TSG SA #5, Kyongju, 11-13 Oct. 1999 ***TSGS#5(99)417***

Source: S3
Subject: CRs to 33.102 for approval

CR	to version	topic	in S3 Tdoc	agreed at	CAT
33.102-012	3.1.0	Re-organisation of clause 6	S3-99338	S3#6	D
33.102-013	3.1.0	Integrity protection procedures	S3-99333	S3#6	C
33.102-014	3.1.0	Security of MAP-Based Transmissions	S3-99334	S3#6	C
33.102-015	3.1.0	Secure UMTS-GSM Interoperation	S3-99332	S3#6	C
33.102-016	3.1.0	Network-wide confidentiality	S3-99344	correspondence after S3#6	C
33.102-017	3.1.0	Authentication management field	S3-99348	correspondence after S3#6	C
33.102-018	3.1.0	Support for window and list mechanisms for sequence number management in authentication scheme	S3-99349	correspondence after S3#6	C
33.102-019	3.1.0	Modification of text for window and list mechanisms	S3-99350	correspondence after S3#6	D

TSG SA WG3 #6, Sophia Antipolis, 29 September – 1 October 1999 **S3-99338**
Technical Specification Group Services and System Aspects
Meeting #5, City, Korea, Date.

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**	**012**	Current Version:	3.1.0

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

For submision to TSG SA#5 *list TSG meeting no. here ↑* for approval **X** for information *(only one box should be marked with an X)*

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

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

Source: TSG SA WG 3 **Date:** 1999-10-01

Subject: Re-organisation of clause 6

3G Work item: Security

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

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

Reason for change: Improve presentation of the material of the security mechanism.

Clauses affected: 6, 8.2

Other specs affected:

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

Other comments:


help.doc

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

6 Network access security mechanisms

6.1 Identification by temporary identities

6.1.1 General

This mechanism allows the identification of a user on the radio access link by means of a temporary mobile user identity (TMUI). A TMUI has local significance only in the location area in which the user is registered. Outside that area it should be a accompanied by an appropriate Location Area Identification (LAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR) in which the user is registered.

The TMUI, when available, is normally used to identify the user on the radio access path, for instance in paging requests, location update requests, attach requests, service requests, connection re-establishment requests and detach requests.

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.

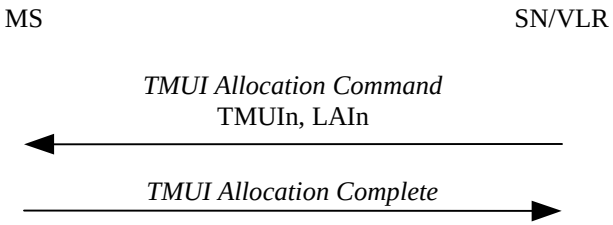


Figure 1: TMUI Allocation

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.

6.1.3 Unacknowledged allocation of a temporary identity

If the serving network does not receive an acknowledgement of the successful allocation of a temporary identity from the user, the network shall maintain the association between the new temporary identity TMUIn and the IMUI and between the old temporary identity TMUIo (if there is any) and the IMUI.

For a~~n~~ user-originated transaction, the network shall allow the user to identify itself by either the old temporary identity TMUIo or the new temporary identity TMUIn. This allows the network to determine the temporary identity stored in the mobile station. The network shall subsequently delete the association between the other temporary identity and the IMUI, to allow the temporary identity to be allocated to another user.

For a network-originated transaction, the network shall identify the user by its permanent identity (IMUI). When radio contact has been established, the network shall instruct the user to delete any stored TMUI. When the network receives an acknowledgement from the user, the network shall delete the association between the IMUI and any TMUI to allow the released temporary identities to be allocated to other users.

Subsequently, in either of the cases above, the network may initiate the normal TMUI reallocation procedure.

Repeated failure of TMUI reallocation (passing a limit set by the operator) may be reported for O&M action.

6.1.4 Location update

In case a user identifies itself using a TMUIo/LAIo pair that was assigned by the visited VLRn the IMUI can normally be retrieved from the database. If this is not the case, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.

In case a user identifies itself using a TMUIo/LAIo pair that was not assigned by the visited VLRn and the visited VLRn and the previously visited VLRo exchange authentication data, the visited VLRn should request the previously visited VLRo to send the permanent user identity. This mechanism is described in 6.3.4, it is integrated in the mechanism for distribution of authentication data between VLRs. If the previously visited VLRo cannot be contacted or cannot retrieve the user identity, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.

6.2 Identification by a permanent identity

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

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

The mechanism is illustrated in Figure 3.

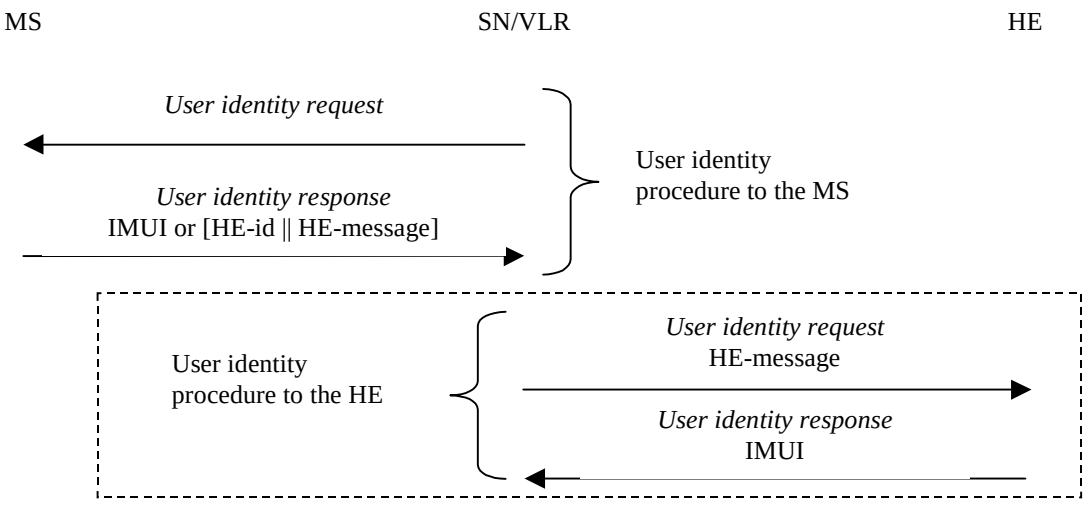


Figure 3: Identification by the permanent identity

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

Note: The term HE-id denotes the 3G equivalent of the information contained in MCC || MNC.

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

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

6.3 Authentication and key agreement

6.3.1 General

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

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

An overview of the mechanism is shown in figure 4.

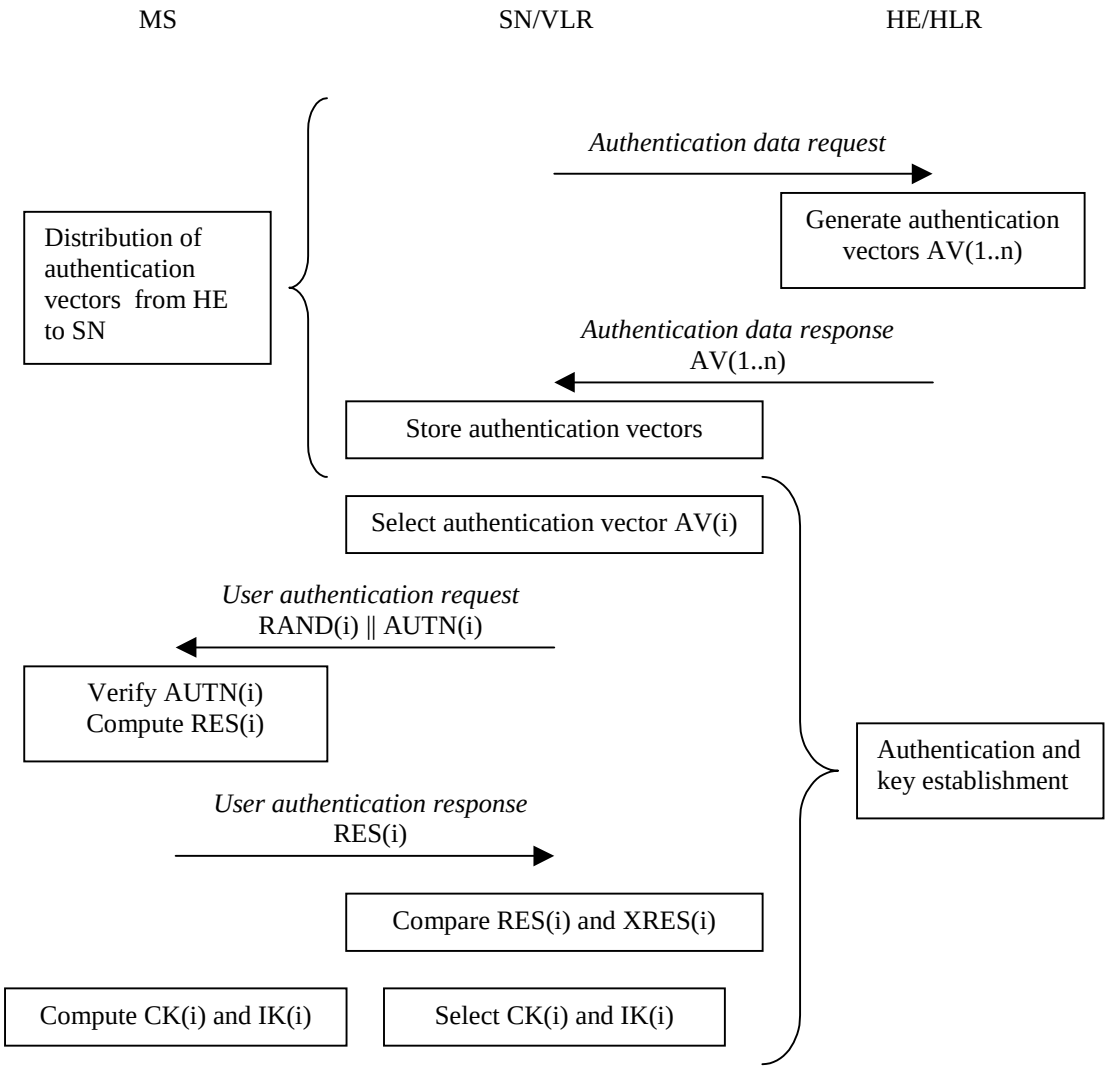


Figure 4: Authentication and key agreement

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

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

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

~~Note: It is ffs. whether a separate mechanism for authentication based on a shared integrity key is required, or whether entity authentication is implicitly provided by means of the data integrity protection of signalling messages. If a separate mechanism is required, it is described in 6.5.~~

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

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

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

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

6.3.2 Distribution of authentication data from HE to SN

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

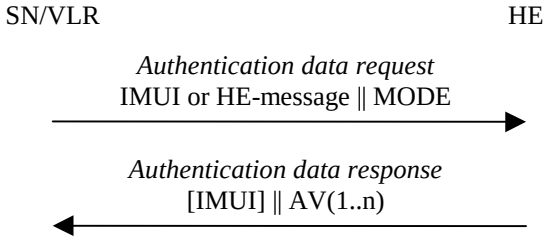


Figure 5: Distribution of authentication data from HE to SN/VLR

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

The *authentication data request* shall include a user identity 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).

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

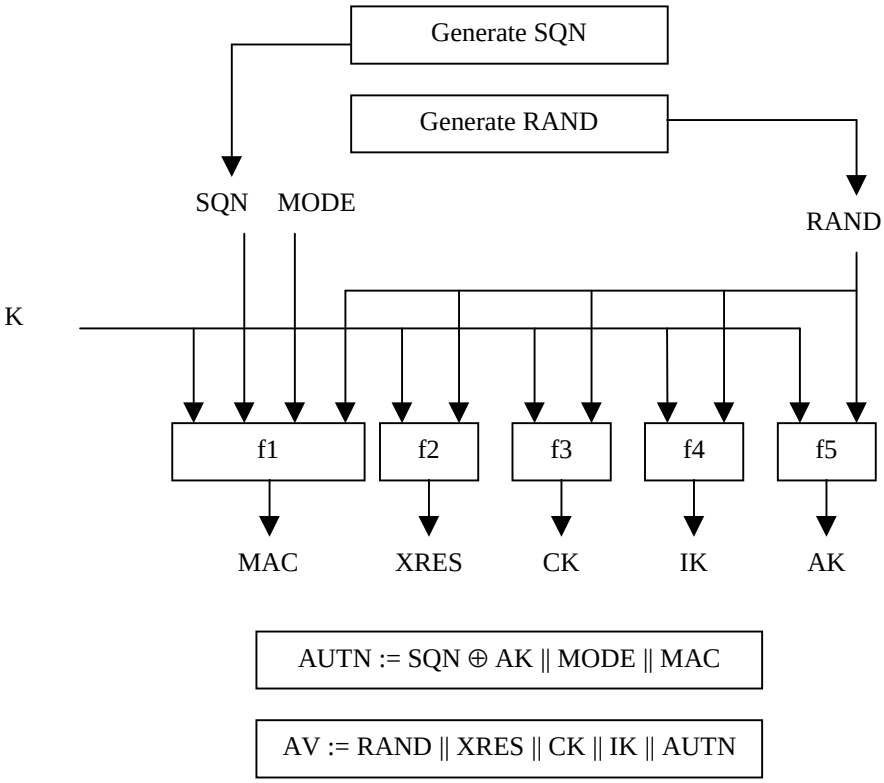


Figure 6: Generation of an authentication vector

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

For each user the HE/AuC keeps track of two counters: $SQN_{HE/CS}$ for authentications initiated by the CS CN nodes, and $SQN_{HE/PS}$ for authentications initiated by the PS CN nodes.

