3GPP TSG_CN#6 / SMG3 #6 NP-99468
Meeting #6, Nice, France
13th - 15th December 1999

Source: **SA2**

Title: **Re. LS on security issues in VHE/OSA**

Agenda item: **4.2**

Document for: **Information**

TSG SA2 #10 **Tdoc S2-99F07**
Abiko, Japan, 29 Nov - 3 Dec 1999

From: TSG SA WG2
To: TSG SA WG3, TSG CN and CN OSA ad-hoc

Response to Liaison Statement on security issues in VHE/OSA

TSG SA WG2 thanks TSG CN OSA for their Liaison statement **NP-OSA-99025/S2-99D54** relating to security requirements. The liaison stated that, "It is the understanding of TSG CN OSA ad-hoc that security requirements are covered within the framework service capability features and that no additional security requirements have been identified".

TSG SA WG2 would like to raise the following issue that relates to network and user security. Which is considered part of the open issue on authorization and administration of User Profile highlighted in the developing Stage 2 specification (TS 23.127).

The proposed OSA API provides to an Application, access to a Service Capability Server (SCSs). The authentication and authorization procedures of this API ensure that only verified applications gain access and that that access is only made available to the use of facilities and operations for which they have are authorized.

However in the current definition, there is a further level of security, which is not being addressed. There is, as yet, no mechanism specified for "authentication and authorization user access to the application and user specific data at the application". Having authorized an application to use a specific method, there is no control over how that method is used or for which particular data set its use would be valid.

The Points are highlighted:
1. Secure User Agent to Application End-to End authentication.
2. Secure User Authorization to the Application via secure access to User Profile Data, (to verify that the User has subscription rights to specific applications) and
3. The transfer of a Secure User Identity (and possibly signature) to the application, to ensure that the Application can secure access to the Appropriate internal data store at the Application/Application Server

Application Authentication to the User Agent (i.e. to make the UA to Application authentication mutual) also may be required dependent of the perceived security threats.

If not resolved, the lack of security between the UA and application could represent a significant breach of data confidentiality and also raise an issue of invasion of privacy. If OSA is specified for

Release ’99 without significant consideration for security and resource control, it could render the OSA application interface unusable.

SA2 requests that SA3 give guidance as to the re-use of the mechanisms defined in the Security Architecture (TS 33.103) under development and on the perceived need for Mutual Authentication between the UA and Application. The CN OSA ad-hoc are requested to note the requirement for the “UA to Application and User Data, Authentication and Authorization”, for which SA2 and SA3 are currently specifying the details. Also to consider the specification work is being developed in SA3 (attached in the copy to go to CN OSA ad-hoc).

Technical Specification Group Services and System Aspects
Meeting #5, Kyongju, Korea, 11-13 October 1999

TSGS#5(99)410

3G TS 33.103 V1.1.~~2~~3 (1999-10)

3GPP TSG SA WG3 meeting #6
Sophia Antipolis, 29 Sept. - 1 Oct, 1999

S3-99----_

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Integration Guidelines 3G TS 33.103 V 1.1.~~2~~3

Reference
DTS/TSGS-_____

Keywords
Security, Authentication and Key Agreement, Security Information Stored, Location of Security Functions, Parameter Lengths

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

Contents

Foreword

This document has been drafted by 3GPP TSG-SA WG 3, i.e., the Workgroup devoted to “Security” issues, within the Technical Specification Group devoted to “System Aspects”.

1 Scope

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

- Home Environment Authentication ~~Center~~Centre (HE/AuC)
- Serving Network Visited Location Register (SN/VLR)
- Radio ~~Node~~ 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 as follows:~~

~~Clause 5 list~~is a series of tables, which describe ~~s~~ 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. ~~in terms of Static information and Dynamic information.~~

~~Clause 6 defines the external specification of the security-related algorithms in terms of input and output parameters, and the parameter lengths.~~

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

2 References

References may be made to:

a) ~~specific~~Specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) ~~all~~All versions up to and including the identified version (identified by “up to and including” before the version identity); or

c) ~~all~~All versions subsequent to and including the identified version (identified by “onwards” following the version identity); or

d) ~~publications~~Publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security;

3G~~TR S3.03~~ Security Architecture 3G TS 33.102

2.2 Informative references

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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.

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.

3.2 Symbols

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

$\|\|$	Concatenation
$\oplus$	Exclusive or
f1	Message authentication function used to compute MAC
f1*	Message authentication function used to compute MACS
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
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:

3GMS	Third Generation Mobile Communication System
AK	Anonymity Key
AUTN	Authentication Token
AUTS	Authentication Token for Synchronisation
AV	Authentication Vector
CK	Cipher Key
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 toY
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption
ECK	Network Wide Cipher Key
ECKC	Network Cipher Key Component for UE
ECKCpeer	Network Cipher Key Component for peer UE
EMSI	Encrypted Subscriber identity
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	The message authentication code included in AUTN, computed using f1
MACS	The message authentication code included in AUTS, computed using f1*
MAC-I	Message authentication code for data integrity
MS	Mobile Station
MSC	Mobile Services Switching Centre
MT	Mobile Termination
NE_X	Network Element of Network X
PS	Packet Switched
RAND	Random challenge
$RAND_{ms}$	Random value stored on MS received during user authentication request
RND_X	Unpredictable Random Value generated by X
SEQ	Sequence number
SN	Serving Network
TE	Terminal Equipment
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
TVP	Time Variant Parameter
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UN	User Name
USIM	User Services Identity Module
VLR	Visited Location Register
X	Network Identifier
XMAC	Expected message authentication code for user authentication
XMAC-I	Expected message authentication code for data integrity
XRES	Expected Response
XUR	Expected User Response
Y	Network Identifier

