Technical Specification Group Services and System Aspects
Meeting #9, Hawaii, USA, 25-28 September 2000

TSGS#9(00)0445

Source: **SA WG3**

Title: **CRs to 33.102, 33.103 and 33.105 on anonymity key calculation during re-synchronisation**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CRs were agreed at SA WG3 meetings #14 and #15 and are presented to TSG SA #09 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Ver	WG	Meeting	S3 doc
33.102	122		R99	Change of computation of the anonymity key in the re-synchronisation procedure	F	3.5.0	S3	S3-15	S3-000601
33.103	012		R99	Computation of the anonymity key for re-synchronisation	F	3.3.0	S3	S3-15	S3-000612
33.105	012		R99	Calculation of AK in re-synchronisation	F	3.4.0	S3	S3-14	S3-000494
33.105	014		R99	Anonymity key computation during re-synchronisation	F	3.4.0	S3	S3-15	S3-000613

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

Document S3000601 (rev574)

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	122	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	X	ME		UTRAN / Radio		Core Network	X

Source: SA WG3 **Date:** 13 Sept. 2000

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

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: 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		→ 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.

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 procedures
f5*	Key generating function used to compute AK in re-synchronisation procedures
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.

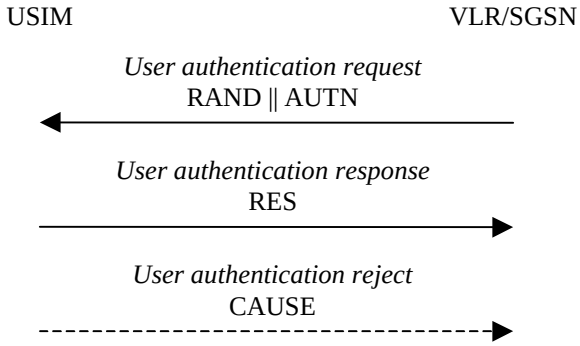


Figure 8: Authentication and key establishment

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.