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

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

Note 2: The solution in the main body uses the parameter MODE to distinguish between the CS and the PS core network nodes such that each node can simultaneously and independently support mobility management for the mobile user. Consequently two counters are required both in the AuC and in the USIM. If a single counter would be used, we would run into the following problem: Suppose that a CS node would order the SQNs 1–5, and use SQN 1 and a PS node would order the SQNs 6–10 and uses 6. Then the CS node would like to use 2, but that SQN is rejected. He orders new authentication vectors, with SQNs 11–15, and authenticates with SQN 11. Then the PS node runs into problems. The separate counters for CS and PS mode provide a solution for this problem.

Subsequently the following values are computed:

- a message authentication code $MAC = f1_K(SQN \| RAND \| MODE)$ where f1 is a message authentication function;
- an expected response $XRES = f2_K(RAND)$ where f2 is a (possibly truncated) message authentication function;
- a cipher key $CK = f3_K(RAND)$ where f3 is a key generating function;

- an integrity key IK = $f4_K$ (RAND) where f4 is a key generating function;
- an anonymity key AK = $f5_K$ (RAND) where f5 is a key generating function.

Finally the authentication token AUTN = SQN ⊕ AK || MODE || MAC is constructed.

Here, AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only.

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

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

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

6.3.3 Authentication and key agreement

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

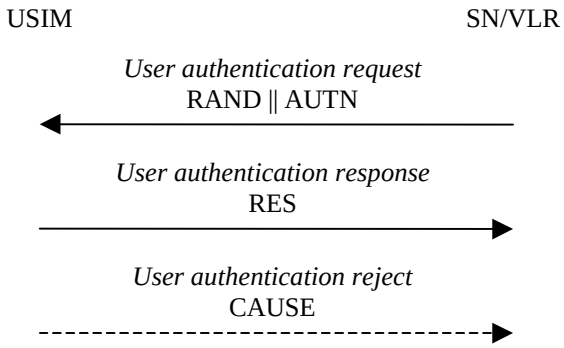


Figure 7: Authentication and key agreement

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

Upon receipt the user proceeds as shown in Figure 8.

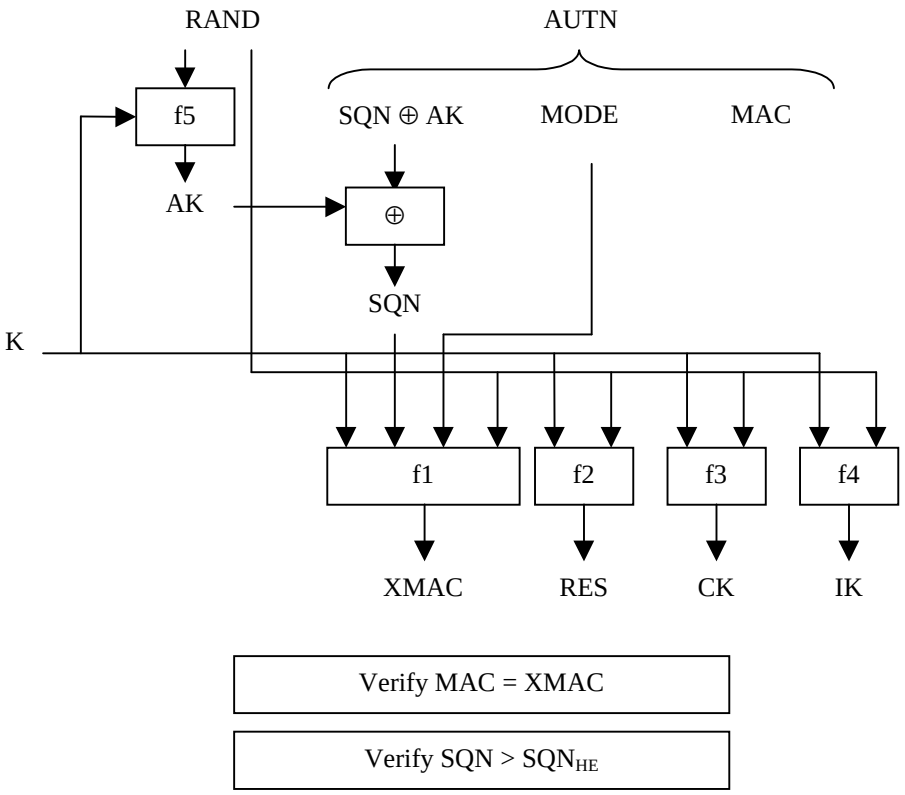


Figure 8: User authentication function in the USIM

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

Next the user computes XMAC = $f1_K$ (SQN || RAND || 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 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 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 to be in the correct range and subsequently sets $SQN_{MS/MODE}$ to SQN.

Note: The MS and the HE have 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 9:

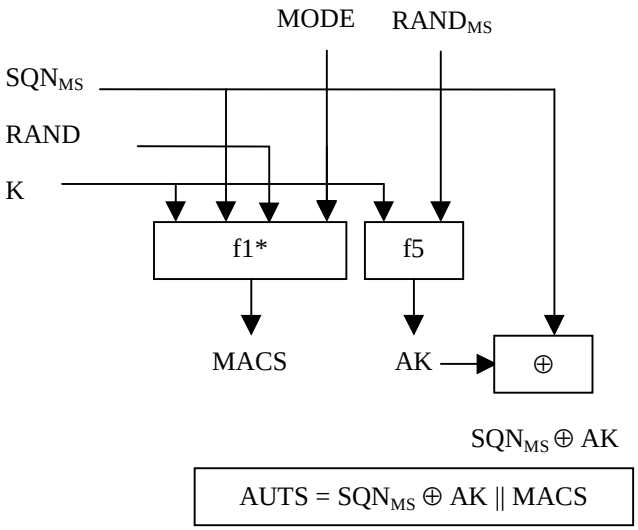


Figure 9: Construction of the parameter AUTS

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

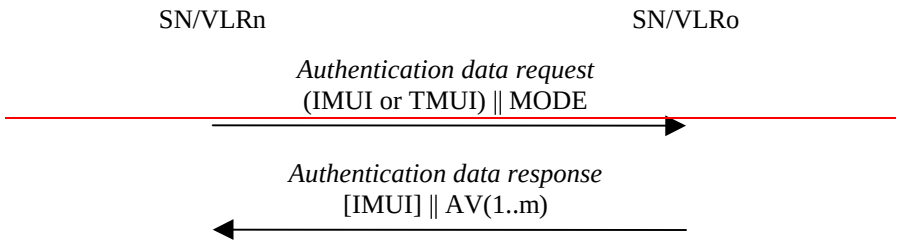
Upon receipt of *user authentication response* the SN/VLR compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The SN/VLR also selects the appropriate cipher key CK and integrity key IK from the selected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

Conditions on the use of authentication information by the SN/VLR: Using the procedures described in subsections 6.3.1, 6.3.2 and 6.3.4, authentication vectors will have to be used in the specific order in which they were generated, otherwise the user will reject the authentication attempt. The SN/VLR shall use an authentication vector only once and, hence, shall send out each user authentication request *RAND* || *AUTN* only once no matter whether the authentication attempt was successful or not. A consequence is that authentication vectors cannot be reused. When a user changes from one VLR to another one and the new VLR requests remaining authentication vectors from the old VLR (cf. subsection 6.3.4) then the old VLR shall not retain any copies of these authentication vectors. When a VLR receives a “cancel location” request for a certain user it shall delete all authentication vectors relating to that user. When a VLR receives a location update request from a user and the VLR notices that authentication vectors relating to that user are still stored in the VLR it will delete this information and request fresh authentication vectors from the HE/AuC.

Different rules may apply when one of the alternative schemes for sequence number handling described in Annex C 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.

6.3.4 Distribution of authentication vectors between VLRs

The purpose of this procedure is to provide a newly visited VLR with unused authentication vectors from a previously visited VLR. ~~The procedure is shown in Figure 10.~~



~~Figure Figure 10: Distribution of authentication vectors between VLRs~~

The procedure is initiated by the visited VLR and illustrated in the following Figure 11:

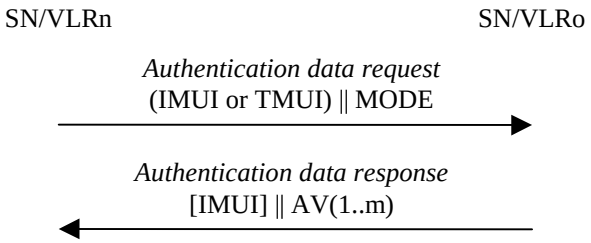


Figure 11: Distribution of authentication data between SN/VLR

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

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 12 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*).*

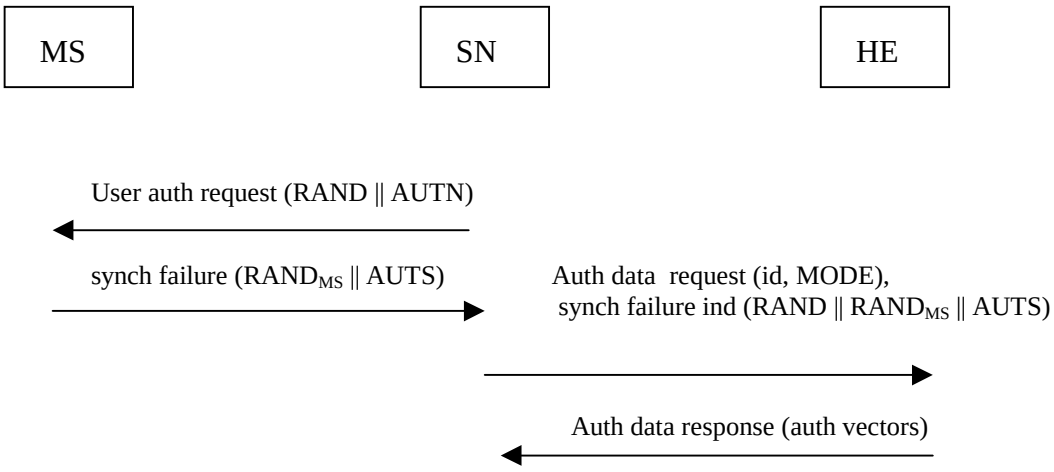


Figure 12: Re-synchronisation procedure

6.3.6 Length of sequence numbers

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

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

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

6.3.7 Interoperability with 2G networks

Note: This section should define the procedures and functions that are required to support roaming of UMTS users in GSM networks and handover of UMTS users between UMTS networks and GSM networks as regards the establishment of cipher and integrity keys.

In case of handover the user should receive the level of security that is usually provided in the network that is entered. Therefore the following functionality has to be provided in case of handover:

- system specific security keys have to be established

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

At least 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.

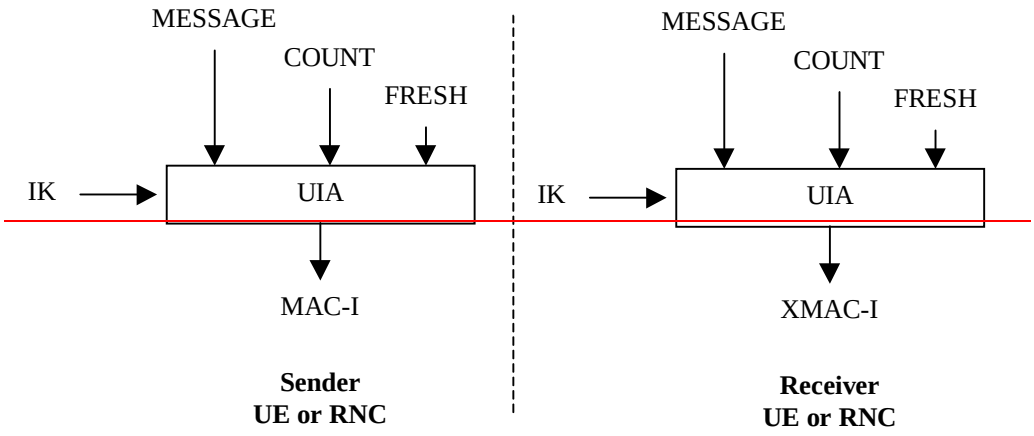
At least the following signalling elements sent by the RNC to the MS should be protected:

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

6.4.2Integrity algorithm

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

Figure 13 illustrates the use of the UIA to authenticate the data integrity of a signalling message.



~~**Figure 13: 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 Local authentication and connection establishment

~~6.4.3 Integrity~~6.4.1 Cipher key and integrity key setting

Mutual key setting is the procedure that allows the MS and the RNC to agree on the key IK used to compute message authentication codes using algorithm UIA. 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.

