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		Current Version: **3.5.0**

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

For submission to:	**SA#14**	for approval	**X**	strategic		*(for SMG*
list expected approval meeting # here ↑		For information		non-strategic		*use only)*

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

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

Source:	Ericsson		**Date:**	2000-07-26

Subject:	Clarification on Sequence Numbers (SQN - SEQ)

Work item:	Security

Category:

(only one category shall be marked with an X)

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

Reason for change:	Corrections and clarifications of the sequence numbers SQN and SEQ. The counter SEQ is introduced in the informative Annex C and shall not be used in the main document.

Clauses affected:	6.3

Other specs affected:	Other 3G core specifications	☐	→ List of CRs:	
	Other GSM core specifications	☐	→ List of CRs:	
	MS test specifications	☐	→ List of CRs:	
	BSS test specifications	☐	→ List of CRs:	
	O&M specifications	☐	→ List of CRs:	

Other comments:	

help.doc

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

6.3 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 $SQN_{MS}\text{SEQ}_{MS}$ and $SQN_{HE}\text{SEQ}_{HE}$ respectively to support network authentication. The sequence number SQN_{HE} is an individual counter for each user and the sequence number SQN_{MS} denotes the highest sequence number the USIM has accepted.

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

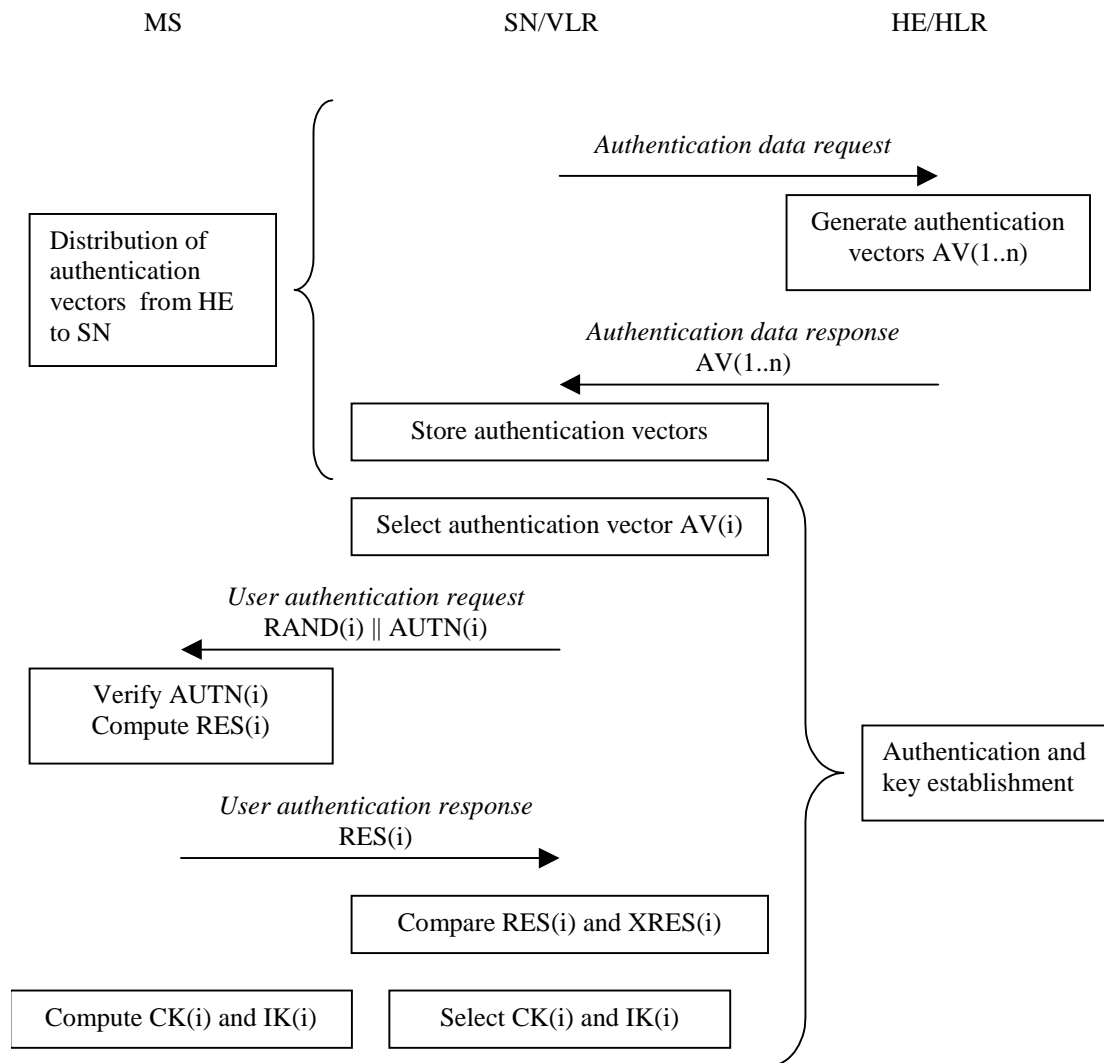An overview of the mechanism is shown in Figure 5.

```
              MS                      SN/VLR                    HE/HLR


                                      Authentication data request
                              ┌──────────────────────────────────────────▶┌─────────────────────────┐
                              │                                            │ Generate authentication │
