3GPP TSG SA WG 3 (Security) meeting #14
Oslo Norway 1st 4th August , 2000

Document **S3-000493**
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 010 Current Version: 3.3.0

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

Source: SA WG3 **Date:** 2000-08-04

Subject: Removal of Network Wide Confidentiality for R99 (clause 6)

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	☒	**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	☒
				Release 00	□

Reason for change: Network Wide Confidentiality is not part of release 99

It was agreed at TSG SA #7 that Network Wide encryption should be removed from Release 1999 specifications.

Clauses affected: 6

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: This CR considers that Network Wide encryption is not part of R99 and therefore these chapters are not updated and proposed to be removed instead.

help.doc

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

3G TS 33.103 V3.3.0 (2000-07)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Integration Guidelines
(Release 1999)

Keywords

Security, Guidelines

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Copyright Notification

Contents

Foreword

This Technical Specification has been produced by the 3GPP.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

3 the first digit:

3 Indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the specification.

1 Scope

This technical specification defines how elements of the 3G-security architecture are to be integrated into the following entities of the system architecture.

- Home Environment Authentication Centre (HE/AuC)
- Serving Network Visited Location Register (VLR/SGSN)
- Radio Network Controller (RNC)
- Mobile station User Identity Module (UIM)
- Mobile Equipment (ME)

This specification is derived from 3G "Security architecture". [1]

The structure of this technical specification is a series of tables, which describe the security information and cryptographic functions to be stored in the above entities of the 3G system.

For security information, this is in terms of multiplicity, lifetime, parameter length and whether mandatory or optional.

For the cryptographic functions, the tables also include an indication of whether the implementation needs to be standardised or can be proprietary.

The equivalent information for the alternative Temporary Key proposal is included in an appendix to this document.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3G TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; 3G Security Architecture".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

Authentication vector: either a quintet or a triplet.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

GSM Entity authentication and key agreement: Entity authentication according to GSM 03.20.

GSM security context: a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

GSM subscriber: a mobile station that consists of user equipment with a SIM inserted.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

Mobile station, user: the combination of user equipment and a user access module.

Quintet, UMTS authentication vector: temporary authentication data that enables an MSC/VLR or SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

SIM – GSM Subscriber Identity Module. In a security context, this module is responsible for performing GSM subscriber authentication and key agreement. This module is **not** capable of handling UMTS authentication nor storing UMTS style keys.

Temporary authentication data: either UMTS or GSM security context data or UMTS or GSM authentication vectors.

Triplet, GSM authentication vector: temporary authentication data that enables an MSC/VLR or SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

User access module: either a USIM or a SIM

USIM – User Services Identity Module. In a security context, this module is responsible for performing UMTS subscriber and network authentication and key agreement. It should also be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network.

UMTS Entity authentication and key agreement: Entity authentication according to this specification.

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI.

UMTS subscriber: a mobile station that consists of user equipment with a USIM inserted.

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
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

3.3 Abbreviations

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

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
$D_{SK(X)}$(data)	Decryption of "data" with Secret Key of X used for signing
$E_{KSXY(i)}$(data)	Encryption of "data" with Symmetric Session Key #i for sending data from X to Y
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption
EMSI	Encrypted Mobile Subscriber Identity
EMSIN	Encrypted MSIN
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
IV	Initialisation Vector
KAC_X	Key Administration Centre of Network X
KS_{XY}(i)	Symmetric Session Key #i for sending data from X to Y
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAP	Mobile Application Part
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
MS	Mobile Station
MSC	Mobile Services Switching Centre
MSIN	Mobile Station Identity Number
MT	Mobile Termination
NE_X	Network Element of Network X
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
RND_X	Unpredictable Random Value generated by X
SQN	Sequence number
SQN_{UIC}	Sequence number user for enhanced user identity confidentiality
SQN_{HE}	Sequence number counter maintained in the HLR/AuC
SQN_{MS}	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
TE	Terminal Equipment
TEMSI	Temporary Encrypted Mobile Subscriber Identity used for paging instead of IMSI
Text1	Optional Data Field
Text2	Optional Data Field
Text3	Public Key algorithm identifier and Public Key Version Number (eventually included in Public Key Certificate)
TMSI	Temporary Mobile Subscriber Identity
TTP	Trusted Third Party
UE	User equipment
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm

UIDN	User Identity Decryption Node
USIM	User Services Identity Module
VLR	Visitor Location Register
X	Network Identifier
XEMSI	Extended Encrypted Mobile Subscriber Identity
XRES	Expected Response
Y	Network Identifier

4 Access link security

4.1 Functional network architecture

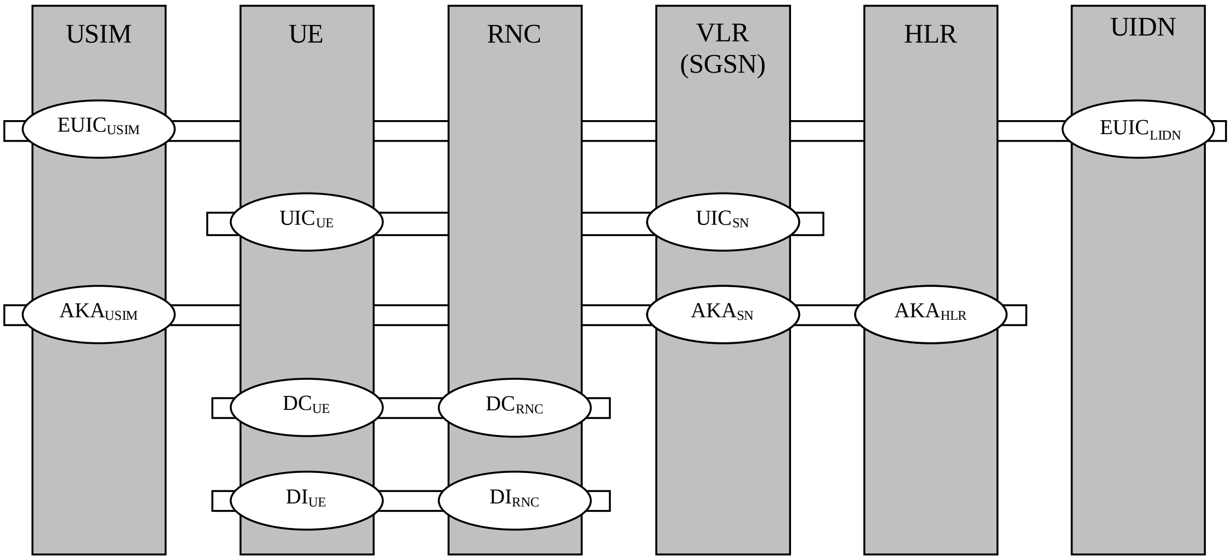


Figure 1 shows the functional security architecture of UMTS.

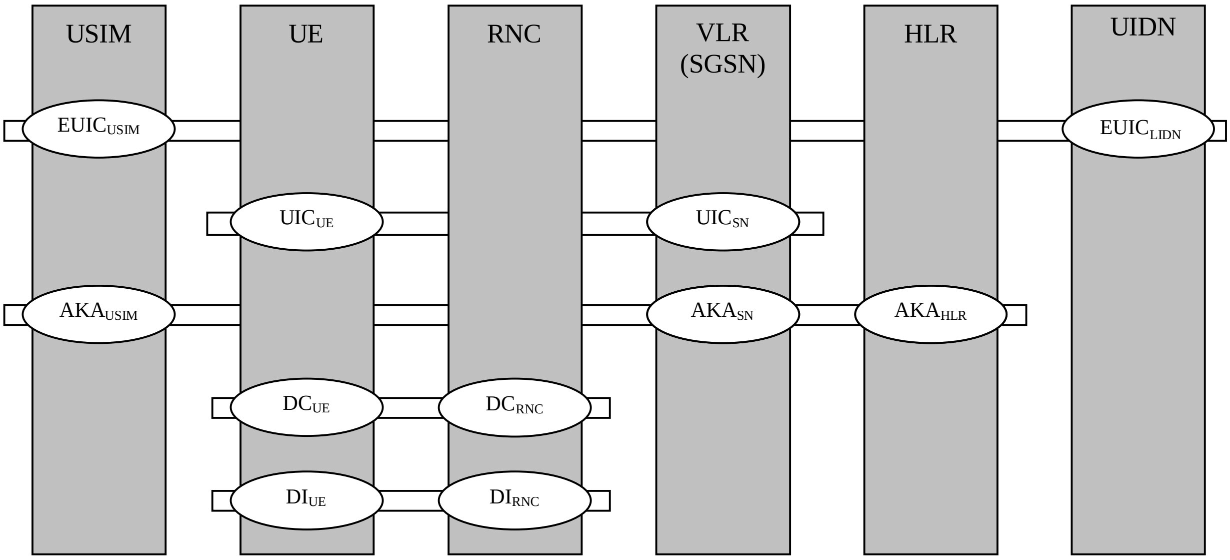


Figure 1: UMTS functional security architecture

The vertical bars represent the network elements:

In the user domain:

USIM (User Service Identity Module): an access module issued by a HE to a user;

UE (User Equipment);

In the serving network (SN) domain:

RNC (Radio Network Controller);

VLR (Visited Location Register), also the SGSN;

In the home environment (HE) domain:

HLR/AuC;

UIDN.

The horizontal lines represent the security mechanisms:

EUIC: mechanism for enhanced user identity confidentiality (optional, between user and HE);

UIC: conventional mechanism for user identity confidentiality (between user and serving network);

AKA: the mechanism for authentication and key agreement, including the functionality to trigger a re-authentication by the user, i.e., to control the access key pair lifetime;

DC: the mechanism for data confidentiality of user and signalling data;

DI: the mechanism for data integrity of signalling data;

DEC: the mechanism for network-wide data confidentiality.

In the remaining section of this specification we describe what data elements and functions need to be implemented in each of the above network elements for each of the above mechanisms and functions.

4.2 User services identity module

4.2.1 Void

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;
- 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.

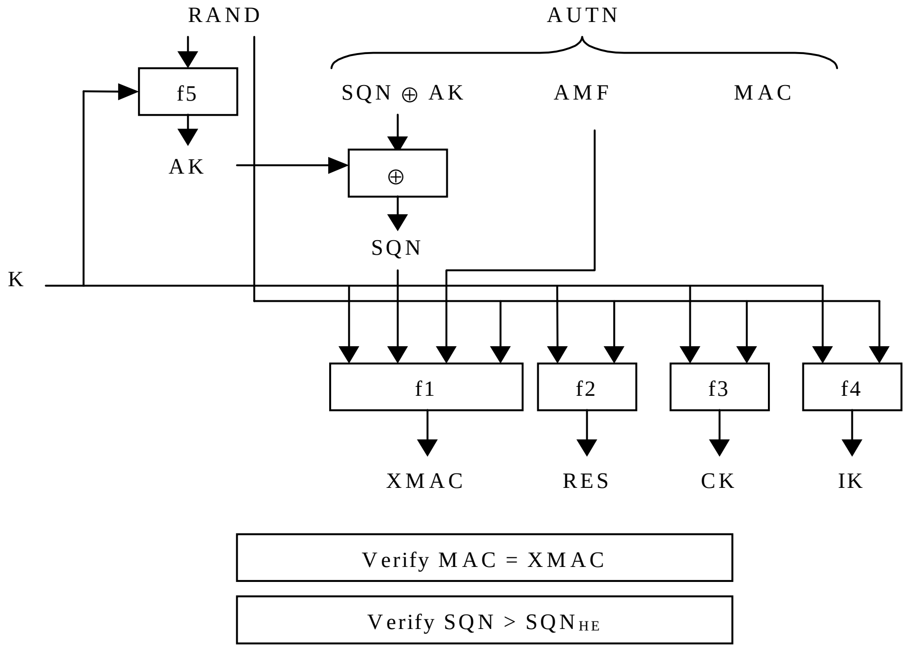


Figure 2: User authentication function in the USIM

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), 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-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.

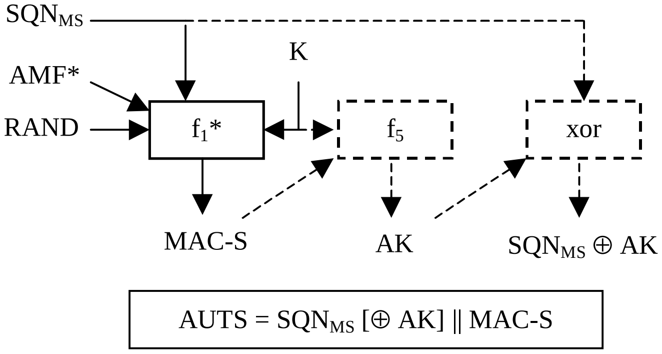


Figure 3: Generation of a token for re-synchronisation AUTS (note 1)

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	1	Permanent	Proprietary	Optional
c2 and c3	Conversion functions for interoperation with GSM	1 of each	Permanent	Standard	Optional

4.3 User equipment

4.3.1 User identity confidentiality (UIC$_{UE}$)

The UE shall support the UMTS conventional mechanism for user identity confidentiality described in 6.1 of 3G TS 33.102.