~~6.4.4 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~~6.4.2 Cipher key and integrity~~key.~~

~~6.4.5 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 amount of data that is protected by a access link key set.~~

~~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.~~

~~The USIM shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches a maximum value set by the operator and stored in the USIM[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.~~

~~6.4.6 UIA numbering~~

~~Table1 - 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~~

~~6.4.7 UIA~~mode 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~~Classmark which cipher and integrity algorithms the 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~~the MS/USIM Classmark the cipher and imust 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.

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~~SN have no versions of the UIA algorithm in common, then the connection shall be released.

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

3) If the MS and the ~~network~~SN 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.

~~6.4.8 Integrity protection procedures~~

~~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.~~

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

6.4.8.1 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.

6.5 Local authentication

Note: This section should define a mechanism for authentication based on a shared integrity key. It is ffs. whether a separate mechanism is required, or whether the security feature is implicitly provided through the use of the integrity key for signalling messages.

6.6 Data confidentiality

6.6.1 General

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

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

6.6.2 Ciphering algorithm

Algorithm UEA is implemented in both the MS and the RNC. On the RNC side the description below assumes that one algorithm UEA is implemented for each dedicated physical channel [not yet decided]. The data flow on dedicated

channels is ciphered by a bit per bit or stream cipher generated by an algorithm UEA.

The UEA shall produce one output as a sequence of keystream bits referred to as a Key Stream Segment (KSS). A KSS of length n shall be produced to encrypt a given segment of plaintext of length n. The bits of KSS are labelled KSS(0), …KSS(n-1), where KSS(0) is the first bit output from the generator. The bits in the KSS shall be used to encrypt or decrypt the data.

Note: [The point at which confidentiality protection is applied in the UTRAN architecture is for further study. At this stage we assume that confidentiality protection is applied at the RNC.]

6.6.3 Cipher key agreement

The establishment of a new cipher key CK is integrated in the user authentication mechanism described in 6.3. A new cipher key CK is established each time an authentication protocol is executed between the USIM and the core network node that initiated the authentication.

6.6.4 Cipher key selection

Because of the separate mobility management for CS and PS services, the USIM establishes cipher keys with both the CS and the PS core network nodes. Currently two options are considered for the selection of the cipher key:

6.6.4.1 Option 1: Two key solution

The CS user data connections are ciphered with the most recent cipher key CK_{CS} agreed between the user and the 3G CS core network node. The PS user data connections are ciphered with the most recently cipher key CK_{PS} agreed between the user and the 3G PS core network node. The (common) signalling data connections are ciphered with the most recently cipher key established between the user and the network, i.e., the youngest of CK_{CS} and CK_{PS}. This requires that the cipher key of an (already ciphered) ongoing signalling connection is changed. This change should be completed within five seconds after an authentication and key agreement protocol has been executed.

6.6.4.2 Option 2: One key solution

All connections (CS user data, PS user data and signalling data) are ciphered with the most recently cipher key CK agreed between the user and either one of the core network nodes. This requires that the cipher key of any (already ciphered) ongoing connection is changed. This change should be completed within five seconds after an authentication an key agreement protocol has been executed.

6.6.5 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.

6.6.6 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 lifetime of the cipher key is controlled by the mechanism described in 6.4.5.

6.6.7 UEA numbering

[The following table is for illustration only]

Table 2 – UEA numbering

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

6.6.8 UEA negotiation

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

When an MS wishes to establish a connection with the network, the MS shall indicate to the network which version of the UEA algorithm it supports.

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

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

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

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

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 Synchronisation6.4.4 Cipher key and integrity key lifetime

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

Each time an RRC connection is released the highest value of the hyperframe number (the current value of COUNT) of the bearers that were protected in that RRC connection is stored in the USIM. When the next RRC connection is

established that value is read from the USIM and incremented by one.

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

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

6.4.4 Cipher key and integrity key identification

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

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

6.4.5 Procedures

6.5 Access link data integrity

6.5.1 General

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

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

At least 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;
- in-call connection authentication messages;
- various location updates, e.g. cell updates and URA updates.

At least 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.
- in-call connection authentication messages.

6.5.2 Integrity algorithm

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

Figure 13 illustrates the use of the UIA to authenticate the data integrity of a signalling message.

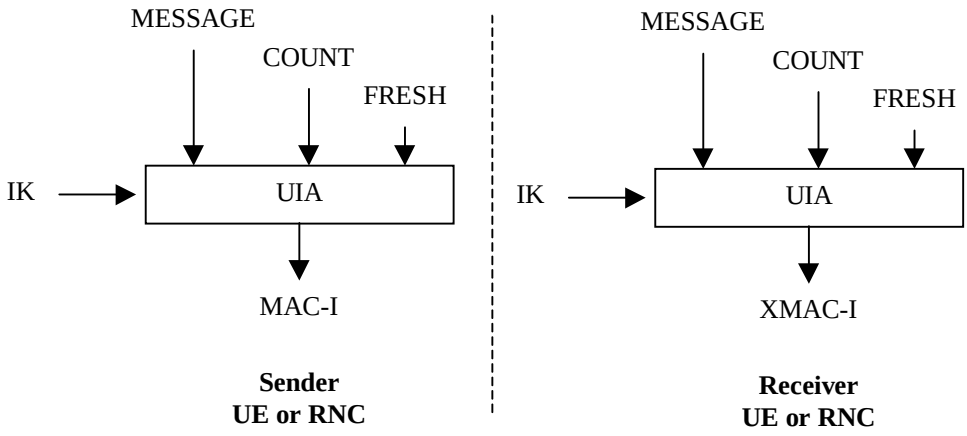


Figure 13: Derivation of MAC-I (or XMAC-I) on a signalling message

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.

6.5.3 UIA identification

Each UIA will be assigned a 4-bit identifier.

Table1 - UIA identifiation

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

6.6 Access link data confidentiality

6.6.1 General

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

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

6.6.2 Ciphering algorithm

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

The UEA shall produce one output as a sequence of keystream bits referred to as a Key Stream Segment (KSS). A KSS of length n shall be produced to encrypt a given segment of plaintext of length n. The bits of KSS are labelled KSS(0), …KSS(n-1), where KSS(0) is the first bit output from the generator. The bits in the KSS shall be used to encrypt or decrypt the data.

6.6.3 UEA identification

Each UEA will be assigned a 4-bit identifier.

Table 2 – UEA identification

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

6.6.4 Synchronisation of ciphering

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

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

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

~~[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.

~~6.6.9.4 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.

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

6.7 Network-wide encryption

6.7.1 Introduction

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

If network-wide confidentiality of user traffic is provided we assume that access link confidentiality of user traffic between UE and RNC will be replaced with the network-wide service. However, we note that access link confidentiality of signalling information and user identity between UE and RNC will be applied regardless of whether the network-wide user traffic confidentiality service is applied or not.

The provision of an network-wide confidentiality service in 3GMS has an obvious impact on lawful interception. We assume that the same lawful interception interface is required in 3GMS as in second generation systems regardless of whether network-wide confidentiality is applied by the network or not. Thus, we assume that it must be possible to remove any network-wide confidentiality protection within the core network to provide access to plaintext user traffic at the lawful interception interface.

We assume that network-wide confidentiality will be provided by protecting transmissions on user traffic channels using a synchronous stream cipher. This will involve the specification of a standard method for ciphering user traffic on an end-to-end basis and a standard method for managing the ciphering key required at the end points of the protected channel.

6.7.2 Ciphering method

It is assumed that the network-wide encryption algorithm shall be a synchronous stream cipher similar to the access link encryption algorithm. Indeed, it would be desirable to use the same algorithm for access link encryption and for network-wide encryption.

The network-wide synchronous stream cipher shall contain a key stream generator which shall have (at least) two inputs:

the end-to-end cipher key (Ks) and an initialisation value (IV). The plaintext shall be encrypted using the key stream by applying an exclusive-or operation to the plaintext on a bit per bit basis to generate the ciphertext. The decryption operation shall involve applying the same key stream to the ciphertext to recover the plaintext.

Synchronisation of the key stream shall be achieved using the initialisation value. Synchronisation information shall be available at both end points of the communication and shall be used to maintain alignment of the key stream. For example, it might be necessary to transmit explicit end-to-end synchronisation frames with the user traffic at certain intervals. Alternatively, it might be possible to use some existing frame structure for network-wide encryption synchronisation purposes. The frequency at which synchronisation information must be made available at each end to ensure reliable transmission will depend on the exact nature of the end-to-end user traffic channel.

Protection against replay of user traffic shall be achieved through the use of a time variable initialisation vector combined with a time variable cipher key. If the same cipher key is used in more than one call then it may be necessary to include a third input to the key stream generator such as a call-id or a time-stamp to protect against replay of the whole call. Note that the stream cipher does not protect against bit toggling so other mechanisms must be used if this type of integrity protection is required on user traffic.

For encryption of voice traffic we assume that Transcoder Free Operation (TFO) is used between the two end points such that the structure and ordering of the transmitted data is maintained with the same boundary conditions at each end of the link. Note that in the initial phases of 3GMS, transcoder free operation may only be possible for user traffic channels which terminate within the same serving network. Furthermore, TFO may only be possible if the entire communication path is within the same serving network. Thus, in non optimal routing cases where the tromboning effect occurs, TFO may not be available, even if the traffic channel terminates within the same serving network.

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

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

Issues for further study:

- Specification of encryption synchronisation mechanism;
- Adaptation of TFO voice traffic channels for network-wide confidentiality;
- Adaptation of data traffic channels for network-wide confidentiality;
- The ability to terminate network-wide encryption at network gateways for inter-network user traffic channels;
- The ability to handle multiparty calls, explicit call transfer and other supplementary services;
- Network-wide encryption control – algorithm selection, mode selection, user control

6.7.3 Key management

6.7.3.1 General case

We assume that signalling links within the network are confidentially protected on a link-by-link basis. In particular, we assume that the UE to RNC signalling links are protected using access link security domain keys (see clause 6). We also assume that VLR to RNC signalling links and core network signalling links are protected using network security domain keys (see clause 7). Note that if network-wide encryption can be provided across serving network boundaries (e.g. because inter-network TFO is available) then the signalling links requiring protection will cross network boundaries. In this situation it is important to note that the two serving networks may not be roaming partners yet they still must be able to confidentially protect inter-network signalling by establishing appropriate keys.

The key management scheme for network-wide encryption involves establishing an end-to-end session key between the end points of the traffic channel. It should not be possible to obtain this key by eavesdropping on any transmission links within the network. However, it may be possible to obtain the end-to-end key by compromising certain nodes within the

network (e.g. nodes where link encryption terminates).

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

Issues for further study:

- Specification of key management scheme for the general case;
- - The ability to terminate network-wide encryption key management at network gateways for inter-network user traffic channels.

6.7.3.2 Outline scheme for intra-serving network case

In this case we make the following assumptions:

- Two UEs registered on the same serving network wish to set up an network-wide confidentiality protected call
- The appropriate user traffic channel for encryption can be established between the two UEs
- During connection establishment, the appropriate control information is transmitted to the called party indicating that the incoming connection is end-to-end encrypted.
- During connection establishment, the appropriate control information is transmitted to the relevant VLRs (or other core network entities) indicating that the connection being established is end-to-end encrypted.
- The keys Ka and Kb used to derive the end-to-end session key shall not be used for access link encryption of other data, nor for the derivation of end-to-end session keys with other parties.

The key management scheme is illustrated in the diagram below.

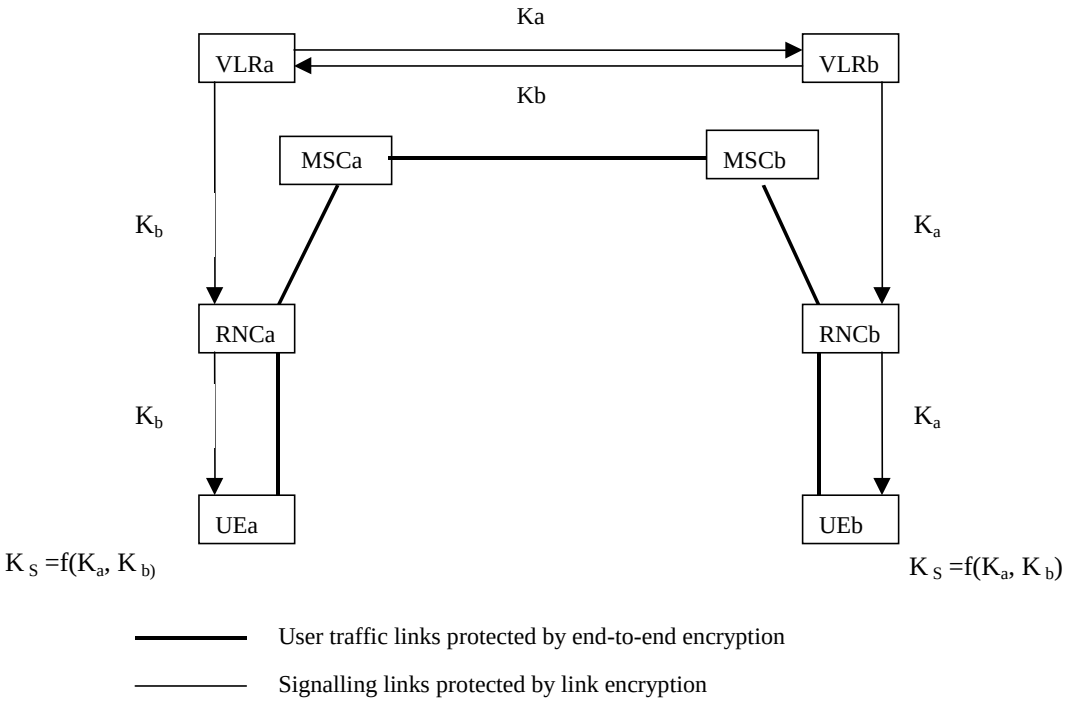


Figure 15: Key management scheme for network-wide encryption

In this scheme VLRa and VLRb exchange access link cipher keys for UEa and UEb. VLRa then passes Kb to UEa, while VLRb passes Ka to UEb. At each end the access link key is transmitted to the UE over protected signalling channels (which may be protected using different access link keys Ka' and Kb'). When each UE has received the other party's access link key, the end-to-end session key Ks is calculated as a function of Ka and Kb.

