Chapter 8
Integration of Cryptographic Algorithms with Communication Protocols

8.1 Introduction: This chapter describes the integration guidelines of 3G security elements with network architecture as specified by 3GPP. The elements of the 3G-security architecture can be integrated into Home Environment /Authentication Centre (HE/AuC), Serving Network Visitor Location Register (VLR/SGSN) ,Radio Network Controller (RNC), Mobile station User Identity Module (UIM) and Mobile Equipment (ME). We first describe Technical Specifications 3GPP TS 33.103 V 4.2.0 (Release 4) and at the end we discuss the cryptographic algorithms' integration with network entities and communication protocols associated with these entities.

8.2 Functional network architecture

Figure 8.1 shows the functional security architecture of UMTS.

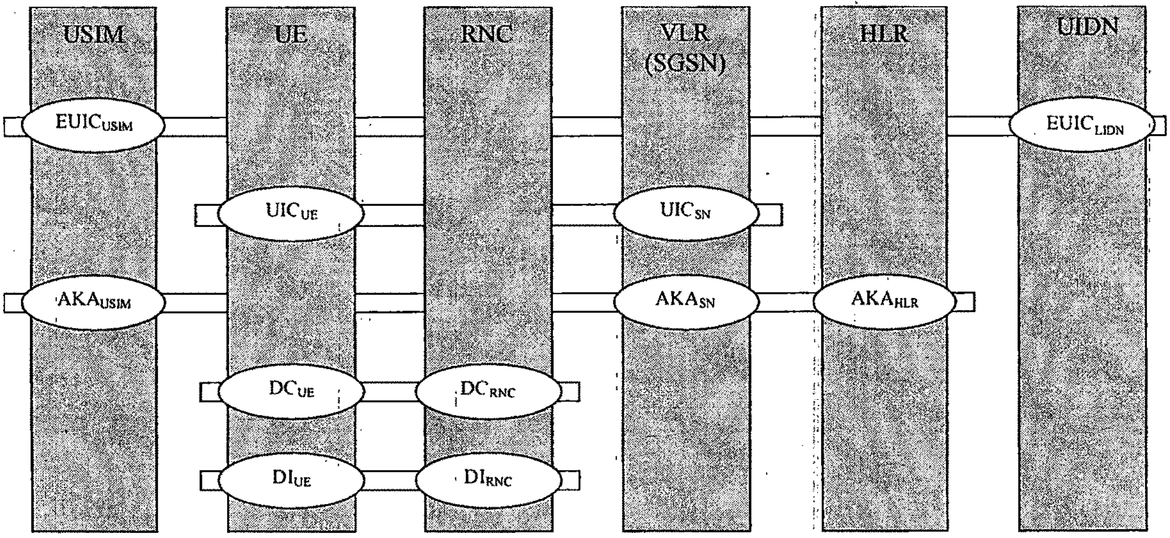

Figure 8.1: UMTS functional security architecture

The vertical bars represent the network elements and the horizontal lines represent the security mechanisms:

8.3 USIM 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: 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.

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

Table 8.1 provides an overview of the data elements stored on the USIM to support authentication and key agreement.

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
K	Permanent secret key	1 (note 1)	Permanent	128 bits	Mandatory
SQN_{MS}	Highest previously accepted sequence number counter	1	Updated when AKA protocol is executed	48 bits	Mandatory
SQN_{MS}[ ] array	array of last accepted sequence number	1	Updated when AKA protocol is executed	at least 32 entries	Optional
$RAND_{MS}$	Random challenge received by the user.	1	Updated when AKA protocol is executed	128 bits	Mandatory
KSI	Key set identifier	2 (note 2)	Updated when AKA protocol is executed	3 bits	Mandatory
THRESHOLD	Threshold value for cipher key	1	Permanent	24 bits	Mandatory
CK	Cipher key	2 (note 2)	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	2 (note 2)	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
Kc	GSM cipher Key	2 (note 2)	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional

Table 8.1: USIM – Authentication and key agreement – Data elements

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

NOTE 2: one for circuit-switched domain, one for packet-switched domain.

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

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

Figure 8.2 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.

