Technical Specification Group Services and System Aspects **TSGS#7(00)0075**

Meeting #7, Madrid, Spain, 15-17 March 2000

Source: **SA WG3**

Title: **CRs on Refinement of EUIC**

Document for: **Approval**

Agenda Item: **5.3.3**

CRs on Refinement of EUIC

Introduction:

This document contains 3 CRs on Refinement of EUIC to **33.102, 33.103** and **33.105** for Release 1999 which is submitted to SA#7 for approval.

SA WG3 TD	Spec	CR	Rev	Phase	Subject	Cat	Current Version	Comments
S3-000197	33.102	045	3	R99	Refinement EUIC	F	3.3.1	For consideration with the EUIC report in S3-000196 (SP-000006)
S3-000198	33.103	005	2	R99	Refinement EUIC (according to TS 33.102)	F	3.1.0	For consideration with the EUIC report in S3-000196 (SP-000006)
S3-000100	33.105	008		R99	Refinement of EUIC for consistency with 33.102	F	3.2.0	For consideration with the EUIC report in S3-000196 (SP-000006)

Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgium - Office: BU 31 2/51.
Telephone: direct line (+32-2)296.86.43, switchboard 299.11.11. Fax: 296.83.95.
Telex: COMEU B 21877. Telegraphic address: COMEUR Brussels.

3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102 **CR** **045r3** Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG: SA #7 *(list TSG meeting no. here ↑)*

for approval **X** *(only one box should be marked with an X)*

for information

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

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

Subject: Refinement of EUIC (revision no. 1 of S3-000081)

3G Work item: Security

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

F	Correction	
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	**X**
D	Editorial modification	

Reason for change:
1) Clarification needed after meeting with TSG CN2 experts.
2) Correction of a potential weakness caused by paging an UE with IMSI in clear was needed. Therefore concealed paging with TEMSI is introduced.
3) Correction for the situation of VLR restart. Therefore requesting the most recently calculated TEMSI from UIDN is introduced.

Clauses affected: 2.1, 3.3, 6.2 and annex B

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, 33.103, 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:

help.doc

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

2.1 Normative references

[1] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3G TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] UMTS 33.21, version 2.0.0: "Security requirements".

[4] UMTS 33.22, version 1.0.0: "Security features".

[5] UMTS 33.23, version 0.2.0: "Security architecture".

[6] Proposed UMTS Authentication Mechanism based on a Temporary Authentication Key.

[7] TTC Work Items for IMT-2000 – System Aspects.

[8] Annex 8 of "Requirements and Objectives for 3G Mobile Services and systems" – "Security Design Principles".

[9] ETSI GSM 09.02 Version 4.18.0: Mobile Application Part (MAP) Specification.

[10] ISO/IEC 11770-3: *Key Management – Mechanisms using Asymmetric Techniques*.

[11] ETSI SAGE: Specification of the BEANO encryption algorithm, Dec. 1995 (confidential).

[12] ETSI SMG10 WPB: SS7 Signalling Protocols Threat Analysis , Input Document AP 99-28 to SMG10 Meeting#28, Stockholm, Sweden.

[13] 3G TS 33.105: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Cryptographic Algorithm Requirements".

[26] 3G TS 23.003: 3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) Core Network (CN); Numbering, addressing and identification

3.3 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
$D_{SK(X)}$(data)	Decryption of "data" with Secret Key of X used for signing
EMSI	Encrypted Mobile Subscriber Identity
EMSIN	Encrypted MSIN
$E_{KSXY(i)}$(data)	Encryption of "data" with Symmetric Session Key #i for sending data from X to Y
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption
GI	Group Identifier
GK	Group Key
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
IV	Initialisation Vector

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

6.2 Identification by a permanent identity

The mechanism described in here allows the identification of a user on the radio path by means of the permanent ~~user~~ subscriber identity (~~IMUI~~IMSI).

The mechanism should be invoked by the serving network whenever the user cannot be identified by means of a temporary identity. In particular, it should be used when the user registers for the first time in a serving network, or when the serving network cannot retrieve the ~~IMUI~~ IMSI from the ~~TMUI~~ TMSI by which the user identifies itself on the radio path.