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

Issues for further study:

- The exact mechanism by which the VLRs exchange access link keys during connection set up.

6.7.3.3 Variant on the outline scheme

VLRa and VLRb mutually agree Ks over a secure signalling link using an appropriate key establishment protocol. VLRa then passes Ks to UEa and VLRb passes Ks to UEb.

Note: As opposed to the scheme in section 8.2.3.2, the access link keys Ka and Kb could be used for access link encryption of other data.

6.8 Interoperation and handover between UMTS and GSM

[To be added]

8 Application security mechanisms

8.1 Secure messaging between the USIM and the network

This clause will specify the structure of the secured messsages in a general format so that they can be used over a variety of transport channels between an entity in a 3GMS network and an entity in the USIM. The sending/receiving entity in the 3GMS network and in the USIM are responsible for applying the security mechanisms to application messages as defined to provide the security features identified in 5.4.1.

Note: A joint 3GPP TSG-SA 'Security'/3GPP TSG-T 'USIM' working group may be required to progress this issue.

~~8.2 Network-wide user traffic confidentiality~~

~~8.2.1 Introduction~~

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

~~If network-wide confidentiality of user traffic is provided we assume that access link confidentiality of user traffic between UE and RNC will be replaced with the network-wide service. However, we note that access link confidentiality of signalling information and user identity between UE and RNC will be applied regardless of whether the network-wide user traffic confidentiality service is applied or not.~~

~~The provision of an network-wide confidentiality service in 3GMS has an obvious impact on lawful interception. We assume that the same lawful interception interface is required in 3GMS as in second generation systems regardless of whether network-wide confidentiality is applied by the network or not. Thus, we assume that it must be possible to remove any network-wide confidentiality protection within the core network to provide access to plaintext user traffic at the lawful interception interface.~~

~~We assume that network-wide confidentiality will be provided by protecting transmissions on user traffic channels using a synchronous stream cipher. This will involve the specification of a standard method for ciphering user traffic on an end-to-end basis and a standard method for managing the ciphering key required at the end points of the protected channel.~~

~~8.2.2 Ciphering method~~

~~It is assumed that the network-wide encryption algorithm shall be a synchronous stream cipher similar to the access link encryption algorithm. Indeed, it would be desirable to use the same algorithm for access link encryption and for network-wide encryption.~~

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

~~Synchronisation of the key stream shall be achieved using the initialisation value. Synchronisation information shall be available at both end points of the communication and shall be used to maintain alignment of the key stream. For example, it might be necessary to transmit explicit end-to-end synchronisation frames with the user traffic at certain intervals. Alternatively, it might be possible to use some existing frame structure for network-wide encryption synchronisation purposes. The frequency at which synchronisation information must be made available at each end to ensure reliable transmission will depend on the exact nature of the end-to-end user traffic channel.~~

Protection against replay of user traffic shall be achieved through the use of a time variable initialisation vector combined with a time variable cipher key. If the same cipher key is used in more than one call then it may be necessary to include a third input to the key stream generator such as a call id or a time stamp to protect against replay of the whole call. Note that the stream cipher does not protect against bit toggling so other mechanisms must be used if this type of integrity protection is required on user traffic.

For encryption of voice traffic we assume that Transcoder Free Operation (TFO) is used between the two end points such that the structure and ordering of the transmitted data is maintained with the same boundary conditions at each end of the link. Note that in the initial phases of 3GMS, transcoder free operation may only be possible for user traffic channels which terminate within the same serving network. Furthermore, TFO may only be possible if the entire communication path is within the same serving network. Thus, in non optimal routing cases where the tromboning effect occurs, TFO may not be available, even if the traffic channel terminates within the same serving network.

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

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

Issues for further study:

- Specification of encryption synchronisation mechanism;
- Adaptation of TFO voice traffic channels for network-wide confidentiality;
- Adaptation of data traffic channels for network-wide confidentiality;
- The ability to terminate network-wide encryption at network gateways for inter-network user traffic channels;
- The ability to handle multiparty calls, explicit call transfer and other supplementary services;
- Network-wide encryption control – algorithm selection, mode selection, user control

8.2.3 Key management

8.2.3.1 General case

We assume that signalling links within the network are confidentially protected on a link-by-link basis. In particular, we assume that the UE-to-RNC signalling links are protected using access link security domain keys (see clause 6). We also assume that VLR-to-RNC signalling links and core network signalling links are protected using network security domain keys (see clause 7). Note that if network-wide encryption can be provided across serving network boundaries (e.g. because inter-network TFO is available) then the signalling links requiring protection will cross network boundaries. In this situation it is important to note that the two serving networks may not be roaming partners yet they still must be able to confidentially protect inter-network signalling by establishing appropriate keys.

The key management scheme for network-wide encryption involves establishing an end-to-end session key between the end points of the traffic channel. It should not be possible to obtain this key by eavesdropping on any transmission links within the network. However, it may be possible to obtain the end-to-end key by compromising certain nodes within the network (e.g. nodes where link encryption terminates).

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

Issues for further study:

- Specification of key management scheme for the general case;
- The ability to terminate network-wide encryption key management at network gateways for inter-network user traffic channels.

8.2.3.2 Outline scheme for intra-serving network case

In this case we make the following assumptions:

- Two UEs registered on the same serving network wish to set up an network-wide confidentiality protected call
- The appropriate user traffic channel for encryption can be established between the two UEs
- During connection establishment, the appropriate control information is transmitted to the called party indicating that the incoming connection is end-to-end encrypted.
- During connection establishment, the appropriate control information is transmitted to the relevant VLRs (or other core network entities) indicating that the connection being established is end-to-end encrypted.
- The keys Ka and Kb used to derive the end-to-end session key shall not be used for access link encryption of other data, nor for the derivation of end-to-end session keys with other parties.

The key management scheme is illustrated in the diagram below.

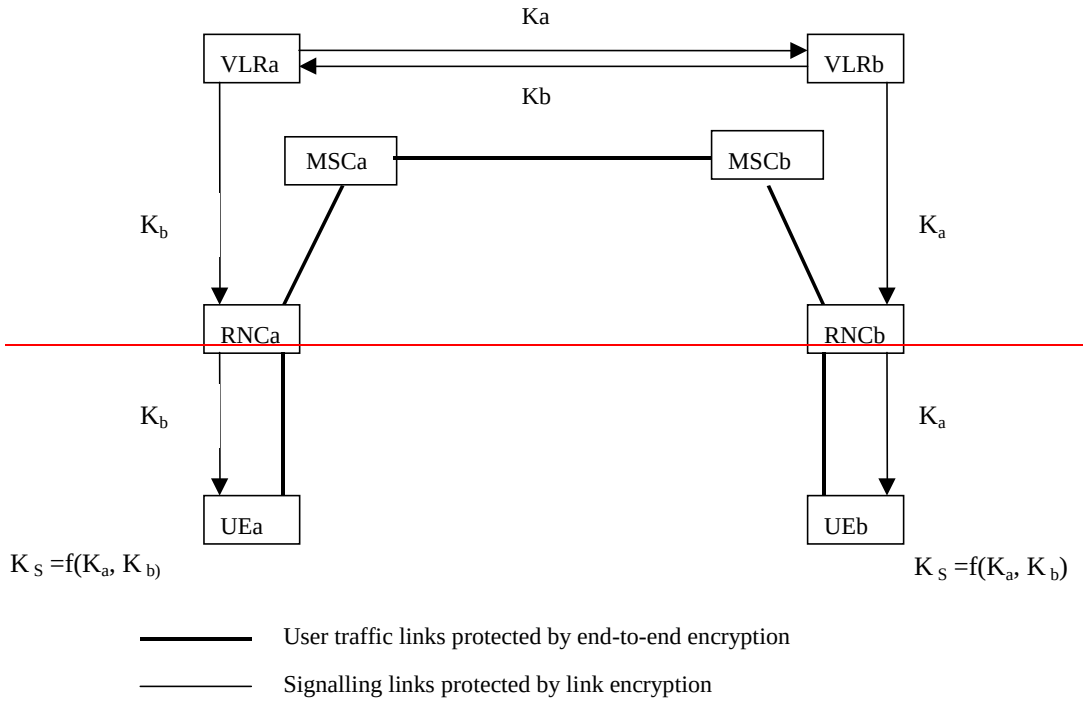


Figure 15: Key management scheme for network-wide encryption

In this scheme VLRa and VLRb exchange access link cipher keys for UEa and UEb. VLRa then passes Kb to UEa, while VLRb passes Ka to UEb. At each end the access link key is transmitted to the UE over protected signalling channels (which may be protected using different access link keys Ka' and Kb'). When each UE has received the other party's access link key, the end-to-end session key Ks is calculated as a function of Ka and Kb.

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

Issues for further study:

- The exact mechanism by which the VLRs exchange access link keys during connection set up.

8.2.3.3 Variant on the outline scheme

VLRa and VLRb mutually agree Ks over a secure signalling link using an appropriate key agreement protocol. VLRa then passes Ks to UEa and VLRb passes Ks to UEb.

~~Note: As opposed to the scheme in section 8.2.3.2, the access link keys Ka and Kb could be used for access link encryption of other data.~~

~~8.3~~8.2 IP security

[ffs]

3GPP TSG SA3#6 **S3-99333**
Sophia-Antipolis, 29 Sep – 01 Oct 1999

3G CHANGE REQUEST

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

TS 33.102 **CR** **13** Current Version: 3.1.0

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

For submission to TSG SA#5 for approval [X]
list TSG meeting no. here ↑ for information [ ]
(only one box should Be marked with an X)

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

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

Source: 3GPP TSG SA WG 3 (Security) **Date:** 1. October 1999

Subject: Integrity protection procedures

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: All details of the integrity protection functionality are not given in the current version. The CR covers the missing parts.

Clauses affected: 6.4.1, 6.4.2, 6.4.7, 6.4.8, 6.6.9

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:

3GPP TSG SA3#6 S3-99333
Sophia-Antipolis, 29 Sep – 01 Oct 1999

6.4 Data integrity of signalling elements

6.4.1 General

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

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

~~At least 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 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.~~

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

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

6.4.2 Integrity algorithm

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

Figure 13 illustrates the use of the UIA to authenticate the data integrity of a signalling message.

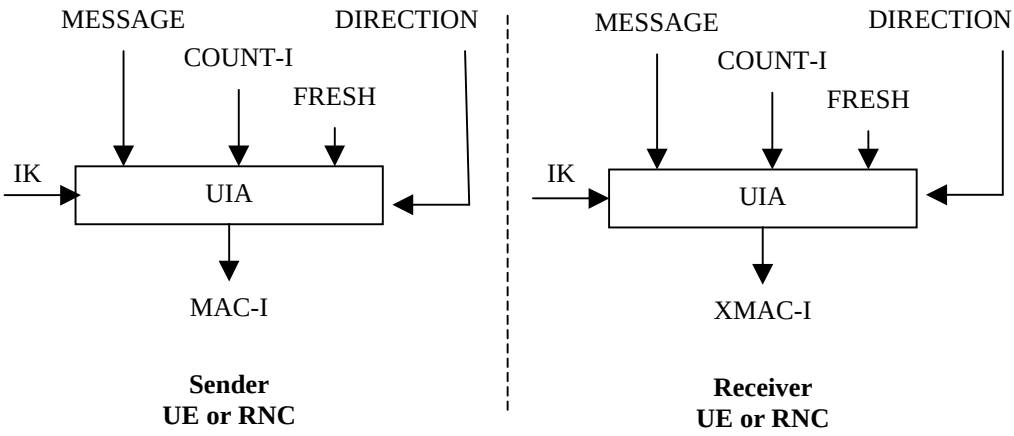


Figure 13: Derivation of MAC-I (or XMAC-I) on a signalling message

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

The input parameter COUNT-I protects against replay during a connection. It is a value incremented by one for each integrity protected message~~at both sides of the radio access link every 10 ms layer 1 frame~~. COUNT-I consists of two parts: the HYPERFRAME NUMBER (HFN) as the most significant part and a RRC Sequence Number as the least significant part. ~~Its~~ The initial value of the hyperframe number is sent by the user to the network at connection set-up. The user stores the greatest~~last~~ used hyperframe number~~COUNT value~~ from the previous connection and increments it by one (see 6.4.5). In this way the user is assured that no COUNT-I 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.

6.4.3 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.

6.4.4 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.

