3GPP TSG SA WG 3 (Security) meeting #15
Washington (USA), 12—14 September, 2000

Document **S3-000612**
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.

33.103	**CR**	**xxx**	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	☒	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	□	UTRAN / Radio	□	Core Network	☒

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

Subject:	Computation of the anonymity key for re-synchronisation
Work item:	Security

Category:	F	Correction	□	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	☒		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change:	ETSI SAGE (designing an example set of functions for authentication and key agreement) signalled that this change would allow for faster processing – and SA-3 identified no security issues with the change.
Clauses affected:	3.2, 4.2.2, 4.6.1

Other specs affected:	Other 3G core specifications	□	→ List of CRs:	33.102 CR xxx, 33.105 CR xxx
	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

3.2 Symbols

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

||	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f1*	Message authentication function used to compute MAC-S
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 in normal operation
f5*	Key generating function used to compute AK for re-synchronisation
f6	Encryption function used to encrypt the IMSI
f7	Decryption function used to decrypt the IMSI (=$f6^{-1}$)
f8	Integrity algorithm
f9	Confidentiality algorithm
f10	Deriving function used to compute TEMSI
K	Long-term secret key shared between the USIM and the AuC

4.2.2 Authentication and key agreement (AKA_{USIM})

The USIM shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored on the USIM:

a) K: a permanent secret key;

b) SQN_{MS}: a counter that is equal to the highest sequence number SQN in an AUTN parameter accepted by the user;

c) $RAND_{MS}$: the random challenge which was received together with the last AUTN parameter accepted by the user. It is used to calculate the re-synchronisation message together with the highest accepted sequence number (SQN_{MS});

d) KSI: key set identifier;

e) $THRESHOLD_C$: a threshold defined by the HE to trigger re-authentication and to control the cipher key lifetime;

f) CK The access link cipher key established as part of authentication;

g) IK The access link integrity key established as part of authentication;

h) $HFN_{MS:}$ Stored Hyper Frame Number provides the Initialisation value for most significant part of COUNT-C and COUNT-I. The least significant part is obtained from the RRC sequence number;

i) AMF: A 16-bit field used Authentication Management. The use and format are unspecified in the architecture but examples are given in an informative annex;

j) The GSM authentication parameter and GSM cipher key derived from the UMTS to GSM conversion functions.

Table 3 provides an overview of the data elements stored on the USIM to support authentication and key agreement.

Table 3: USIM – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
K	Permanent secret key	1 (note 1)	Permanent	128 bits	Mandatory
SQN_{MS}	Sequence number counter	1	Updated when AKA protocol is executed	48 bits	Mandatory
WINDOW (option 1)	accepted sequence number array	1	Updated when AKA protocol is executed	10 to 100 bits	Optional
LIST (option 2)	Ordered list of sequence numbers received	1	Updated when AKA protocol is executed	32-64 bits	Optional
$RAND_{MS}$	Random challenge received by the user.	1	Updated when AKA protocol is executed	128 bits	Mandatory
KSI	Key set identifier	1	Updated when AKA protocol is executed	3 bits	Mandatory
$THRESHOLD_{C}$	Threshold value for ciphering	1	Permanent	32 bits	Optional
CK	Cipher key	1	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	1	Updated when AKA protocol is executed	128 bits	Mandatory
$HFN_{MS:}$	Initialisation value for most significant part for COUNT-C and for COUNT-I	1	Updated when connection is released	25 bits	Mandatory
AMF	Authentication Management Field (indicates the algorithm and key in use)	1	Updated when AKA protocol is executed	16 bits	Mandatory
$RAND_{G}$	GSM authentication parameter from conversion function	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
SRES	GSM authentication parameter from conversion function	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
Kc	GSM cipher Key	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional

NOTE 1: HE policy may dictate more than one, the active key signalled using the AMF function.

The following cryptographic functions need to be implemented on the USIM:

- f1: a message authentication function for network authentication;
- f1*: a message authentication function for support to re-synchronisation;
- f2: a message authentication function for user authentication;
- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;
- f5: a key generating function to derive the anonymity key for normal operation;
- f5*: a key generating function to derive the anonymity key for re-synchronisation;
- c2: Conversion function for interoperation with GSM from XRES (UMTS) to SRES (GSM);
- c3: Conversion function for interoperation with GSM from Ck and IK (UMTS) to Kc (GSM).