  ┌─────────────────────┐     │                                            │   vectors AV(1..n)      │
  │ Distribution of     │     │                                            └─────────────────────────┘
  │ authentication      │     │
  │ vectors  from HE    │     │      Authentication data response
  │ to SN               │     │              AV(1..n)
  └─────────────────────┘     │◀──────────────────────────────────────────
                              │  ┌──────────────────────────────────┐
                              │  │ Store authentication vectors     │
                              │  └──────────────────────────────────┘

                                 ┌──────────────────────────────────┐
                                 │ Select authentication vector AV(i)│
                                 └──────────────────────────────────┘

                        User authentication request
                            RAND(i) || AUTN(i)
              ◀────────────────────────────────────
  ┌───────────────────────┐
  │ Verify AUTN(i)        │
  │ Compute RES(i)        │                                     ┌─────────────────────┐
  └───────────────────────┘                                     │ Authentication and  │
                                                                │ key establishment   │
                        User authentication response            └─────────────────────┘
                                RES(i)
              ────────────────────────────────────▶
                                 ┌──────────────────────────────────┐
                                 │ Compare RES(i) and XRES(i)       │
                                 └──────────────────────────────────┘
  ┌───────────────────────┐     ┌──────────────────────────────────┐
  │ Compute CK(i) and IK(i)│    │ Select CK(i) and IK(i)           │
  └───────────────────────┘     └──────────────────────────────────┘
```