6.4.5 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 amount of data that is protected by a access link key set.

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.

The USIM shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches a maximum value set by the operator and stored in the USIM[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.

6.4.6 UIA numbering

Table1 - 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

6.4.7 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 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.

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.~~

6.4.8 Integrity protection procedures

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.

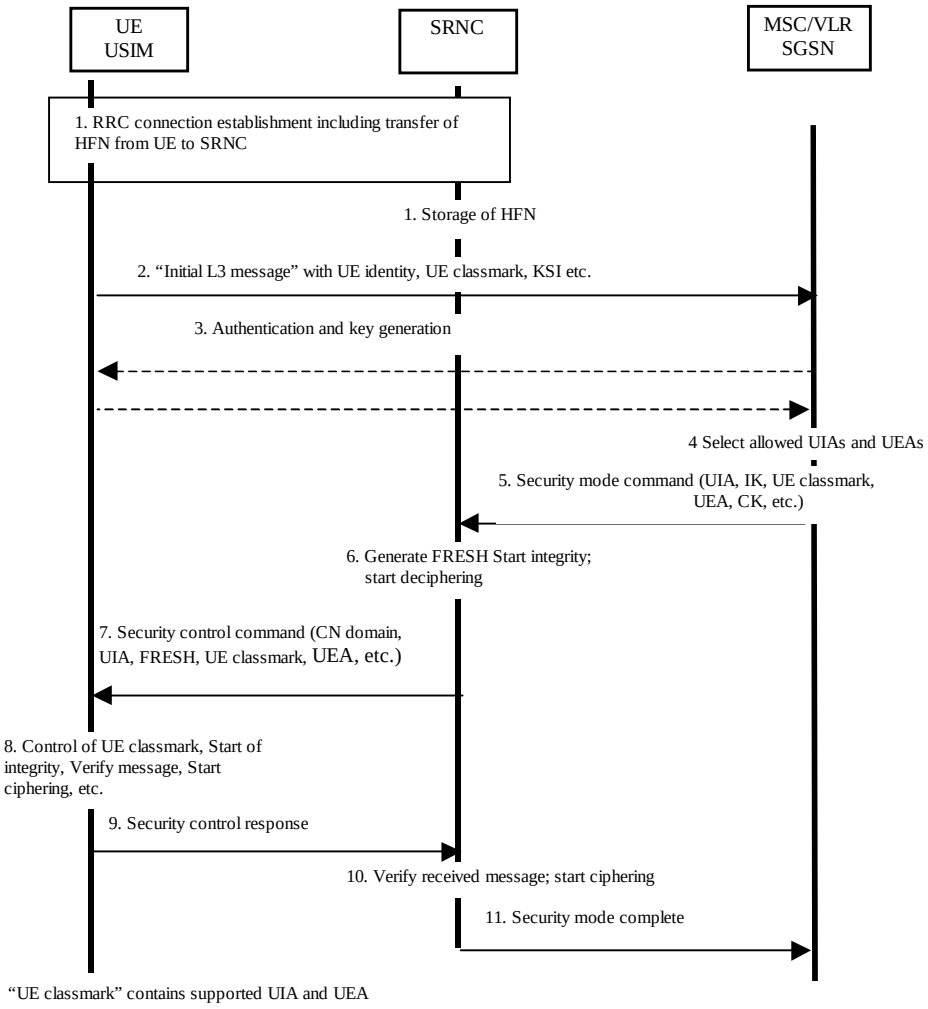
If the value of HFN_{MS} is larger or equal to the maximum value stored in the USIM, the MS indicates to the network in the RRC connection set-up that it is required to initialize a new authentication and key agreement.

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

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

6.4.8.1 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. This procedure is mandatory.The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.



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

Detailed description of the flow above:

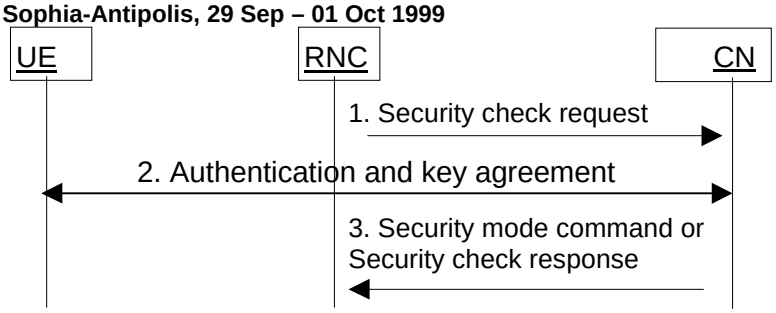
1. RRC connection establishment includes the transfer from UE to RNC of the hyperframe number to be used as part of one of the input parameters for the integrity algorithm and for the ciphering algorithm. The COUNT-I parameter (together with COUNT which is used for ciphering) is stored in the SRNC.
2. The UE sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the relevant CN domain. This message contains relevant MM information and the UE classmark IE, which includes information on the UIA(s) and UEA(s) supported by the UE. The KSI (Key Set Identifier) is the number allocated by the CN at the last authentication for this CN domain.

3. Authentication of the user and generation of new security keys (IK and CK) may be performed. A new KSI will then also be allocated.
4. The CN node determines which UIAs and UEAs that are allowed to be used.
5. The CN initiates integrity (and possible also ciphering) by sending the RANAP message Security Mode Command to SRNC. This message contains a list of allowed UIAs and the IK to be used. It may also contain the allowed UEAs and the CK to be used. This message contains also the UE classmark IE to be sent transparently to the UE.
6. The SRNC decides which algorithms to use by selecting the first UEA and the first UIA it supports from the list.The SRNC generates a random value FRESH and initiates the downlink integrity protection. If SRNC supports no UIA algorithms in the list, it sends a SECURITY MODE REJECT message to CN.
7. The SRNC generates the RRC message Security control command. The message includes the UE classmark IE, the UIA and FRESH to be used and possibly also the UEA to be used. Additional information (start of ciphering) may also be included. Since we have two CNs with an IK each, the network must indicate which IK to use. This is obtained by including a CN type indicator information in "Security control command". Before sending this message to the UE, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.
8. At reception of the Security control command message, the UE controls that the UE classmark IE received is equal to the UE classmark IE sent in the initial message. The UE computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The UE verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.
9. If all controls are successful, the UE compiles the RRC message Security control command response and generates the MAC-I for this message. If any control is not successful, a SECURITY CONTROL REJECT message is sent from the UE .
10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.
11. The transfer of the RANAP message Security Mode Complete response from SRNC to the CN node ends the procedure.

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

Signalling procedures in the case of an unsuccessful integrity check

The following procedure is used by the RNC to request the CN to perform an authentication and to provide a new CK and IK in case of unsuccessful integrity check. This can happen on the RNC side or in the UE side. In the latter case the UE sends a SECURITY CONTROL REJECT message to the RNC.



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

1. RNC sends a SECURITY CHECK REQUEST message to CN (indicating cause of the request).

2. The CN performs the authentication and key agreement procedure.

3. If the authentication is successful, the CN sends a Security mode command to RNC. This will restart the ciphering and integrity check with new parameters. If the authentication is not successful, the CN sends a SECURITY CHECK RESPONSE (Cause) to RNC.

4. If the failure situation persists, the connection should be dropped.

6.4.8.1 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.

6.5 Local authentication

Note: This section should define a mechanism for authentication based on a shared integrity key. It is ffs. whether a separate mechanism is required, or whether the security feature is implicitly provided through the use of the integrity key for signalling messages.

6.6 Data confidentiality

6.6.1 General

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

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

6.6.2 Ciphering algorithm

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

The UEA shall produce one output as a sequence of keystream bits referred to as a Key Stream Segment (KSS). A KSS of length n shall be produced to encrypt a given segment of plaintext of length n. The bits of KSS are labelled KSS(0), …KSS(n-1), where KSS(0) is the first bit output from the generator. The bits in the KSS shall be used to encrypt or decrypt the data.

Note: [The point at which confidentiality protection is applied in the UTRAN architecture is for further study. At this stage we assume that confidentiality protection is applied at the RNC.]

6.6.3 Cipher key establishment

The establishment of a new cipher key CK is integrated in the user authentication mechanism described in 6.3. A new cipher key CK is established each time an authentication protocol is executed between the USIM and the core network node that initiated the authentication.

6.6.4 Cipher key selection

Because of the separate mobility management for CS and PS services, the USIM establishes cipher keys with both the CS and the PS core network nodes. Currently two options are considered for the selection of the cipher key:

6.6.4.1 Option 1: Two key solution

The CS user data connections are ciphered with the most recent cipher key CK_{CS} agreed between the user and the 3G CS core network node. The PS user data connections are ciphered with the most recently cipher key CK_{PS} agreed between the user and the 3G PS core network node. The (common) signalling data connections are ciphered with the most recently cipher key established between the user and the network, i.e., the youngest of CK_{CS} and CK_{PS}. This requires that the cipher key of an (already ciphered) ongoing signalling connection is changed. This change should be completed within five seconds after an authentication and key establishment protocol has been executed.

6.6.4.2 Option 2: One key solution

All connections (CS user data, PS user data and signalling data) are ciphered with the most recently cipher key CK agreed between the user and either one of the core network nodes. This requires that the cipher key of any (already ciphered) ongoing connection is changed. This change should be completed within five seconds after an authentication an key establishment protocol has been executed.

6.6.5 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.

6.6.6 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 lifetime of the cipher key is controlled by the mechanism described in 6.4.5.

6.6.7 UEA numbering

[The following table is for illustration only]

Table 2 – UEA numbering

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

6.6.8 UEA negotiation

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

When an MS wishes to establish a connection with the network, the MS shall indicate to the network which version of the UEA algorithm it supports.

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

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

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

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

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]~~

See Section 6.4.8.1.

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.

6.6.9.4 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.

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

TSG SA WG3 #6, Sophia Antipolis, 29th September - 1st October **S3-99334**

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** **14** Current Version: V3.1.0

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

For submission to TSG SA#6 *list TSG meeting no. here ↑* for approval [X] 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: S3 **Date:** 1-10-99

Subject: Security of MAP-Based Transmissions

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:

- Most MAP commands are bi-directional, e.g. they can take the form of a request and a response containing sensitive data. Since it is not a-priori clear which of the two directions has to be protected, both should be protected using the key intended for communication in the respective direction. Therefore, it is necessary that session keys for **both** directions are transported between the involved networks, using the mechanism of layer I as specified in section 7.2 of 33.102
- GTP based transmission will also contain sensitive data. This data will require an equal level of security (e.g. authentication parameters, subscriber profile information, etc). Therefore securing GTP based transmission messages needs to be secured as well.

Clauses affected: Sections 7.1.1, 7.2.2, 7.4.1

Other specs affected:

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

Other comments:

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~~ shall choose a symmetric session key of its own, used for sending data in the other direction. This second key shall be transported immediately after the first key has been successfully transported. 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.

7.2.2 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.

Since most of the signalling messages to be secured are bidirectional in character, immediately after successful completion the procedure described here shall be repeated, now with Y choosing a key $KS_{YX}(i)$ to be used in the reverse direction, and X being the receiving party. Thereby keys for both directions are established.

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

[Note: GTP based transmission data will also contain sensitive data. This data will require an equal level of security (e.g. authentication parameters, subscriber profile information, etc.). The specifications will extended to address GTP based transmissions using industry standard techniques (such as IPSEC) where appropriate. The possibility of extending these mechanisms to secure CAP/INAP signalling is also being investigated.]

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.

TSG SA WG3 #6, Sophia Antipolis, 29th September - 1st October **S3-99332**

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** **15** Current Version: V3.1.0

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

For submission to TSG SA#6 for approval [X]
list TSG meeting no. here ↑ for information [ ]
(only one box should Be marked with an X)

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

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

Source: S3 **Date:** 1-10-99

Subject: Secure UMTS-GSM Interoperation

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 proposed mechanism allows secure UMTS-GSM interoperability by using standardised conversion functions for generating the authentication vectors needed in each network. The proposed conversion functions are designed with the aim to define a simple, efficient and secure system to facilitate secure interoperation for all envisaged GSM/UMTS roaming and handover scenarios, based on the following principles:

- GSM security parameters are generated from the UMTS security parameters, when needed.
- GSM security parameters depend on the UMTS security algorithms, under the control of the HPLMN.
- UMTS security parameters are generated from the GSM security parameters, when needed.
- Traffic load (sometimes international signalling) is optimised, just the needed security parameters (GSM or UMTS) are transmitted.
- Conversion functions are very simple and efficient. No additional either computational load or memory is introduced.