~~3.1 Definitions~~

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

~~**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.~~
~~**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.~~

~~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~~
~~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~~

4 Access link security

4.1 Functional network architecture

Figure 1 shows the functional security architecture of UMTS.

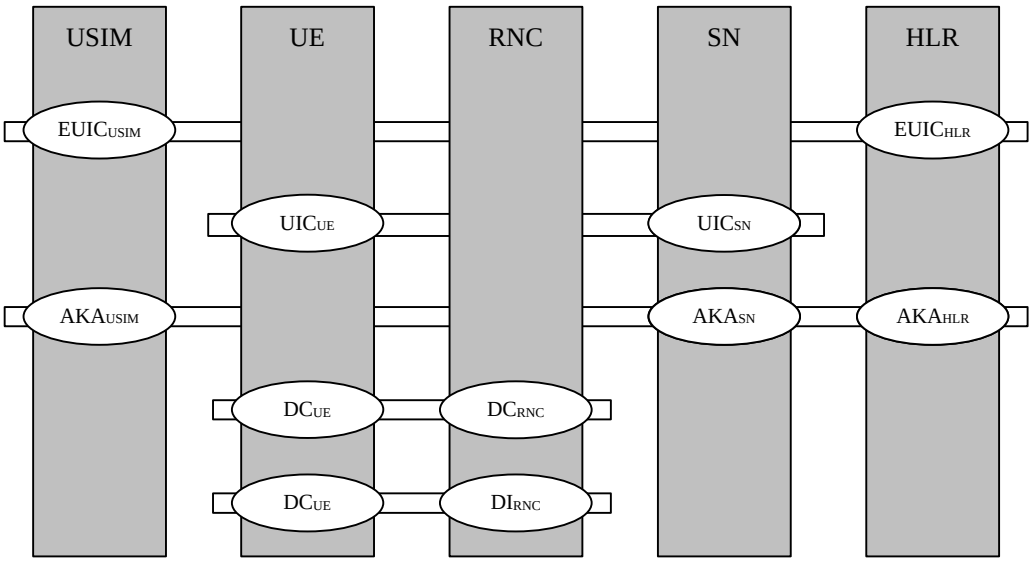


Figure 1: UMTS functional security architecture

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.

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 Enhanced User Identity Confidentiality ($EUIF_{USIM}$)

For UMTS users with EUIC, the USIM has to store additional data and have additional functions implemented to encrypt the permanent user identity (~~IMUI~~IMSI). We describe the requirements as regards data storage and algorithm implementation for an example mechanism in annex B of 3G TS 33.102.

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

a) $SQN_{UIC/MS}$: a counter that is equal to the highest SQN_{UIC} generated and sent by the USIM to the HE/AuC;

b) GK: the group key used to encrypt the ~~IMUI~~IMSI, SQN_{UIC} and the SQN_{MS} ;

Table 1: USIM – Enhanced User Identity Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
GK	Group key	1 per user group the user belongs to	Permanent	128[1] bits	Optional
$SQN_{UIC/MS}$	Counter	1 per user	Updated when protocol for EUIC is executed	32 bits	Optional
GMSI	Group Identity	1 per user	Permanent	32 bits	Optional

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

– f6: the user identity encryption function.

For a summary of the data elements and cryptographic function of the $EUIC_{HE}$ function see Table 2.

[1] the table entry is for the example secret key mechanism given in annex B of 33.102

Table 2: HLR/AuC – Enhanced User Identity Confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f6	User identity encryption function	1	Permanent	Proprietary	Optional

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) For the WINDOW option: an array of Boolean values over the interval [SQN_{MS} - w, SQN_{MS}), that indicate whether the USIM has accepted a certain sequence number in an AUTN parameter.

d) For the LIST option: an ordered list of the highest values that the USIM has received

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

f) KSI: key set identifier.