The mechanism is illustrated in Figure 4.

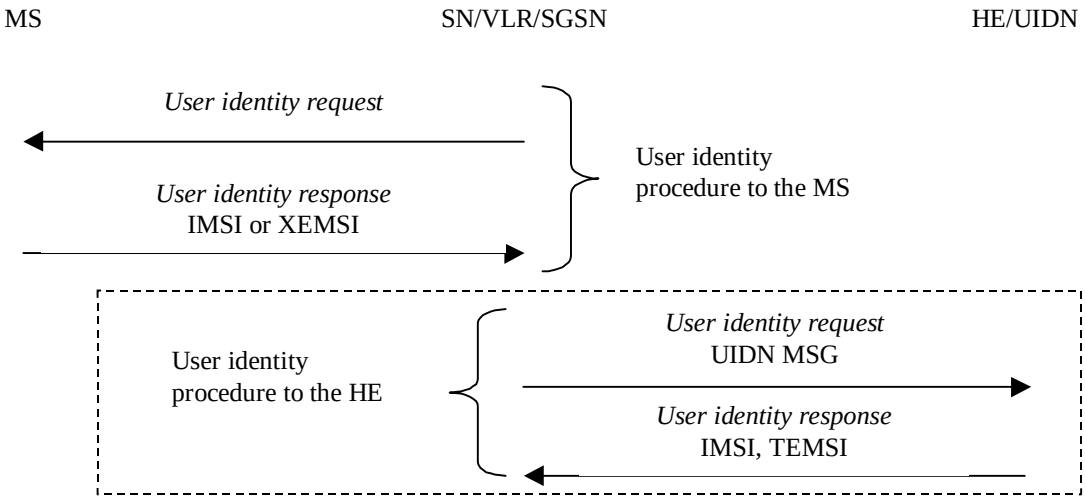


Figure 4: Identification by the permanent identity

The mechanism is initiated by the visited SN/VLR that requests the user to send its permanent identity. According to the user's preferences, his response may contain either 1) the ~~IMUI~~ IMSI in cleartext, or 2) the Extended Encrypted Mobile Subscriber Identity (XEMSI).

A mobile station configured for Enhanced User Identity Confidentiality shall always use the XEMSI instead of the IMSI. XEMSI consists of the User Identity Decryption Node address (UIDN_ADR, see below) ~~address~~ and a ~~UIDN-message~~container transporting the Encrypted Mobile Subscriber Identity EMSI. UIDN_ADR shall consist of a global title according to E164. For details concerning the structure of the XEMSI see [26]. ~~UIDN address shall exist of a global title according to E164.~~ ~~user's HE identity in cleartext and an HE message that contains an encrypted IMUI.~~

~~The term HE id denotes an expression which is sufficient to route the user identity request message to an appropriate network element in the HE. Annex B contains a proposal to use MCC, MNC and the first three digits of the user's MSIN as routing information to address an HE/HLR.~~

In case the response contains the ~~IMUI~~ IMSI in cleartext, the procedure is ended successfully. This variant represents a breach in the provision of user identity confidentiality.

In case the response contains ~~an encrypted IMUI~~the XEMSI, the visited SN/VLR/SGSN forwards ~~the HE UIDN message~~ EMSI to the user's UIDN/HE in a request to send the user's ~~IMUI~~ IMSI and TEMSI (temporary EMSI). The user's UIDN/HE then derives the ~~IMUI~~ IMSI from ~~the HE~~UIDN ~~message~~EMSI, calculates TEMSI and sends ~~the IMUI~~ IMSI and TEMSI back to the SN/VLR/SGSN. Annex B describes an example mechanism that makes use of group keys to encrypt the ~~IMUI~~IMSI and to calculate the TEMSI and provides details on ~~the UIDN message~~EMSI.