Figure 5: Authentication and key agreement

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

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

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

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

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

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

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

6.3.2   Distribution of authentication data from HE to SN

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

VLR/SGSN   HE

Authentication data request
IMSI

Authentication data response
AV(1..n)
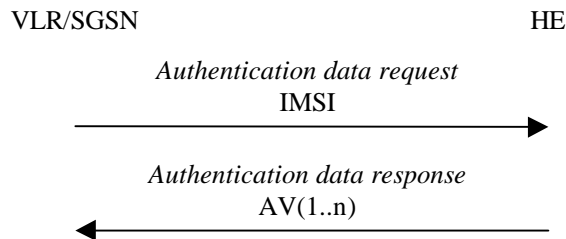
Figure 6: Distribution of authentication data from HE to VLR/SGSN

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

The *authentication data request* shall include the IMSI.

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

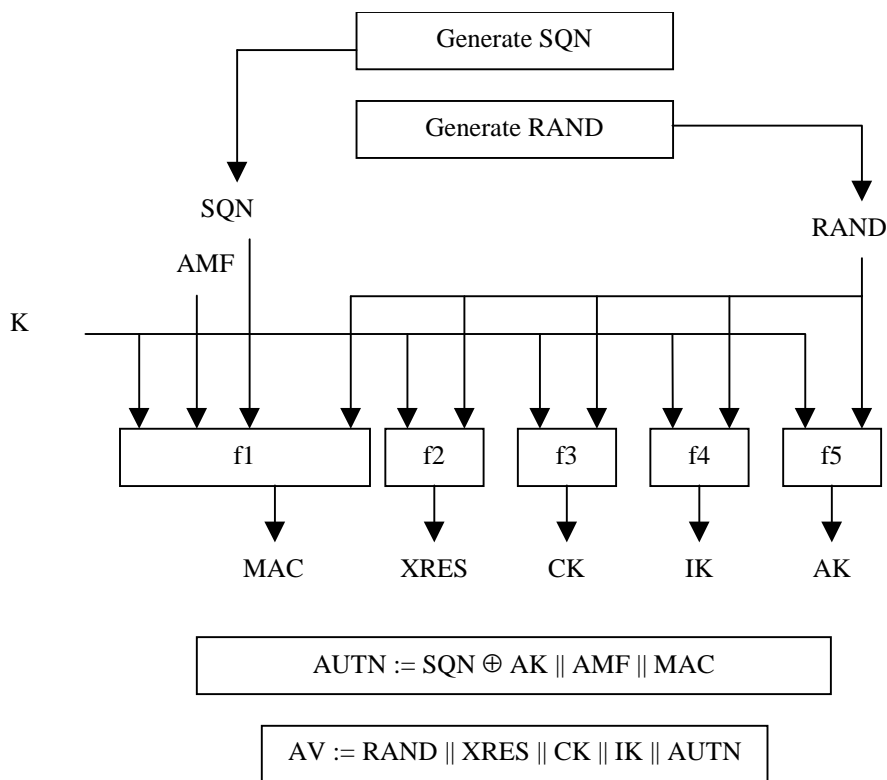Figure 7 shows the generation of an authentication vector AV by the HE/AuC.

Figure 7: Generation of authentication vectors

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

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

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

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

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

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

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

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

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

Subsequently the following values are computed:

- a message authentication code $MAC = f1_K(SQN \parallel RAND \parallel AMF)$ where f1 is a message authentication function;

- an expected response $XRES = f2_K (RAND)$ where f2 is a (possibly truncated) message authentication function;

- a cipher key $CK = f3_K (RAND)$ where f3 is a key generating function;

- an integrity key $IK = f4_K (RAND)$ where f4 is a key generating function;

- an anonymity key $AK = f5_K (RAND)$ where f5 is a key generating function or $f5 \equiv 0$.

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

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

6.3.3   Authentication and key agreement

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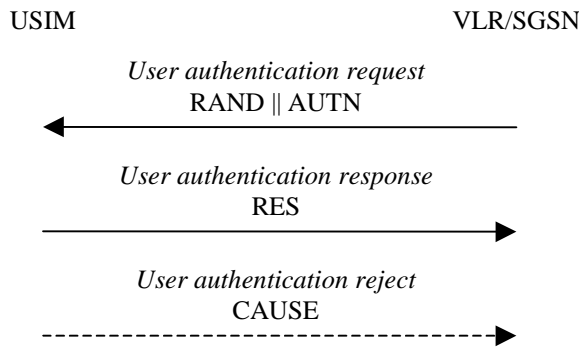

