

### 3G 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 005r1**

Current Version: **3.1.0**

3G specification number ↑

↑ CR number as allocated by 3G support team

For submission to **SA #7** for approval **X** (only one box should  
TSG list TSG meeting no. here ↑ for information be marked with an X)

Form: 3G CR cover sheet, version 1.0 The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf

**Proposed change affects:** USIM  ME  UTRAN  Core Network   
(at least one should be marked with an X)

**Source:** T-Mobil **Date:** 2000-Feb-24

**Subject:** Refinement EUIC (according to TS 33.102)

**3G Work item:** Security

**Category:** F Correction   
(only one category shall be marked with an X)  
A Corresponds to a correction in a 2G specification   
B Addition of feature   
C Functional modification of feature   
D Editorial modification

**Reason for change:** Changes needed to keep consistency with TS 33.102:  
- Clarification needed after meeting with CN2 experts.  
- Correction of a potential weakness caused by paging an UE with IMSI in clear was needed. Therefore concealed paging with TEMSI is introduced.

**Clauses affected:** 3.2, 3.3, 4.1, 4.2, 4.3, 4.5, 4.6

**Other specs affected:** Other 3G core specifications  → List of CRs: 23.003, 23.008, 23.012, 23.018, 23.060, 24.008, 25.331, 29.002, 31.102, 33.102, 33.105  
Other 2G 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:** Numbering of figures not consistent (editorial)



help.doc

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

## 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
⊕	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 <sup>-1</sup> )
f8	Integrity algorithm
f9	Confidentiality algorithm
<u>f10</u>	<u>Deriving function used to compute TEMSI</u>
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 <sub>SK(X)</sub> (data)	Decryption of "data" with Secret Key of X used for signing E <sub>K<sub>SKXY(i)</sub></sub> (data) Encryption of "data" with Symmetric Session Key #i for sending data from X to Y
E <sub>PK(X)</sub> (data)	Encryption of "data" with Public Key of X used for encryption
<u>EMSI</u>	<u>Encrypted Mobile Subscriber Identity</u>
ECK	Network Wide Cipher Key
ECKC	Network Cipher Key Component for UE
ECKCpeer	Network Cipher Key Component for peer UE
EMSI	Encrypted Subscriber identity
<u>EMSIN</u>	<u>Encrypted MSIN</u>
GK	Group Key
GI	Group Identifier
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"