The SN shall use TEMSI instead of IMSI to page a particular user because using the IMSI in clear would compromise the security goal of the Enhanced User Identity Confidentiality feature. Therefore on UE side the TEMSI is calculated and stored by USIM and transmitted to the UE. On both sides, in the UE and VLR/SGSN, the TEMSI shall become active if the following authentication procedure has successfully been performed. After the current TEMSI has successfully been used once SN shall trigger the *User Identity Request* procedure to establish a new TEMSI.

For the case the VLR/SGSN has lost the TEMSI related to a particular IMSI the VLR/SGSN shall request the most recently derived TEMSI from the UIDN. Therefore the UIDN has to store necessary information for each IMSI.

For the purpose of the Enhanced User Identity Confidentiality a new logical network node UIDN is introduced. The serving VLR or SGSN shall be able to request decryption of the user identity and calculation/providing of paging identities by this home network node.

The UIDN is in charge of decrypting the encrypted IMSI provided by the mobile station in ~~the UIDN message~~EMSI and of calculating the TEMSI. The UIDN is a home network operator specific logical network node and may be co-located with the HLR.

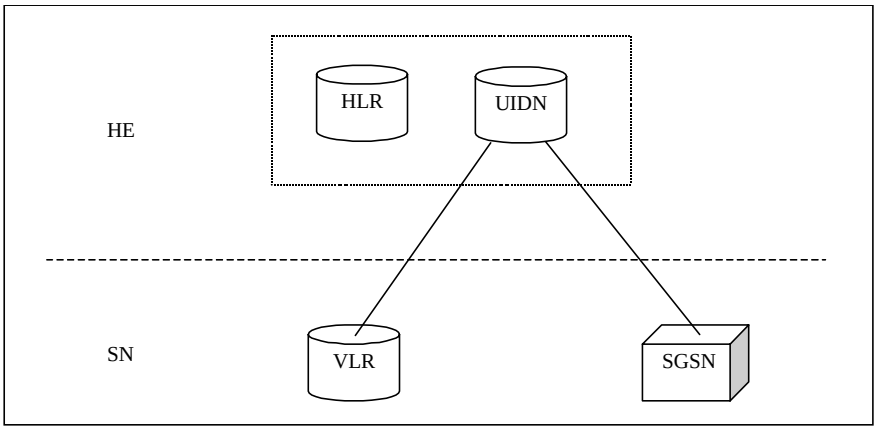


Figure 5: Core Network Architecture for Enhanced User Identity Confidentiality

The interface between the VLR/SGSN and the UIDN is used by the VLR/SGSN to request the

- revelation ~~decryption of~~ the ~~E~~IMSI contained in ~~the UIDN message~~EMSI from the UIDN;
- calculation of the TEMSI for the circuit/packet switched domain;~~.~~
- most recently derived TEMSI.

