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 **XX**	Current Version:	3.3.1

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

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

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

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

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

Subject:	Clarification on the reuse of AVs

3G Work item:	Security

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

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

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

Clauses affected:	6.3.3

Other specs affected:

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

Other comments:

help.doc

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

6.3.3   Authentication and key agreement

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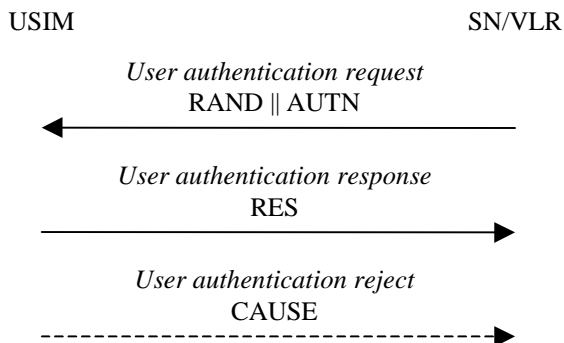
```
        USIM                                    SN/VLR

                  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 database. The VLR/SGSN sends to the user the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.

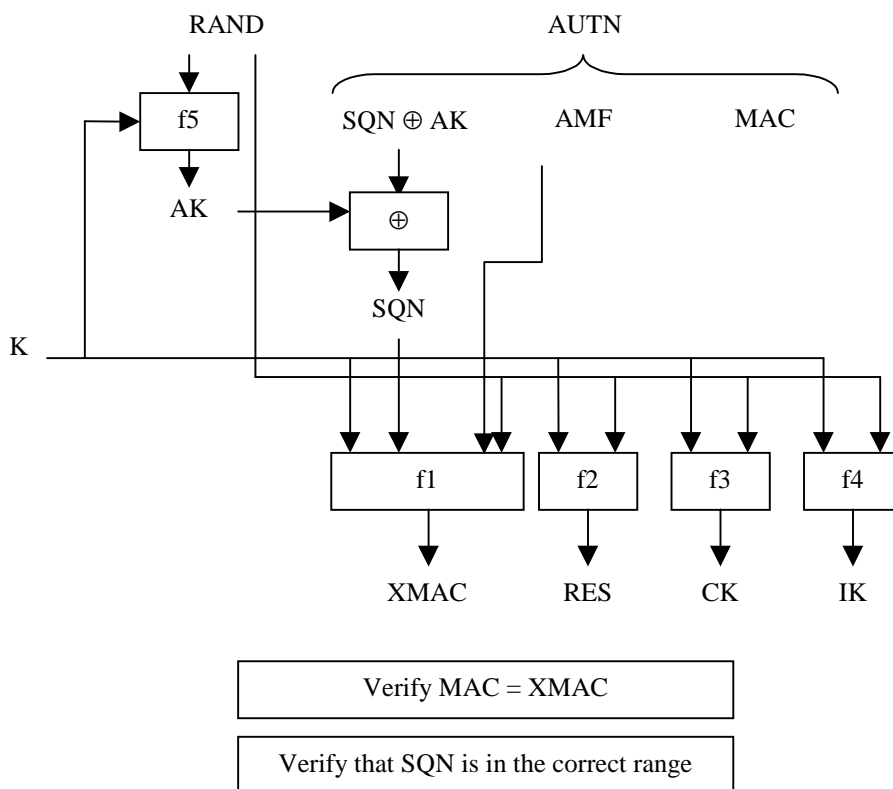Upon receipt the user proceeds as shown in Figure 9.

Figure 9: User authentication function in the USIM

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

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

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

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

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

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

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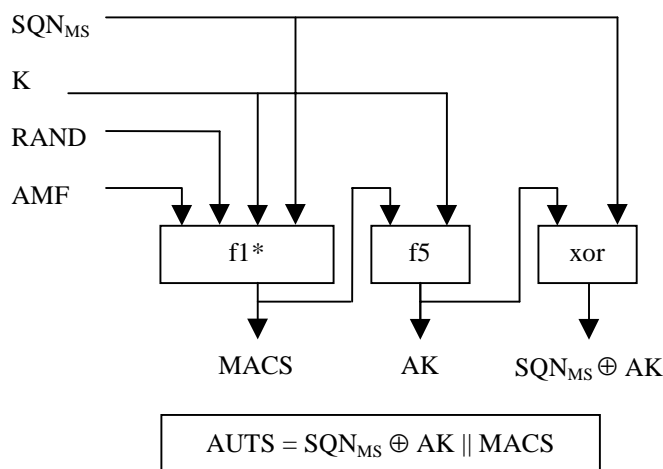

$$AUTS = SQN_{MS} \oplus AK \ || \ MACS$$

Figure 10: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range however, the user computes RES = f2$_K$ (RAND) and includes this parameter in a *user authentication response* back to the VLR/SGSN. Finally the user computes the cipher key CK = f3$_K$ (RAND) and the integrity key IK = f4$_K$ (RAND). Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND. The MS stores RAND for re-synchronisation purposes.

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

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