Figure 2 provides an overview of the data integrity, data origin authentication and verification of the freshness by the USIM of the RAND and AUTN parameters received from the VLR/SGSN, and the derivation of the response RES, the cipher key CK and the integrity key IK. Note that the anonymity Key (AK) is optional.

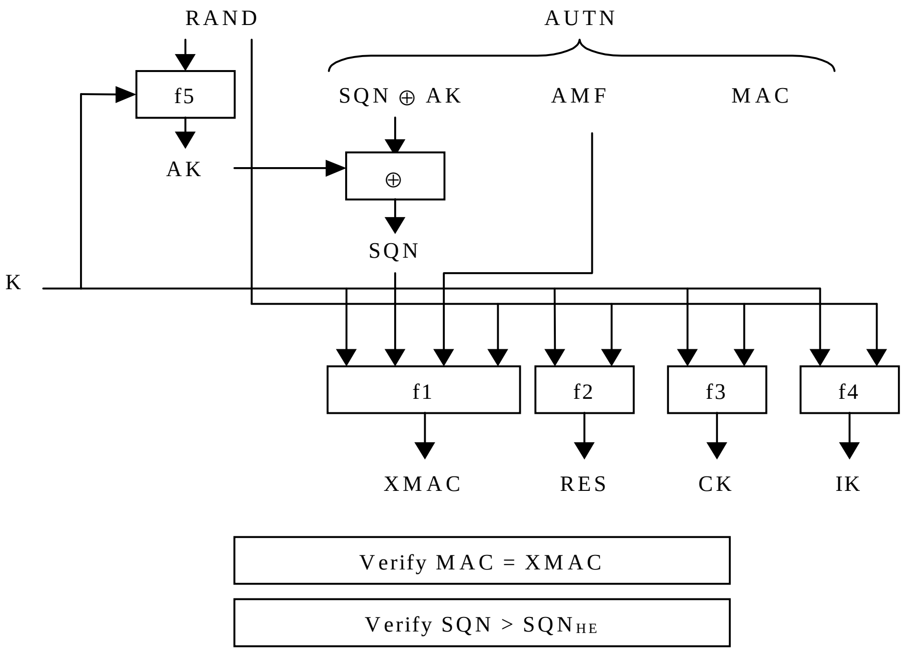

Figure 1: User authentication function in the USIM

Figure 3 provides an overview of the generation in the USIM of a token for re-synchronisation AUTS.

a) The USIM computes MAC-S = f1*$_{K}$(SQN$_{MS}$ || RAND || AMF*), whereby AMF* is a default value for AMF used in re-synchronisation.

b) If SQN$_{MS}$ is to be concealed with an anonymity key AK, the USIM computes AK = f5$_{K}$(~~MAC-S || 0…0~~RAND)~~, whereby MAC-S forms the 12 most significant octets and 32 zeros form the 4 least significant octets of the required 16 octet input parameter,~~ and the concealed counter value is then computed as SQN$_{MS}$ ⊕ AK.

c) The re-synchronisation token is constructed as AUTS = SQN$_{MS}$ [⊕ AK] || MAC-S.

~~Upon receipt of an indication of synchronisation failure and a (AUTS, RAND) pair, the HLR/AuC may perform the following cryptographic functions:~~

~~a) If SQN_{MS} is concealed with an anonymity key AK, the HLR/AuC computes AK = $f5_K$(MAC-S || 0…0), whereby MAC-S forms the 12 most significant octets and 32 zeros form the 4 least significant octets of the required 16 octet input parameter and retrieves the unconcealed counter value as SQN_{MS} = (SQN_{MS} ⊕ AK) xor AK.~~

~~b) If SQN generated from SQN_{HE} would not be acceptable, then the HLR/AuC computes XMAC-S = $f1*_K$(SQN_{MS} || RAND || AMF*), whereby AMF* is a default value for AMF used in re-synchronisation.~~