The UE shall store the following data elements:

- TMUI-CS: a temporary identity allocated by the CS core network;
- LAI: a location area identifier;
- the TMUI-PS: a temporary identity allocated by the PS core network;
- the RAI: a routing area identifier

Table 5: UE – User Identity Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
TMUI-CS	Temporary user identity	1 per user	Updated when TMUI allocation protocol is executed by CS core network	As per GSM TMSI	Mandatory
LAI	Location area identity	1 per user	Updated when TMUI allocation protocol is executed by CS core network		Mandatory
TMUI-PS	Temporary user identity	1 per user	Updated when TMUI allocation protocol is executed by PS core network		Mandatory
RAI	Routing area identity	1 per user	Updated when TMUI allocation protocol is executed by PS core network		Mandatory

4.3.2 Data confidentiality (DC$_{UE}$)

The UE shall support the UMTS mechanism for confidentiality of user and signalling data described in 6.6 of 3G TS 33.102.

The UE shall store the following data elements:

a) UEA-MS: the ciphering capabilities of the UE;

b) CK: the cipher key;

c) UEA: the selected ciphering function;

In addition, when in dedicated mode:

d) COUNT-C$_{UP}$: a time varying parameter for synchronisation of ciphering for the uplink;

e) COUNT-C$_{DOWN}$: a time varying parameter for synchronisation of ciphering for the downlink;

f) BEARER: a logical channel identifier;

g) DIRECTION: An indication of the direction of transmission uplink or downlink to ensure a different cipher is applied.

Table 6 provides an overview of the data elements stored on the UE to support the mechanism for data confidentiality:

Table 6: UE – Data Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UEA-MS	Ciphering capabilities of the UE	1 per UE	Permanent	16 bits	Mandatory
CK	Cipher key	1 per mode	Updated at execution of AKA protocol	128 bits	Mandatory
UEA	Selected ciphering capability	1 per UE	Updated at connection establishment	4 bits	Mandatory
COUNT-C_{UP}	Time varying parameter for synchronisation of ciphering	1 per logical channel	Lifetime of a logical channel	32 bits	Mandatory
COUNT-C_{DOWN}	Time varying parameter for synchronisation of ciphering	1 per logical channel	Lifetime of a logical channel	32 bits	Mandatory
BEARER	Logical channel identifier	1 per logical channel	Lifetime of a logical channel	8 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per logical channel	Lifetime of a logical channel	1 bit	Mandatory

The following cryptographic functions shall be implemented on the UE:

- f8: access link encryption function (note 1).
- c4: Conversion function for interoperation with GSM from Kc (GSM) to CK (UMTS).

NOTE 1: The security architecture TS 33.102 refers to UEA , f8 is a specific implementation of UEA as defined in Cryptographic algorithm requirements TS 33.105.

Table 7 provides an overview of the cryptographic functions implemented on the UE to support the mechanism for data confidentiality.

Table 7: UE – Data Confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f8	Access link encryption function	1-16	Permanent	Standardised	One at least is mandatory
c4	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional

4.3.3 Data integrity (DI_{UE})

The UE shall support the UMTS mechanism for integrity of signalling data described in 6.4 of 3G TS 33.102.

The UE shall store the following data elements:

a) UIA-MS: the integrity capabilities of the UE.