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

h) CK ~~UMTS~~The access link ~~C~~cipher ~~K~~key established as part of authentication

i) IK ~~UMTS~~The access link - ~~I~~integrity ~~K~~key established as part of authentication

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

k) AMF: A ~~16 bit~~16-bit field used Authentication Management. The use and format are unspecified in the architecture but examples are given in an informative annex. ~~containing, at a minimum, the authentication algorithm id and the identifier for K, for the window option, the window size and the PS or CS mode bit.~~

l) 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[2]	Permanent	128 bits	Mandatory
SQN_{MS}	Sequence number counter	1	Updated when AKA protocol is executed	32-64 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	4 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 protocol is executed~~Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	~~Mandatory~~Optional
SRES	GSM authentication parameter from conversion function	1	Updated when GSM AKA or UMTS AKA protocol is executed~~Updated when GSM AKA protocol is executed~~	As for GSM	~~Mandatory~~Optional

[2] HE policy may dictate more than one, the active key signalled using the AMF function

Kc	GSM cipher Key	1	Updated when GSM AKA or UMTS AKA protocol is executed~~GSM Updated when AKA protocol is executed~~	As for GSM	~~Mandatory~~Optional

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.
- C1 to C~~4~~2 : Conversion functions for interoperation with GSM (UMTS RES > GSM RES and UMTS CK IK > GSM Kc)

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

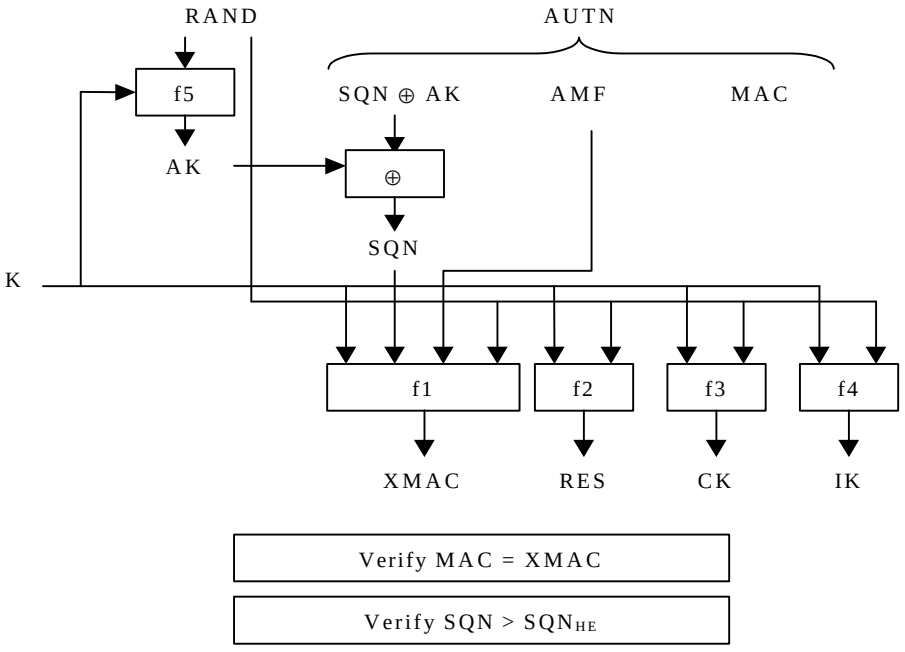


Figure 2: User authentication function in the USIM

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

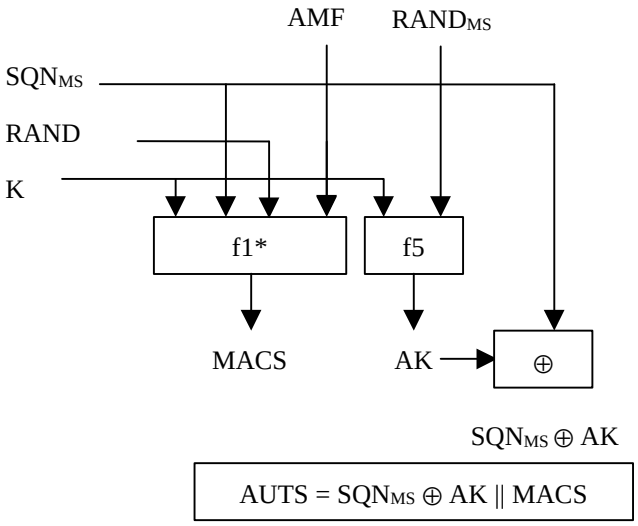


Figure 3: Generation of a token for re-synchronisation AUTS

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
C1 to C~~4~~2	Conversion functions for interoperation with GSM	1 of each	Permanent	Standard	~~Mandatory~~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;
- MASK-CS: a mask allocated by the CS core network to send SQN_{MS} to the network;
- the TMUI-PS: a temporary identity allocated by the PS core network;
- the RAI: a routing area identifier
- MASK-PS: a mask allocated by the PS core network to send SQN_{MS} to the network;

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
MASK-CS	Mask	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
MASK-PS	Mask	1 per user	Updated when TMUI allocation protocol is executed by PS core network		Mandatory

4.3.2 Data ~~confidentiality~~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.

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

Table 7: UE – Enhanced User Identity 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

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;

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

f) 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.

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

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:

Table 11: 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:

Table 12: 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 ~~Visited location register~~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;

– MASK-CS: a mask allocated by the CS core network to send SQN_{MS} and the window size w to the network.