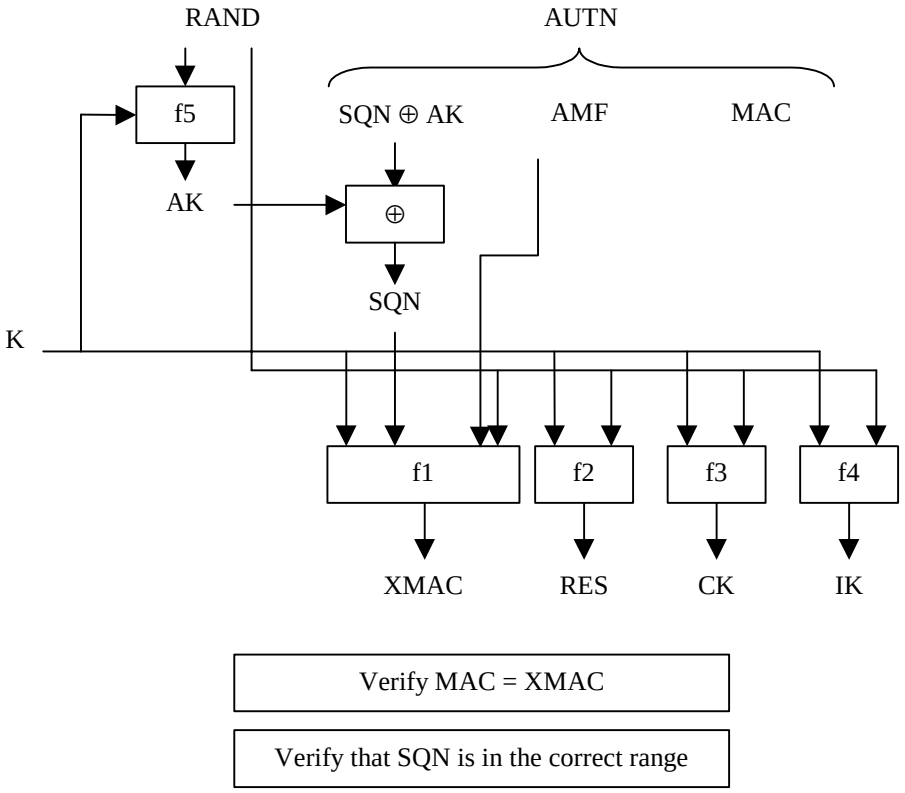


Figure 9: User authentication function in the USIM

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

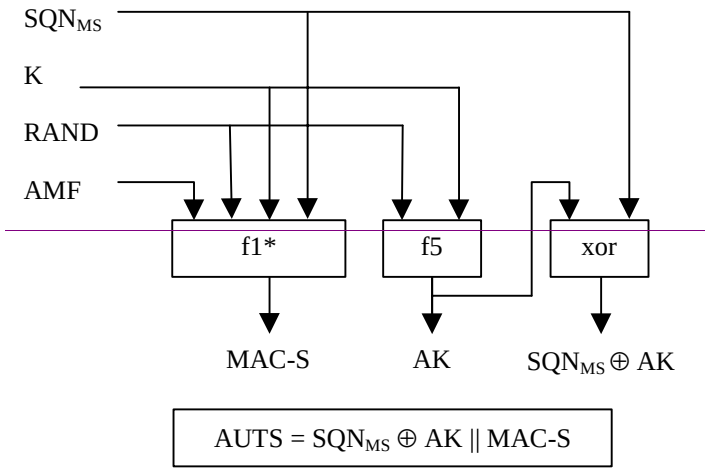
Next the USIM verifies that the received sequence number SQN is in the correct range.

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.

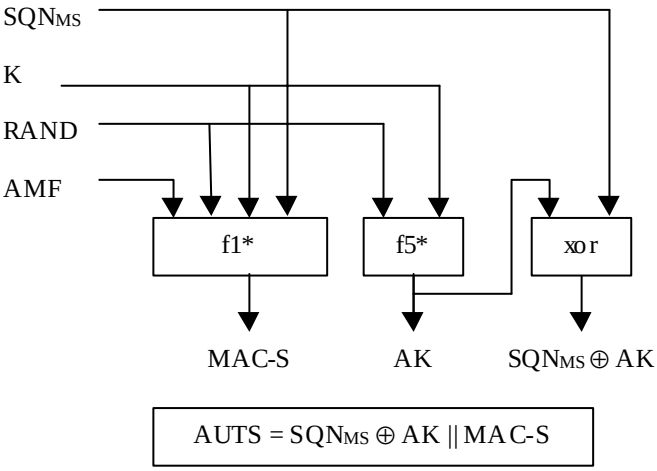
The synchronisation failure message contains the parameter AUTS. It is AUTS = Conc(SQN_{MS}) || MAC-S. Conc(SQN_{MS}) = SQN_{MS} ⊕ $f5^*_K$(RAND~~MAC-S || 0...0~~) is the concealed value of the counter ~~SEQ~~SQN_{MS} in the MS, and MAC-S = $f1^*_K$(~~SEQ~~SQN_{MS} || RAND || AMF) where RAND is the random 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 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~~

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 $SQN SEQ_{MS}$ from Conc($SQN SEQ_{MS}$) by computing $f5^*_K(RAND ~~MAC-S \| 0...0~~)$,.
2. The HE/AuC checks if $SQN SEQ_{HE}$ is in the correct range, i.e. if the next sequence number generated $SQN SEQ_{HE}$ using would be accepted by the USIM.
3. If $SQN SEQ_{HE}$ 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 $SQN SEQ_{HE}$ to $SQN SEQ_{MS}$.
6. The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the VLR/SGSN. If the counter $SQN SEQ_{HE}$ was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting $SQN SEQ_{HE}$. 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).