Clauses affected: Sections 6.3.7, 6.4.8.1 , 6.6.9.4

Other specs affected:

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

Other comments:

6.3.7 Interoperability with 2G networks

~~Note: This section should define the procedures and functions that are required to support roaming of UMTS users in GSM networks and handover of UMTS users between UMTS networks and GSM networks as regards the establishment of cipher and integrity keys.~~

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

6.3.7.1 Interoperability for UMTS users

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

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

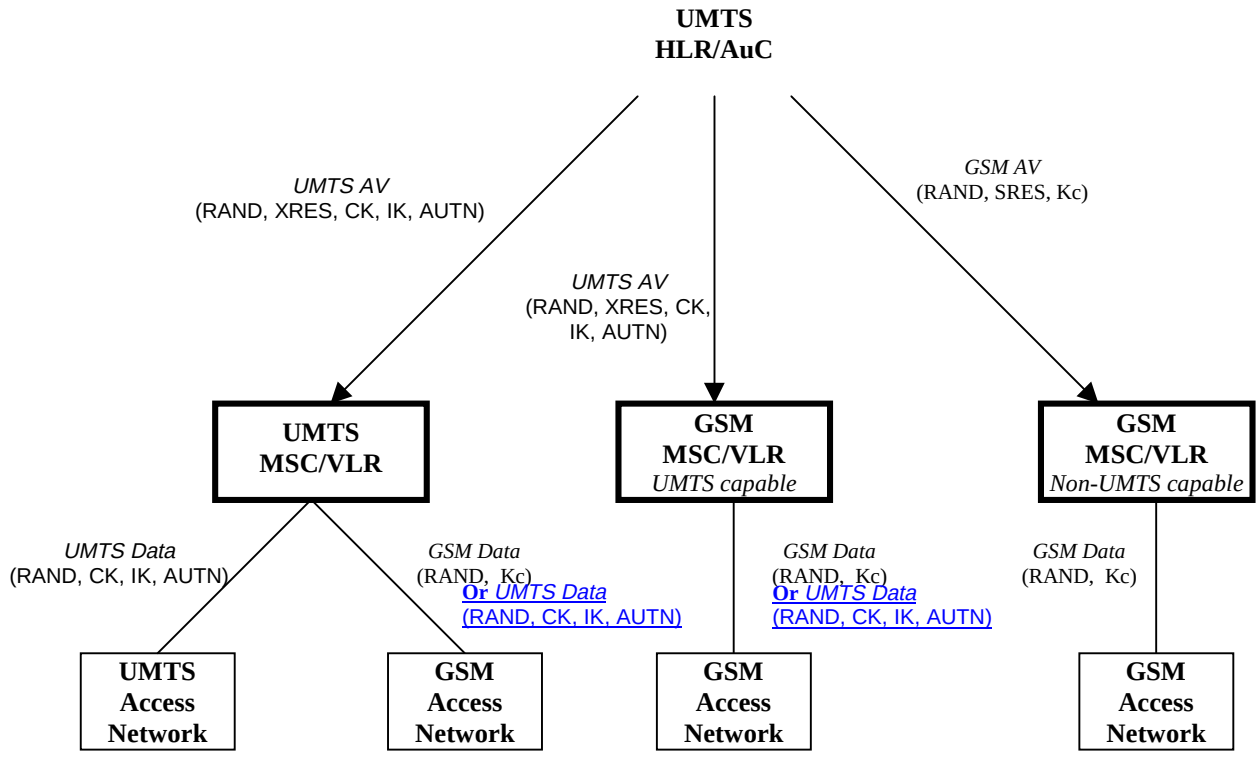


Figure 13: Interoperability for UMTS Users

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

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

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

Upon receipt of an *authentication data request* from a non-UMTS capable GSM SN/VLR, the HLR/AuC shall derive the GSM authentication vectors from the UMTS vectors, by means of the standardised conversion functions defined below. Then, the HLR/AuC sends an *authentication response* back to the SN/VLR that contains an ordered array of *n*

GSM authentication vectors (triples). The HLR/AuC may have pre-computed GSM authentication vectors or may derive them on demand from the UMTS authentication vectors.

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

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

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

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

Interoperability with non-UMTS capable GSM entities is achieved by use of the standardised conversion functions implemented in the HLR/AuC. The handover case is described in sections 6.4.8.1 and 6.6.9.4.

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

- **Generation of GSM RAND**

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

- **Generation of GSM SRES**

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

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

- **Generation of GSM Kc**

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

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

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

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

A3: $RAND_G$ -> SRES; $SRES = f(f2_K(RAND_U))$

A8: $RAND_G$ -> Kc; $Kc = f(f3_K(RAND_U), f4_K(RAND_U))$

6.3.7.2 Interoperability for GSM users

The mechanism described here achieves intersystem operability between UMTS and GSM networks allowing secure

interoperation between both networks for GSM users (SIM). The following figure illustrates the different scenarios of interoperability for 2G users:

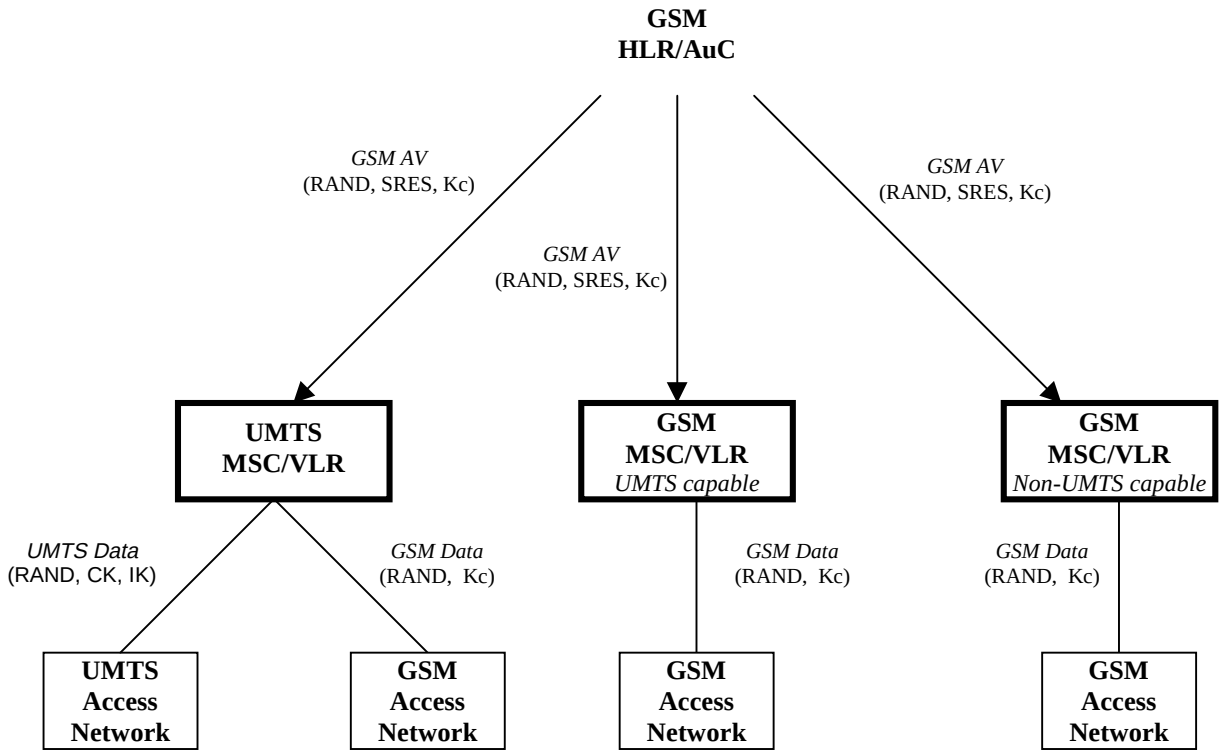


Figure 14: Interoperability for GSM Users

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

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

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

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

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

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

- UMTS MSC/VLR
- UMTS SGSN
- UE

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

- **Generation of UMTS RAND**

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

- **Generation of UMTS XRES**

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

- **Generation of UMTS CK**

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

- **Generation of UMTS IK**

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

- **Generation of UMTS AUTN**

  The authentication token AUTN is not used for GSM users.

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

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

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

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

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

f_4: $RAND_u$ -> IK; $IK = A8(RAND_G) \,||\, A8(RAND_G)$

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

~~In case of handover the user should receive the level of security that is usually provided in the network that is entered. Therefore the following functionality has to be provided in case of handover:~~

- ~~system specific security keys have to be established~~

6.4.8 Integrity protection procedures

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.

6.4.8.1 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.~~

UMTS → GSM

The GSM network entered by the user handing over from UMTS does not provide integrity protection and the integrity key (IK) is not needed in the GSM network.

GSM → UMTS

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

a) Handover from a UMTS capable GSM network

When handover occurs, the IK is transmitted from the old MSC/VLR to the new one to enable the communication to proceed.

b) Handover from a non-UMTS capable network. The method below is not recommended but presened if it will be a service requirement. There are doubts whether there is a requirement for this kind of handover and whether it is possible on, for instance, the MAP/E interface.

The UMTS integrity key shall be derived by the UMTS network an UE by using the conversion functions specified in section 6.3.7.2 for this purpose.

When handover occurs, the Kc is transmitted form the old MSC/VLR to the new one to enable the communication to proceed.

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.

6.6.9.4 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.~~

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

UMTS → GSM

The GSM network entered by the user handing over will enable ciphering protection. This involves setting the GSM cipher key (Kc).

The GSM cipher key shall be derived by the UMTS network by using the conversion functions specified in section 6.3.7.1 for this purpose.

When handover occurs, the generated Kc is transmitted from the old MSC/VLR to the new one to enable the communication to proceed.

GSM → UMTS

The UMTS network entered by the user handing over from GSM will enable confidentiality protection. This will involve setting the cipher key (CK). There are two options:

a) Handover from a UMTS capable GSM network

When handover occurs, the CK is transmitted from the old MSC/VLR to the new one to enable the communication to proceed.

b) Handover ~~form~~ from a non-UMTS capable network. The method below is not recommended but presented if it will be a service requirement. There are doubts whether there is a requirement for this kind of handover and whether it is possible on, for instance, the MAP/E interface

The UMTS cipher key shall be derived by the UMTS network an UE by using the conversion functions specified in section 6.3.7.2 for this purpose.

When handover occurs, the derived Kc is transmitted form the old MSC/VLR to the new one to enable the communication to proceed.

Technical Specification Group Services and System Aspects Meeting #5, ***S3-99344***

TSG SA WG3 #6, Sophia Antipolis, 29 September – 1 October, 1999

3G CHANGE REQUEST

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

TS 33.102 **CR** **16** Current Version: V3.1.0

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

For submission to TSG SA#5 *list TSG meeting no. here ↑* for approval [X] for information [ ] *(only one box should be marked with an X)*

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

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

Source: S3 **Date:** 99-10-09

Subject: Network-wide confidentiality

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: Refinement of network-wide confidentiality specification.

Clauses affected: 8.2

Other specs affected:

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

Other comments: The abbreviations ECK and ECKC should be listed in section 3.3. TS33.107 should be added to the list of references in section 2.

8.2 Network-wide user traffic confidentiality

8.2.1 Introduction

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

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

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

~~The provision of an network-wide confidentiality service in 3GMS has an obvious impact on lawful interception. We assume that t~~A~~he same~~ lawful interception interface may be implemented according to TS33.107 regardless~~is required in 3GMS as in second generation systems regardless~~ of whether or not network-wide confidentiality is applied by the network ~~or not. Thus, we assume that I~~it ~~must~~shall be possible to remove any network-wide confidentiality protection within the core network to provide access to plaintext user traffic at the lawful interception interface.

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

8.2.2 Ciphering method

~~It is assumed that t~~The network-wide encryption algorithm shall be a synchronous stream cipher ~~similar to the access link encryption algorithm~~. It shall be possible to use ~~Indeed, it would be desirable to use t~~the same algorithm UEA for access link encryption and ~~for~~ network-wide encryption.

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

Synchronisation of the key stream shall be achieved using the initialisation value. Synchronisation information shall be available at both end points of the communication and shall be used to maintain alignment of the key stream. ~~For example, it might be necessary to transmit explicit end-to-end synchronisation frames with the user traffic at certain intervals. Alternatively, it might be possible to use some existing frame structure for network-wide encryption synchronisation purposes. The frequency at which synchronisation information must be made available at each end to ensure reliable transmission will depend on the exact nature of the end-to-end user traffic channel.~~

Protection against replay of user traffic shall be achieved through the use of a time variable initialisation vector combined with a time variable cipher key. ~~If the same cipher key is used in~~

~~more than one call then it may be necessary to include a third input to the key stream generator such as a call-id or a time-stamp to protect against replay of the whole call.~~

Note ~~1~~: ~~that t~~The stream cipher does not protect against bit toggling so other mechanisms must be used if this type of integrity protection is required on user traffic.

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

Note ~~1~~: ~~that i~~In the initial phases of 3G~~MS~~PP, transcoder free operation may only be possible for user traffic channels which terminate within the same serving network. Furthermore, TFO may only be possible if the entire communication path is within the same serving network. Thus, in non optimal routing cases where the tromboning effect occurs, TFO may not be available, even if the traffic channel terminates within the same serving network.

