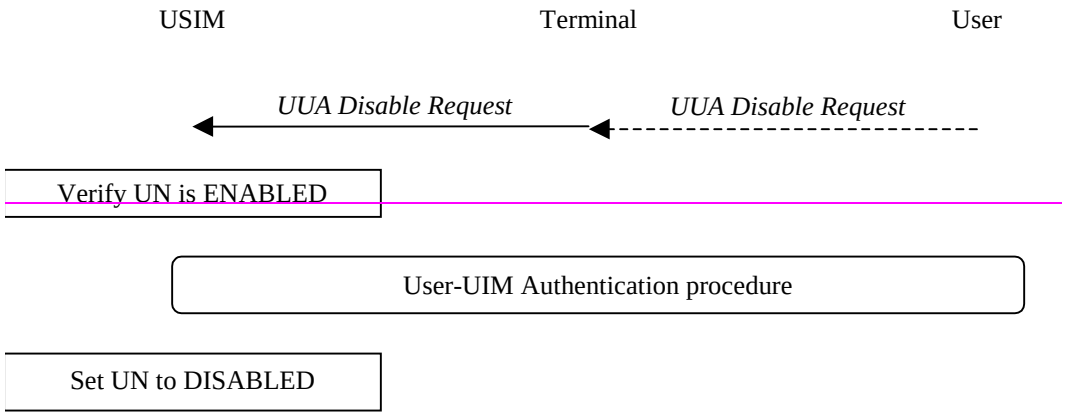


Figure 14: Disable User-USIM Authentication

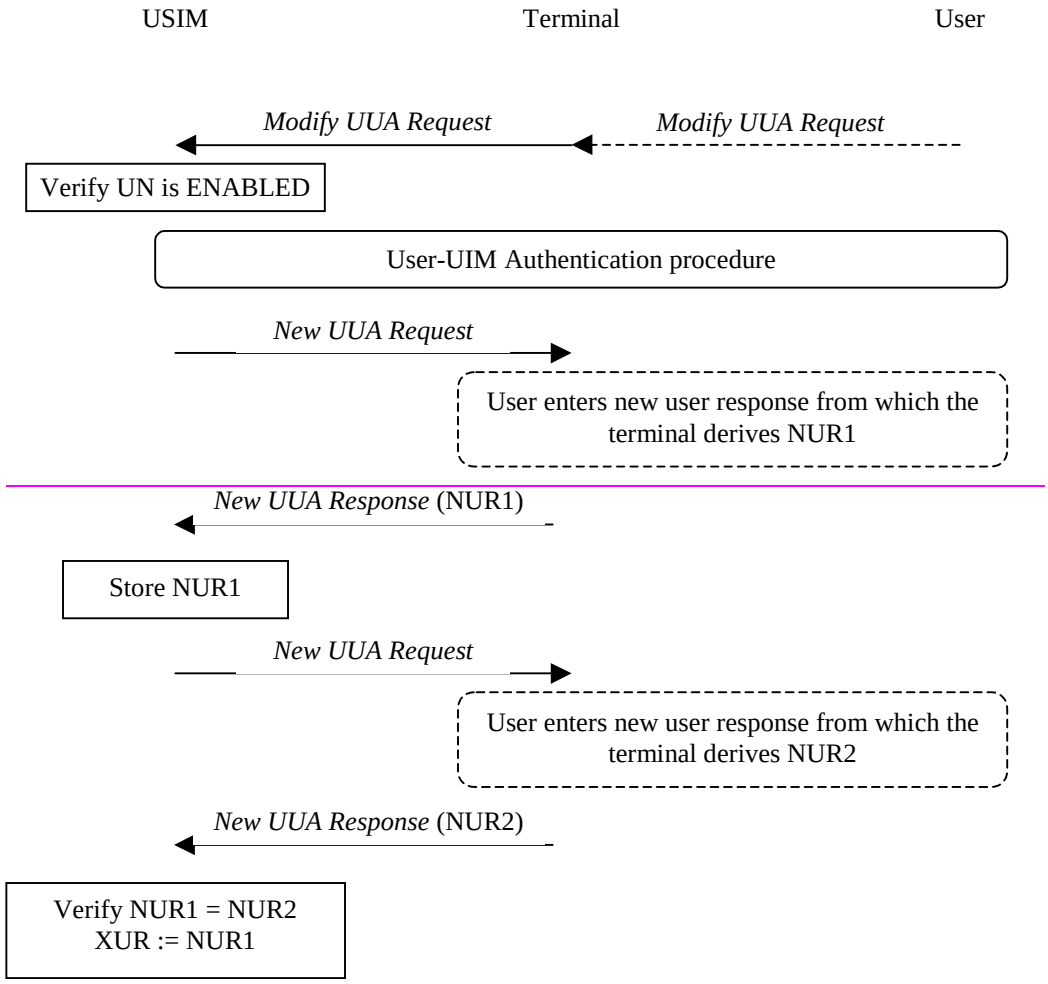
The terminal initiates the procedure sending a request to the USIM. The USIM then checks whether the User-USIM Authentication is enabled. If this is not the case, the procedure is abandoned unsuccessfully.

The USIM then initiates the User-USIM Authentication procedure described in 8.1.2. If this procedure is ended successfully, the UUA state for the user is set to DISABLED.

8.1.5 Modify expected user response

This procedure is used by the user to modify the expected user response for a user name.

The procedure is described in Figure 15.



~~Figure 15: Modify expected user response~~

~~The procedure is invoked by the user who enters a request to modify the XUR for a UN. The terminal forwards the request to the USIM. The USIM then checks whether the User-USIM Authentication is enabled for that user name. If this is not the case, the procedure is ended unsuccessfully.~~

~~The USIM then initiates the User-USIM Authentication procedure described in 8.1.2. If this procedure is ended successfully, the user is asked a first time to enter his new user response. This value is subsequently stored in the USIM and the user is requested a second time to enter his new user response. The value received the second time is compared with the value received the first time. If both are unequal, the procedure is ended unsuccessfully without changing the expected user response. If there is a match the user response is modified accordingly to the new value.~~

~~8.1.6 Unblock User-USIM Authentication~~

~~This procedure is used by the user to unblock a user name. The procedure is described in Figure 16.~~

~~The procedure is invoked by a user request. The terminal forwards the request to the USIM. Upon receipt the USIM verifies that the user name is BLOCKED. If this is not the case, the procedure is abandoned.~~

~~The USIM invokes the User-USIM Authentication procedure for the user name UN* that controls the block state of the user name. If User-USIM authentication is ended successfully for UN*, the block state for UN is set to UNBLOCKED and the failure counter is reset to zero.~~