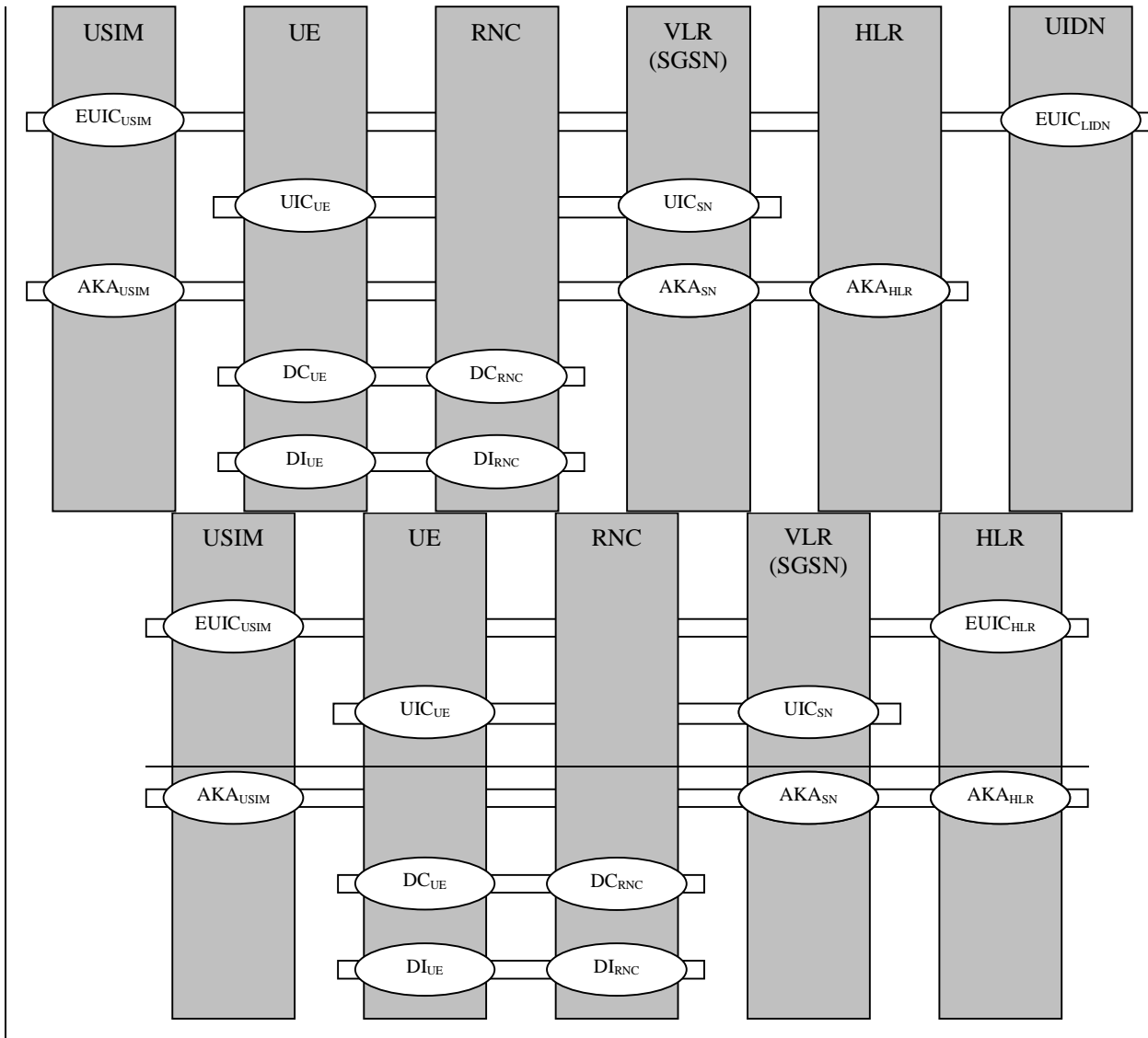
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
IV	Initialisation Vector
KAC <sub>X</sub>	Key Administration Centre of Network X
KS <sub>XY(i)</sub>	Symmetric Session Key #i for sending data from X to Y
KSI	Key Set Identifier
KSS	Key Stream 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
<u>MSIN</u>	<u>Mobile Station Identity Number</u>
MT	Mobile Termination
NE <sub>X</sub>	Network Element of Network X
PS	Packet Switched
RAND	Random challenge
RAND <sub>ms</sub>	Random value stored on MS received during user authentication request
RND <sub>X</sub>	Unpredictable Random Value generated by X
SEQ	Sequence number
SEQ <sub>UIC</sub>	Sequence number
SN	Serving Network
TE	Terminal Equipment
<u>TEMSI</u>	<u>Temporary Encrypted Mobile Subscriber Identity used for paging instead of IMSI</u>
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
TVP	Time Variant Parameter
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
<u>UIDN</u>	<u>User Identity Decryption Node</u>
UN	User Name
USIM	User Services Identity Module
VLR	Visited Location Register
X	Network Identifier
<u>XEMSI</u>	<u>Extended Encrypted Mobile Subscriber Identity</u>
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

---

## 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:

EUC: 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 (EUIC<sub>USIM</sub>)

For UMTS users with EUIC, the USIM has to store additional data and have additional functions implemented to encrypt the permanent user identity (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<sub>UIC</sub>: a counter that is equal to the highest SQN<sub>UIC</sub> generated and sent by the USIM to the HE/HLR/AuC/UIDN;
- b) GK: the group key used to encrypt the IMSI and SQN<sub>UIC</sub>;
- c) GI: a group identifier that identifies the group the user refers to as well as the GK;
- d) TEMSI: a temporary identity used for paging instead of IMSI
- e) HLR-id consists of the first 3 digits of MSIN as a subaddress of HLR the user is related to UIDN\_ADR: address of UIDN according to E.164;

**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 <sup>1</sup> bits	Optional
SQN <sub>UIC</sub>	Counter	1 per user	Updated when protocol for EUIC is executed	32 bits	Optional
GI	Group Identity	1 per user	Permanent	32 bits	Optional
<u>TEMSI</u>	<u>Temporary identity used for paging instead of IMSI</u>	<u>1 per user</u>	<u>Updated when a new identity request has been performed</u>	<u>As per IMSI</u>	<u>Optional</u>
<u>HLR-id</u> <u>UIDN_ADR</u>	<u>SubAddress of UIDN according to E.164 entity which can perform</u>	1 per user	Permanent	3-15 digits	Optional

<sup>1</sup> the table entry is for the example secret key mechanism given in annex B of 33.102

	decryption (first 3 digits of MSIN)				
--	---	--	--	--	--

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

- f6: the user identity encryption function;
- f10: TEMSI calculation function.