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
MASK-CS	Mask	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

– MASK-PS: a mask allocated by the PS core network to send SQN_{MS} and the window size w to the network;

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
MASK-PS	Mask	1 per user	Updated when TMUI allocation protocol is executed by PS core network		Mandatory

4.5.2 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
SQN	Sequence number	1	32-64
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:	96-128
SQN ⊕ AK	Concealed sequence number	1 per AUTN	32-64
AMF	Authentication Management Field ~~(indicates the algorithm and key in use)~~	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	544-640	Mandatory
KSI	Key set identifier	1 per user	Updated when AKA protocol is executed	4 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

4.6 Home location register / Authentication centre

4.6.1 Enhanced User Identity Confidentiality ($EUIC_{HE}$)

For UMTS users with EUIC, the HLR/AuC has to store additional data and have additional function implemented to decrypt the permanent user identity (~~IMUI~~IMSI). We describe the requirements as regards data storage and algorithm implementation for the example mechanism in annex B of 3G TS 33.102.

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

a) $SQN_{UIC/HE}$: a counter that is equal to the highest SQN_{UIC} generated and sent by the USIM to the HLR/AuC;

b) GK: the group key used to decrypt the ~~IMUI~~IMSI, SQN_{UIC} the SQN_{MS} and the window size w;

Table 18: HLR/AuC –Enhanced User Identity Confidentiality –Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
GK	Group key	1 per user group	Permanent	128	Optional
$SQN_{UIC/HE}$	Counter	1 per user	Updated when protocol for EUIC is executed	32	Optional

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

– f7: the user identity decryption function.

For a summary of the data elements and cryptographic function of the $EUIC_{HE}$ function see Table 2.

Table 19: HLR/AuC – Enhanced User Identity Confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f7	User identity decryption function	1	Permanent	Proprietary	Optional

4.6.2 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 20 provides an overview of the data elements stored on the HLR/AuC to support authentication and key agreement.

Table 20: 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	32-64 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~~ Optional
RAND	GSM Random challenge			128 bits	Optional
SRES	GSM Expected response			32 bits	Optional
Kc	GSM cipher key			64 bits	Optional

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

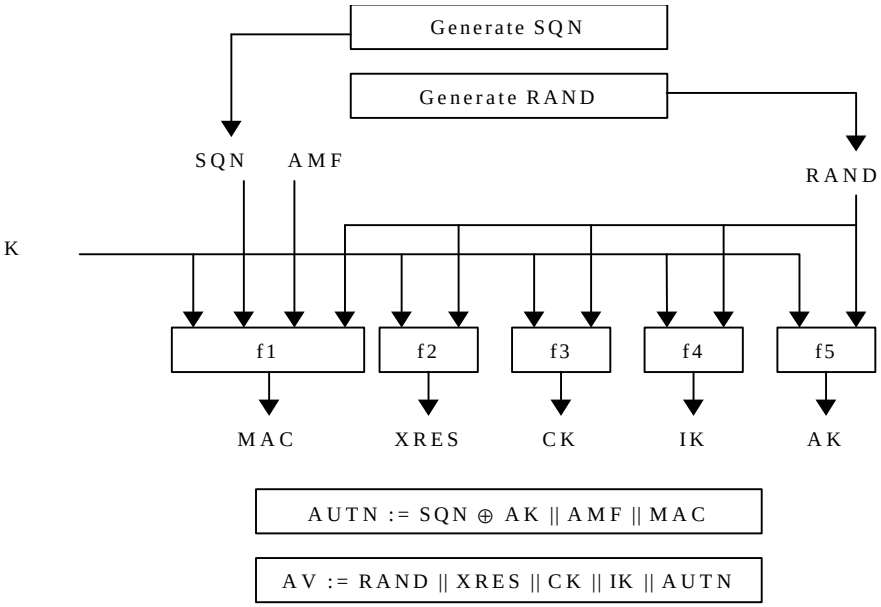


Figure 4: Generation of an authentication vector

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.