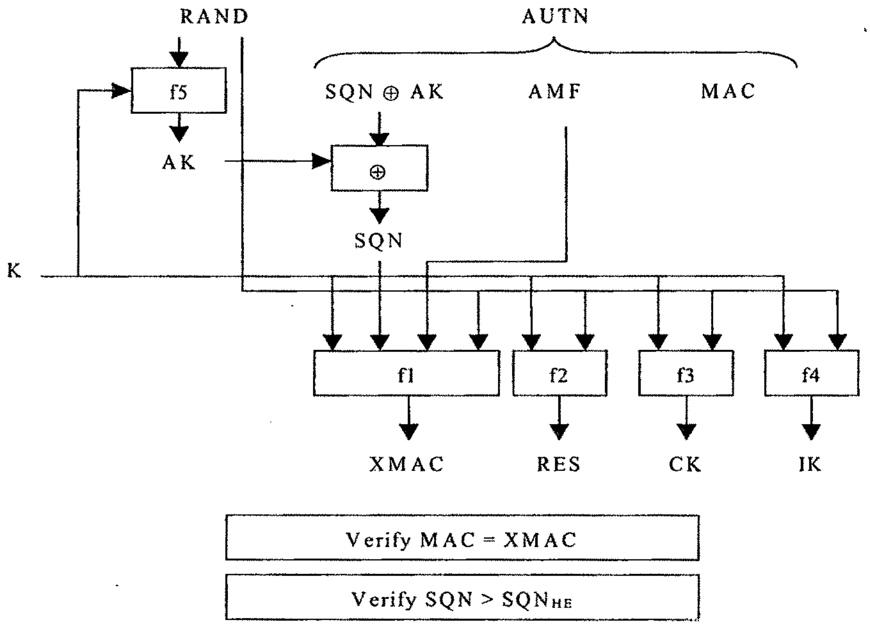

Figure 8.2: User authentication function in the USIM

Figure 8.3 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$_K$(RAND), and the concealed counter value is then computed as SQN$_{MS}$ ⊕ AK.

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

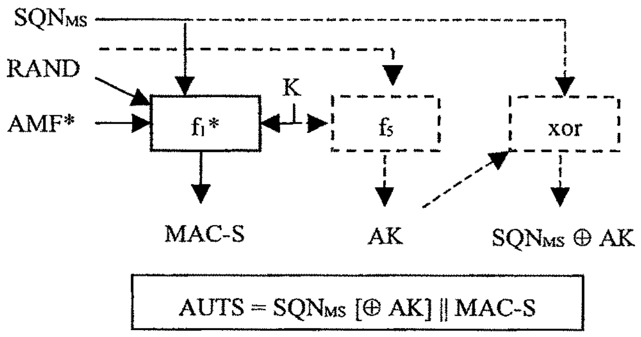

Figure 8.3: Generation of a token for re-synchronisation AUTS (note 1)

NOTE 1: The lengths of AUTS and MAC-S are specified in table 8.18

Table 8.2 provides a summary of the cryptographic functions implemented on the USIM to support authentication and key agreement.

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

Table 8.2 : USIM – Authentication and key agreement – Cryptographic functions

8.4 User equipment

8.4.1 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

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

Table 8.3: UE – User Identity Confidentiality – Data elements

8.4.2 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 radio bearer identifier;

g) DIRECTION: An indication of the direction of transmission uplink or downlink to ensure a different cipher is applied.Table 8.4 provides an overview of the data elements stored on the UE to support the mechanism for data confidentiality:

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 radio bearer	Lifetime of a radio bearer	32 bits	Mandatory
COUNT-C_{DOWN}	Time varying parameter for synchronisation of ciphering	1 per radio bearer	Lifetime of a radio bearer	32 bits	Mandatory
BEARER	Radio bearer identifier	1 per radio bearer	Lifetime of a radio bearer	5 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per radio bearer	Lifetime of a radio bearer	1 bit	Mandatory

Table 8.4: UE – Data Confidentiality – Data elements

The following cryptographic functions shall be implemented on the UE:

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

Table 8.5 provides an overview of the cryptographic functions implemented on the UE to support the mechanism for data confidentiality.