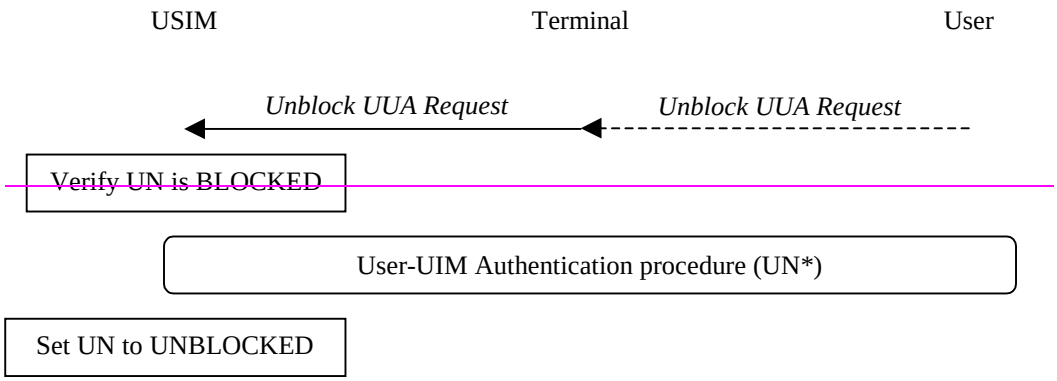


Figure 16: Unblock User-USIM Authentication

8.2 USIM-Terminal Lock

Note: The text included here is written starting from GSM 11.11. It should be compared with GSM 02.22 and it should be studied whether the mechanisms specified in there can be used as a basis for the specification of user-USIM authentication is UMTS.

8.2.1 Overview

This mechanism allows the owner of mobile equipment who is at the same time the user associated to a USIM, to restrict the usage of certain mobile equipment to his USIM.

The mechanism assumes that two passwords V1 and V2 are stored permanently in the USIM. Furthermore, it assumes that two user names are defined in the USIM: UN1 and UN2. Access to V1 is granted after an authentication as UN1 or UN2, access to V2 is granted after an authentication as UN2.

The mechanism consists of three procedure: 1) a procedure to enable the lock, whereby the USIM exports both passwords, 2) a procedure to verify the USIM by the terminal, whereby the USIM exports V1 which is verified by the terminal, and 3) a procedure to disable the lock, whereby the USIM exports V2.

8.2.2 Enable USIM-Terminal Lock

This procedure is used to lock a terminal and a USIM.

The procedure is described in Figure 17.

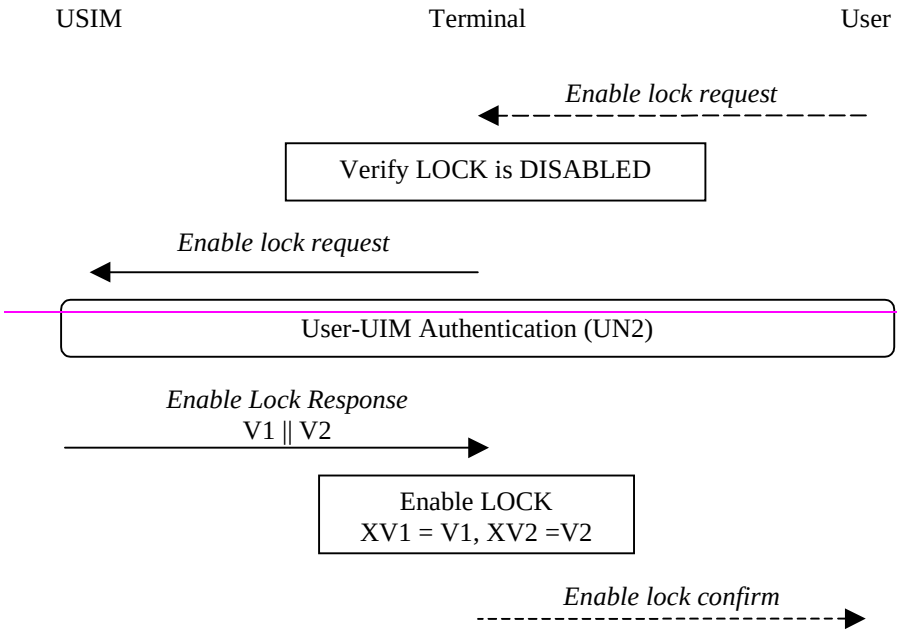


Figure 17: Enable USIM-Terminal lock

The user enters a request to enable the USIM-terminal lock. The terminal first verifies the lock state is set to DISABLED. Only if this is the case, the terminal sends a request to the USIM to enable the USIM-terminal lock. Upon receipt, the USIM initiates a User-USIM Authentication for the user name UN2. If that procedure is successful, the USIM sends V1 and V2 to the terminal. Upon receipt the terminal sets the USIM-terminal LOCK-STATE to ENABLED and stores V1 and V2 in protected memory.

8.2.3 USIM-terminal authentication

This procedure is used to authenticate the USIM.

The procedure is described in Figure 18:

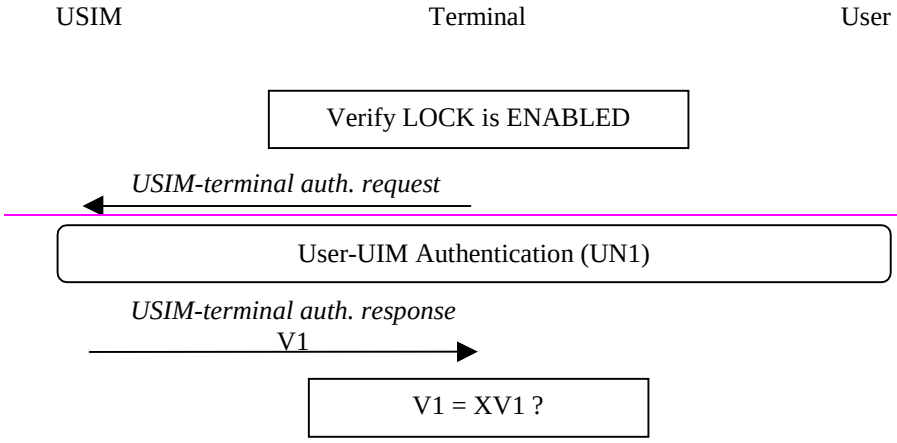


Figure 18: USIM-terminal Authentication

If the mobile station is powered on or a USIM is inserted in the terminal and the USIM-terminal LOCK-STATE in the terminal is set to ENABLED, the terminal sends a request to the USIM to authenticate. If the user-USIM authentication for UN1 is enabled, the USIM initiates a procedure to authenticate the user. If the authentication is disabled or if it is enabled and the authentication is successful, the USIM sends V1 to the terminal. Upon receipt the terminal compares the received value with the one which is stored in protected memory. If there is a match the procedure ends successfully. Otherwise, the terminal refuses operation.