USIM   VLR/SGSN

User authentication request
RAND ∥ AUTN

User authentication response
RES

User authentication reject
CAUSE

Figure 8: Authentication and key establishment

The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR/SGSN database. The VLR/SGSN sends to the USIM the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.
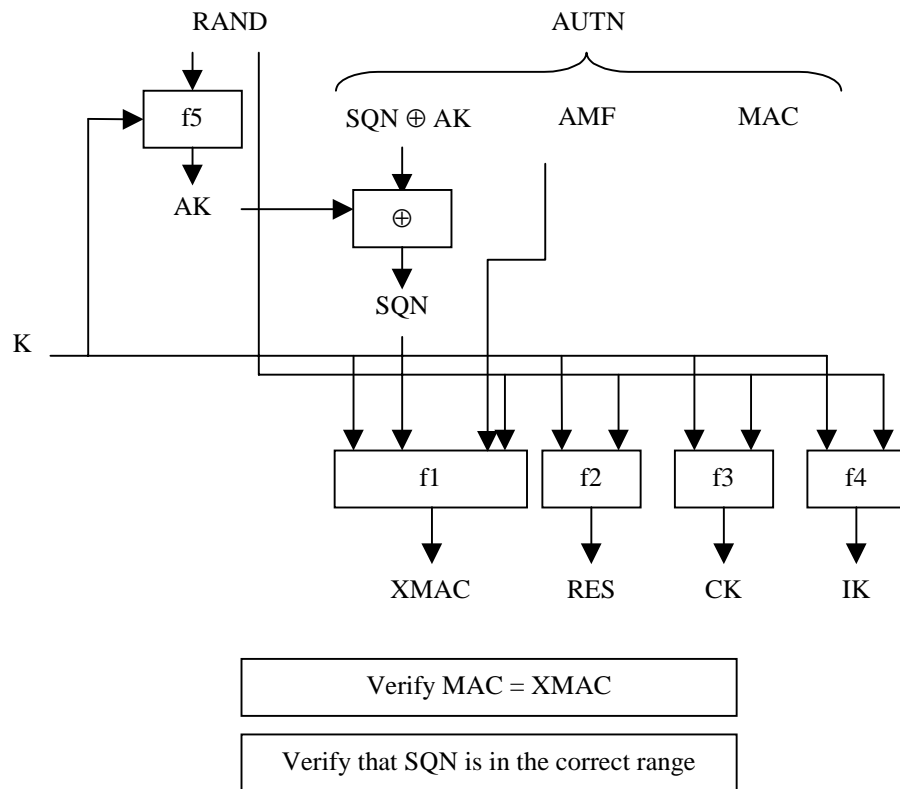
Upon receipt the user proceeds as shown in Figure 9.

Figure 9: User authentication function in the USIM

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

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

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

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

The synchronisation failure message contains the parameter AUTS. It is $AUTS = Conc(SQN_{MS}) \parallel MAC\text{-}S$. $Conc(SQN_{MS}) = SQN_{MS} \oplus f5_K(MAC\text{-}S \parallel 0...0)$ is the concealed value of the counter $\underline{SQN_{MS}}\overline{SEQ_{MS}}$ in the MS, and $MAC\text{-}S = f1^*_K(\underline{SQN_{MS}}\overline{SEQ_{MS}} \parallel RAND \parallel AMF)$ where RAND is the random value received in the current user authentication request. $f1^*$ is a message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of $f1^*$ about those of $f1, ... , f5$ and vice versa.

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

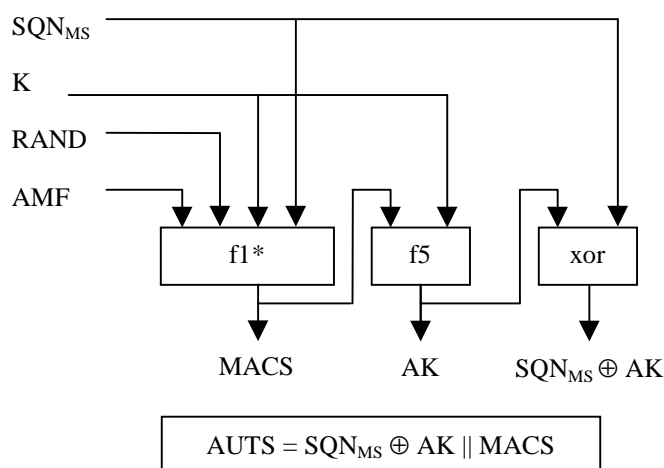The construction of the parameter AUTS in shown in the following Figure 10:

Figure 10: Construction of the parameter AUTS

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

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

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

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

The purpose of this procedure is to provide a newly visited MSC/VLR or SGSN with temporary authentication data from a previously visited MSC/VLR or SGSN within the same serving network domain.
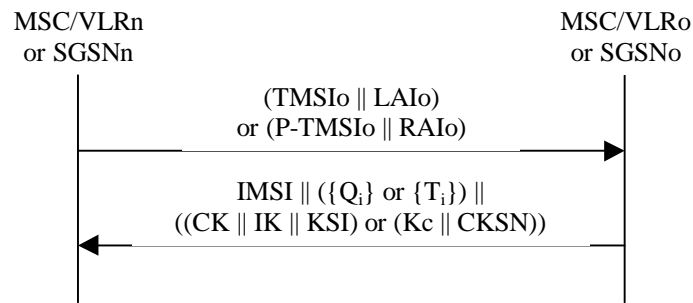
The procedure is shown in Figure 11.

```
        MSC/VLRn                                              MSC/VLRo
        or SGSNn                                              or SGSNo
           │                                                     │
           │                   (TMSIo ‖ LAIo)                    │
           │                 or (P-TMSIo ‖ RAIo)                 │
           │────────────────────────────────────────────────────▶│
           │                                                     │
           │              IMSI ‖ ({Q_i} or {T_i}) ‖              │
           │          ((CK ‖ IK ‖ KSI) or (Kc ‖ CKSN))          │
           │◀────────────────────────────────────────────────────│
           │                                                     │
```

