3GPP TSG SA 3 Meeting #14
Oslo, Norway, 1-4 August 2000

***Document* S3-000406**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

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	104	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#9	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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 [ ] ME [X] UTRAN / Radio [ ] Core Network [X]

Source: Siemens Atea **Date:** 11 July 2000

Subject: Re-transmission of authentication request using the same quintet

Work item: Security

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

F	Correction	X	**Release:**	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:

In GSM it occurs frequently that due to the loss of an authentication request or an authentication response, an VLR or SGSN has to re-transmit the authentication request.

The modifications proposed in this CR allow for the same re-transmission procedures in UMTS - where special measures are required to allow this re-transmissions, due to the verification of the freshness of the sequence number in the USIM

Clauses affected: 6.3.3

Other specs Affected:

Other 3G core specifications	X	→ List of CRs:	TS 24.008 CR nnn
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.

6.3.3 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.

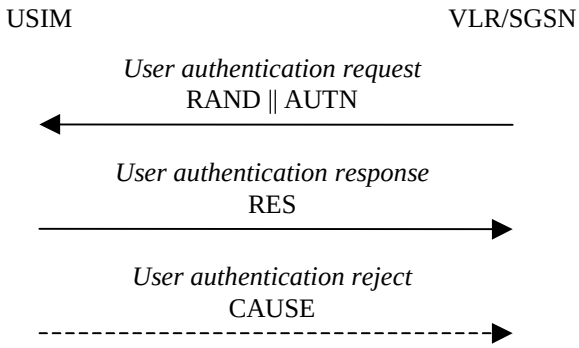

Figure 8: Authentication and key establishment

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. 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.

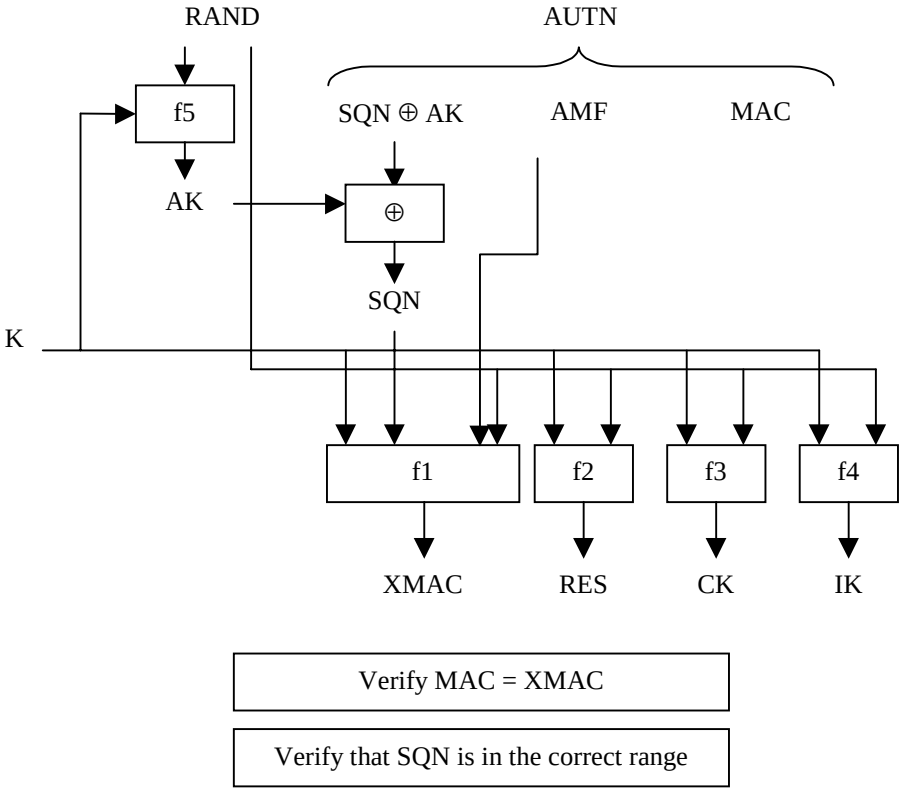

Figure 9: User authentication function in the USIM

Upon receipt of RAND and AUTN the USIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ 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}) = $SQN_{MS} \oplus f5_K$(MAC-S || 0...0) is the concealed value of the counter SEQ_{MS} in the MS, and MAC-S = $f1^*_K$(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 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:

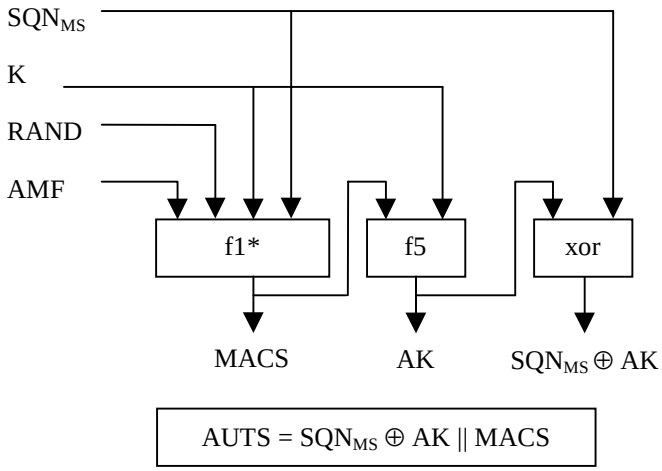

Figure 10: Construction of the parameter AUTS

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.~~

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 or 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 or 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. The VLR or SGSN may repeat an *authentication request* using the same quintet up to four times. However, as soon as a response message arrives, no further re-transmissions are allowed. When after the initial transmission and after a series of re-transmissions (maximum four) further re-transmission is abandoned and no response arrives, the VLR or 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 the last (RAND, AUTN) pair as well as the corresponding response message. When the ME receives an *authentication request* and discovers that a (RAND, AUTN) pair is repeated, it shall re-transmit the response (without interrogation of the USIM). The ME shall delete the stored (RAND, AUTN) pair and the corresponding response message as soon as the mandatory *security mode control* message is received, or when the ME is powered-off.