For a summary of the data elements and cryptographic function of the EUIC<sub>HE</sub> function see Table 2.

**Table 2: USIM– Enhanced User Identity Confidentiality – Cryptographic functions**

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f6	User identity encryption function	1	Permanent	Proprietary	Optional
<u>f10</u>	<u>TEMSI calculation function</u>	<u>1</u>	<u>Permanent</u>	<u>Proprietary</u>	<u>Optional</u>

#### 4.2.2 Authentication and key agreement (AKA<sub>USIM</sub>)

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<sub>MS</sub>: 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<sub>MS</sub> - w, SQN<sub>MS</sub>), 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<sub>MS</sub>: 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<sub>MS</sub>).
- f) KSI: key set identifier.
- g) THRESHOLD<sub>C</sub>: a threshold defined by the HE to trigger re-authentication and to control the cipher key lifetime;
- h) CK The access link cipher key established as part of authentication
- i) IK The access link integrity key established as part of authentication
- j) HFN<sub>MS</sub>: 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.
- k) 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.
- 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

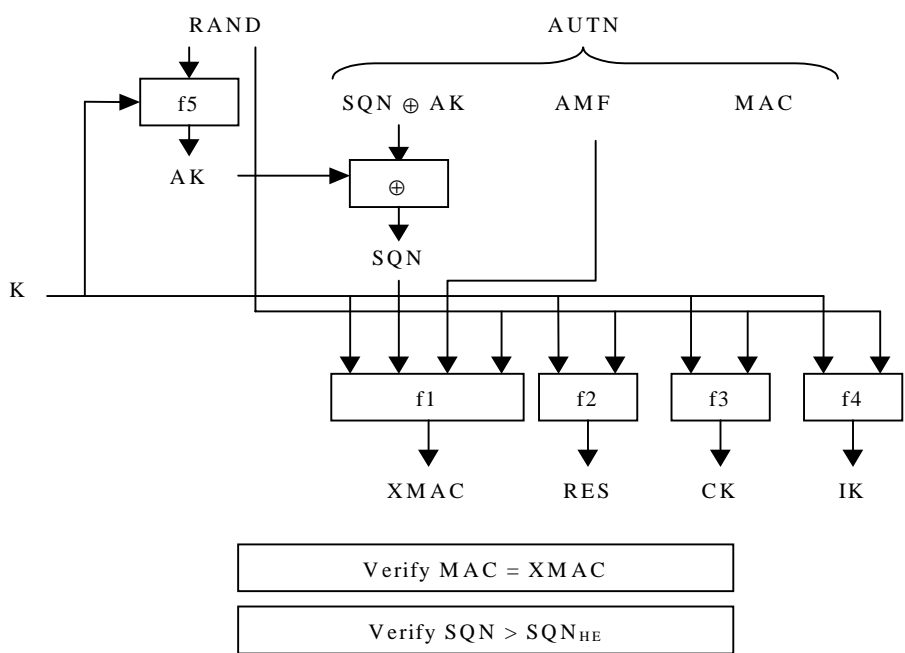
Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
K	Permanent secret key	1 <sup>2</sup>	Permanent	128 bits	Mandatory
SQN <sub>MS</sub>	Sequence number counter	1	Updated when AKA protocol is executed	32-64 bits	Mandatory
WINDOW (option 1)	<b>accepted sequence number array</b>	1	Updated 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 <sub>MS</sub>	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 <sub>C</sub>	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 <sub>MS</sub>	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 <sub>G</sub>	GSM authentication parameter from conversion function	<b>1</b>	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

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

<sup>2</sup> HE policy may dictate more than one, the active key signalled using the AMF function

- 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 C2 : 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, 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.



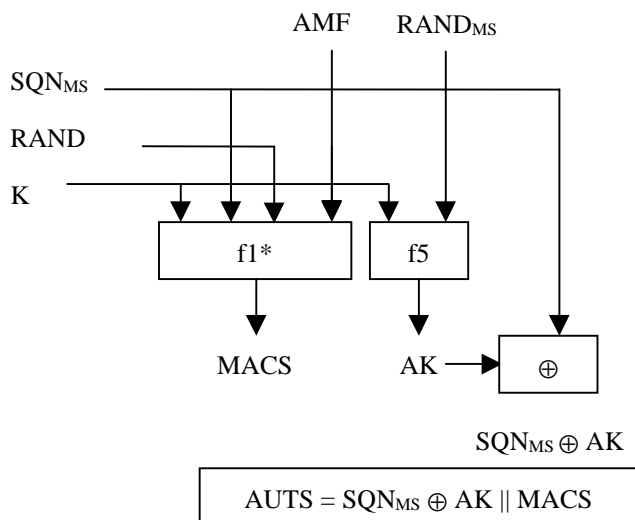


Figure 3: Generation of a token for re-synchronisation AUTS

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 C2	Conversion functions for interoperation with GSM	1 of each	Permanent	Standard	Optional

