

27 February – 2 March, 2001

Göteborg, Sweden

CR-Form-v3

CHANGE REQUEST
 ⌘ **33.102 CR ?** ⌘ rev **-** ⌘ Current version: **3.7.0** ⌘

 For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: ⌘ (U)SIM ME/UE Radio Access Network Core Network
Title: ⌘ Correction to the handling of re-transmitted authentication request messages on the ME

Source: ⌘ Vodafone

Work item code: ⌘ ?

Date: ⌘ 2001-03-01

Category: ⌘ **F**
Release: ⌘ REL-99

 Use one of the following categories:

- F** (essential correction)
- A** (corresponds to a correction in an earlier release)
- B** (Addition of feature),
- C** (Functional modification of feature)
- D** (Editorial modification)

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

 Use one of the following releases:

- 2** (GSM Phase 2)
- R96** (Release 1996)
- R97** (Release 1997)
- R98** (Release 1998)
- R99** (Release 1999)
- REL-4** (Release 4)
- REL-5** (Release 5)

Reason for change: ⌘ N1 have stated that the most critical procedure for which re-transmission is expected to occur with the highest probability is the UMTS Authentication procedure via the Gb interface. Therefore it is specified that the mechanism shall be implemented for PS and may be implemented for CS.

In addition, it has been identified that the ME is required to delete the stored RAND and RES when the GSM cipher mode command is received.

Summary of change: ⌘ It is specified that the mechanism shall be implemented for PS and may be implemented for CS.

In addition, it is added that the ME deletes the stored RAND and RES when the GSM cipher mode command is received.

Consequences if not approved: ⌘ Specification that the mechanism shall be implemented in PS and may be implemented in CS was a compromise position reached in N1 and it provides the basis for N1 stage 3 CRs to be presented at CN#10. If this corresponding stage 2 CR is not approved then completion of the stage 3 specifications may be further delayed.

In addition, if the stored RAND and RES are not deleted when the GSM cipher mode command is received then a 3G authentication request could be successfully replayed during a GSM BSS connection.

Clauses affected: ⌘ 6.3

Other specs affected: ⌘ Other core specifications ⌘ 24.008-CR-xxx
 Test specifications

O&M Specifications

Other comments: ⌘

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.

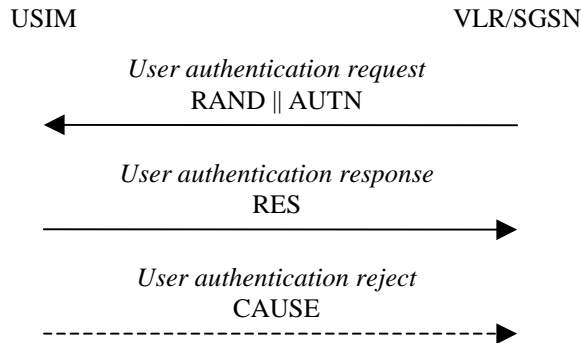


Figure 8: Authentication and key establishment

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. Authentication vectors in a particular node are used on a first-in / first-out basis. 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.