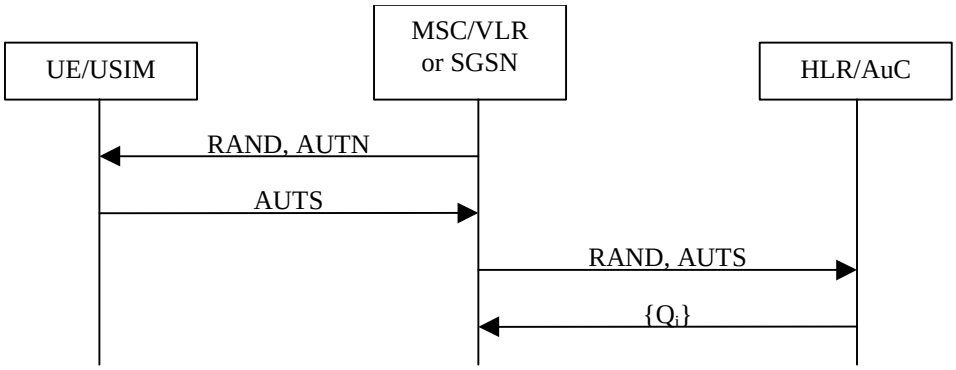


Figure 12: Resynchronisation mechanism

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**	**012**	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: (U)SIM [X] ME [ ] UTRAN / Radio [ ] Core Network [X]
(at least one should be marked with an X)

Source: SA WG3 **Date:** 13 Sept. 2000

Subject: Computation of the anonymity key for re-synchronisation

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: 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.

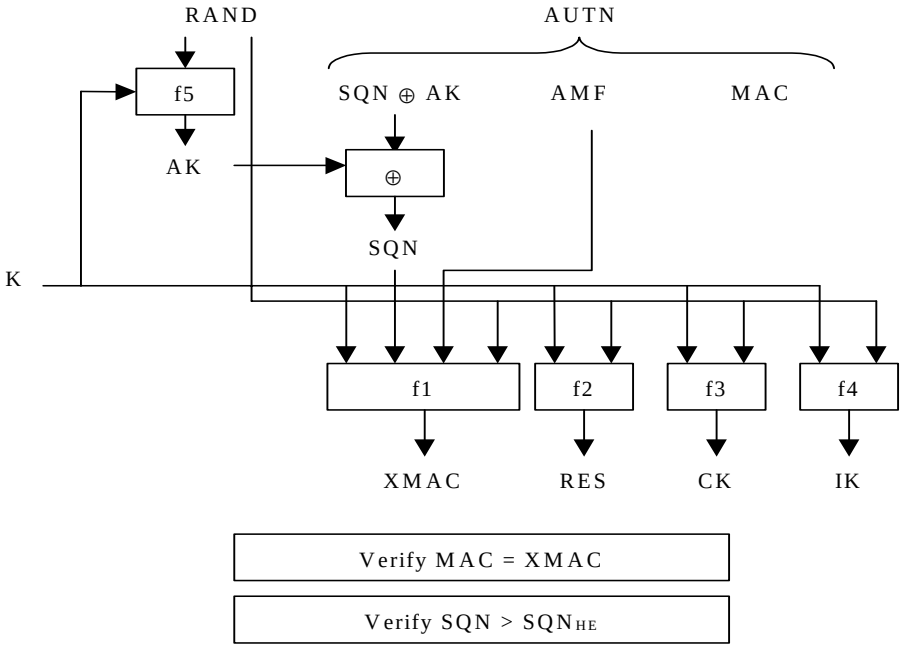


Figure 1: User authentication function in the USIM

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 $SQN_{MS} \oplus AK$.

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 $AK = f5_K(MAC\text{-}S \| 0\ldots0)$, 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 $SQN_{MS} = (SQN_{MS} \oplus AK)$ xor AK.~~

