

S3000601
(rev574)

3GPP TSG SA 3 Meeting #15
Washington, USA, 12-14 September 2000

Document

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

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**
list expected approval meeting # here ↑

for approval
for information

strategic
non-strategic (for SMG 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: (U)SIM ME UTRAN / Radio Core Network
(at least one should be marked with an X)

Source: Siemens **Date:** 13 Sept. 2000

Subject: Change of computation of the anonymity key in the re-synchronisation procedure

Work item: Security

Category: <small>(only one category shall be marked with an X)</small>	F Correction	<input checked="" type="checkbox"/>	Release:	Phase 2	<input type="checkbox"/>
	A Corresponds to a correction in an earlier release	<input type="checkbox"/>		Release 96	<input type="checkbox"/>
	B Addition of feature	<input type="checkbox"/>		Release 97	<input type="checkbox"/>
	C Functional modification of feature	<input type="checkbox"/>		Release 98	<input type="checkbox"/>
	D Editorial modification	<input type="checkbox"/>	Release 99	<input checked="" type="checkbox"/>	
			Release 00	<input type="checkbox"/>	

Reason for change: The proposed new version is more amenable to the implementation of the example cryptographic functions for authentication currently being developed by ETSI SAGE while still satisfying the security requirements

Clauses affected: Section 3.2, 6.3.3, 6.3.5

Other specs Affected:	Other 3G core specifications	<input type="checkbox"/>	→ List of CRs:	
	Other GSM core specifications	<input type="checkbox"/>	→ List of CRs:	
	MS test specifications	<input type="checkbox"/>	→ List of CRs:	
	BSS test specifications	<input type="checkbox"/>	→ List of CRs:	
	O&M specifications	<input type="checkbox"/>	→ List of CRs:	

Other comments:



help.doc

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

3.2 Symbols

For the purposes of the present document, the following symbols apply:

	Concatenation
\oplus	Exclusive or
f1	Message authentication function used to compute MAC
<u>f1*</u>	<u>Message authentication function used to compute MAC-S</u>
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK <u>in normal procedures</u>
<u>f5*</u>	<u>Key generating function used to compute AK in re-synchronisation procedures</u>
K	Long-term secret key shared between the USIM and the AuC

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.

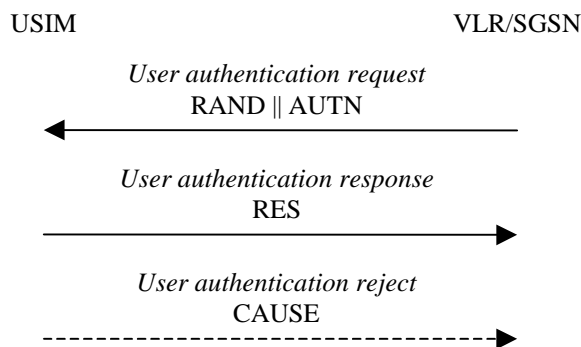


Figure 8: Authentication and key establishment

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.

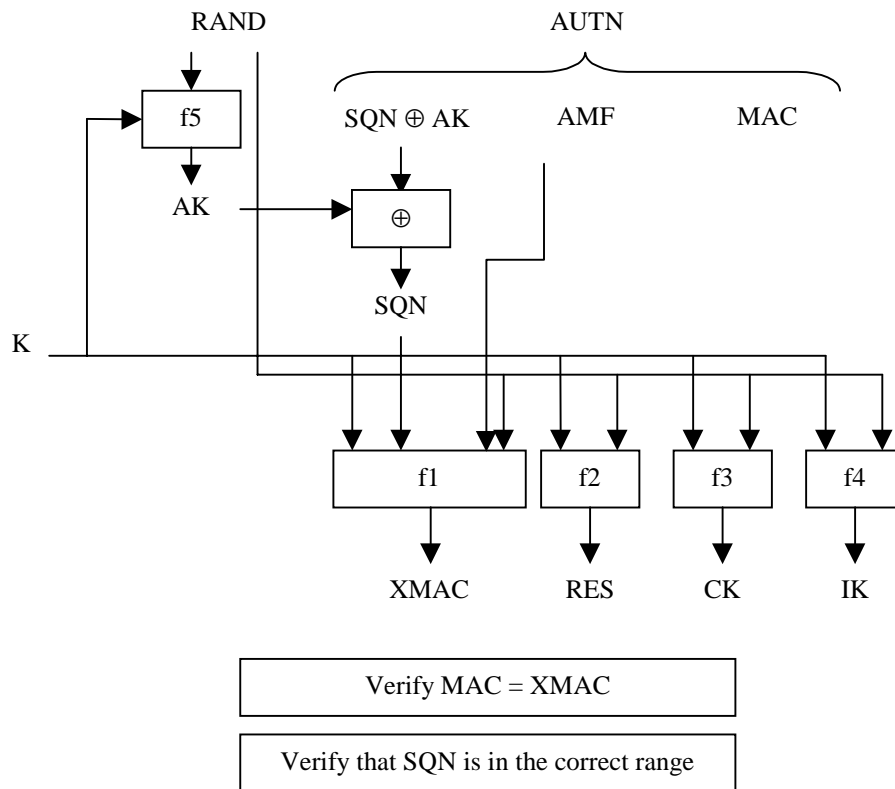


Figure 9: User authentication function in the USIM

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

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 $AUTS = Conc(SQN_{MS}) \parallel MAC-S$.