8.2.4 Disable USIM-terminal Lock

This procedure is used to unlock a terminal and a USIM.

The procedure is described in Figure 19.

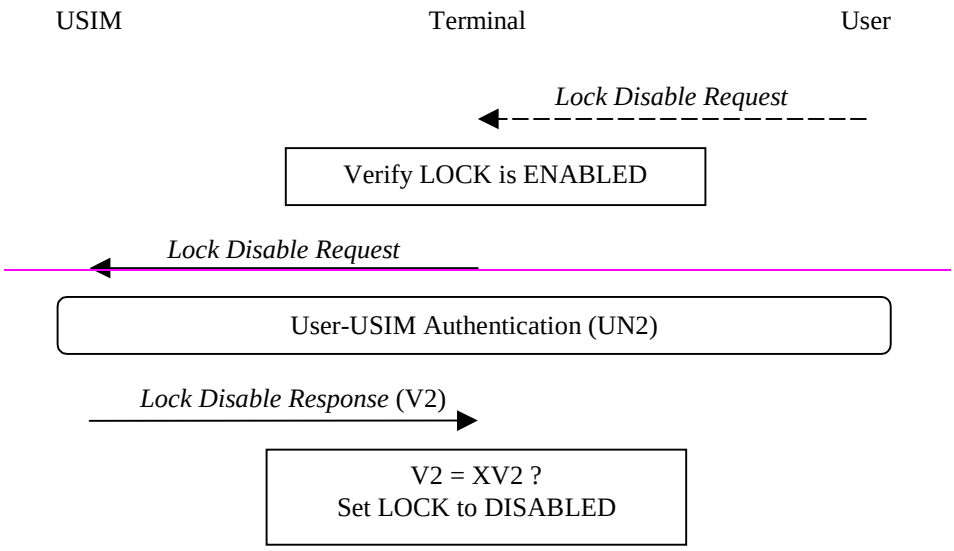


Figure 19: Disable USIM-terminal lock

The user enters a request to disable the USIM-terminal lock. The terminal first verifies the USIM-terminal LOCK STATE is set to ENABLED. Only if this is the case, the terminal sends a request to the USIM to disable the USIM-terminal lock. Upon receipt, the USIM initiates a User-Authentication for the user name UN2. If the user authentication is successful, the USIM sends V2 to the terminal. Upon receipt the terminal compares the received value with the value stored in its protected memory. If there is a match the terminal sets the LOCK to DISABLED and removes XV1 and XV2 from protected memory.

Technical Specification Group Services and System Aspects ***TSG SA#4(99)___***
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **S3-99202**

Subject: 3G TS 33.103 V1.0.0

Source: TSG SA WG3

Document for: Information

3G TS 33.103 V1.0.0 (1999-06)

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Integration Guidelines
3G TS 33.103 V 1.0.0

Reference
DTS/TSGS-_____

Keywords
Security, Authentication and Key Agreement, Security Information Stored, Location of Security Functions, Parameter Lengths

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This document has been drafted by 3GPP TSG-SA WG 3, i.e., the Workgroup devoted to “Security” issues, within the Technical Specification Group devoted to “System Aspects”.

1 Scope

This technical specification defines how elements of the security architecture are to be integrated into the following entities of the system architecture.

- Home Environment Authentication Center (HE/AuC)
- Serving Network Visited Location Register (SN/VLR)
- Radio Node Controller (RNC)
- Mobile station User Identity Module (UIM)
- Mobile Equipment (ME)

This specification is derived from 3G "Security architecture".

The structure of this technical specification is as follows:

Clause 5 lists the security information to be stored in the above entities of the 3G system in terms of Static information and Dynamic information.

Clause 6 defines the external specification of the security-related algorithms in terms of input and output parameters, and the parameter lengths.

The equivalent information for the alternative Temporary Key proposal is included in an appendix to this document

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by “up to and including” before the version identity); or

c) all versions subsequent to and including the identified version (identified by “onwards” following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] TR S3.03 Security Architecture

2.2 Informative references

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.

3.2 Symbols

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

||	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK
f6	Encryption function used to encrypt the IMUI
f7	Decryption function used to decrypt the IMUI ($=f6^{-1}$)
f8	Access link encryption function
f9	Access link message authentication function
K	Long-term secret key shared between the USIM and the AuC

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AK	Anonymity key
AuC	Authentication Centre
AUTN	Authentication token
CK	Cipher key
EMUI	Encrypted Mobile User Identity
GK	User group key
IK	Integrity key
IMUI	International Mobile User Identity
IPR	Intellectual Property Right
MAC	Medium access control (sublayer of Layer 2 in RAN)
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
PDU	Protocol data unit
RAND	Random challenge
RES	User response
RLC	Radio link control (sublayer of Layer 2 in RAN)

RNC	Radio network controller
SEQ_UIC	Sequence for user identity confidentiality
SDU	Signalling data unit
SQN	Sequence number
UE	User equipment
USIM	User Services Identity Module
XMAC-A	Expected MAC used for authentication and key agreement
XMAC-I	Expected MAC used for data integrity of signalling messages
XRES	Expected user response