### 4.3 User equipment

#### 4.3.1 User identity confidentiality (UIC<sub>UE</sub>)

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<sub>UP</sub>: a time varying parameter for synchronisation of ciphering for the uplink;
- e) COUNT-C<sub>DOWN</sub>: 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 <sub>UP</sub>	Time varying parameter for synchronisation of ciphering	<b>1 per logical channel</b>	Lifetime of a logical channel	32 bits	Mandatory
COUNT-C <sub>DOWN</sub>	Time varying parameter for synchronisation of ciphering	<b>1 per logical channel</b>	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<sub>UE</sub>)

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<sub>UP</sub>: a time varying parameter for synchronisation of data integrity in the uplink direction;
- e) COUNT-I<sub>DOWN</sub>: 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 <sub>UP</sub>	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
COUNT-I <sub>DOWN</sub>	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

#### 4.3.4 Enhanced user identity confidentiality (EUIC<sub>UE</sub>)

The UE shall support the UMTS mechanism for enhanced user identity confidentiality described in 6.2 of 3G TS 33.102.

The UE shall store the following data elements:

- the TEMSI: a temporary identity used for paging instead of IMSI

**Table 5: UE – User Identity Confidentiality – Data elements**

<u>Symbol</u>	<u>Description</u>	<u>Multiplicity</u>	<u>Lifetime</u>	<u>Length</u>	<u>Mandatory / Optional</u>
<u>TEMSI</u>	<u>Temporary identity used for paging instead of IMSI</u>	<u>1 per user</u>	<u>Updated when a new identity request has been performed</u>	<u>As per IMSI</u>	<u>Optional</u>

## 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<sub>UP</sub>: a time varying parameter for synchronisation of ciphering for the uplink;  
 e) COUNT-C<sub>DOWN</sub>: 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 <sub>UP</sub>	Time varying parameter for synchronisation of ciphering	<b>1 per logical channel</b>	Lifetime of a logical channel	32 bits	Mandatory
COUNT-C <sub>DOWN</sub>	Time varying parameter for	<b>1 per logical channel</b>	Lifetime of a logical	32 bits	Mandatory

	synchronisation of ciphering		channel		
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<sub>UP</sub>: a time varying parameter for synchronisation of data integrity in the uplink direction;
- e) COUNT-I<sub>DOWN</sub>: 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 <sub>UP</sub>	Synchronisation value	1	Lifetime of a connection	32 bits	Mandatory
COUNT-I <sub>DOWN</sub>	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<sub>SN</sub>)

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 -Enhanced user identity confidentiality (EUIC<sub>SN</sub>)

The VLR (equivalently the SGSN) shall support the UMTS mechanism for enhanced user identity confidentiality described in 6.2 of 3G TS 33.102.

The UE shall store the following data elements:

- the TEMSI: a temporary identity used for paging instead of IMSI

**Table ??: VLR – User Identity Confidentiality – Data elements**

<u>Symbol</u>	<u>Description</u>	<u>Multiplicity</u>	<u>Lifetime</u>	<u>Length</u>	<u>Mandatory / Optional</u>
<u>TEMSI</u>	<u>Temporary identity used for paging instead of IMSI</u>	<u>1 per user</u>	<u>Updated when a new identity request has been performed</u>	<u>As per IMSI</u>	<u>Optional</u>

Equivalently, the SGSN shall store the following data elements:

- the TEMSI: a temporary identity used for paging instead of IMSI



**Table ??: SGSN – User Identity Confidentiality – Data elements**

<u>Symbol</u>	<u>Description</u>	<u>Multiplicity</u>	<u>Lifetime</u>	<u>Length</u>	<u>Mandatory / Optional</u>
TEMSI	Temporary identity used for paging instead of IMSI	1 per user	Updated when a new identity request has been performed	As per IMSI	Optional

### 4.5.24.5.3 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:	112-144
SQN or $SQN \oplus AK$	Sequence number or Concealed sequence number	1 per AUTN	32-64
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	several per user, SN	Depends on many	528-656	Mandatory

	Authentication vectors	dependent	things		
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