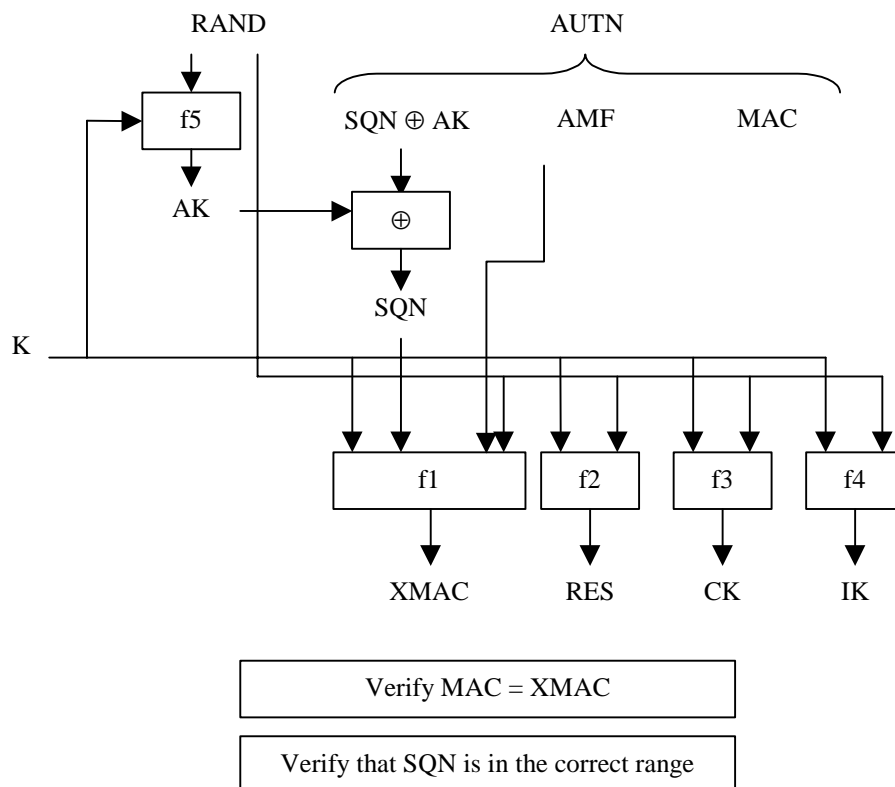


Figure 9: User authentication function in the USIM

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 $AUTS = Conc(SQN_{MS}) \parallel MAC-S$. $Conc(SQN_{MS}) = SQN_{MS} \oplus f5^*_K(RAND)$ is the concealed value of the counter SQN_{MS} in the MS, and $MAC-S = f1^*_K(SQN_{MS} \parallel RAND \parallel AMF)$ 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 $f1, \dots, f5, f5^*$ and vice versa. $f5^*$ is the key generating function used to compute AK in re-synchronisation procedures with the property that no valuable information can be inferred from the function values of $f5^*$ about those of $f1, f1^*, f2, \dots, f5$ 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 is shown in the following Figure 10:

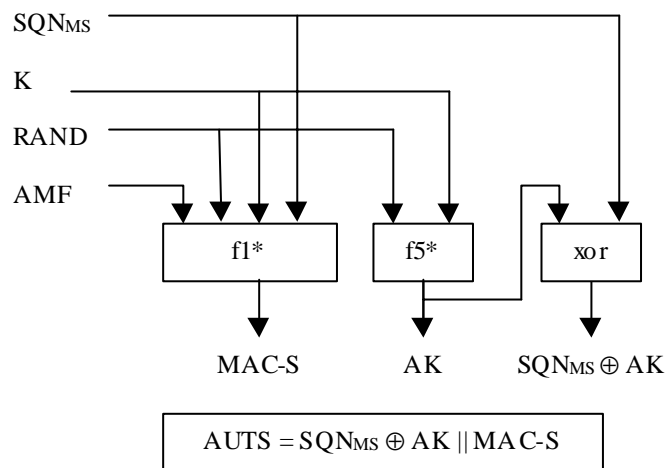


Figure 10: Construction of the parameter AUTS

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.

Re-use and re-transmission of (RAND, AUTN)

The verification of the SQN by the USIM will cause the MS to reject an attempt by the VLR/SGSN to re-use a quintet to establish a particular UMTS security context more than once. In general therefore the VLR/SGSN shall use a quintet only once.

There is one exception however: in the event that the VLR/SGSN has sent out an *authentication request* using a particular quintet and does not receive a response message (*authentication response* or *authentication reject*) from the MS, it may re-transmit the *authentication request* using the same quintet. However, as soon as a response message arrives no further re-transmissions are allowed. If after the initial transmission or after a series of re-transmissions no response arrives, retransmissions may be abandoned. If retransmissions are abandoned then the VLR/SGSN shall delete the quintet. At the MS side, in order to allow this re-transmission without causing additional re-synchronisation procedures, the ME shall store [for the PS domain \(and optionally the CS domain\)](#) the last received RAND as well as the corresponding RES, CK and IK. If the USIM returned SRES and Kc (for GSM access), the ME shall store these values. When the ME receives an *authentication request* and discovers that a RAND is repeated, it shall re-transmit the response. The ME shall delete the stored values RAND, RES and SRES (if [they existed](#)) as soon as the [3G](#) security mode command [or the GSM cipher mode command](#) is received by the ME or the connection is aborted. [If the ME can handle the retransmission mechanism for CS domain then](#) ~~The ME~~it shall be able to handle the retransmission for both PS and CS domain simultaneously.