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

Table 8.5: UE – Data Confidentiality – Cryptographic functions

8.4.3 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 8.6 provides an overview of the data elements stored on the UE to support the mechanism for data confidentiality:

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 radio bearer	Lifetime of a radio bearer	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

Table 8.6: UE – Data Integrity – Data elements

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 8.7 provides an overview of the cryptographic functions implemented in the UE:

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

Table 8.7: UE – Data Integrity – Cryptographic functions

8.5 Radio network controller :

8.5.1 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 radio bearer identifier.

Table 8.8 provides an overview of the data elements stored in the RNC to support the mechanism for data confidentiality:

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UEA-RNC	Ciphering capabilities of the RNC	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 radio bearer	Lifetime of a radio bearer	32 bits	Mandatory
COUNT-C_{DOWN}	Time varying parameter for synchronisation of ciphering	1 per radio bearer	Lifetime of a radio bearer	32 bits	Mandatory
BEARER	Radio bearer identifier	1 per radio bearer	Lifetime of a radio bearer	5 bits	Mandatory
DIRECTION	An indication of the direction of transmission uplink or downlink	1 per radio bearer	Lifetime of a radio bearer	1 bit	Mandatory

Table 8.8: RNC – Data Confidentiality – Data elements

The following cryptographic functions shall be implemented in the RNC:

- f8:access link encryption function.

Table 8.9 provides an overview of the cryptographic functions implemented in the RNC to support the mechanism for data confidentiality:

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f8	Access link encryption function	1-16	Permanent	Standardised	One at least is mandatory

Table 8.9: RNC – Data confidentiality – Cryptographic functions

8.5.2 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 8.10 provides an overview of the data elements stored on the RNC to support the mechanism for data confidentiality:

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 radio bearer	Lifetime of a radio bearer	1 bit	Mandatory
COUNT-I_{UP}	Synchronisation value	1 per radio bearer	Lifetime of a connection	32 bits	Mandatory
COUNT-I_{DOWN}	Synchronisation value	1 per radio bearer	Lifetime of a connection	32 bits	Mandatory
FRESH	MS challenge	1 per user	Lifetime of a connection	32 bits	Mandatory
MAC-I XMAC-I	Message authentication code	1 per user	Updated by the execution of the f9 function	32 bits	Mandatory

Table 8.10: RNC – Data Integrity – Data elements

The following cryptographic functions shall be implemented on the RNC:

f9: access link integrity function.

Table 8.11 provides an overview of the cryptographic functions implemented in the RNC:

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

Table 8.11: RNC – Data Integrity – Cryptographic functions

8.6 Serving Network (SN) (or MSC/VLR or SGSN) :

8.6.1 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;

Symbol	Description	Multiplicity	Lifetime	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

Table 8.12: VLR – User Identity Confidentiality – Data elements

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.

Symbol	Description	Multiplicity	Lifetime	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

Table 8.13: SGSN – User Identity Confidentiality – Data elements

8.6.2 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;

b) KSI: Key set identifier;

c) CK: Cipher key;

d) IK: Integrity key;

e) GSM AV: Authentication vectors for GSM.

Table 8.14 provides an overview of the 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

Table 8.14: Composition of an authentication vector

Table 8.15 provides an overview of the data elements stored in the VLR/SGSN to support authentication and key agreement.

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

Table 8.15: VLR/SGSN – Authentication and key agreement – Data elements

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 8.16 provides an overview of VLR / SGSN 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

Table 8.16: VLR/SGSN Authentication and Key Agreement – Cryptographic functions

8.7 Home location register / Authentication centre- 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 ;

c) AV: authentication vectors computed in advance;

Table 8.17 provides an overview of the data elements stored on the HLR/AuC to support authentication and key agreement.

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 8.17: HLR/AuC – Authentication and key agreement – Data elements

Table 8.18 shows how the construction of authentication token for synchronisation failure messages used to support authentication and key agreement.

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

Table 8.18: Composition of an authentication token for synchronisation failure messages

Figure 8.4 provides an overview of how authentication vectors are generated in the HLR/AuC.