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

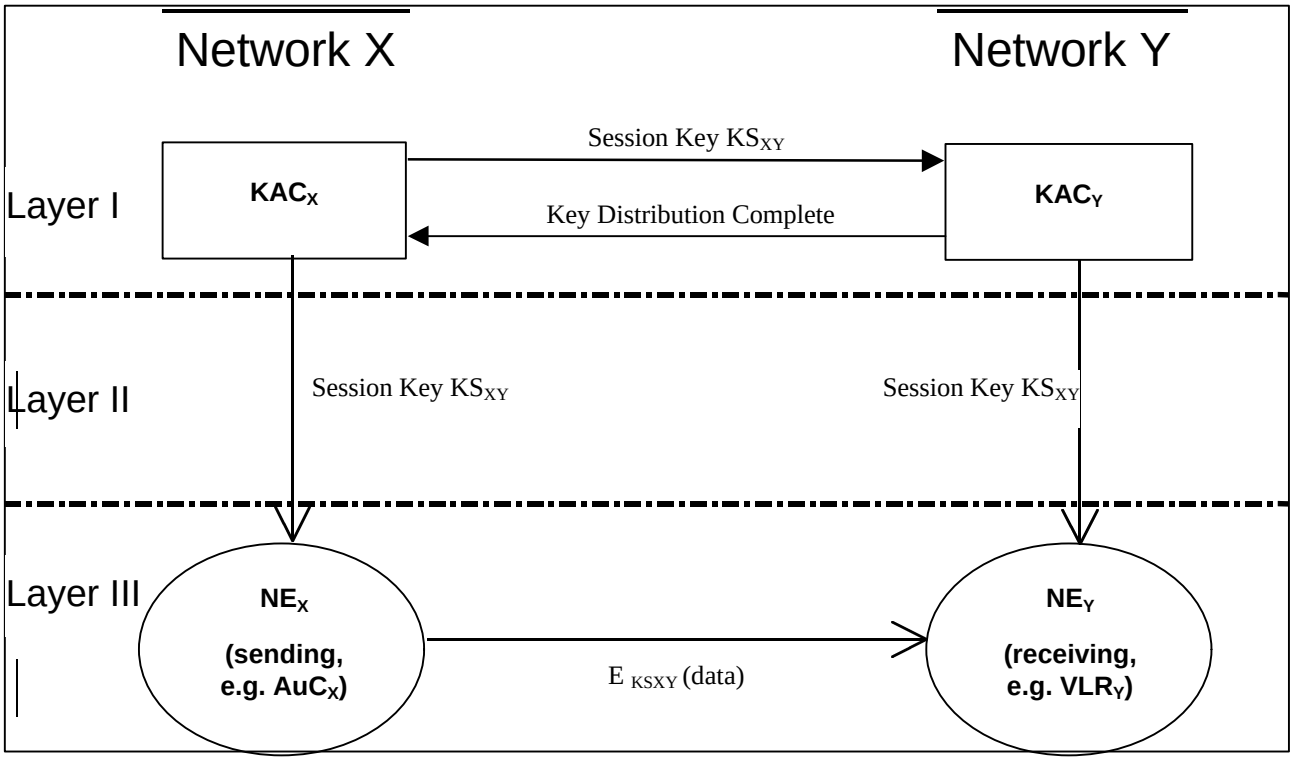
Table 21: HLR/AuC ~~-~~Authentication and key agreement ~~-~~Cryptographic functions

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 to C42	Functions for converting UMTS AV's to GSM AV's	1 for each	Permanent	Standard	Optional

5 Provider domain security

5.1 Functional security architecture



Overview of Proposed Mechanism

This mechanism establishes a secure signalling links between network nodes, in particular between SN/VLRs and HE/AuCs. Such procedures may be incorporated into the roaming agreement establishment process.

A secret key transport mechanism based on an asymmetric crypto-system i used to agree on a symmetric session key for each direction of communication between two networks X and Y.

The party wishing to send sensitive data initiates the mechanism and chooses the symmetric session key it wishes to use for sending the data to the other party. The other party shall choose a symmetric session key of its own, used for sending data in the other direction. This second key shall be transported immediately after the first key has been successfully transported. The session symmetric keys are protected by asymmetric techniques. They are exchanged between certain elements called the *Key Administration Centres* (KACs) of the network operators X and Y.

Transport of Session Keys

In order to establish a symmetric session key with version no. i to be used for sending data from X to Y, the KAC_X sends a message containing the following data to the KAC_Y:

$$E_{PK(Y)}\{X||Y||i||KS_{XY}(i)||RND_X||Text1||D_{SK(X)}(Hash(X||Y||i||KS_{XY}(i)||RND_X||Text1))||Text2\}||Text3$$

After having successfully distributed the symmetric session key received by network X to its own network entities, network Y sends to X a Key Distribution Complete Message. This is an indication to KAC_X to start with the distribution of the key to its own entities, which can then start to use the key immediately.

The message takes the form

$$KEY\_DIST\_COMPLETE||Y||X||i||RND_Y||D_{SK(Y)}(Hash(KEY\_DIST\_COMPLETE||Y||X||i||RND_Y)$$

where i indicates the distributed key and RND_Y is a random number generated by Y. The digital signature is appended for integrity and authenticity purposes. Y includes RND_Y to make sure that the message contents determined by X will be modified before signing.

Since most of the signalling messages to be secured are bidirectional in character, immediately after successful completion the procedure described here shall be repeated, now with Y choosing a key $KS_{YX}(i)$ to be used in the reverse direction, and X being the receiving party. Thereby keys for both directions are established.

5.2 Key Authentication Centre

Details in security architecture to be finalised

5.3 Core network entities

Table 22 Signalling Protection- Data Elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
PVTK s	Network's own Private Key (signing)	1	According to roaming agreement	< or = 2048 bits	Mandatory
PVTK d	Network's own Private Key (decryption)	1	According to roaming agreement	< or = 2048 bits	Mandatory
$PUBKv_1$	PKR_1 Public Key for network #1 (~~verfiy~~verify)	1 per roaming agreement	According to roaming agreement	< or = 2048 bits	Mandatory

$PUBKe_1$	PKR_1 Public Key for network #1 (encryption)	1 per roaming agreement	According to roaming agreement	< or = 2048 bits	Mandatory
$KS_{XY}(i)$	Symmetric Send Key #i for sending data from X to Y	1 per session	According to roaming agreement	128 bits	Mandatory
KS_{YX} (j)	Symmetric Send Key #j for sending data from Y to X	1 per session	According to roaming agreement	128 bits	Mandatory
I	Session key Sequence Number (for sending data from X to Y)	1 per session	According to roaming agreement	32 – 64 bits	Mandatory
J	Session key Sequence Number (for sending data from Y to X)	1 per session	According to roaming agreement	32 – 64 bits	Mandatory
RND_X	Unpredictable Random Value generated by X	1 per session	Session	128 bits	Mandatory
RND_y	Unpredictable Random Value generated by Y	1 per session	Session	128 bits	Mandatory