$Conc(SQN_{MS}) = SQN_{MS} \oplus f5^*_K(RAND \parallel MAC-S \parallel 0 \dots 0)$ is the concealed value of the counter $SEQSQN_{MS}$ in the MS, and $MAC-S = f1^*_K(SEQSQN_{MS} \parallel RAND \parallel AMF)$ 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 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:

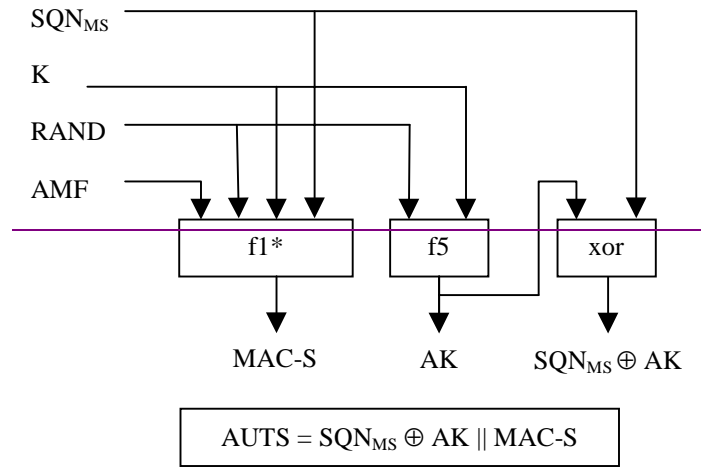


Figure 10: Construction of the parameter

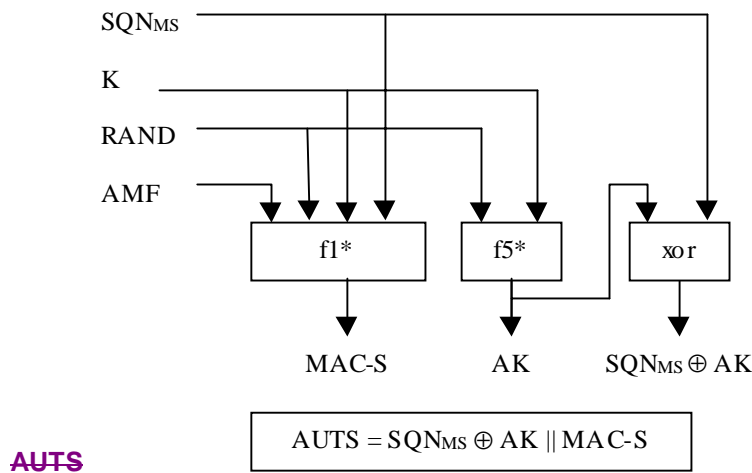


Figure 10: Construction of the parameter AUTS

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.

6.3.5 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 $SONSEQ_{MS}$ from $Conc(SONSEQ_{MS})$ by computing $f5_{K^*}(RANDMAC-S//0...0)$.
2. The HE/AuC checks if $SONSEQ_{HE}$ is in the correct range, i.e. if the next sequence number generated $SONSEQ_{HE}$ using would be accepted by the USIM.
3. If $SONSEQ_{HE}$ 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 $SONSEQ_{HE}$ to $SONSEQ_{MS}$.
6. The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the VLR/SGSN. If the counter $SONSEQ_{HE}$ was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting $SONSEQ_{HE}$. 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).

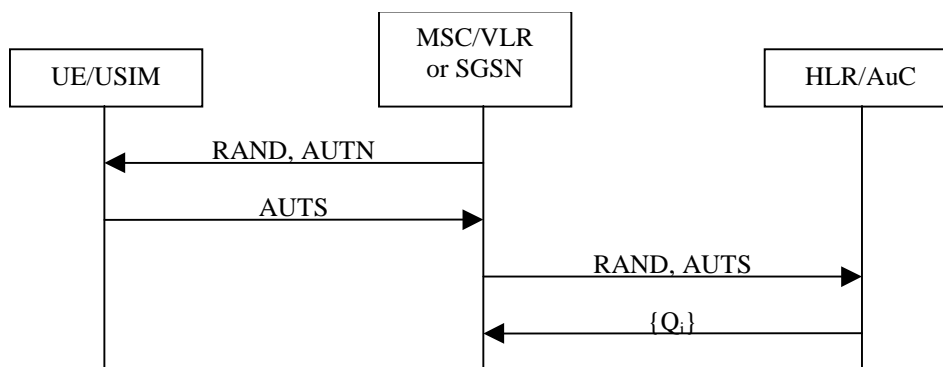


Figure 12: Resynchronization mechanism