3GPP TSG SA WG3 Security — S3#16 **S3-000706**
28-30 November, 2000
Sophia Antipolis, France

TIPHON 21 Temporary Document 057
Kyoto, Japan page 1 of 9
December 4-8, 2000

Source:	STF114, Scott
Title:	**Extensions to TD36 for 3GPP security**
Notice:	The author of this document declares that ETSI **may** make the document publicly available.

Document for:

Decision:	**X**
Discussion:	**X**
Meeting Report:	
Liaison:	
Information:	

Contact details:
First Name, Last Name Scott W Cadzow
e-mail: Scott.Cadzow@etsi.fr

1. Decision/Action Requested

To consider the attached text as content of WI-08004.

The text shows a set of cryptographic functions and how they are applied to achieve the goals described by the authentication framework in 21TD036. An algorithm set exists that implements each of the functions in this paper and is referred to as "Milenage" (use a *French* pronunciation) and is based upon AES which is assumed to be free of IPR restrictions.

2. Definitions and abbreviation and 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

In addition to (and partly in overlap to) the abbreviations included in TR 21.905 [3], for the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	The message authentication code included in AUTN, computed using f1
MAC	The message authentication code included in AUTN, computed using f1*
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
SAGE	Security Algorithm Group of Experts
SQN	Sequence number
SQN_{HE}	Individual sequence number for each user maintained in the HLR/AuC
SQN_{MS}	The highest sequence number the USIM has accepted
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TMSI	Temporary Mobile Subscriber Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Identity Module
VLR	Visitor Location Register
XRES	Expected Response

Authenticatee The entity that is making a claim.

Authenticator The entity that makes the decision that the authenticatee is as claimed

Claimant	See also authenticatee
Verifier	See also authenticator
Signer	See also authenticatee

3. References

3G TS 33.102

3G TS 33.105

4. Contents

5. Introduction to 3G security

Figure 1 gives an overview of the complete 3G security architecture (see clause 4 of 3G TS 33.102).