Table 23 Signalling Protection ~~C~~ryptographic Functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
BEANO	BLOCK ENCRYPTION ALGORITHM FOR NETWORK OPERATORS	1	Permanent	Standardised	Mandatory

6 Network Wide Confidentiality

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~~, using a synchronous stream ~~cipher which~~cipher. This ~~*may*[3]~~ use~~s~~ the same algorithm ~~UEA~~ as for access link encryption ~~and network-wide encryption~~.

~~If network-wide confidentiality of user traffic is provided, then access link confidentiality of user traffic between UE and RNC is replaced with the network-wide service.~~

~~Access link confidentiality of signalling information and user identity between UE and RNC is applied regardless of whether or not the network-wide user traffic confidentiality service is applied.~~

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 ~~also~~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 ~~be also~~ 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.

~~[3] This is FFS and a check needs to be made that the UEA specification reflects this~~

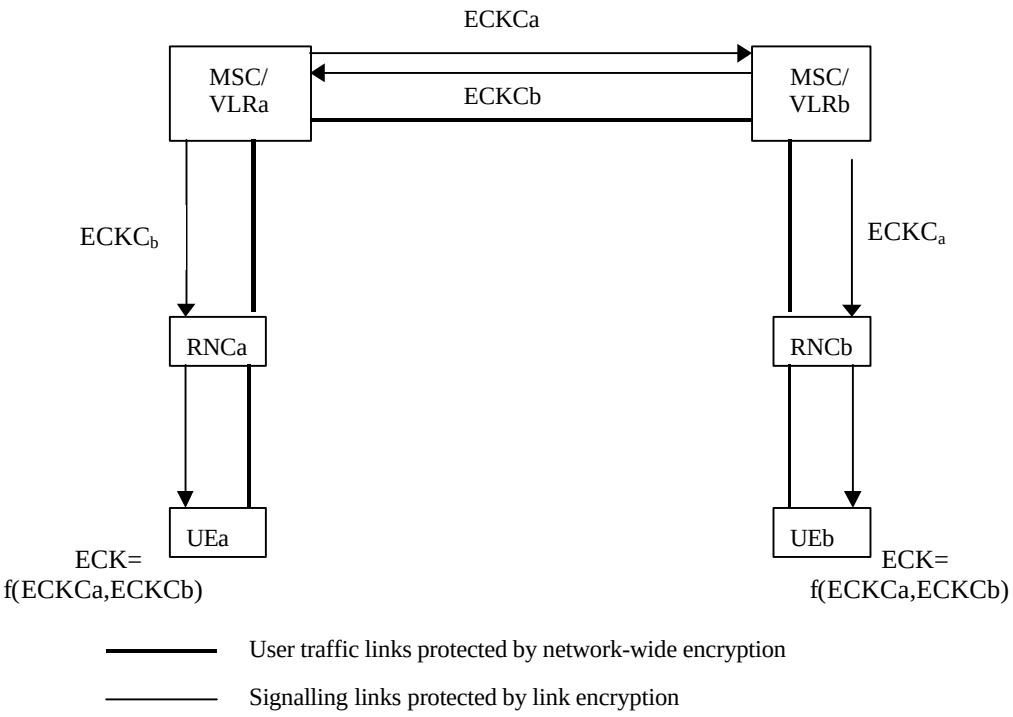

ECKCa
MSC/
VLRa
ECKCb
MSC/
VLRb
ECKC$_b$
ECKC$_a$
RNCa
RNCb
UEa
UEb
ECK=
f(ECKCa,ECKCb)
ECK=
f(ECKCa,ECKCb)
User traffic links protected by network-wide encryption
Signalling links protected by link encryption

Table 24 MSC/VLR Network Wide Confidentiality ~~-~~Data Elements

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

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

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

Annex A: Authentication mechanism based on a temporary key

When the mobile first requests service from the SN/VLR, a random seed RSu created by the user (USIM or terminal) is included in the request message. The message including RSu is forwarded to the HE/AuC, which generates its own random challenge RSn. An authentication vector is returned to the SN/VLR. The vector contains {RSn, RES1, XRES2, KT}, where RES1 is the response to the user's challenge, XRES2 is the response to the network's challenge which is expected from the user, and KT is the temporary authentication key shared with the SN/VLR. The network's challenge RSn and the network authentication response RES1 are sent to the MS. If the MS verifies RES1, thereby authenticating the identity of the network, it responds with RES2 and generates the new temporary key KT. The SN/VLR then verifies that RES2 equals XRES2, thereby authenticating the identity of the USIM, and stores the new temporary key KT. Furthermore, both the USIM and the SN/VLR immediately use KT with the random seeds RSu and RSn to generate the first session keys CK and IK. This process is shown in Figure 4 below.

