CR-Form-v3

CHANGE REQUEST

| ⌘ | **33.102 CR xx** | ⌘ rev | **-** | ⌘ Current version: | **3.6.0** | ⌘ |

*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 **X** ME/UE **X** Radio Access Network ☐ Core Network ☐

Title: ⌘	Re-transmission of authentication request using the same quintet	
Source: ⌘	S3	
Work item code: ⌘	Security	***Date:*** ⌘ 28 Nov. 2000
Category: ⌘	**F**	***Release:*** ⌘ R99

Use <u>one</u> 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 <u>one</u> 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: ⌘	The implementation of the retransmission mechanism on USIM is considered inefficient.	
Summary of change: ⌘	The retransmission-mechanism is moved from USIM to ME.	
Consequences if not approved: ⌘	Inefficient implementation	

Clauses affected: ⌘			
Other specs affected: ⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications		
Other comments: ⌘			

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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.
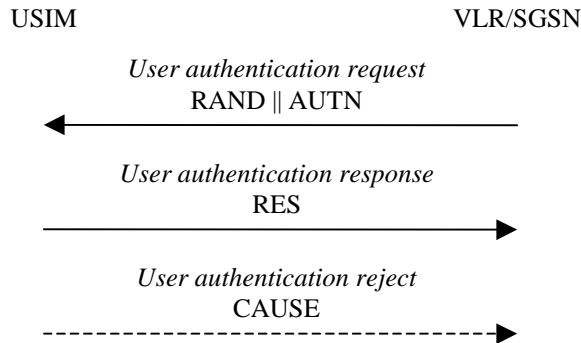
USIM   VLR/SGSN

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. 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.
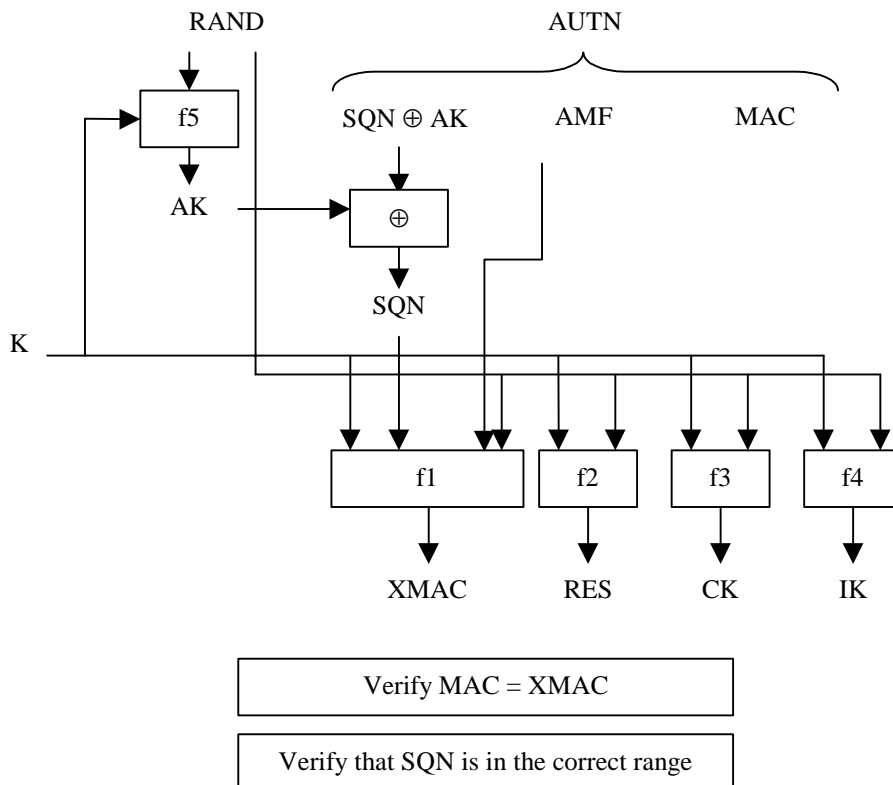
Upon receipt the user proceeds as shown in Figure 9.

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 || 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. 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}) || 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} || 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, 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, ... , 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.

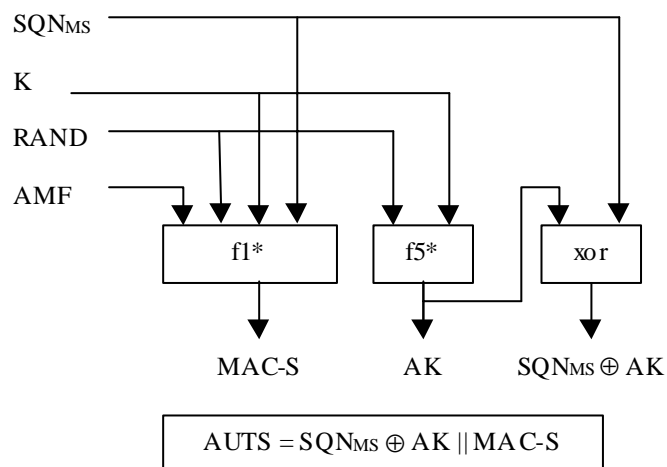The construction of the parameter AUTS in shown in the following Figure 10:

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.

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 ~~USIM~~ ME shall store the last received (RAND~~, AUTN) pair~~ 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 ~~USIM~~ ME receives an *authentication request* and discovers that a (RAND~~, AUTN) pair~~ is repeated ~~and the associated START parameter is 0~~, it shall re-transmit the response. The ~~USIM~~ ME shall delete the stored values (RAND~~, AUTN) pair~~, RES and SRES (if existed) ~~and the corresponding RES~~ as soon as the security mode command is received by the ME or the connection is aborted. ~~the START parameter is updated by the ME (see subclause 6.4.8).~~ The ME shall be able to handle the retransmission for both PS and CS domain simultaneously.