3GPP TSG SA WG 3 (Security) meeting #11
Mainz, 22—24 February, 2000

Document **S3-000111**
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**	**051**	Current Version:	3.3.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	SA #7	for approval	X	strategic		*(for SMG*
list expected approval meeting # here ↑		for information		non-strategic		*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: *(at least one should be marked with an X)*	(U)SIM	X	ME	X	UTRAN / Radio		Core Network	

Source: Ericsson **Date:** 2000-02-16

Subject: Conversion function c3 at USIM

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:

Conversion function c3 (CK, IK → Kc) is located at USIM only. USIM shall derive Kc using c3 in order to provide it to a R99 UE for UMTS-GSM interoperability purposes.

The terms ‘user’ and ‘MS’ have been replaced by ‘USIM’ where applicable.

Clauses affected: 6.3.3

Other specs affected:

Other 3G core specifications		→ List of CRs:
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 ~~MS~~USIM. During the authentication, the ~~user~~ USIM verifies the freshness of the authentication vector that is used.

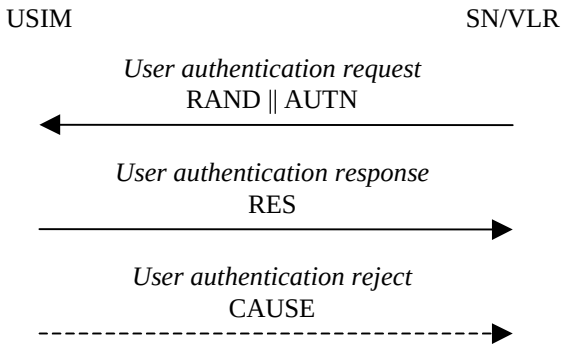

Figure 8: Authentication and key establishment

The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR database. The VLR/SGSN sends to the ~~user~~ 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.

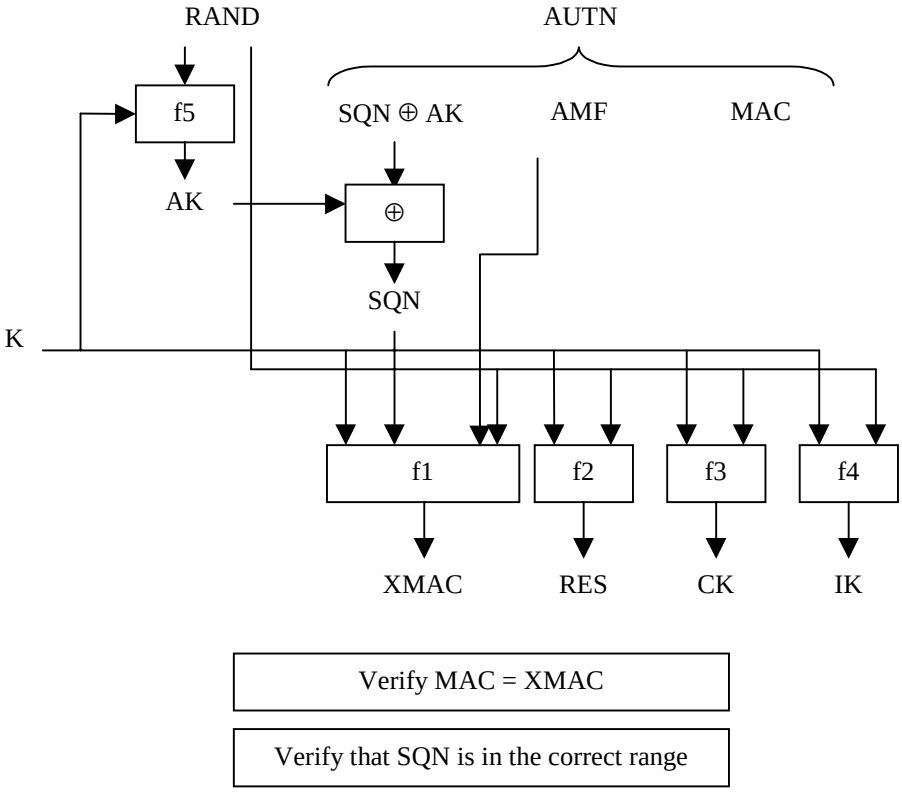

Figure 9: User authentication function in the USIM

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

Next the ~~user~~ 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.

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

If the ~~user~~ USIM considers the sequence number to be not in the correct range, ~~he~~ 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 = $Conc(SQN_{MS})$ || 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:

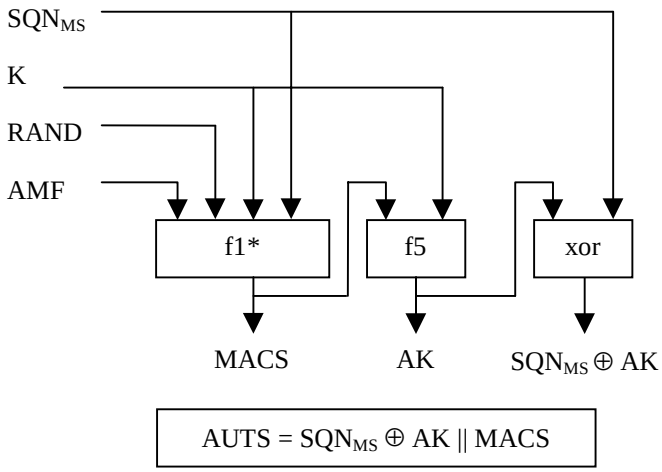

Figure 10: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range however, the ~~user~~ USIM computes $RES = f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the VLR/SGSN. Finally the ~~user~~ 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 GSM AKA, it shall derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3. UMTS keys are sent to the MS along with the derived GSM key for UMTS-GSM interoperability purposes. USIM shall store original CK, IK as current security context data. The ~~MS~~ USIM also stores RAND for re-synchronisation purposes. All keys (original CK, IK and derived Kc) shall be passed to the MS.

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.