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

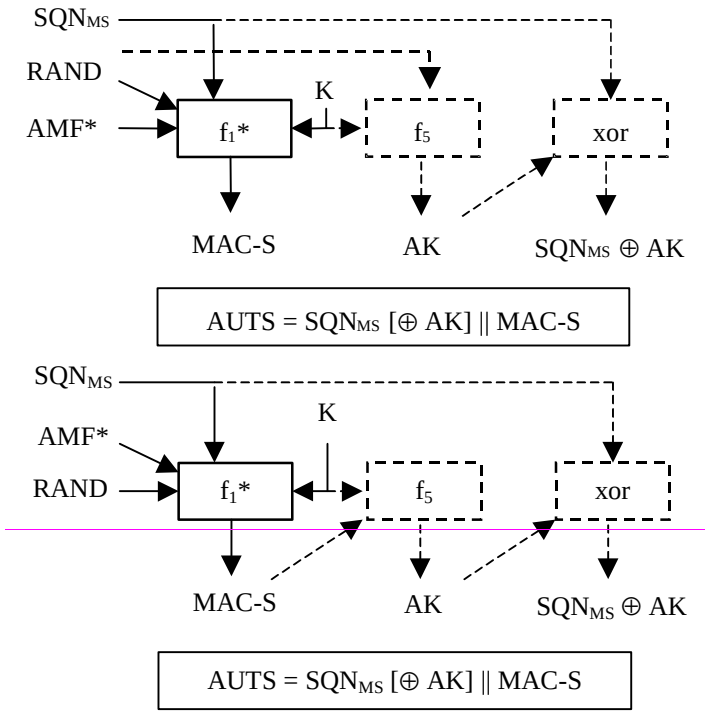


Figure 2: Generation of a token for re-synchronisation AUTS (note 1)

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.

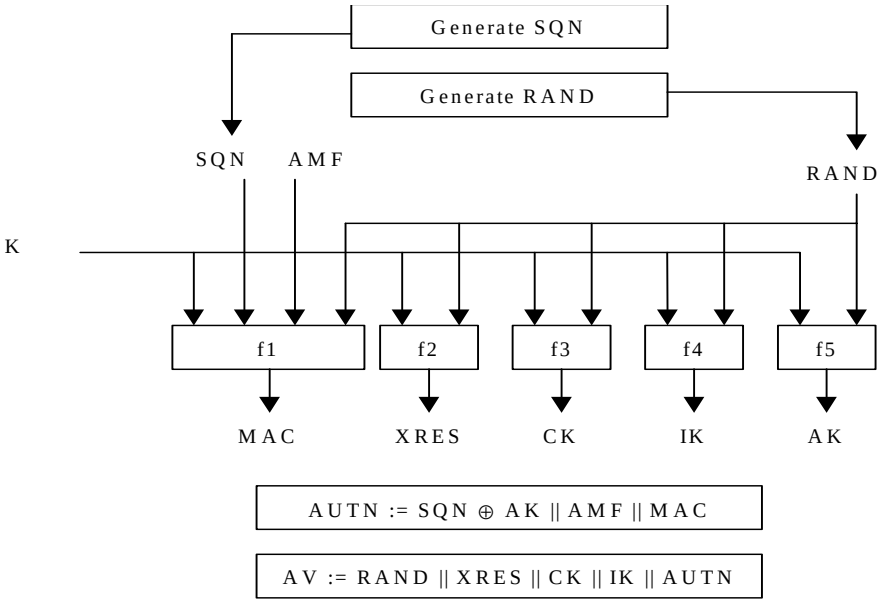


Figure 3: Generation of an authentication vector

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

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

Document S3-000494
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.

33.105	CR	012	Current Version:	3.4.0

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	X	ME		UTRAN / Radio		Core Network	

Source: SA WG3 **Date:** 1 August 2000

Subject: Calculation of AK in re-synchronisation

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: The length of MAC-S was described as 12 octets. It should have been 8 octets.
Editorial change to description of maximum length of RES

Clauses affected: 5.1.1.3, 5.1.1.4, 5.1.7.8

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.

5.1.1.3 Generation of re-synchronisation token in the USIM

Upon the assertion of a synchronisation failure, the USIM generates a re-synchronisation token as follows:

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), whereby MAC-S forms the ~~12~~ 8 most significant octets and ~~32~~ 64 zeros form the 8~~4~~ least significant octets of the required 16 octet input parameter, and the concealed counter value is then computed as $SQN_{MS} \oplus AK$.

c) The re-synchronisation token is constructed as AUTS = $SQN_{MS} [\oplus AK] \| MAC\text{-}S$.