In addition, when in dedicated mode:

b) UIA: the selected UMTS integrity algorithm;

c) IK: an integrity key;

d) COUNT-I_{UP}: a time varying parameter for synchronisation of data integrity in the uplink direction;

e) COUNT-I_{DOWN}: a time varying parameter for synchronisation of data integrity in the downlink direction;

f) DIRECTION An indication of the direction of transmission uplink or downlink to ensure a different cipher is applied;

g) FRESH: a network challenge;

Table 8 provides an overview of the data elements stored on the UE to support the mechanism for data confidentiality:

Table 8: UE – Data Integrity – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UIA-MS	Ciphering capabilities of the UE	1 per UE	Permanent	16 bits	Mandatory
UIA	Selected ciphering capability	1 per UE	Updated at connection establishment	4 bits	Mandatory
IK	Integrity key	1 per mode	Updated by the execution of the AKA protocol	128 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per logical channel	Lifetime of a logical channel	1 bit	Mandatory
COUNT-I_{UP}	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
COUNT-I_{DOWN}	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
FRESH	Network challenge	1	Lifetime of a connection	32 bits	Mandatory
MAC-I XMAC-I	Message authentication code	1	Updated by the execution of the AKA protocol	32 bits	Mandatory

The following cryptographic functions shall be implemented on the UE:

- f9: access link integrity function (note 1).
- c5: Conversion function for interoperation with GSM Kc (GSM) > IK (UMTS)

NOTE 1: The security architecture TS 33.102 refers to UIA, f9 is a specific implementation of UIA as defined in Cryptographic algorithm requirements TS 33.105.

Table 9 provides an overview of the cryptographic functions implemented in the UE:

Table 9: UE – Data Integrity – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f9	Access link data integrity function	1-16	Permanent	Standardised	One at least is mandatory
c5	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional

4.3.4 Void

4.4 Radio network controller

4.4.1 Data confidentiality (DC$_{rnc}$)

The RNC shall support the UMTS mechanism for data confidentiality of user and signalling data described in 6.6 of 3G TS 33.102.

The RNC shall store the following data elements:

a) UEA-RNC: the ciphering capabilities of the RNC;

In addition, when in dedicated mode:

b) UEA: the selected ciphering function;

c) CK: the cipher key;

d) COUNT-C$_{UP}$: a time varying parameter for synchronisation of ciphering for the uplink;

e) COUNT-C$_{DOWN}$: a time varying parameter for synchronisation of ciphering for the downlink;

f) DIRECTION: An indication of the direction of transmission uplink or downlink to ensure a different cipher is applied

g) BEARER: a logical channel identifier.

Table 10 provides an overview of the data elements stored in the RNC to support the mechanism for data confidentiality:

Table 10: RNC – Data Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UEA-RNC	Ciphering capabilities of the UE	1	Permanent	16 bits	Mandatory
UEA	Selected ciphering capability	1 per user and per mode	Updated at connection establishment	4 bits	Mandatory
CK	Cipher key	1 per user and per mode	Updated at connection establishment	128 bits	Mandatory
COUNT-C$_{UP}$	Time varying parameter for synchronisation of ciphering	1 per logical channel	Lifetime of a logical channel	32 bits	Mandatory
COUNT-C$_{DOWN}$	Time varying parameter for synchronisation of ciphering	1 per logical channel	Lifetime of a logical channel	32 bits	Mandatory
BEARER	Logical channel identifier	1 per logical channel	Lifetime of a logical channel	8 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per logical channel	Lifetime of a logical channel	1 bit	Mandatory

The following cryptographic functions shall be implemented in the RNC:

- f8: access link encryption function.

Table 11 provides an overview of the cryptographic functions that shall be implemented in the RNC:

Table11: RNC – Data integrity – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f9	Access link data integrity function	1-16	Permanent	Standardised	One at least is mandatory

4.4.2 Data integrity (DI_{rnc})

The RNC shall support the UMTS mechanism for data integrity of signalling data described in 6.4 of 3G TS 33.102.

The RNC shall store the following data elements:

a) UIA-RNC: the integrity capabilities of the RNC;

In addition, when in dedicated mode:

b) UIA: the selected UMTS integrity algorithm;

c) IK: an integrity key;

d) COUNT-I_{UP}: a time varying parameter for synchronisation of data integrity in the uplink direction;

e) COUNT-I_{DOWN}: a time varying parameter for synchronisation of data integrity in the downlink direction;

f) DIRECTION An indication of the direction of transmission uplink or downlink to ensure a different cipher is applied;

g) FRESH: an MS challenge.