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

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

~~Issues f~~For further study:

- Specification of encryption synchronisation mechanism;
- Adaptation of TFO voice traffic channels for network-wide confidentiality;
- Adaptation of data traffic channels for network-wide confidentiality;
- The ability to terminate network-wide encryption at network gateways for inter-network user traffic channels;
- The ability to handle multiparty calls, explicit call transfer and other supplementary services;
- Network-wide encryption control – algorithm selection, mode selection, user control

8.2.3 Key management

~~8.2.3.1 General case~~

~~We assume that s~~Signalling links within the network ~~are~~ shall be ~~confidentially~~ protected on a link-by-link basis. In particular, ~~we assume that~~ the UE to RNC signalling links shall be~~are~~ protected using access link ~~security domain~~ keys (see clause 6)~~. We also assume that VLR to RNC signalling links~~ and core network signalling links shall be~~are~~ protected using network security domain keys (see clause 7). ~~Note that i~~If network-wide encryption ~~can~~ is~~be~~ provided across serving network boundaries (~~e.g. because~~ which requires that inter-network TFO is available) then the signalling links requiring protection will cross network boundaries. ~~In this situation it is important to note that the t~~

Note ~~1~~: If network-wide encryption is provided across serving network boundaries then the two serving networks may not be roaming partners yet they still must be able to ~~confidentially~~ protect inter-network signalling by establishing appropriate keys.

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

Note ~~1~~: However, it ~~may~~ is be possible to obtain the network-wide~~end-to-end~~ key by compromising certain nodes within the network (e.g. nodes where link encryption terminates).

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

~~Issues for further study:~~

- ~~Specification of key management scheme for the general case;~~
- ~~The ability to terminate network-wide encryption key management at network gateways for inter-network user traffic channels.~~

~~8.2.3.2 Outline scheme for intra-serving network case~~

~~In this case we make the following assumptions:~~

- ~~Two UEs registered on the same serving network wish to set up an network-wide confidentiality protected call~~
- ~~The appropriate user traffic channel for encryption can be established between the two UEs~~
- ~~During connection establishment, the appropriate control information is transmitted to the called party indicating that the incoming connection is end-to-end encrypted.~~
- ~~During connection establishment, the appropriate control information is transmitted to the relevant VLRs (or other core network entities) indicating that the connection being established is end-to-end encrypted.~~
- ~~The keys Ka and Kb used to derive the end-to-end session key shall not be used for access link encryption of other data, nor for the derivation of end-to-end session keys with other parties.~~

The key management scheme is illustrated in the diagram below.

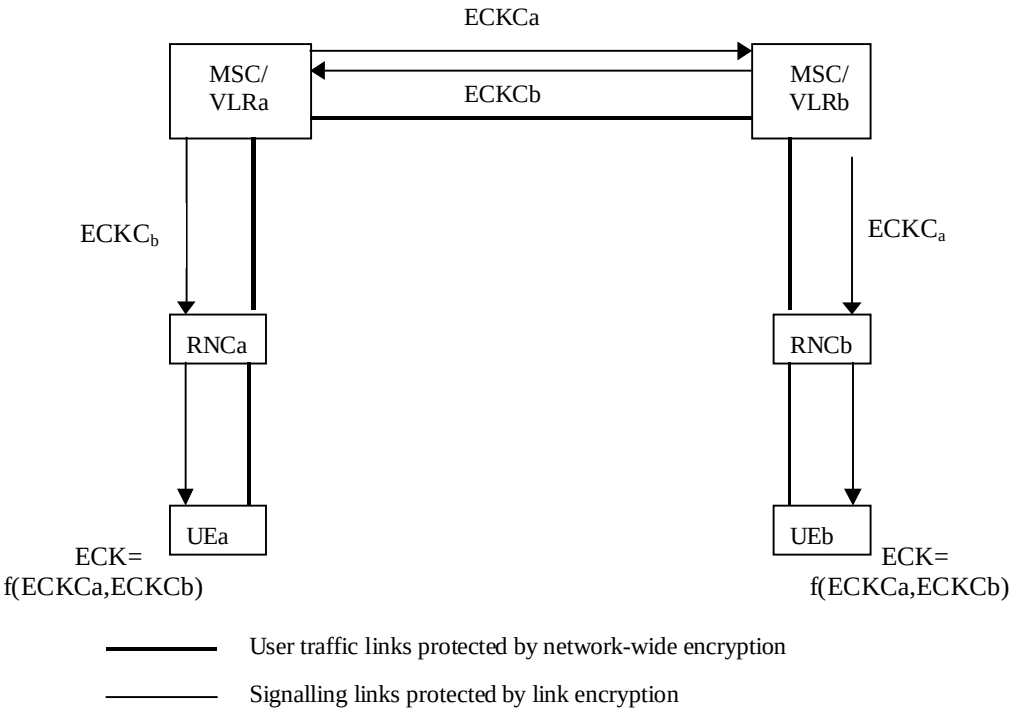


Figure 15: Key management scheme for network-wide encryption

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

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

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

F~~Issues f~~or further study:

- ~~The exact~~Specification of mechanism ~~by which the VLRs exchange access link keys during connection set up~~to exchange network-wide cipher key components.

~~8.2.3.3 Variant on the outline scheme~~

~~VLRa and VLRb mutually agree Ks over a secure signalling link using an appropriate key agreement protocol. VLRa then passes Ks to UEa and VLRb passes Ks to UEb.~~

~~Note: As opposed to the scheme in section 8.2.3.2, the access link keys Ka and Kb could be used for access link encryption of other data.~~

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

Technical Specification Group Services and System Aspects Meeting #5, ***S3-99348***

TSG SA WG3 #6, Sophia Antipolis, 29 September – 1 October, 1999

3G CHANGE REQUEST

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

TS 33.102 **CR** **017** Current Version: V3.1.0

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

For submission to TSG SA#5 *list TSG meeting no. here ↑* for approval [X] for information [ ] *(only one box should be marked with an X)*

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

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

Source: S3 **Date:** 99-10-09

Subject: Authentication management field

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: An extra parameter, called the authentication management field (AMF), is added to the authentication token (AUTN) in the *user authentication request* message. A new informative annex is added which gives examples of how AMF may be used. The use of a MODE parameter for sequence number management across CS/PS domains is moved to the new informative annex as an example use of AMF.

Clauses affected: 6.3.2, 6.3.3, 6.3.4, 6.3.5, new Annex F

Other specs affected:

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

Other comments:

The abbreviation AMF should be listed in section 3.3.

Figures after number 9 need to be renumbered across the whole document because this CR deletes Figure 10.

A new annex F is inserted before the current annex F (change history).

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.

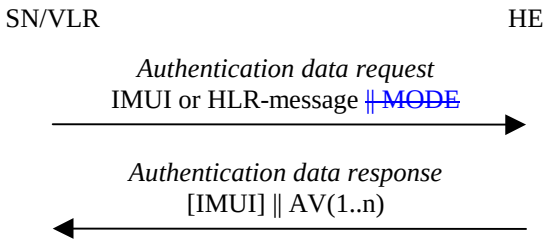


Figure 5: Distribution of authentication data from HE to SN/VLR

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).

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

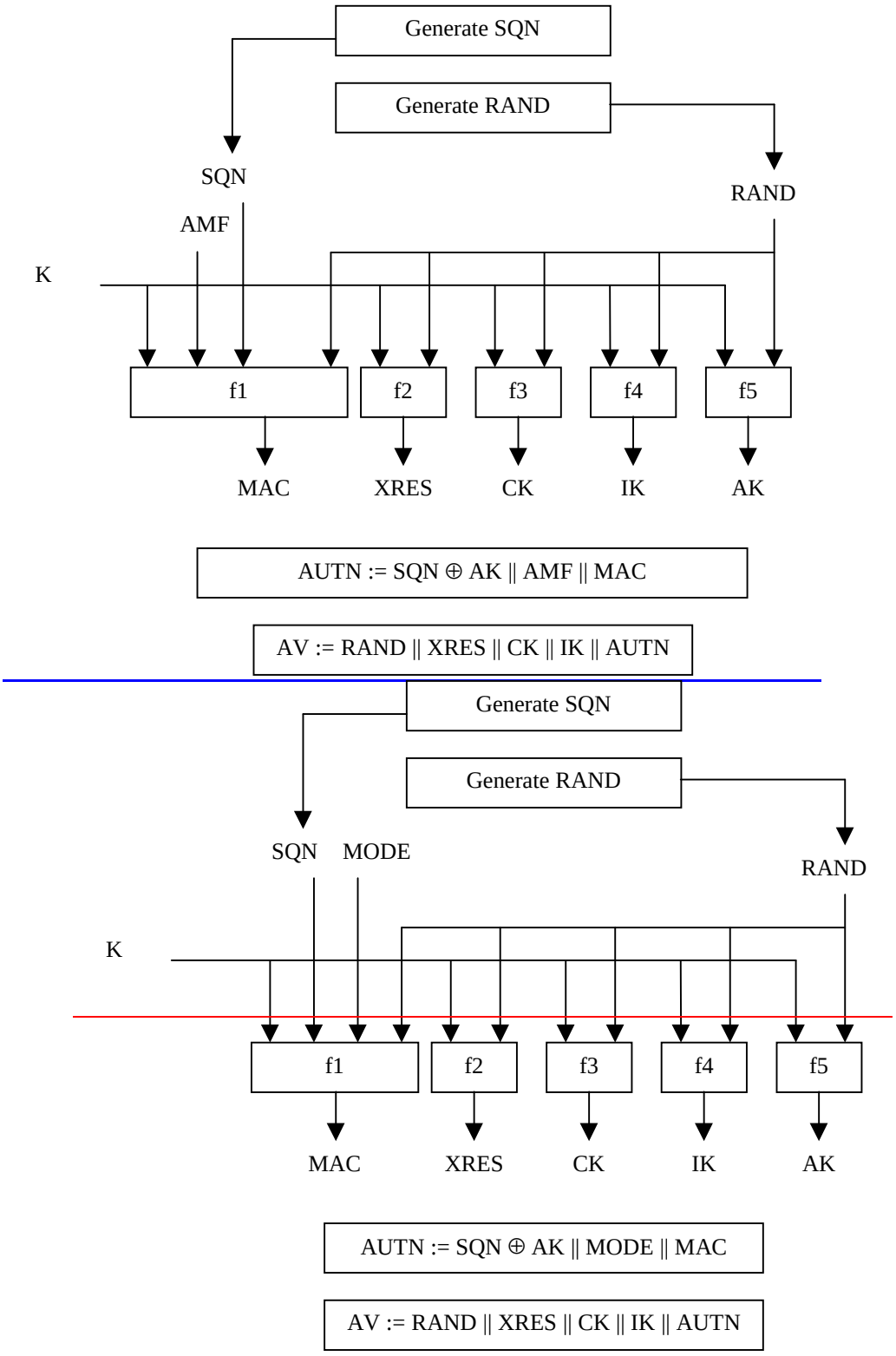


Figure 6: Generation of an authentication vector

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

For each user the HE/AuC keeps track of ~~two~~ a counter~~s~~: $SQN_{HE/CS}$ ~~for authentications initiated by the CS CN nodes, and~~ $SQN_{HE/PS}$ ~~for authentications initiated by the PS CN nodes~~.

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

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

~~Note 2: The solution in the main body uses the parameter MODE to distinguish between the CS and the PS core network nodes such that each node can simultaneously and independently support mobility management for the mobile user. Consequently two counters are required both in the AuC and in the USIM. If a single counter would be used, we would run into the following problem: Suppose that a CS node would order the SQNs 1–5, and use SQN 1 and a PS node would order the SQNs 6–10 and uses 6. Then the CS node would like to use 2, but that SQN is rejected. He orders new authentication vectors, with SQNs 11–15, and authenticates with SQN 11. Then the PS node runs into problems. The separate counters for CS and PS mode provide a solution for this problem.~~

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

Subsequently the following values are computed:

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

Finally the authentication token AUTN = SQN ⊕ AK || AMF ~~|| MODE~~ || MAC is constructed.

Here, AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only.

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

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

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

6.3.3 Authentication and key agreement

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

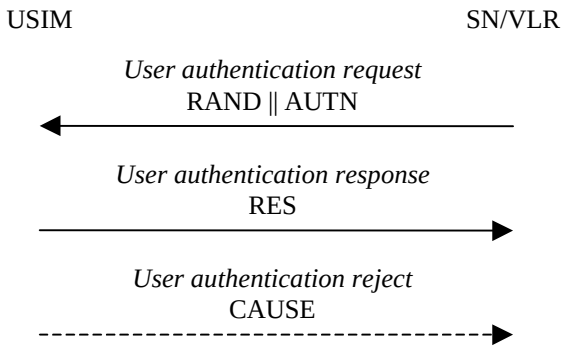


Figure 7: Authentication and key establishment

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

Upon receipt the user proceeds as shown in Figure 8.