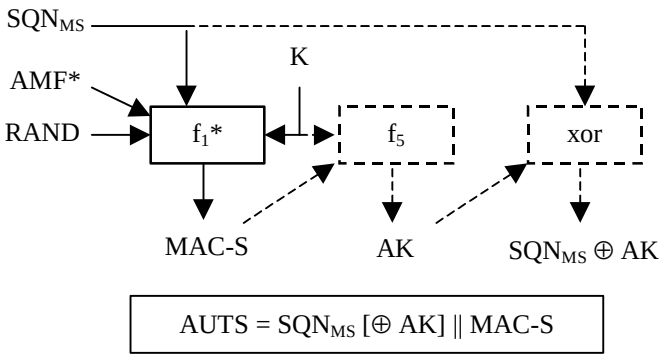


Figure 3: Generation of re-synchronisation token in the USIM

5.1.1.4 Re-synchronisation in the HLR/AuC

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

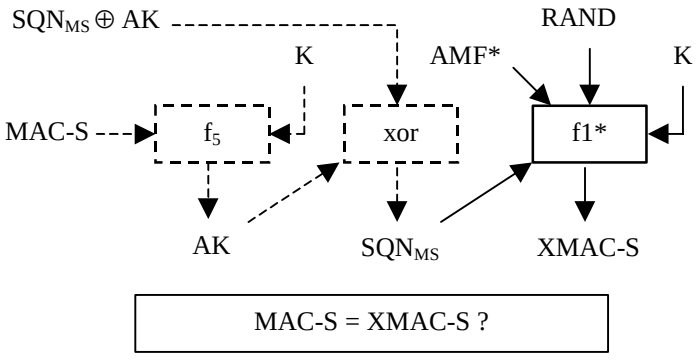


Figure 4: Re-synchronisation in the HLR/AuC

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~~ 8 most significant octets and ~~32~~ 64 zeros form the 8~~4~~ least significant octets of the required 16 octet input parameter and retrieves the unconcealed counter value as $SQN_{MS} = (SQN_{MS} \oplus AK)$ 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.

5.1.7.8 RES (or XRES)

RES: the user response

RES[0], RES[1], …, RES[~~31 ... 127~~n-1]

The ~~maximum~~ length n of RES and XRES is at most 128 bits and ~~the minimum is~~ at least 32 bits. RES and XRES constitute to entity authentication of the user to the network.

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

Document **S3-000613**
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.

33.105	**CR**	**014**	Current Version:	3.4.0

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

For submission to:	SA #10	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: (U)SIM [X] ME [ ] UTRAN / Radio [ ] Core Network [X]
(at least one should be marked with an X)

Source: SA WG3 **Date:** 13 Sept. 2000

Subject: Anonymity key computation during re-synchronisation

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: ETSI SAGE (developing the example set of functions for AKA) signalled that computing the anonymity key this way would allow for faster processing – and SA-3 did no see security issues related to the change.

Clauses affected: 3.2, 5.1.1, 5.1.1.3, 5.1.1.4, 5.1.2, 5.1.3, 5.1.4, 5.1.6.7, 5.1.6.8 (new)

Other specs affected:

Other 3G core specifications	X	→ List of CRs:	33.102 CR xxx, 33.103 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
f0	random challenge generating function
f1	network authentication function
f1*	the re-synchronisation message authentication function;
f2	user authentication function
f3	cipher key derivation function
f4	integrity key derivation function
f5	anonymity key derivation function for normal operation
f5*	anonymity key derivation function for re-synchronisation
f6	user identity encryption function
f7	user identity decryption function
f8	UMTS encryption algorithm
f9	UMTS integrity algorithm

5.1.1 Overview

The mechanism for authentication and key agreement described in clause 6.3 of [1] requires the following cryptographic functions:

f0	the random challenge generating function;
f1	the network authentication function;
f1*	the re-synchronisation message authentication function;
f2	the user authentication function;
f3	the cipher key derivation function;
f4	the integrity key derivation function;
f5	the anonymity key derivation function for normal operation;
f5*	the anonymity key derivation function for re-synchronisation.