Table 12 provides an overview of the data elements stored on the UE to support the mechanism for data confidentiality:

Table12: UE – Data Integrity – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UIA-RNC	Data integrity capabilities of the RNC	1	Permanent	16 bits	Mandatory
UIA	Selected data integrity capability	1 per user	Lifetime of a connection	4 bits	Mandatory
IK	Integrity key	1 per user	Lifetime of a connection	128 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per logical channel	Lifetime of a logical channel	1 bit	Mandatory
COUNT-I_{UP}	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
COUNT-I_{DOWN}	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
FRESH	MS challenge	1	Lifetime of a connection	32 bits	Mandatory
MAC-I XMAC-I	Message authentication code	1	Updated by the execution of the AKA protocol	32 bits	Mandatory

The following cryptographic functions shall be implemented on the UE:

- f9: access link integrity function.

Table 13 provides an overview of the cryptographic functions implemented in the UE:

Table 13: UE – Data Integrity – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f9	Access link data integrity function	1-16	Permanent	Standardised	One at least is mandatory

4.5 SN (or MSC/VLR or SGSN)

4.5.1 User identity confidentiality (UIC$_{SN}$)

The VLR (equivalently the SGSN) shall support the UMTS conventional mechanism for user identity confidentiality described in 6.1 of 3G TS 33.102.

The VLR shall store the following data elements:

- TMUI-CS: a temporary identity allocated by the CS core network;
- LAI: a location area identifier;

Table 14: VLR – User Identity Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
TMUI-CS	Temporary user identity	2 per user	Updated when TMUI allocation protocol is executed by CS core network		Mandatory
LAI	Location area identity	2 per user	Updated when TMUI allocation protocol is executed by CS core network		Mandatory

Equivalently, the SGSN shall store the following data elements:

- TMUI-PS: a temporary identity allocated by the PS core network;
- RAI: a routing area identifier.

Table 15: SGSN – User Identity Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
TMUI-PS	Temporary user identity	1 per user	Updated when TMUI allocation protocol is executed by PS core network		Mandatory
RAI	Routing area identity	1 per user	Updated when TMUI allocation protocol is executed by PS core network		Mandatory

4.5.2 Void

4.5.3 Authentication and key agreement (AKA_{SN})

The VLR (equivalently the SGSN) 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 VLR (and SGSN):

a) AV: Authentication vectors;

Table 16 provides an overview of the composition of an authentication vector

Table 16: Composition of an authentication vector

Symbol	Description	Multiplicity	Length
RAND	Network challenge	1	128
XRES	Expected response	1	32-128
CK	Cipher key	1	128
IK	Integrity key	1	128
AUTN	Authentication token	1 that consists of:	128
SQN or SQN ⊕ AK	Sequence number or Concealed sequence number	1 per AUTN	48
AMF	Authentication Management Field	1 per AUTN	16
MAC-A	Message authentication code for network authentication	1 per AUTN	64

b) KSI: Key set identifier;

c) CK: Cipher key;

d) IK: Integrity key;

e) GSM AV: Authentication vectors for GSM.

Table 17 provides an overview of the data elements stored in the VLR/SGSN to support authentication and key agreement.

Table 17: VLR/SGSN – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UMTS AV	UMTS Authentication vectors	several per user, SN dependent	Depends on many things	528-640	Mandatory
KSI	Key set identifier	1 per user	Updated when AKA protocol is executed	3 bits	Mandatory
CK	Cipher key	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
GSM AV	GSM Authentication vectors	As for GSM	As for GSM	As for GSM	Optional

The following cryptographic functions shall be implemented in the VLR/SGSN:

- c4: Conversion function for interoperation with GSM from Kc (GSM) to CK (UMTS);
- c5: Conversion function for interoperation with GSM from Kc (GSM) to IK (UMTS).

Table 18 provides an overview of the cryptographic functions implemented on the UE to support the mechanism for data confidentiality.

Table 18: VLR/SGSN Authentication and Key Agreement – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
c4	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional
c5	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional

4.6 Home location register / Authentication centre

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.