Figure 5 shows how the SN/VLR can offer secure service to the USIM without reference to the home system HE/AuC by using the temporary key KT.

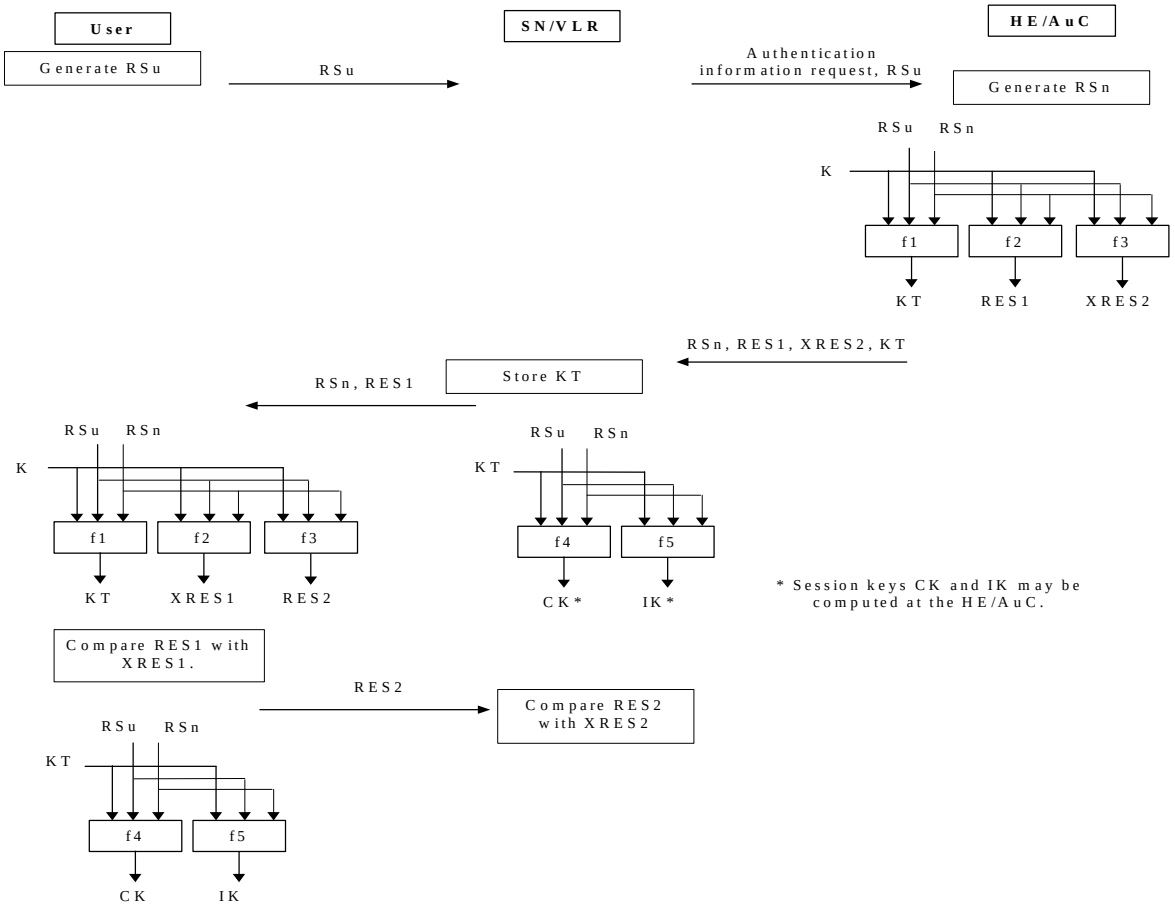


Figure 4: Temporary Key Generation Protocol

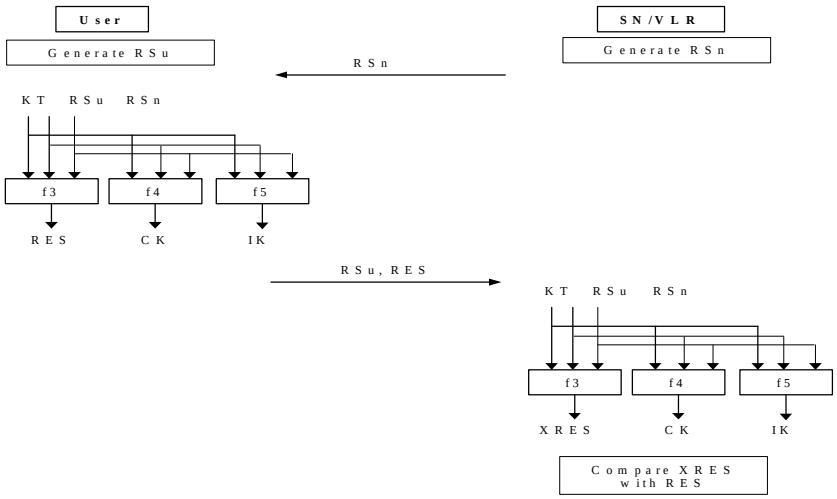


Figure 5. Locally authenticated session key agreement

A1 Security Information stored

A1.1 Home Environment Authentication Centre HE/AuC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Dynamic Information			
Random Seed User	RS_U	128 bits	c
AV_1Random Seed Network	RS_N	128 bits	c
Response to User Challenge RS_U	RES1	32-128 bits	c
Response to User Challenge RS_N	XRES2	32-128 bits	c
Temporary Key	KT	128 bits	b
AVn Random Seed Network	RS_N	128 bits	c
Response to User Challenge RS_U	RES1	32-128 bits	c
Expected Response to Nwk Challenge RS_N	XRES2	32-128 bits	c
Temporary Key	KT	128 bits	b
Fixed Initial Value	PAR1	TBD	a
Fixed Initial Value	PAR2	TBD	a
Fixed Initial Value	PAR3	TBD	a
Fixed Initial Value	PAR4	TBD	a
Fixed Initial Value	PAR5	TBD	a
- and common items – section 5.1			

A1.2 Serving Node Visited Location Register SN/VLR

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
Dynamic Information			
Temporary Key	KT	128 bits	b
Random Seed User	RS_U	128 bits	c
Random Seed Network	RS_N	128 bits	c
Response to Users Challenge	RES1	32-128 bits	c
Response to Network Challenge	RES2	32-128 bits	b
Response to Network Challenge	XRES2	32-128 bits	b
Cipher Key	CK*	128 bits	b
Integrity Key	IK*	128 bits	b
Response to SN/VLR challenge (local)	RES	32-128 bits	c
Expected response to challenge	XRES	32-128 bits	C

* May be computed at HE/AuC

A1.3 Radio Node Controller RNC

Name	**Symbol**	**Parameter Length (actual or min-max)**	**Lifetime**
See common items – section 5.1			

A1.4 USIM

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
Dynamic Information			
Temporary Key	KT	128 bits	B
Random Seed User	RS_U	128 bits	c
Random Seed Network	RS_N	128 bits	c
Computed Response (local authent.)	RES	32-128 bits	B
Response to Users Challenge	RES1	32-128 bits	B
Response to Network Challenge	RES2	32-128 bits	c
Expected response to network challenge	XRES1	32-128 bits	c
- and common items – section 5.1			

A1.5 Mobile Equipment

Name	Symbol	Parameter Length (actual or min-max)	Lifetime
See common items – section 5.1			

A2 Location of Security Functions