4 Overview of the security architecture

4.1 Overview of the complete 3G security architecture.

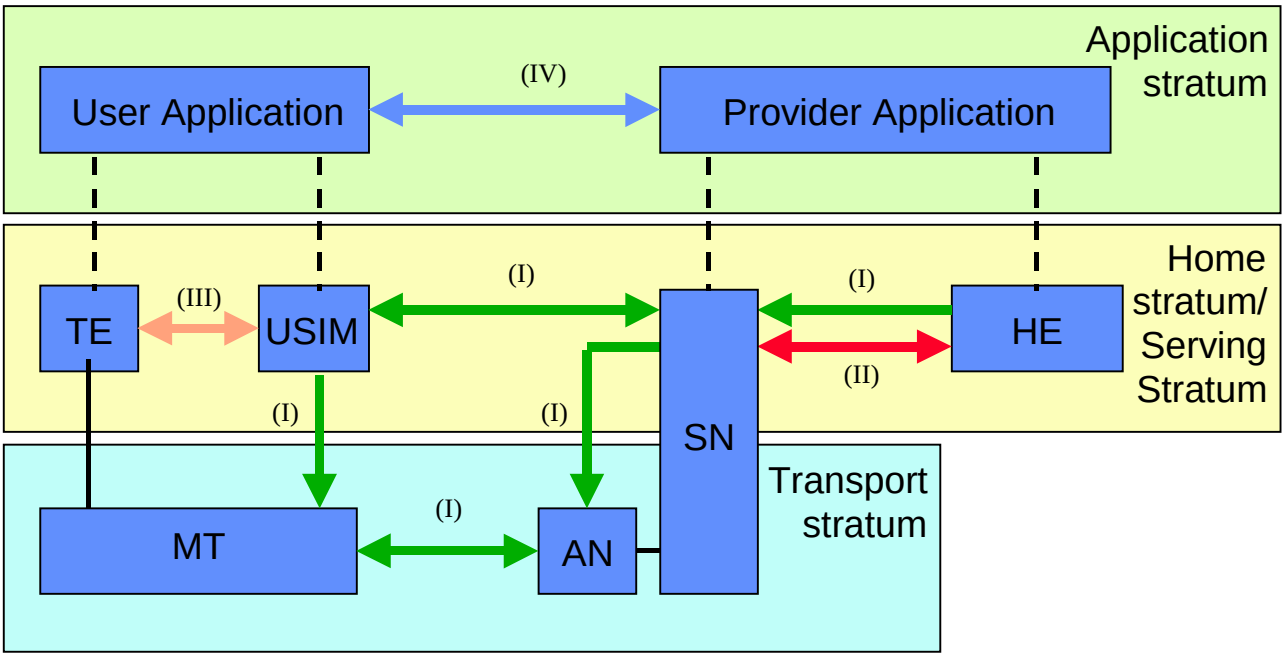


Figure 1 : Overview of the security architecture

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.

4.2 Overview of Authentication and Key Agreement Mechanism

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.

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.

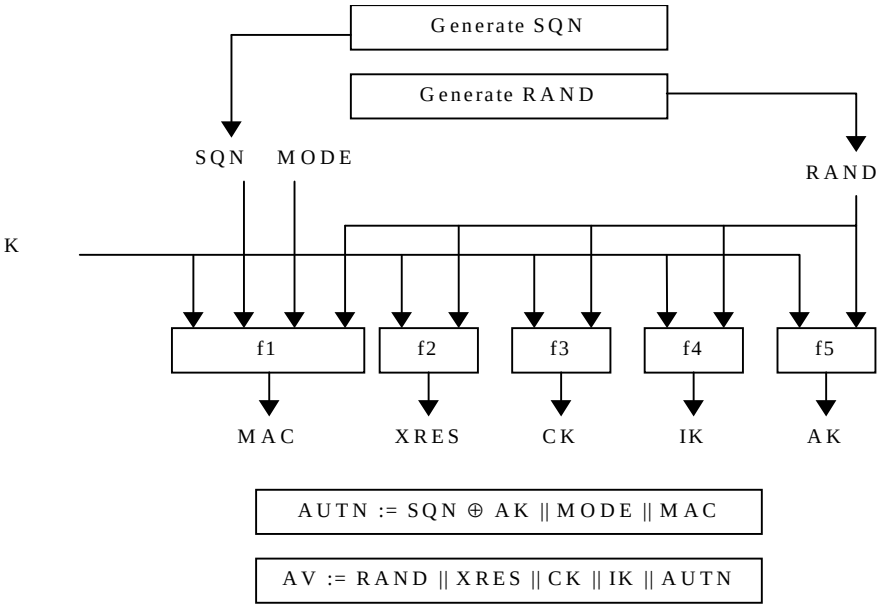


Figure 2: Generation of an authentication vector

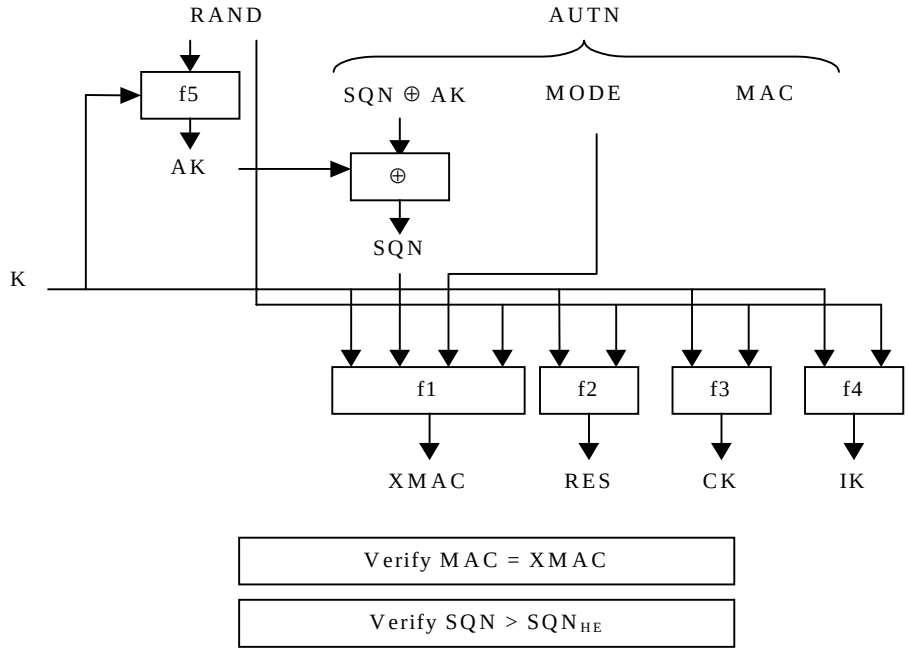


Figure 3: User authentication function in the USIM

5 Security Information Stored

5.1 Information common to Sequence Number and Temporary Key Mechanism

This Clause lists the security information to be stored in the relevant entities of the 3G system in terms of Static information and Dynamic information and relates to the preferred sequence number mechanism, the alternative temporary key mechanism is detailed in the Appendix. However, sections 5.1 contains information, which is common to both mechanisms.

Notes on tables

Parameter Lengths: The length of the parameters is given to allow estimates of the message sizes on the air interface to be determined and the maximum width for algorithm design. The effective key length used will be determined by national policy.