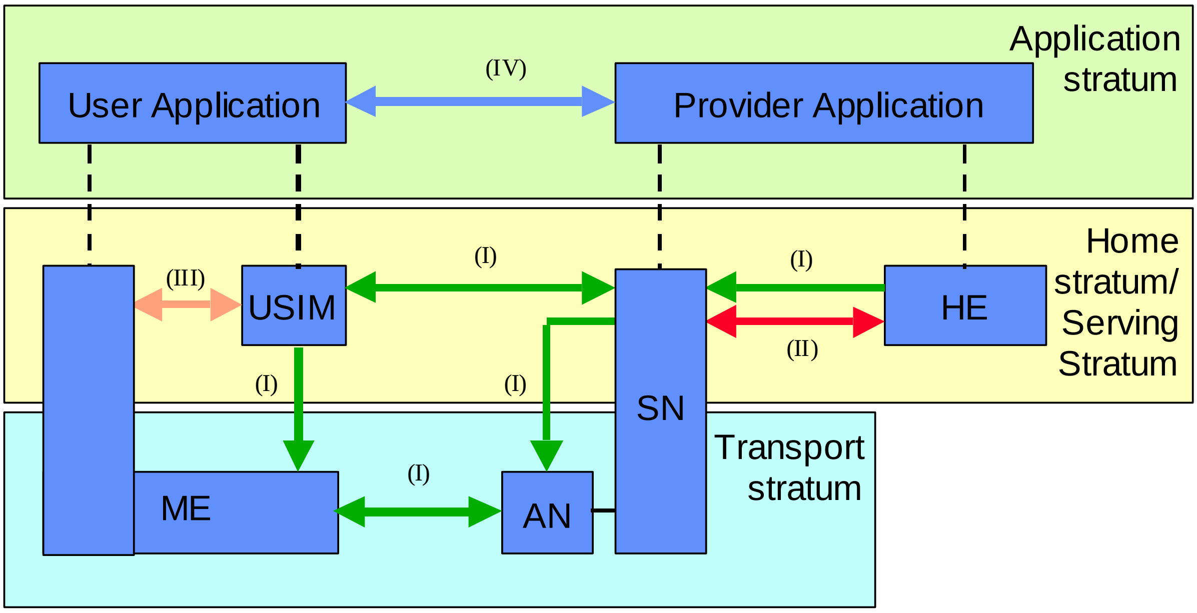


Figure 1: Overview of the security architecture

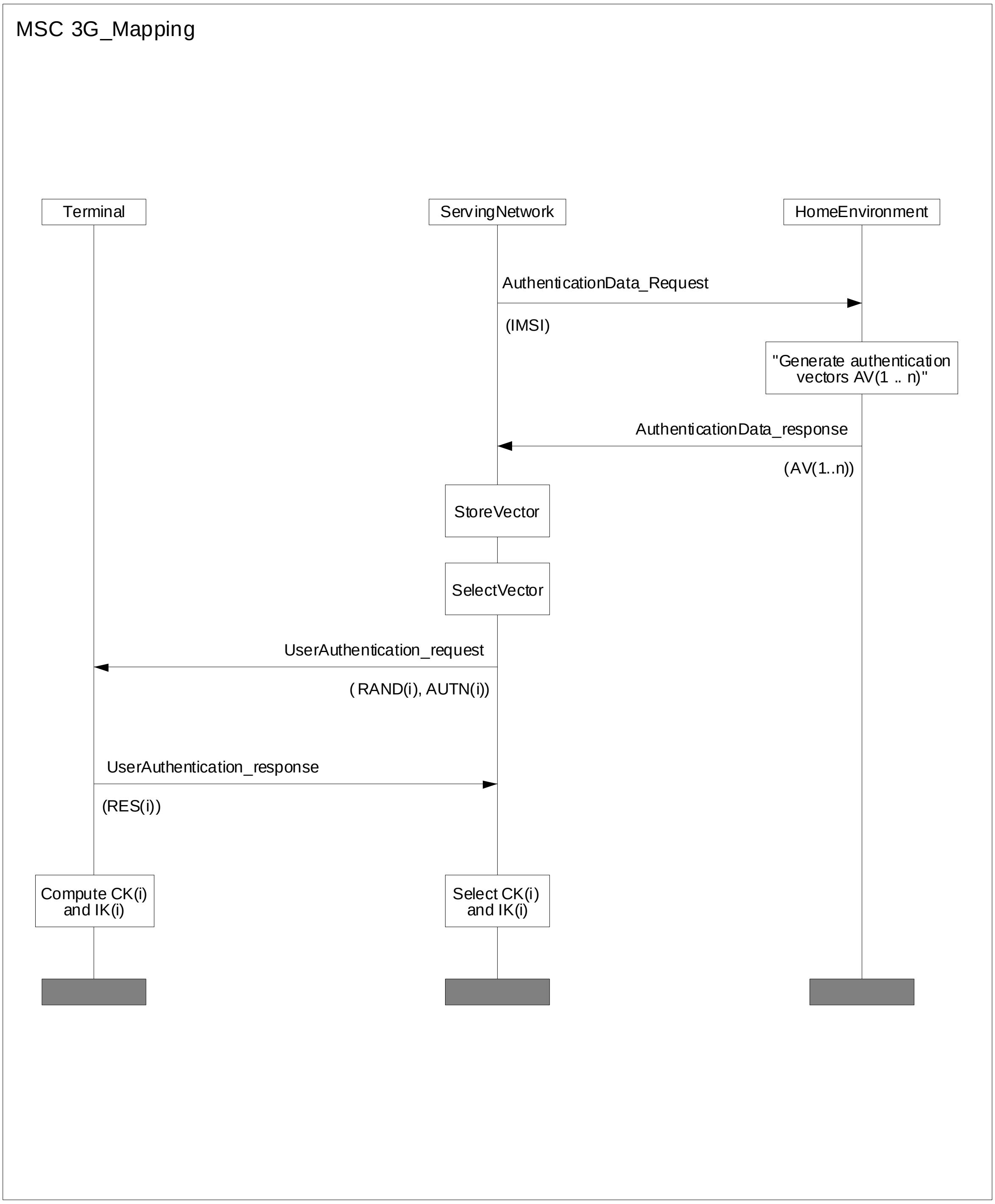
Five security feature groups are defined. Each of these feature groups meets certain threats and accomplishes certain security objectives:

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security (III):** the set of security features that secure access to mobile stations
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

In 21TD036 a number of information flows were identified within the framework. The flows between the serving network registration server and the user's authentication server are mapped to the flows in the 3G architecture from the Home Environment to the Serving Network and identified as Network access security (I) and Network domain security (II).