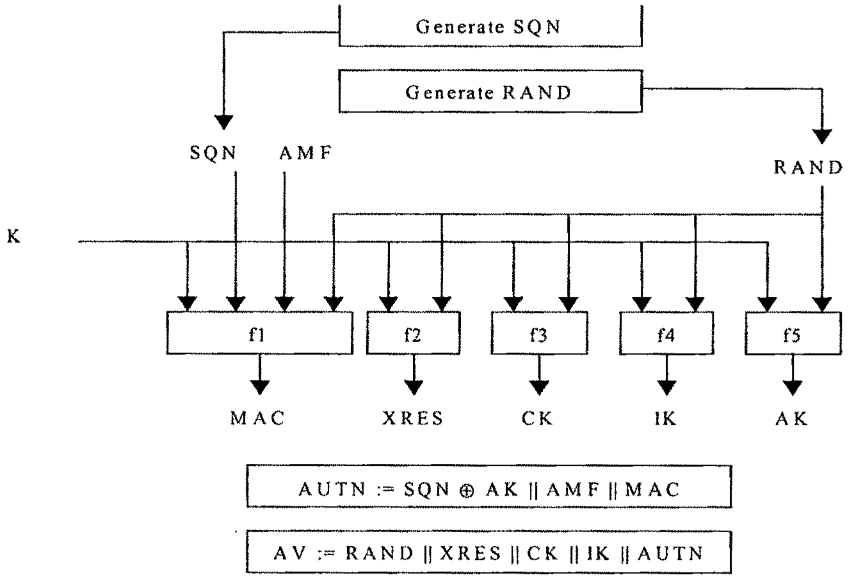
Generate SQN
Generate RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figure 8.4: 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 for normal operation;
- f5*: a key generating function to derive the anonymity key for re-synchronisation;
- c1: Conversion function for interoperation with GSM from RAND (UMTS) > RAND (GSM);
- c2: Conversion function for interoperation with GSM from XRES (UMTS) to SRES (GSM);
- c3: Conversion function for interoperation with GSM from CK and IK (UMTS) to Kc (GSM)

Table 8.19 provides a summary of the cryptographic functions implemented in the HLR / AuC to support authentication and key agreement.

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

Table 8.19: HLR/AuC – Authentication and key agreement – Cryptographic functions

8.8 Proposed Integration:

8.8.1 f8 algorithm : f8 is implemented in the UE and the RNC. Encryption is applied in the Medium Access Sublayer(MAC) and the Radio Link Control(RLC) sublayer of the data link layer. RLC layer provides encryption in unacknowledged and acknowledged RLC modes when ciphering is applied to the whole RLC PDU except the PDU header. In UE, algorithm may be implemented in hardware but DSP implementation can also give a throughput of 64 Mbps which is very good looking at peak data rate requirement of 2 Mbps. The memory requirements vary between 2.2 Kbytes -2.7 Kbytes which is easily available inside UE.

8.8.2 f9 algorithm : The f9 function is implemented in the UE and the RNC. Both hardware and software implementations are possible. This algorithm is implemented at the RRC layer i.e. between the terminal and the RNC. RRC protocol basically manages the allocation and maintenance of radio communication paths. RRC also provides encryption control i.e., it decides whether encryption is on or off between the UE and the RNC as well as executing integrity protection of both RRC level signalling and higher layer signalling in the form of message authentication codes (MAC-I).We get software implementation speed of 62 Mbps (for 64 bit data) and hardware encryption speed of 217 Mbps/ 339 Mbps (for 5114 bits of message length) for Altera and Xilinx chips respectively. Memory requirements vary between 2043 bytes to 2570 bytes. This can be easily made available in UE.

8.8.3 MILENAGE functions: The memory requirements for full algorithm set was defined as 8 Kbytes of ROM and 300 bytes of RAM out of which 6 Kbytes of ROM and 200 bytes of RAM allocated to Kernel function (AES). Our software implementation shows that the encryption speed is 276 Mbps in software and Memory requirements vary between 4 Kbytes- 8 Kbytes . The algorithms are implemented at the network operator's Authentication Centres (AuCs) and in the USIMs (Universal Subscriber Identity Modules) .These authentication related control messages are carried on the MAP(Mobile Application Part) protocol . The MAPsec protocols protects MAP messages at the application layer.3GPP also specifies how the MAP protocol can be run on top of IP. This allows even using IPsec for protection covering lower layer headers.

8.9 Summary : This chapter has described integration guidelines for cryptographic algorithms in 3G network architecture. We discuss the implementation considerations of f8, f9 and MILENAGE functions for integration within network entities and communication protocols associated with them. The conclusions based on these integration requirements are made in the next chapter.