A2.1 Home Environment Authentication Centre HE/AuC

Name	**Symbol**	**Input Parameters**
Algorithms		
Key Generating Function	F1	Input: K, RS_U, RS_N Output: KT
Message Authentication Function	F2	Input: K, RS_U, RS_N Output: RES1
Message Authentication Function	F3	Input: K, RS_U , RS_N Output: XRES1
-and common items		

A2.2 Serving Node Visited Location Register SN/VLR

Name	**Symbol**	**Input Parameters**
Algorithms		* May be computed at HE/AuC
Message Authentication Function (local authentication only)	F3	Input: KT, RS_U, RS_N Output: XRES
Cipher Key Generating Function	F4	Input: KT, RS_U, RS_N Output: CK*
Integrity Key Generating Function	F5	Input: KT, RS_U,RS_N Output: IK*
and common items		

A2.3 Radio Node Controller RNC

Name	**Symbol**	**Input Parameters**
Algorithms		
See common items		

A2.4 Mobile Equipment user identity Module USIM

Name	**Symbol**	**Input Parameters**
Algorithms		
Key generating function	F1	Input: K, RS_U, RS_N Output: KT
Message Authentication Function	F2	Input: K, RS_U, RS_N Output: XRES1
Message Authentication Function	F3	Input: K, RS_U, RS_N Output: RES2
Message Authentication Function (for local authentication)	F3	Input: KT, RS_U, RS_N Output: RES
Cipher Key Generating Function	F4	Input: KT, RS_U, RS_N Output: CK
Integrity Key Generating Function	F5	Input: KT, RS_U RS_N Output: IK

A2.5 Mobile Equipment ME

Name	Symbol	**Input Parameters**
Algorithms		
see common items		

Annex B: Document history

Document history		
0.0.0	2nd May 1999	Initial draft: Rapporteur- Colin Blanchard
0.0.1	28th May 1999	After review at TSG SA WG3 #3 Bonn 11- 12th May 1999
0.0.2	11th June 1999	To incorporate comments from Takeshi Igarashi, Adam Berenzweig, Benno Tietz, Takeshi Chikazawa
0.0.3	18th June 1999	After review at TSG SA WG3#4 London 16th –18th June 1999
1.0.0	21st June 1999	Version for information at SA#4
1.1.0	6th August 1999	After review at SA3# with additions from BV and incorporating comments from AB and TW
1.1.1	26th September 99	Incorporating comments from Peter Howard
1.1.2	01 October 99	After review at SA3 no.6 incorporating CR.'s for • Authentication Management Field • GSM UMTS Interoperation conversion functions • COUNT-I, COUNT-C DIRECTION etc • Network Wide Confidentiality • MAP Security • MAC-I 32 bits
1.1.3	6th October 99	Comments from Nigel Barnes and Peter Howard incorporated