If we look further into the problem of distribution of security data from HE to SN we can consider adoption of the techniques identified in clause 6.3 of 3G TS 33.102. Parts of the reference document have been copied here to illustrate the convergence.

The overall scheme is shown in the MSC below showing a challenge-response protocol. The 3G specification also describes a number of function to generate the vectors and SAGE have generated an outline framework for these functions based upon AES:


MSC 3G_Mapping
Terminal
ServingNetwork
HomeEnvironment
AuthenticationData_Request
(IMSI)
"Generate authentication vectors AV(1 .. n)"
AuthenticationData_response
(AV(1..n))
StoreVector
SelectVector
UserAuthentication_request
(RAND(i), AUTN(i))
UserAuthentication_response
(RES(i))
Compute CK(i) and IK(i)
Select CK(i) and IK(i)

The authenticating parties in 3GPP are the AuC of the user's HE (HE/AuC) and the USIM in the user's mobile station. The generation of an authentication vector AV by the HE/AuC is shown below.

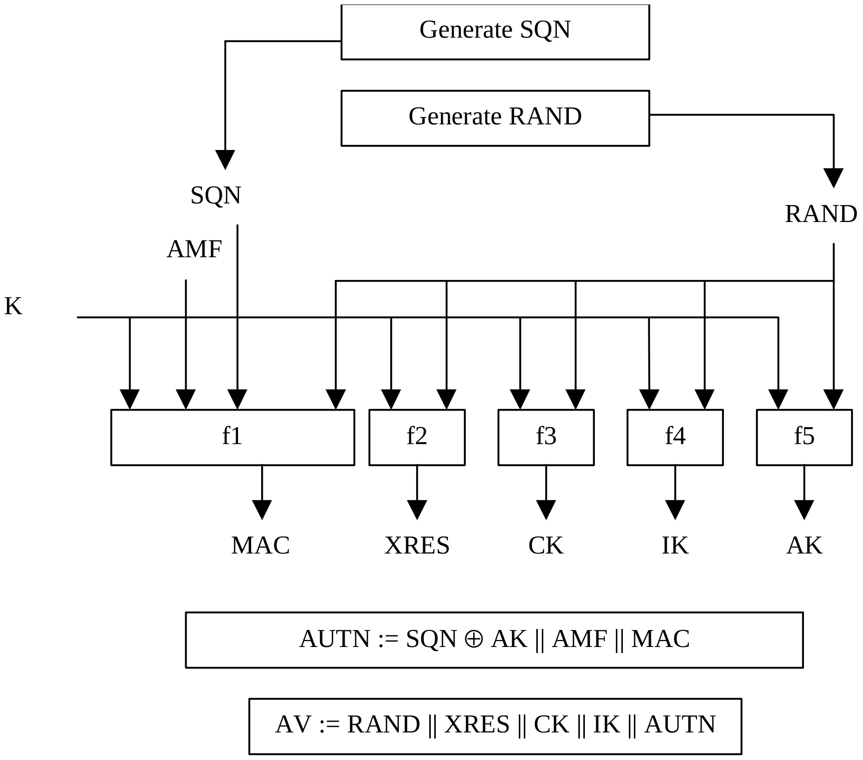

Generate SQN
Generate RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figure 7: Generation of authentication vectors

The following values are computed by these functions:

- a message authentication code MAC = $f1_K$(SQN || RAND || AMF) where f1 is a message authentication function;
- an expected response XRES = $f2_K$ (RAND) where f2 is a (possibly truncated) message authentication function;
- a cipher key CK = $f3_K$ (RAND) where f3 is a key generating function;
- an integrity key IK = $f4_K$ (RAND) where f4 is a key generating function;
- an anonymity key AK = $f5_K$ (RAND) where f5 is a key generating function or $f5 \equiv 0$.