Figure 11: Distribution of IMSI and temporary authentication data within one serving network domain

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

The protocol steps are as follows:

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

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

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

   i)   shall include the IMSI,

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

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

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

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

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

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

6.3.5   Re-synchronisation procedure

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

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

- *RAND* sent to the MS in the preceding user authentication request and

- *AUTS* received by the VLR/SGSN in the response to that request, as described in subsection 6.3.3.

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

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

When the HE/AuC receives an *authentication data request* with a "*synchronisation failure indication*" it acts as follows:

1. The HE/AuC retrieves SQN_{MS}~~SEQ_{MS}~~ from Conc(SQN_{MS}~~SEQ_{MS}~~) by computing *f5$_K$(MAC-S || 0...0),*.

2. The HE/AuC checks if SQN_{HE}~~SEQ_{HE}~~ is in the correct range, i.e. if the next sequence number generated SQN_{HE}~~SEQ_{HE}~~ using would be accepted by the USIM.

3. If SQN_{HE}~~SEQ_{HE}~~ is in the correct range then the HE/AuC continues with step (6), otherwise it continues with step (4).

4. The HE/AuC verifies *AUTS* (cf. subsection 6.3.3.).

5. If the verification is successful the HE/AuC resets the value of the counter SQN_{HE}~~SEQ_{HE}~~ to SQN_{MS}~~SEQ_{MS}~~.

6. The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the VLR/SGSN. If the counter SQN_{HE}~~SEQ_{HE}~~ was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting SQN_{HE}~~SEQ_{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 VLR/SGSN receives a new batch of authentication vectors from the HE/AuC in an authentication data response to an authentication data request with synchronisation failure indication it deletes the old ones for that user in the VLR/SGSN.

The user may now be authenticated based on a new authentication vector from the HE/AuC. 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).
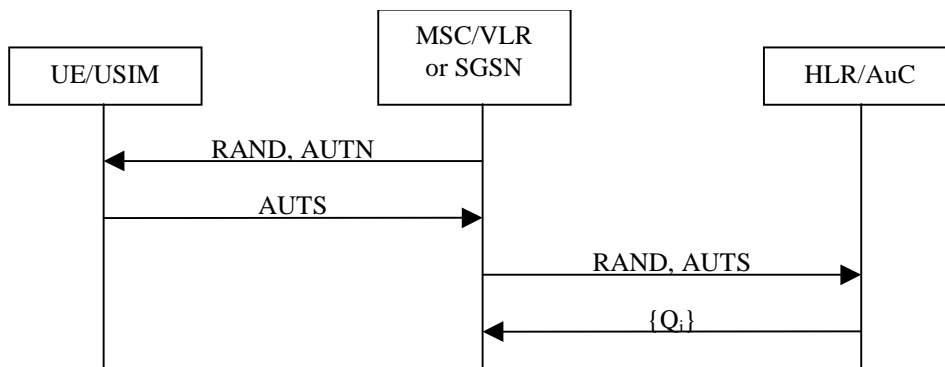
Figure 12: Resynchronisation mechanism

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

The purpose of this procedure is to provide a mechanism for reporting authentication failures from the serving environment back to the home environment.
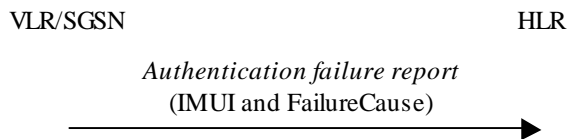
The procedure is shown in Figure 13.

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

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

The HE may decide to cancel the location of the user after receiving an *authentication failure report*.

6.3.7 Length of sequence numbers

Sequence numbers shall have a length of 6 octets.