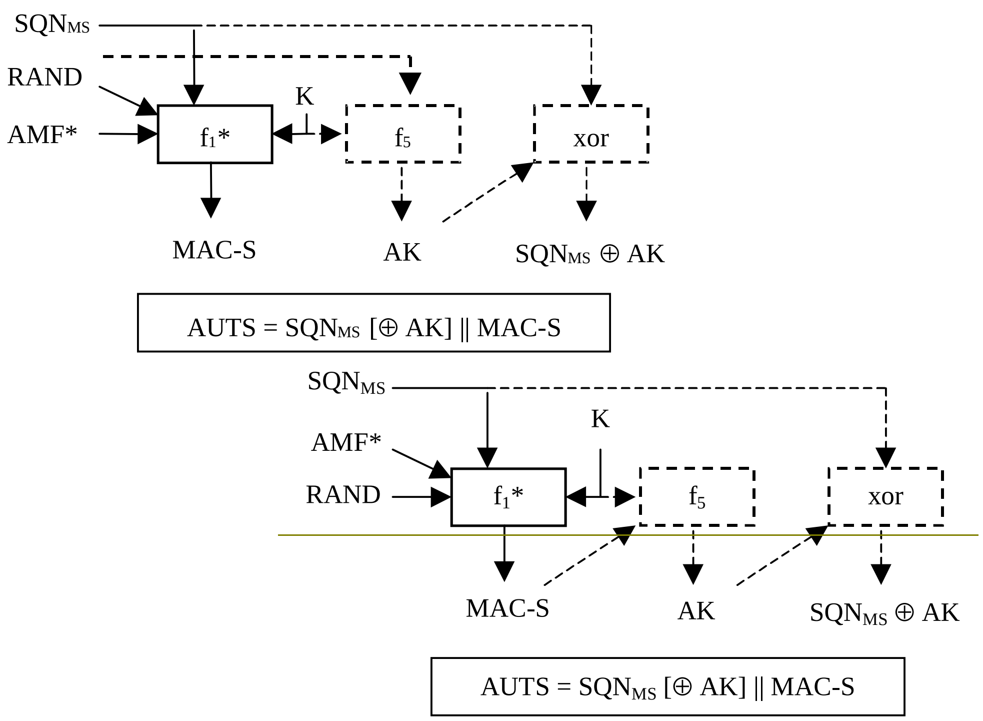

Figure 2: Generation of a token for re-synchronisation AUTS (note 1)

NOTE 1: The lengths of AUTS and MAC-S are specified in table 20.

Table 4 provides a summary of the cryptographic functions implemented on the USIM to support authentication and key agreement.

Table 4: USIM – Authentication and key agreement – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f1	Network authentication function	1	Permanent	Proprietary	Mandatory
f1*	Message authentication function for synchronisation	1	Permanent	Proprietary	Mandatory
f2	User authentication function	1	Permanent	Proprietary	Mandatory
f3	Cipher key generating function	1	Permanent	Proprietary	Mandatory
f4	Integrity key generating function	1	Permanent	Proprietary	Mandatory
f5	Anonymity key generating function (for normal operation)	1	Permanent	Proprietary	Optional
f5*	Anonymity key generating function (for re-synchronisation)	1	Permanent	Proprietary	Optional
c2 and c3	Conversion functions for interoperation with GSM	1 of each	Permanent	Standard	Optional

4.6.1 Authentication and key agreement (AKA_{he})

The HLR/AuC shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored in the HLR/AuC:

a) K: a permanent secret key;

b) SQN_{HE}: a counter used to generate SQN from;

c) AV: authentication vectors computed in advance;

Table 19 provides an overview of the data elements stored on the HLR/AuC to support authentication and key agreement.

Table 19: HLR/AuC – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
K	Permanent secret key	1	Permanent	128 bits	Mandatory
SQN_{HE}	Sequence number counter	1	Updated when AVs are generated	48 bits	Mandatory
UMTS AV	UMTS Authentication vectors	HE option	Updated when AVs are generated	544-640 bits	Optional
GSM AV	GSM Authentication vectors	HE option that consists of:	Updated when AVs are generated	As GSM	Optional
RAND	GSM Random challenge			128 bits	Optional
SRES	GSM Expected response			32 bits	Optional
Kc	GSM cipher key			64 bits	Optional

Table 20 shows how the construction of authentication token for synchronisation failure messages used to support authentication and key agreement.