Finally the authentication token AUTN = SQN ⊕ AK || AMF || MAC is constructed.

Here, AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only. If no concealment is needed then $f5 \equiv 0$ (AK = 0).

Upon receipt the user proceeds as shown in Figure 9.

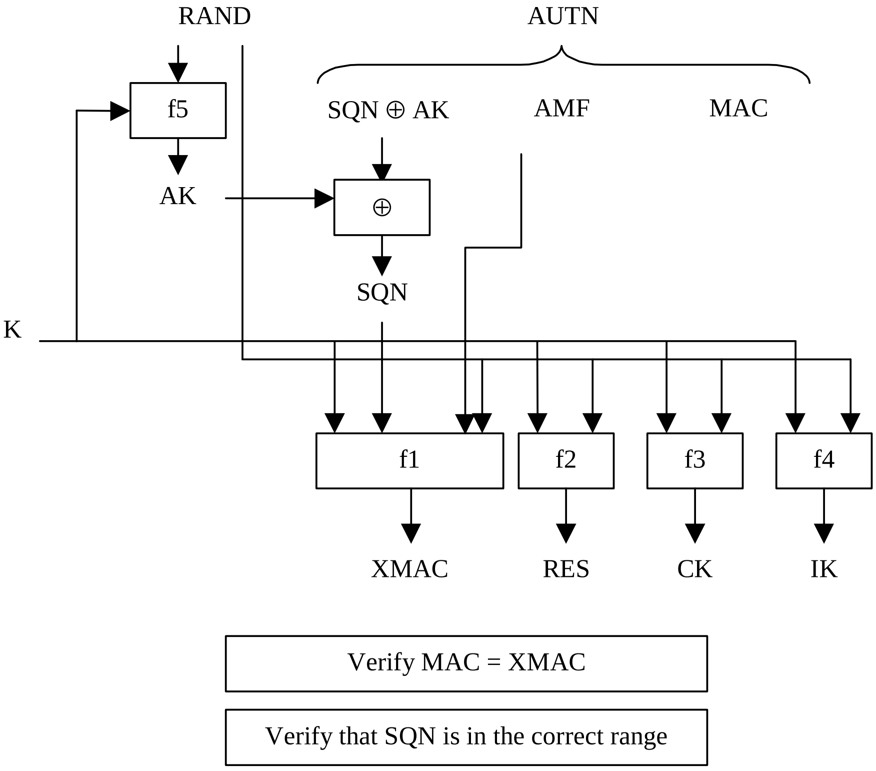


Figure 9: User authentication function in the USIM

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) is the concealed value of the counter SQN_{MS} in the MS, and MAC-S = $f1^*_K$(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 the 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:

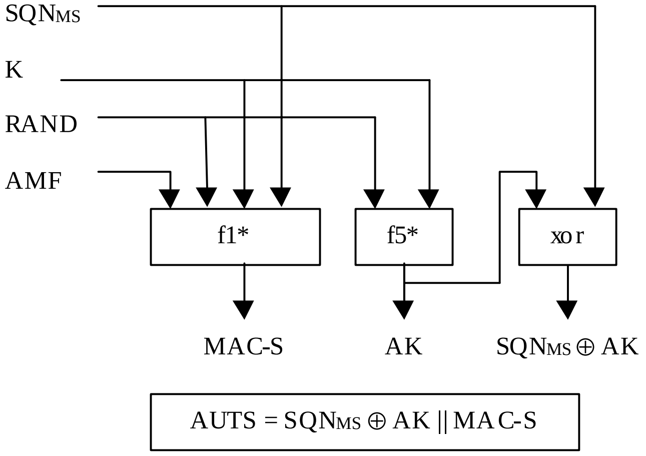


Figure 10: Construction of the parameter AUTS

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.