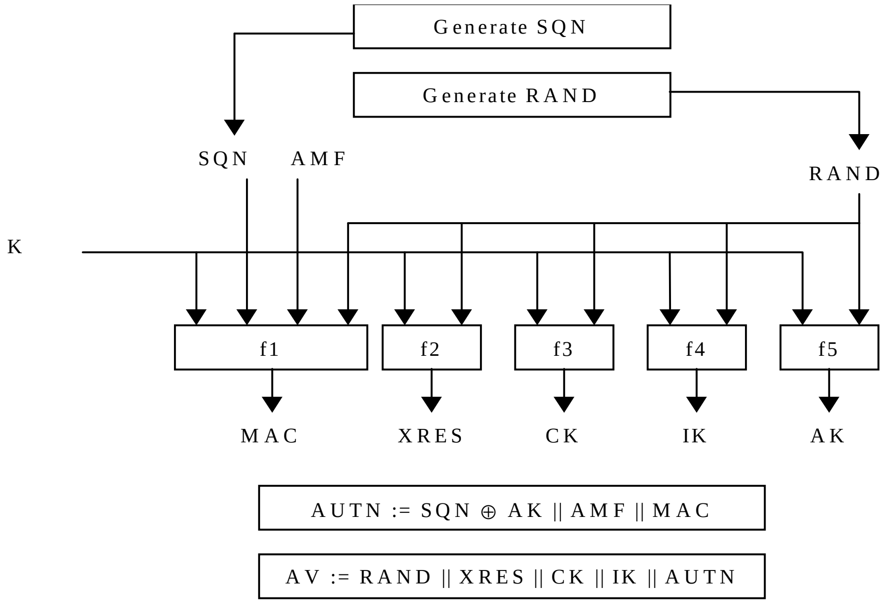

Generate SQN
Generate RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figure 4: 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;
- 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	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

4.7 Void

5 Void

6 ~~Network Wide Confidentiality~~Void

~~Network-wide confidentiality is an option, which provides a protected mode of transmission on user traffic channels across the entire network. This gives users assurance that their traffic is protected against eavesdropping on every link within the network, i.e. not just the particularly vulnerable radio links in the access network, but also on the fixed links within the core network.~~

~~Network-wide confidentiality is provided by protecting transmissions on user traffic channels, using a synchronous stream cipher. This uses the same algorithm as for access link encryption.~~

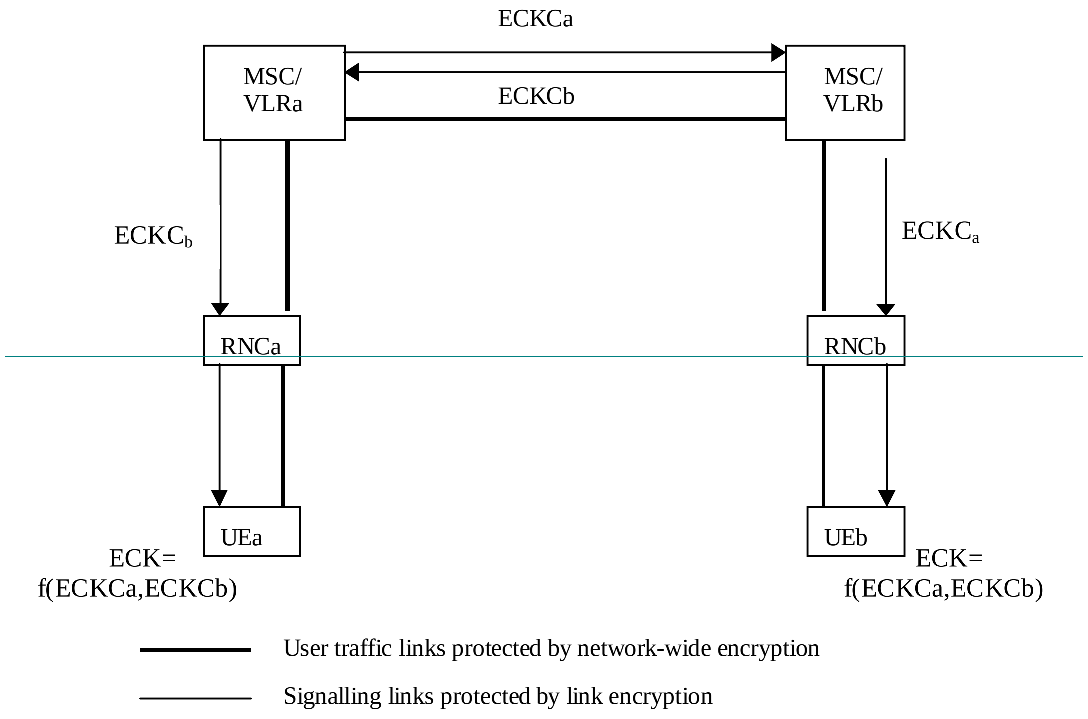
~~The key management scheme for network-wide encryption involves establishing a network-wide cipher key between the end points of the traffic channel. In addition to the access link cipher and integrity keys, the USIM and the MSC/VLR or equivalent SGSN also establish a network-wide cipher key component ECKC as part of the authentication and key agreement procedure. This key component will be used to generate the network-wide cipher key ECK.~~