## 4.6 Home location register / Authentication centre

### 4.6.1 Enhanced User Identity Confidentiality (EUIC<sub>HE</sub>)

For UMTS users with EUIC, the HLR/AuC has to store additional data and have additional function implemented to decrypt the permanent user identity (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) GK: the group key used to decrypt the IMSI and  $SQN_{UIC}$ ;
- b) GI: a group identifier that identifies the group the user refers to as well as the GK;

**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
GI	Group Identity	1 per user	Permanent	32 bits	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<sub>HE</sub> 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

#### 4.6.24.6.1 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:

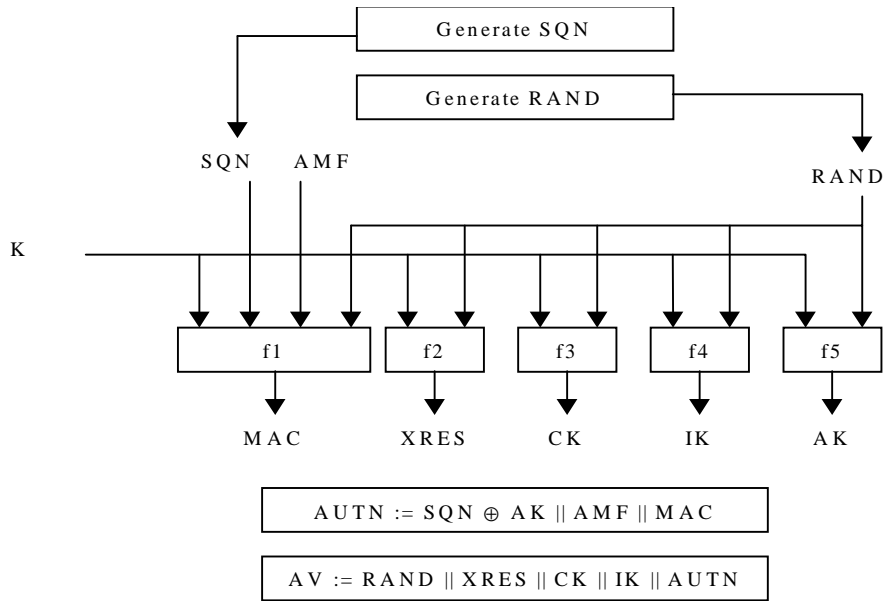
- a) K: a permanent secret key;
- b)  $SQN_{HE}$ : a counter used to generate SQN from;
- c) AV: authentication vectors computed in advance;

Table 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
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 C2	Functions for converting UMTS AV's to GSM AV's	1 for each	Permanent	Standard	Optional

## 4.7 Enhanced user identity confidentiality (EUIC<sub>HE</sub>)

For UMTS users with EUIC, the UIDN has to store additional data and have additional function implemented to decrypt the permanent user identity (IMSI) and to calculate the paging identity TEMSI to be used instead of 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 UIDN:

- GK: the group key used to decrypt the IMSI and SQN<sub>UIC</sub>:
- GI: a group identifier that identifies the group the user refers to as well as the GK;
- TEMSI: a temporary identity used for paging instead of IMSI;
- IMSI: the IMSI of that users the feature is applied for.

**Table ??: UIDN – Enhanced User Identity Confidentiality – Data elements**

<u>Symbol</u>	<u>Description</u>	<u>Multiplicity</u>	<u>Lifetime</u>	<u>Length</u>	<u>Mandatory / Optional</u>
<u>GK</u>	<u>Group key</u>	<u>1 per user group</u>	<u>Permanent</u>	<u>128</u>	<u>Optional</u>
<u>GI</u>	<u>Group Identity</u>	<u>1 per user</u>	<u>Permanent</u>	<u>32 bits</u>	<u>Optional</u>
<u>TEMSI</u>	<u>Temporary identity used for paging instead of IMSI</u>	<u>1 per user</u>	<u>Updated when a new identity request has been performed</u>	<u>As per IMSI</u>	<u>Optional</u>
<u>IMSI</u>	<u>IMSI</u>	<u>1 per user</u>	<u>Permanent</u>	<u>64 bits</u>	<u>Optional</u>

The following cryptographic functions need to be implemented in UIDN:

- f7: the user identity decryption function.
- f10: TEMSI calculation function

For a summary of the data elements and cryptographic function of the EUIC<sub>HE</sub> function see Table 2.

**Table ??: UIDN – Enhanced User Identity Confidentiality – Cryptographic functions**

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

<u>f10</u>	<u>TEMSEI calculation function</u>	<u>1</u>	<u>Permanent</u>	<u>Proprietary</u>	<u>Optional</u>
------------	------------------------------------	----------	------------------	--------------------	-----------------