5.1.1.3 Generation of re-synchronisation token in the USIM

Upon the assertion of a synchronisation failure, the USIM generates a re-synchronisation token as follows:

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 $AK = f5^*_K(RAND)$ and the concealed counter value is then computed as $SQN_{MS} \oplus AK$.

c) The re-synchronisation token is constructed as $AUTS = SQN_{MS} [\oplus AK] \| MAC\text{-}S$.

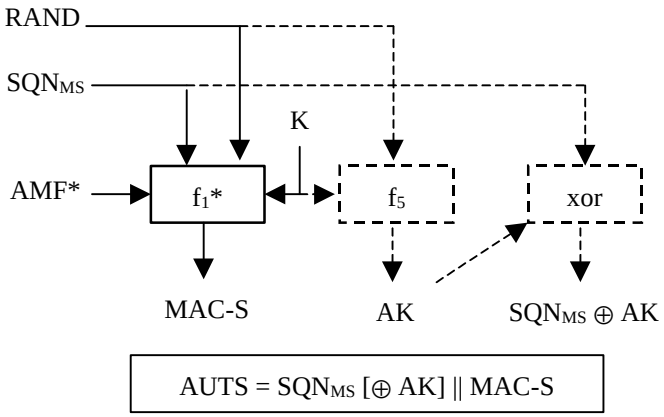


Figure 3: Generation of re-synchronisation token in the USIM

5.1.1.4 Re-synchronisation in the HLR/AuC

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

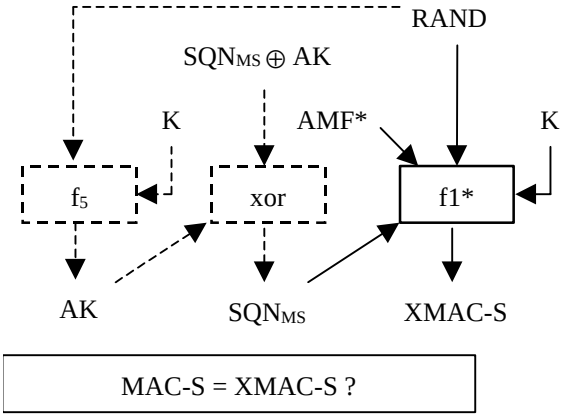


Figure 4: Re-synchronisation in the HLR/AuC

a) If SQN_{MS} is concealed with an anonymity key AK, the HLR/AuC computes $AK = f5^*_K(RAND)$ and retrieves the unconcealed counter value as $SQN_{MS} = (SQN_{MS} \oplus AK)$ xor AK.

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

5.1.2 Use

The functions f0—f5 shall only be used to provide mutual entity authentication between USIM and AuC, derive keys to protect user and signalling data transmitted over the radio access link and conceal the sequence number to protect user identity confidentiality. The function f1* shall only be used to provide data origin authentication for the synchronisation failure information sent by the USIM to the AuC. The function f5* shall only be used to provide user identity confidentiality during re-synchronisation.

5.1.3 Allocation

The functions f1—f5, f1*and f5* are allocated to the Authentication Centre (AuC) and the USIM. The function f0 is allocated to the AuC.

5.1.4 Extent of standardisation

The functions f0—f5, f1*and f5* are proprietary to the home environment. Examples of the functions f1, f1* and f2 are CBC-MACs or H-MACs [3].

5.1.5 Implementation and operational considerations

The functions f1—f5, f1* and f5* shall be designed so that they can be implemented on an IC card equipped with a 8-bit microprocessor running at 3.25 MHz with 8 kbyte ROM and 300byte RAM and produce AK, XMAC-A, RES, CK and IK in less than 500 ms execution time.

5.1.6.7 f5

f5: the anonymity key derivation function for normal operation

f5: (K; RAND) → AK

f5 should be a key derivation function. In particular, it shall be computationally infeasible to derive K from knowledge of RAND and AK.

The use of f5 is optional.

5.1.6.8 f5*

f5*: the anonymity key derivation function for re-synchronisation

f5*: (K; RAND) → AK

f5* should be a key derivation function. In particular, it shall be computationally infeasible to derive K from knowledge of RAND and AK.

The use of f5* is optional.