Lifetimes: The entry in the tables for parameter lifetime is defined in the table below

ref.	**Definition**
a	For the life of the equipment
b	For lifetime of a registration (from one registration to the next)
c	Changed stored from one authentication to the next
d	Lifetime dependent on Home Environment policy
e	Lifetime dependent on Serving Node policy
f	Lifetime dependent on User Policy
g	Lifetime Dependent on Manufacturer Policy
h	No need to be stored in non-volatile memory

Identities: These are shown in the tables, but unless TSG SA WG3 have a specific security issue with the length uniqueness etc there are shown in Italics as these are defined in other TSG working groups. For example

IMUI	** 96 bits?*

5.1.1 Home Environment Authentication Center HE/AuC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Long Term Secret Key	K	128 bits	a
User 1 permanent identity	*IMUI*	*	
User n permanent identity	*IMUI*	*	
Optional Enhanced user identity confidentiality			
Home Environment Id	He_id	32 bit	a
user group 1			
Group Key	GK	128 bits	a
Group Identity	GI	32 bits	d
user 1			
Sequence for UIC	SEQ_UIC	32 bits	c
Encrypted IMUI	EMUI	128 bit	h
user group n			
Group Key	GK	128 bits	a
Group Identity	GI	32 bits	d
user n			
Sequence for UIC	SEQ_UIC	32 bits	c
Encrypted IMUI	EMUI	128 bit	h
Network Domain Security			
Network's own Private Key (signing)	PVTK s	< or = 2048 bits	d,e
Network's own Private Key (decryption)	PVTK d	< or = 2048 bits	d,e
PKR_1 Public Key for network #1 (verfiy)	$PUBKv_1$	< or = 2048 bits	d,e
PKR_n Public Key for network #n (encryption)	$PUBKe_n$	< or = 2048 bits	d,e
PKR_1 Public Key for network #1 (verify)	$PUBKv_1$	< or = 2048 bits	d,e
PKR_n Public Key for network #n (encryption)	$PUBKe_n$	< or = 2048 bits	d,e
Symmetric Send Key #i for sending data from X to Y	$KS_{XY}(i)$	128 bits	d,e
Symmetric Send Key #j for sending data from Y to X	KS_{YX} (j)	128 bits	d,e
Session key Sequence Number (for sending data from X to Y)	I	32 – 64 bits	d,e
Session key Sequence Number	j	32 – 64 bits	d,e

(for sending data from Y to X)			
Unpredictable Random Value generated by X	RND_X	128 bits	h
Unpredictable Random Value generated by Y	RND_y	128 bits	h

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Time Variant Parameter	TVP	64 bits	h
Network Operator Identifier A, B	X, Y	32 bits	a
Network-Wide User Traffic Confidentiality			
Access link cipher key (traffic)	Ka	128 bits	c
Access link cipher key (signaling)	Ka'	128 bits	c
Received access link cipher key	Kb	128 bits	c
Received access link cipher key (signaling)	Kb'	128 bits	c
NWUTC Session key	K_S	128 bits	c

5.1.2 Serving Node Visited Location Register SN/VLR

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Registered User1 Permanent Identity	*IMUI*		
Registered User1 Old Temporary Identity	$TMUI_o$	*	
Registered User1 New Temporary Identity	$TMUI_n$	*	
Optional Enhanced user identity confidentiality for user 1			
Encrypted IMUI	EMUI	128 bit	h
Home Environment Id	He_id	32 bit	a
Group Identity	GI	32 bits	d
Registered User n Permanent Identity	*IMUI*		a
Registered User n Old Temporary Identity	$TMUI_o$	*	c
Registered User n New Temporary Identity	$TMUI_n$	*	c
Optional Enhanced user identity confidentiality for user n			
Encrypted IMUI	EMUI	128 bit	h
Home Environment Id	He_id	32 bit	a
Group Identity	GI	32 bits	d

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Network Domain Security			
Symmetric Send Key #i for sending data from X to Y	$KS_{XY}(i)$	128 bits	d,e
Symmetric Send Key #j for sending data from Y to X	KS_{YX} (j)	128 bits	d,e
Network-Wide User Traffic Confidentiality			
Access link cipher key (traffic)	Ka	128 bits	c
Access link cipher key (signaling)	Ka’	128 bits	c
Received access link cipher key	Kb	128 bits	c
Received access link cipher key (signaling)	Kb’	128 bits	c

5.1.3 Radio Node Controller RNC

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Cipher Key – Circuit switched	CK_{CS}	128 bits	c
Cipher Key – Packet switched	CK_{PS}	128 bits	c
Integrity key	IK	128 bits	c
Access link cipher key (traffic)	Ka	128 bits	**c**
Access link cipher key (signaling)	Ka’	128 bits	**c**
Received access link cipher key	Kb	128 bits	c
Received access link cipher key (signaling)	Kb’	128 bits	c

5.1.4 USIM

Name	**Symbol**	**Parameter Length actual or min-max**	Lifetime
Long Term Secret Key	K	128 bits	a
User Permanent Individual Identity	*IMUI*	*****	**a**
Registered User Old Temporary Identity	$TMUI_o$	*	c
Registered User New Temporary Identity	$TMUI_n$	*	c
Optional Enhanced user identity confidentiality			
Home Environment Id	He_id	32 bits	a
Group Key	GK	128 bits	a
Group Identity	GI	32 bits	d
Sequence for UIC	SEQ_UIC	32 bits	c
Encrypted IMUI	EMUI	128 bits	h
confidentiality and integrity			
Cipher Key – Circuit switched	CK_{CS}	128 bits	c
Cipher Key – Packet switched	CK_{PS}	128 bits	c
Integrity Key	IK	128 bits	c
Key set identifier	KSI	32 bits	c
Cipher Key Lifetime	$LIFE_{CKCS}$	32 bits	d
Integrity Key Lifetime	$LIFE_{IKCS}$	32 bits	d
Cipher Key Use Counter – Circuit switched	USE_{CKCS}	32 bits	a
Integrity Key Use Counter – Circuit switched	USE_{IKCS}	32 bits	a

5.1.5 Mobile Equipment ME

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Cipher Key Circuit Switched	CK_{CS}	128 bits	c
Cipher Key Packet Switched	CK_{PS}	128 bits	c
Integrity Key	IK	128 bits	c
Access link cipher key (traffic)	Ka	128 bits	**c**
Received access link cipher key	Kb	128 bits	c
NWUTC Session key	K_S	128 bits	c

5.2 Sequence Number Mechanism

5.2.1 Home Environment Authentication Center HE/AuC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Sequence Number	SQN	32-64 bits	d
Anonymity Key	AK	32-64 bits	d
Message Authentication Code	MAC-A	64 bits	Is part of AUTN change with each new request
AV1 Random Number	RAND	128 bits	Is part of AUTN change with each new request
Expected Response	XRES	32-128 bits	Is part of AUTN change with each new request
Cipher Key	CK	128 bits	Is part of AUTN change with each new request
Integrity Key	IK	128 bits	Is part of AUTN change with each new request
Authentication Token	AUTN	97- 129 bits	Is part of AUTN change with each new request
AVn Random Number	RAND	128 bits	Is part of AUTN change with each new request
Expected Response	XRES	32-128 bits	Is part of AUTN change with each new request
Cipher Key	CK	128 bits	Is part of AUTN change with each new request
Integrity Key	IK	128 bits	Is part of AUTN change with each new request
Authentication Token	AUTN	**1**	Is part of AUTN change with each