~~Since this ECK can also be generated by MSC/VLRa or MSC/VLRb and then used by decryption facilities in the core network, the requirement for lawful interception is satisfied.~~

1) ~~MSC/VLRa and MSC/VLRb shall exchange network-wide cipher keys components for UEa and UEb. MSC/VLRa passes ECKCb to UEa, while MSC/VLRb passes ECKCa to UEb.~~

2) ~~At each end the access link key is transmitted to the UE over signalling channels which are protected using the access link cipher keys CK.~~

3) ~~When each UE has received the other party's network-wide cipher key component, the network-wide cipher key ECK shall be calculated as a function of ECKCa and ECKCb.~~


ECKCa
MSC/ VLRa
ECKCb
MSC/ VLRb
ECKC$_b$
ECKC$_a$
RNCa
RNCb
UEa
UEb
ECK= f(ECKCa,ECKCb)
ECK= f(ECKCa,ECKCb)
User traffic links protected by network-wide encryption
Signalling links protected by link encryption

~~Table 24: MSC/VLR Network Wide Confidentiality – Data Elements~~

~~Symbol~~	~~Description~~	~~Multiplicity~~	~~Lifetime~~	~~Length~~	~~Mandatory / Optional~~
~~ECKC~~	~~Network-wide cipher key component for UE~~	~~1 per user~~	~~Updated when AKA protocol is executed~~	~~128 bits~~	~~Optional~~
~~ECKCpeer~~	~~Network-wide cipher key component for peer UE~~	~~1 per user~~	~~Updated when AKA protocol is executed~~	~~128 bits~~	~~Optional~~
~~ECK~~	~~the network-wide cipher key~~	~~1 per user~~	~~When required for Lawful Interception purposes~~	~~128 bits~~	~~Optional~~

~~Table 25: UE Network Wide Confidentiality – Data Elements~~

~~Symbol~~	~~Description~~	~~Multiplicity~~	~~Lifetime~~	~~Length~~	~~Mandatory / Optional~~
~~ECKC~~	~~Network-wide cipher key component for UE~~	~~1 per user~~	~~Updated when network wide traffic channel is established~~	~~128 bits~~	~~Optional~~
~~ECKCpeer~~	~~network-wide cipher key component for peer UE~~	~~1 per user~~	~~Updated when network wide traffic channel is established~~	~~128 bits~~	~~Optional~~
~~ECK~~	~~the network-wide cipher key~~	~~1 per user~~	~~Updated when network wide traffic channel is established~~	~~128 bits~~	~~Optional~~

~~Table 26: UE Network Wide Confidentiality - Cryptographic functions~~

~~Symbol~~	~~Description~~	~~Multiplicity~~	~~Lifetime~~	~~Standardised / Proprietary~~	~~Mandatory / Optional~~
~~f9~~	~~Network-wide user traffic confidentiality Algorithm~~	~~1~~	~~Permanent~~	~~Standardised~~	~~Mandatory~~

Annex A (informative): Change history

Change history					
TSG SA #	**Version**	**CR**	**Tdoc SA**	**New Version**	**Subject/Comment**
S_05	2.0.0	-	-	3.0.0	Approved at SA#5 and placed under TSG SA Change Control
S_06	3.0.0	001r1	SP-99586	3.1.0	Refinement of Enhanced User Identity Confidentiality
S_06	3.0.0	002r1	SP-99586	3.1.0	Corrections to figure 1
S_06	3.0.0	004	SP-99586	3.1.0	Change length of KSI (and other miscellaneous corrections)
S_07	3.1.0	005r2	SP-000075	3.2.0	Refinement EUIC (according to TS 33.102)
S_07	3.1.0	006	SP-000047	3.2.0	Alignment of integration Guidelines with Security Architecture
S_08	3.2.0	007	SP-000273	3.3.0	Removal of EUIC from 33.103
S_08	3.2.0	008	SP-000273	3.3.0	Removal of MAP Security from 33.103
S_08	3.2.0	009	SP-000271	3.3.0	SQN length
	3.3.0				Removal of Network Wide Confidentiality