Table 20: Composition of an authentication token for synchronisation failure messages

Symbol	Description	Multiplicity	Length
AUTS	Synchronisation Failure authentication token	that consists of:	112
SQN	Sequence number	1 per AUTS	48
MAC-S	Message authentication code for Synchronisation Failure messages	1 per AUTS	64

Figure 4 provides an overview of how authentication vectors are generated in the HLR/AuC.

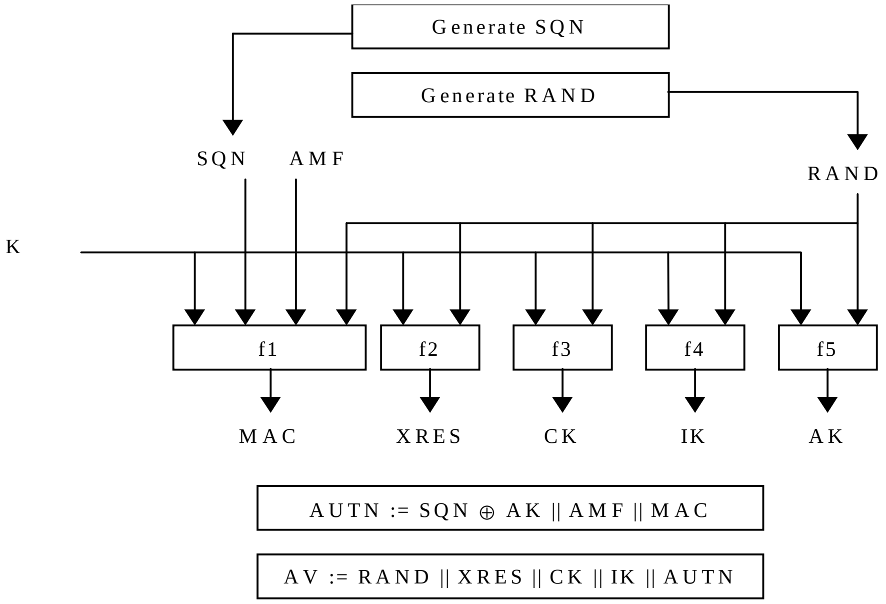
Generate SQN
Generate RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figure 3: Generation of an authentication vector

The following cryptographic functions need to be implemented in the HLR/AuC:

- f1: a message authentication function for network authentication;
- f1*: a message authentication function for support to re-synchronisation;
- f2: a message authentication function for user authentication;
- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;
- f5: a key generating function to derive the anonymity key for normal operation;
- f5*: a key generating function to derive the anonymity key for re-synchronisation;
- c1: Conversion function for interoperation with GSM from RAND (UMTS) > RAND (GSM);
- c2: Conversion function for interoperation with GSM from XRES (UMTS) to SRES (GSM);
- c3: Conversion function for interoperation with GSM from CK and IK (UMTS) to Kc (GSM).

Table 21 provides a summary of the cryptographic functions implemented on the USIM to support authentication and key agreement.

Table 21: HLR/AuC – Authentication and key agreement – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f1	Network authentication function	1	Permanent	Proprietary	Mandatory
f1*	Message authentication function for synchronisation	1	Permanent	Proprietary	Mandatory
f2	User authentication function	1	Permanent	Proprietary	Mandatory
f3	Cipher key generating function	1	Permanent	Proprietary	Mandatory
f4	Integrity key generating function	1	Permanent	Proprietary	Mandatory
f5	Anonymity key generating function (for normal operation)	1	Permanent	Proprietary	Optional
f5*	Anonymity key generating function (for re-synchronisation)	1	Permanent	Proprietary	Optional
A3/A8	GSM user authentication functions	1	Permanent	Proprietary	Optional
c1, c2 and c3	Functions for converting UMTS AV's to GSM AV's	1 for each	Permanent	Standard	Optional