1 AUTN = (SQN xor AK) || MODE || MAC eg AUTN = (32-64) + 1 + 64 = 97-129 bits

			new request
Key set identifier	KSI	32 bits	d
Anonymity Key	AK	32-64 bits	h
Mode	MODE	1 bit	c
Re-synchronisation MAC	XMAC-S	64 bits	
Re-synchronisation token	XAUTS		
Option 1			
User 1 Counter- Circuit switched	$SQN_{HE/CS}$	32-64 bits	c
User 1 Counter – Packet switched	$SQN_{HE/PS}$	32-64 bits	c
User n Counter- Circuit switched	$SQN_{HE/CS}$	32-64 bits	c
User n Counter – Packet switched	$SQN_{HE/PS}$	32-64 bits	c
Option 2			
Global Counter	SQN_{he}	32-64 bits	c

Note: The Authentication center will store up to 10 Authentication vectors

5.2.2 Serving Node Visited Location Register SN/VLR

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
AV1 Random Number	RAND	128 bits	c
Expected Response	XRES	32-128 bits	c
Cipher Key	CK	128 bits	c
Integrity Key	IK	128 bits	c
Authentication Token	AUTN	[1]	c
AVn Random Number	RAND	128 bits	c
Expected Response	XRES	32-128 bits	c
Cipher Key	CK	128 bits	c
Integrity Key	IK	128 bits	c
Authentication Token	AUTN	97 –129 bits	c
	MODE	1 bit	c

5.2.3 Radio Node Controller RNC

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
See Common items section 5.1			

5.2.4 USIM

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Received Random Number	RAND	128 bits	c
Received Authentication Token	AUTN	97–129 bits	h
Computed Anonymity Key	AK	32-64 bits	h
Computed Message authentication Code	XMAC-A	64 bits	h
Retrieved Sequence Number	SQN	32-64 bits	c
Computed Response	RES	32-128 bits	h
Re-synchronisation MAC	MAC-S	64 bits	h
Re-synchronisation token	AUTS	[2]97–129 bits	h
- and common items – section 5.1			
Option 1			
Counter- Circuit switched	$SQN_{MS/CS}$	32-64 bits	c
Counter – Packet switched	$SQN_{MS/PS}$	32-64 bits	c
SQN Threshold	delta	24 bits	
Option 2			
Sequence Number Window- Circuit switched	$SQN_{MS/CS}$ - W	10-30	c
Sequence Number Window- Packet switched	$SQN_{MS/PS}$ - W	10-30	c
Option 3			
Sequence Number List – Circuit switched	$LIST_{SQNCS}$	10-30	c
Sequence Number List – Packet switched	$LIST_{SQNPS}$	10-30	c

[2] AUTS = SQNms ⊕ AK || MAC-S

5.2.5 Mobile Equipment ME

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
See common items – section 5.1			

6 Location of Security Functions

6.1 Functions common to Sequence Number and Temporary Key Mechanism

6.1.1 Home Environment Key Administration Center HE/KAC

Block Encryption Algorithm for Network Operators	BEANO	Input: KS_{XY}, Data Output: Encrypted data
Secure Hash Function	HASH	Input: Data Output: hashed data
Public Key encryption Function	E_PK(data)	Input: PK, data Output: edata
Public Key decryption Function	D_SK(edata)	Input: SK, edata Output: data
Public Key Signing Function		
Public Key Verifying Function		

6.1.2 Serving Node Visited Location Register SN/VLR

Name	Symbol	**Input Parameters**
Algorithms		
Public Key Signing Function		
Public Key Verifying Function		

6.1.3 Radio Node Controller RNC

Name	Symbol	**Input Parameters**
Algorithms		
Encryption algorithm	F8	Input: Count, Direction Bearer, Length, CK Output: Keystream
Integrity algorithm	F9	Input: Message, Count, Fresh, IK Output: MAC-I

6.1.4 USIM

Integrity algorithm	UIA	

The location of the integrity function is for further study.

6.1.5 Mobile Equipment ME

Name	Symbol	**Input Parameters**
Algorithms		
Encryption algorithm	F8	Input: Count, Direction Bearer, Length, CK Output: Keystream
Integrity algorithm	F9	Input: Message, Count, Fresh, IK Output: MAC-I
Network-wide user traffic confidentiality Algorithm	UNA	Input: IV, K_S Output: Keystream

The location of the integrity function is for further study.

6.2 Sequence Number Mechanism

6.2.1 Home Environment Authentication Center HE/AuC

Name	Symbol	**Input Parameters**
Algorithms		
Message Authentication Function	F1	Input: K,SQN,RAND, MODE Output: MAC-A
Resynchronisation Message Authentication Function	F1*	Input: K, SQN_{MS} , RAND MODE output: MACS
Message Authentication Function	F2	Input: K,RAND Output: XRES
Cipher Key Generating Function	F3	Input: K,RAND Output: CK
Integrity Key Generating Function	F4	Input: K, RAND Output: IK
Anonymity Key Generating Function	F5	Input: K, RAND Output: AK
Identity Decryption Function	F7	Input: GK, EMUI Output: SEQ_UIC IMUI

6.2.2 USIM

Name	Symbol	**Input Parameters**
Algorithms		
Message Authentication Function	F1	Input: K,SQN,RAND, MODE Output: XMAC-A
Message Authentication Function	F2	Input: K,RAND Output: RES
Cipher Key Generating Function	F3	Input: K,RAND Output: CK
Integrity Key Generating Function	F4	Input: K,RAND Output: IK
Anonymity Key Generating Function	F5	Input: K, RAND Output: AK

Appendix 1 Temporary Key Mechanism

When the mobile first requests service from the SN/VLR, a random seed RSu created by the user (USIM or terminal) is included in the request message. The message including RSu is forwarded to the HE/AuC, which generates its own random challenge RSn. An authentication vector is returned to the SN/VLR. The vector contains {RSn, RES1, XRES2, KT}, where RES1 is the response to the user's challenge, XRES2 is the response to the network's challenge which is expected from the user, and KT is the temporary authentication key shared with the SN/VLR. The network's challenge RSn and the network authentication response RES1 are sent to the MS. If the MS verifies RES1, thereby authenticating the identity of the network, it responds with RES2 and generates the new temporary key KT. The SN/VLR then verifies that RES2 equals XRES2, thereby authenticating the identity of the USIM, and stores the new temporary key KT. Furthermore, both the USIM and the SN/VLR immediately use KT with the random seeds RSu and RSn to generate the first session keys CK and IK. This process is shown in Figure 4 below.