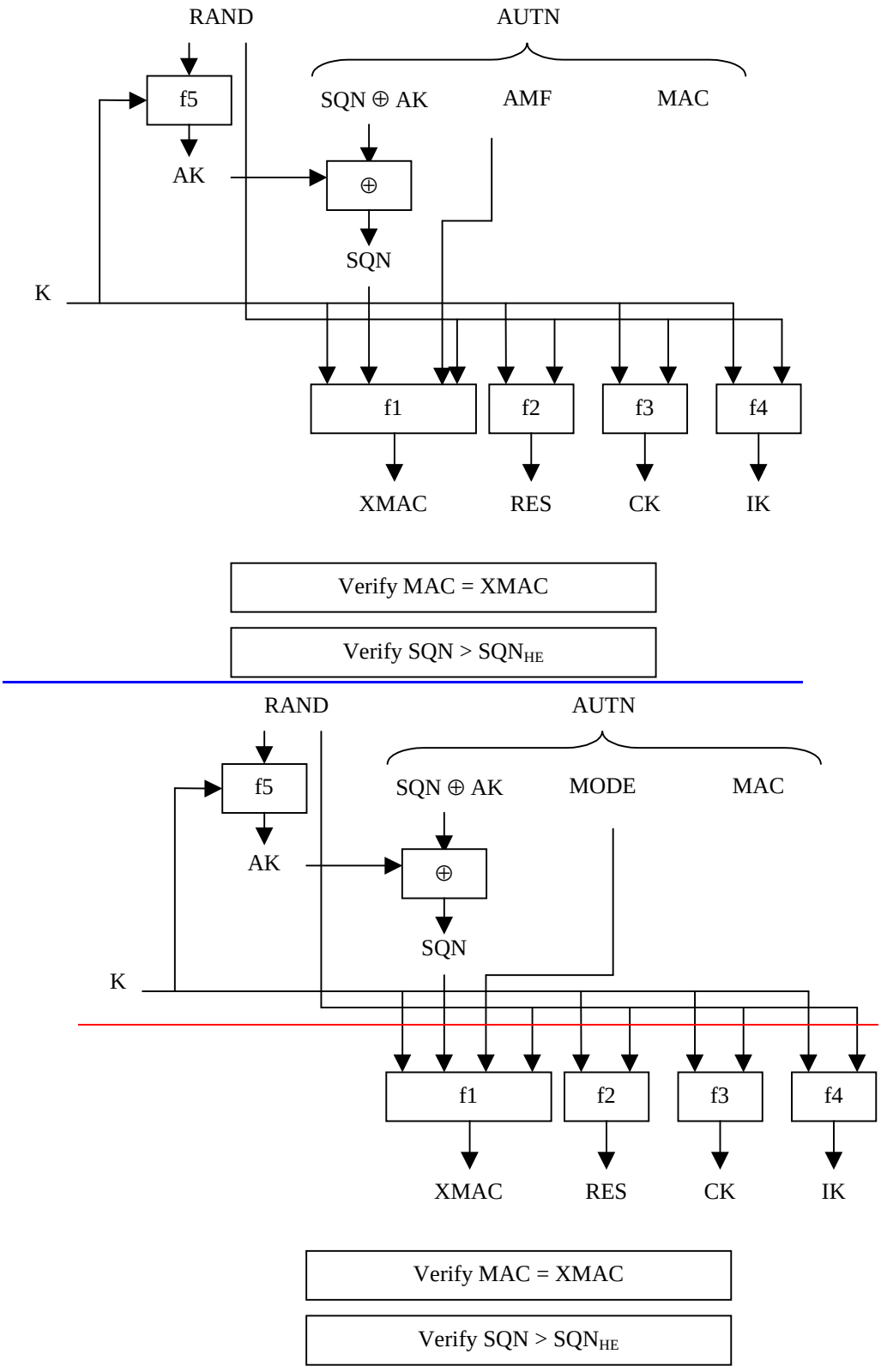


Figure 8: User authentication function in the USIM

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

Next the user computes XMAC = $f1_K$ (SQN || RAND || AMF~~|| 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 that the received sequence number SQN is in the correct range.

~~For each mode~~ T~~t~~he USIM keeps track of ~~one~~ a 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 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 to be in the correct range and subsequently sets $SQN_{MS/MODE}$ to SQN.

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

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

The *synchronisation failure* message contains the parameter $RAND_{MS}$ || $AUTS$.
Here $RAND_{MS}$ is the random value stored on the MS which was received in user authentication request causing the last update of SQN_{MS} .
It is $AUTS = Conc(SQN_{MS}) || MACS$.
$Conc(SQN_{MS}) = SQN_{MS} \oplus f5_K(RAND_{MS})$ is the concealed value of the counter SQN_{MS} in the MS, and.
$MACS = f1^*_K(SQN_{MS} || RAND$ || AMF~~|| 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 AMF used to calculate MACS assumes a dummy value of all zeros so that it does not need to be transmitted in the clear in the re-synch message.

The construction of the parameter AUTS in shown in the following Figure 9:

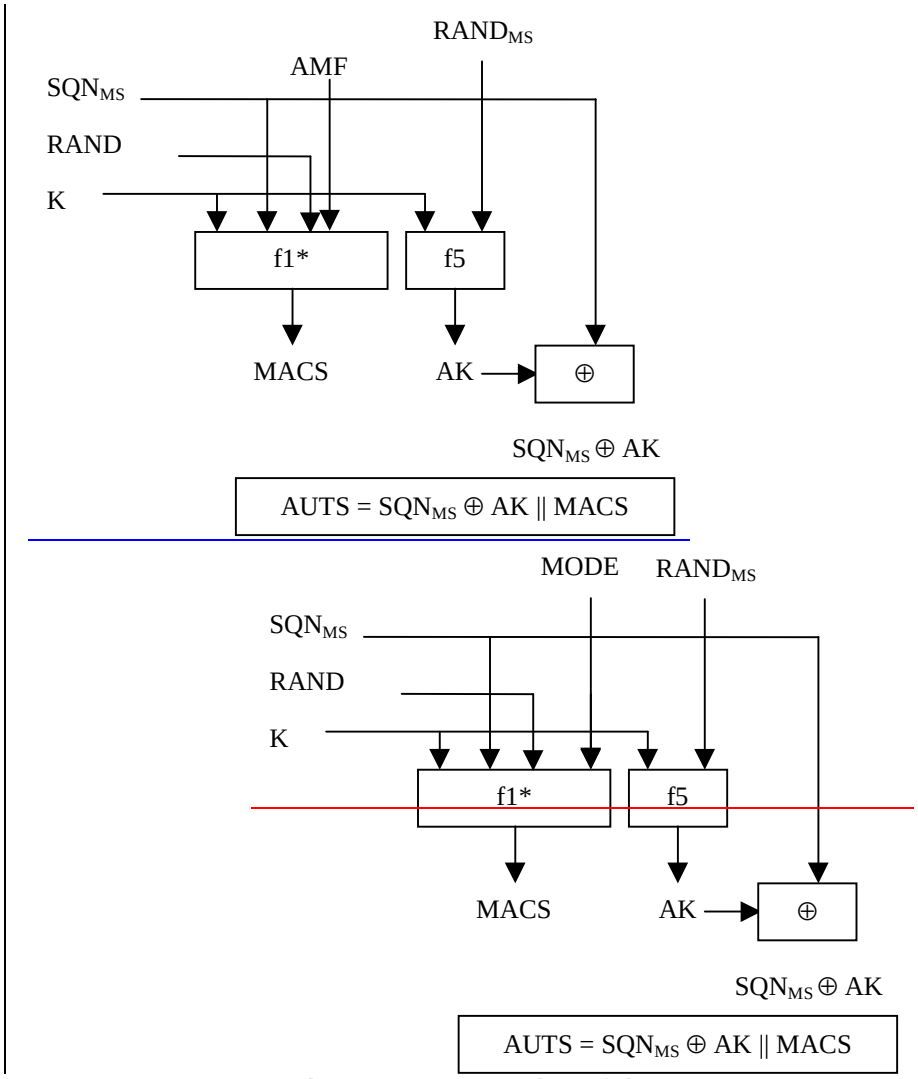


Figure 9: Construction of the parameter AUTS

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

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

Conditions on the use of authentication information by the SN/VLR: Using the procedures described in subsections 6.3.1, 6.3.2 and 6.3.4, authentication vectors will have to be used in the specific order in which they were generated, otherwise the user will reject the authentication attempt. The SN/VLR shall use an authentication vector only once and, hence, shall send out each user authentication request *RAND || AUTN* only once no matter whether the authentication attempt was successful or not. A consequence is that authentication vectors cannot be reused. When a user changes from one VLR to another one and the new VLR requests remaining authentication vectors from the old VLR (cf. subsection 6.3.4) then the old VLR shall not retain any copies of these authentication vectors. When a VLR receives a "cancel location" request for a certain user it shall delete all authentication vectors relating to that user. When a VLR receives a location update request from a user and the VLR notices that authentication vectors relating to that user are still stored in the VLR it will delete this information and request fresh authentication vectors from the HE/AuC.

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

6.3.3 Distribution of authentication vectors between VLRs

The purpose of this procedure is to provide a newly visited VLR with unused authentication vectors from a previously visited VLR. The procedure is shown in Figure 10.

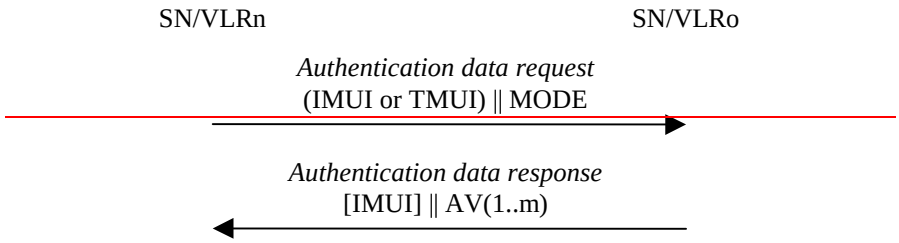


Figure Figure 10: Distribution of authentication vectors between VLRs

The procedure is initiated by the visited VLR and illustrated in the following Figure 11:

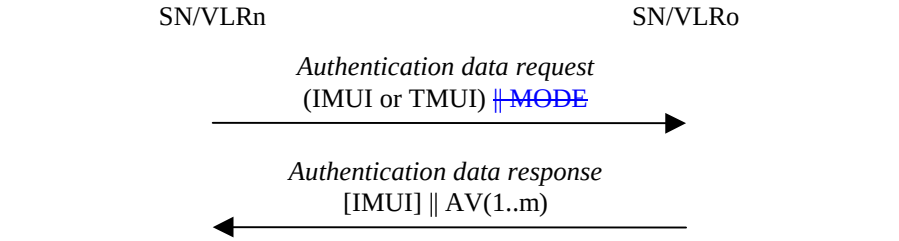


Figure 11: Distribution of authentication data between SN/VLR

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

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 12 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*).*

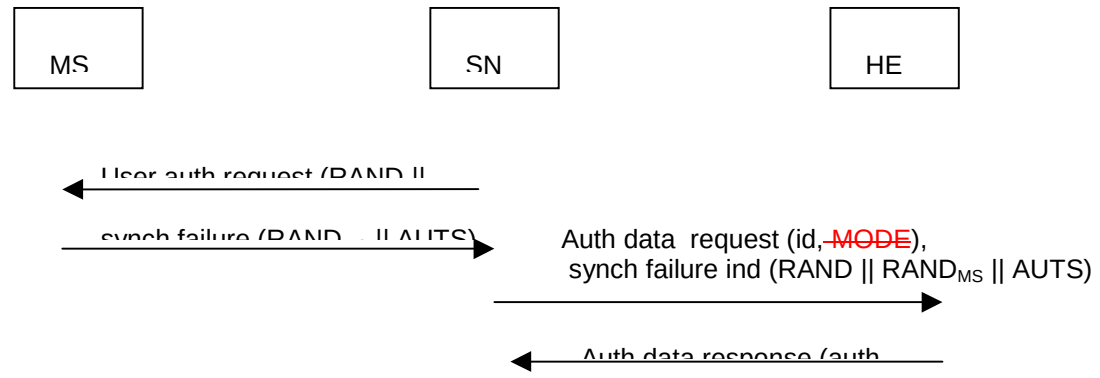


Figure 12: Re-synchronisation procedure

Annex F (Informative): Example uses of AMF

F.1 Support multiple authentication algorithms and keys

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

The USIM keeps track of the authentication algorithm and key identifier and updates it according to the received value.

F.2 Changing the size of windows and lists

This mechanisms is used in conjunction with the window and list mechanisms described in Annexes C.3 and C.4.

A mechanism to change the window and list size dynamically is useful since the optimum window and list size may change over time. AMF is used to indicate the maximum admissible window or list size to be used by the user when verifying the authentication token.

The USIM keeps track of the window or list size and updates it according to the received value providing that SQN > SQN_{MS}.

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

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

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

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

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** **018** Current Version: V3.1.0

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

For submission to TSG SA#5 for approval [X] *(only one box should*
list TSG meeting no. here ↑ for information [ ] *be marked with an X)*

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

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

Source: 3GPP TSG SA WG 3 **Date:** 01-10-99

Subject: Support for window and list mechanisms for sequence number management in authentication scheme

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 proposed mechanism increases the efficiency of the use of authentication vectors in conjunction with the window and list mechanisms described in Annexes C.3 and C.4.

Clauses affected: Sections 6.3

Other specs affected:

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

Other comments:

help.doc

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

6.3 Authentication and key agreement

6.3.8 Support for window and list mechanisms

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

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

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** **019** Current Version: V3.1.0

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

For submission to TSG SA#5 for approval [X] *(only one box should be marked with an X)*
list TSG meeting no. here ↑ for information [ ]

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

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

Source: 3GPP TSG SA WG 3 **Date:** 01-10-99

Subject: Modification of text for window and list mechanisms

3G Work item: Security

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

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

Reason for change: The current text in Annexes C.3 and C.4 contains inaccuracies which are clarified in this change request. In addition, the editorial effects of CRs 017 and 019 agreed by 3GPP TSG SA WG 3 are taken into account.

Clauses affected: Annex C.3, Annex C.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.

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

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

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

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

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

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

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

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