Figure 5 shows how the SN/VLR can offer secure service to the USIM without reference to the home system HE/AuC by using the temporary key KT.

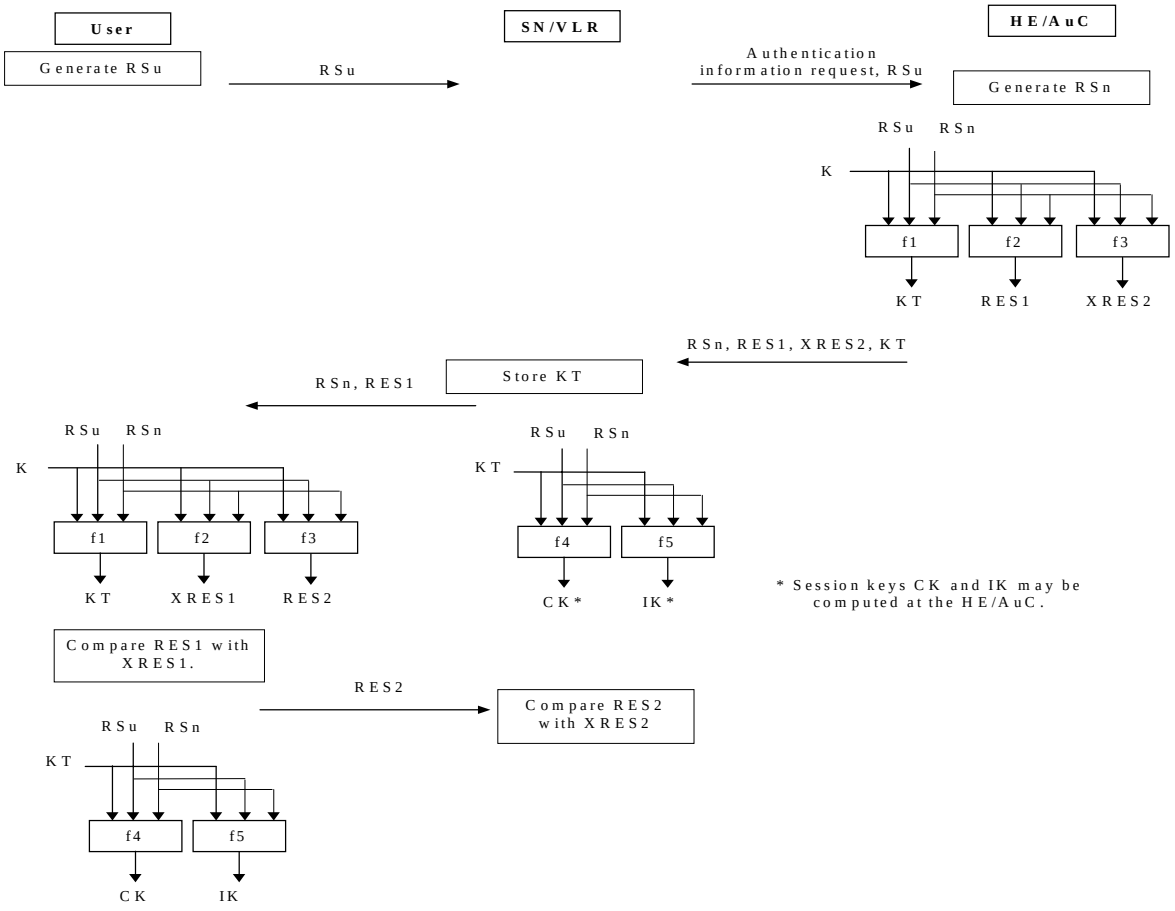


Figure 4: Temporary Key Generation Protocol

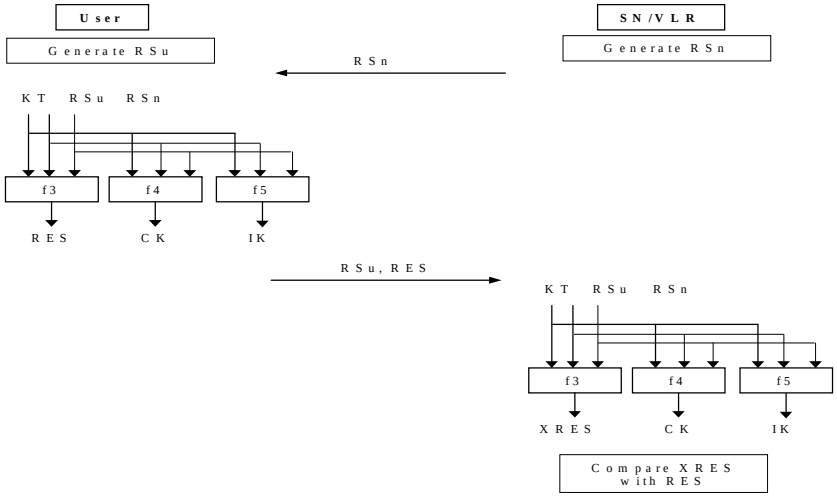


Figure 5. Locally authenticated session key agreement

A1 Security Information stored

A1.1 Home Environment Authentication Centre HE/AuC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Dynamic Information			
Random Seed User	RS_U	128 bits	c
AV_1Random Seed Network	RS_N	128 bits	c
Response to User Challenge RS_U	RES1	32-128 bits	c
Response to User Challenge RS_N	XRES2	32-128 bits	c
Temporary Key	KT	128 bits	b
AVn Random Seed Network	RS_N	128 bits	c
Response to User Challenge RS_U	RES1	32-128 bits	c
Expected Response to Nwk Challenge RS_N	XRES2	32-128 bits	c
Temporary Key	KT	128 bits	b
Fixed Initial Value	PAR1	TBD	a
Fixed Initial Value	PAR2	TBD	a
Fixed Initial Value	PAR3	TBD	a
Fixed Initial Value	PAR4	TBD	a
Fixed Initial Value	PAR5	TBD	a
- and common items – section 5.1			

A1.2 Serving Node Visited Location Register SN/VLR

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Dynamic Information			
Temporary Key	KT	128 bits	b
Random Seed User	RS_U	128 bits	c
Random Seed Network	RS_N	128 bits	c
Response to Users Challenge	RES1	32-128 bits	c
Response to Network Challenge	RES2	32-128 bits	b
Response to Network Challenge	XRES2	32-128 bits	b
Cipher Key	CK*	128 bits	b
Integrity Key	IK*	128 bits	b
Response to SN/VLR challenge (local)	RES	32-128 bits	c
Expected response to challenge	XRES	32-128 bits	C

* May be computed at HE/AuC

A1.3 Radio Node Controller RNC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
See common items – section 5.1			

A1.4 USIM

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Dynamic Information			
Temporary Key	KT	128 bits	B
Random Seed User	RS_U	128 bits	c
Random Seed Network	RS_N	128 bits	c
Computed Response (local authent.)	RES	32-128 bits	B
Response to Users Challenge	RES1	32-128 bits	B
Response to Network Challenge	RES2	32-128 bits	c
Expected response to network challenge	XRES1	32-128 bits	c
- and common items – section 5.1			

A1.5 Mobile Equipment

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
See common items – section 5.1			

A2 Location of Security Functions

A2.1 Home Environment Authentication Centre HE/AuC

Name	**Symbol**	**Input Parameters**
Algorithms		
Key Generating Function	F1	Input: K, RS_U, RS_N Output: KT
Message Authentication Function	F2	Input: K, RS_U, RS_N Output: RES1
Message Authentication Function	F3	Input: K, RS_U , RS_N Output: XRES1
-and common items		

A2.2 Serving Node Visited Location Register SN/VLR

Name	**Symbol**	**Input Parameters**
Algorithms		* May be computed at HE/AuC
Message Authentication Function (local authentication only)	F3	Input: KT, RS_U, RS_N Output: XRES
Cipher Key Generating Function	F4	Input: KT, RS_U, RS_N Output: CK*
Integrity Key Generating Function	F5	Input: KT, RS_U,RS_N Output: IK*
and common items		

A2.3 Radio Node Controller RNC

Name	**Symbol**	**Input Parameters**
Algorithms		
See common items		

A2.4 Mobile Equipment user identity Module USIM

Name	**Symbol**	**Input Parameters**
Algorithms		
Key generating function	F1	Input: K, RS_U, RS_N Output: KT
Message Authentication Function	F2	Input: K, RS_U, RS_N Output: XRES1
Message Authentication Function	F3	Input: K, RS_U, RS_N Output: RES2
Message Authentication Function (for local authentication)	F3	Input: KT, RS_U, RS_N Output: RES
Cipher Key Generating Function	F4	Input: KT, RS_U, RS_N Output: CK
Integrity Key Generating Function	F5	Input: KT, RS_U RS_N Output: IK

A2.5 Mobile Equipment ME

Name	Symbol	**Input Parameters**
Algorithms		
see common items		

Appendix 2 Document history

Document history		
0.0.0	2nd May 1999	Initial draft: Rapporteur- Colin Blanchard
0.0.1	28th May 1999	After review at TSG SA WG3 #3 Bonn 11- 12th May 1999
0.0.2	11th June 1999	To incorporate comments from Takeshi Igarashi, Adam Berenzweig, Benno Tietz, Takeshi Chikazawa
0.0.3	18th June 1999	After review at TSG SA WG3#4 London 16th –18th June 1999

Technical Specification Group Services and System Aspects
Meeting #4, Miami, USA, 21-23 June 1999

TSG SA WG3 #4, London, 16-18 June 1999 **Annex K of S3-99203**

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	011	Current Version:	3.0.0

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

For submision to TSG SA#3 *list TSG meeting no. Here ↑*

for approval [X]
for information [ ]

(only one box should be marked with an X)

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

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

Source: SA WG3 **Date:** 99-06-18

Subject: Precision of the status of annex B

3G Work item: 3G 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	[ ]
C	Functional modification of feature	[X]
D	Editorial modification	[ ]

Reason for change: Modification of status of annex B on user identity confidentiality

Clauses affected: Annex B

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 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 which is shared between all members of the user group and the user's HE, and securely stored in the USIM and in the HE.

The mechanism is illustrated in Figure B.1.

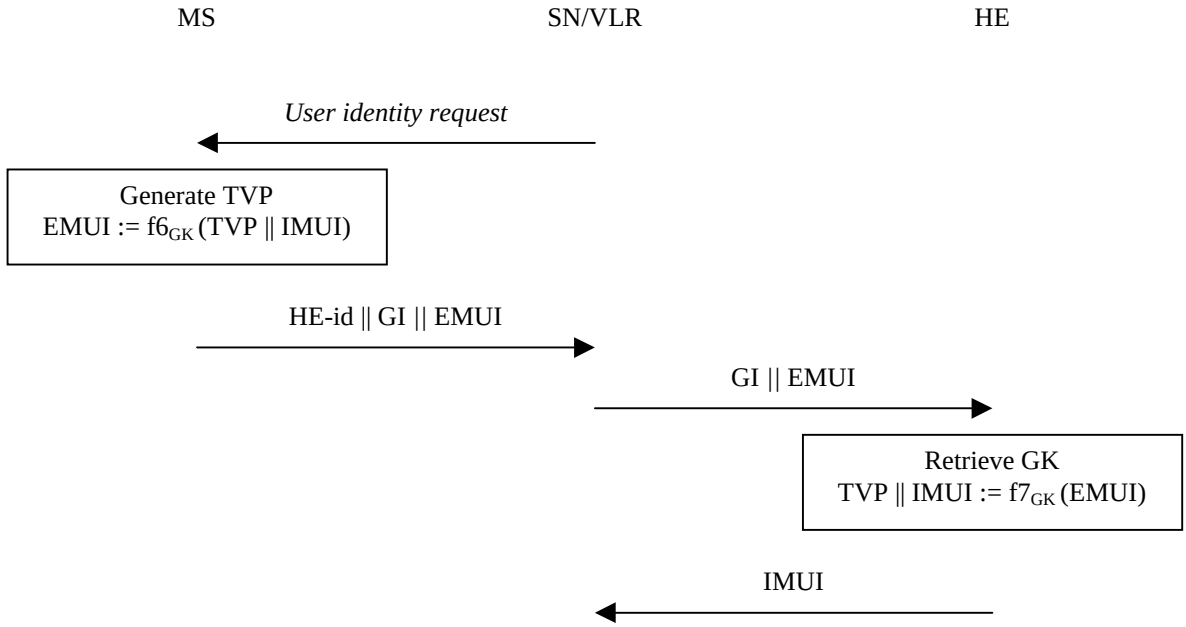


Figure B.1: Identification by means of the IMUI encrypted by means of a group key

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

Upon receipt the user generates a time variant parameter TVP. The user encrypts the time variant parameter TVP and the IMUI with enciphering algorithm f6 and his group key GK. The TVP prevents traceability attacks. The user sends a response to the VLR that includes the HE identity, the group identity GI and the encrypted mobile user identity (EMUI).

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

Upon receipt the HE retrieves the group key GK associated with the group identity GI. The HE then decrypts EMUI with the deciphering algorithm f7 ($f7 = f6^{-1}$) and the group key GK and retrieves TVP and IMUI. The HE then sends the IMUI in a response to the visited SN/VLR.