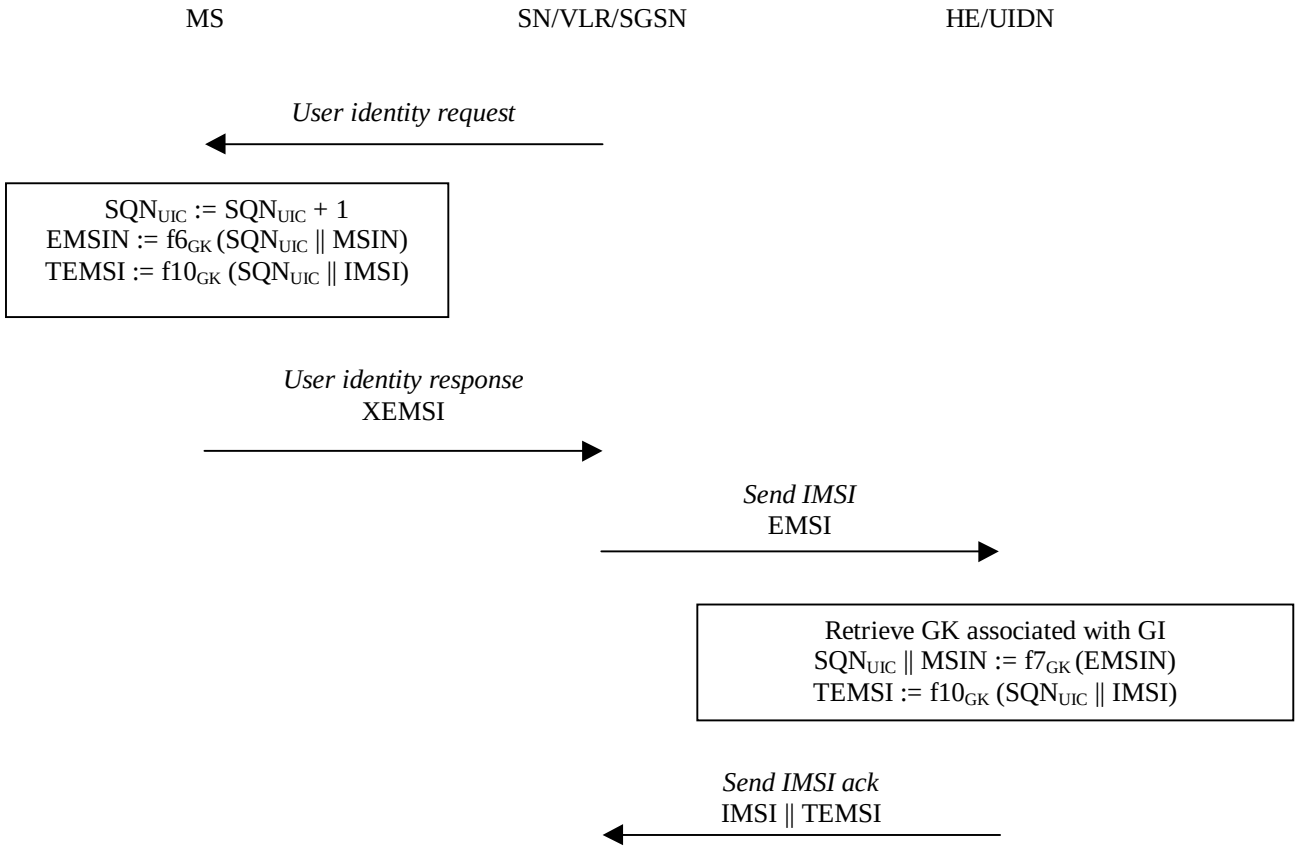
~~The interface between the SGSN and the UIDN is used by the SGSN to request the decryption of the EIMSI contained in the UIDN message from the UIDN for the packet switched domain.~~

Annex B (informative): Enhanced user identity confidentiality

This mechanism allows the identification of a user on the radio access by means of the permanent user identity encrypted by means of a group key. The mechanism described here can be used in combination with the mechanism described in 6.2 to provide user identity confidentiality in the event that the user not known by means of a temporary identity in the serving network.

The mechanism assumes that the user belongs to a user group with group identity GI. Associated to the user group is a secret group key GK which is shared between all members of the user group and the user's HE, and securely stored in the USIM and in the HE/~~HLR~~UIDN.

The mechanism is illustrated in Figure B.1.



Abbreviations
EMSI := GI || EMSIN
XEMSI := UIDN_ADR || EMSI
UIDN_ADR := UIDN's global title (according to 6.2)

Figure B.1: Identification by means of the ~~IMUI~~ IMSI encrypted by means of a group key

The mechanism illustrated in Figure B.1 works as follows:

1. The user identity procedure is initiated by the visited VLR/SGSN. The visited VLR/SGSN requests the ~~user~~ USIM to send its XEMSI.~~permanent user identity.~~

2. Upon receipt the ~~user~~ USIM
   - increments SQN_{UIC} as a time variant parameter. ~~The user~~
   - encrypts SQN_{UIC} and ~~the~~ its ~~IMUI~~ IMSIN with enciphering algorithm f6 and ~~his~~ its group key GK. The result is called EMSIN, encrypted MSIN.
   - constructs EMSI as concatenation of the group identifier GI and EMSIN.
   - constructs XEMSI as concatenation of UIDN_ADR and EMSI.
   - sends XEMSI in a response to the SN/VLR/SGSN.
   - derives TEMSI from IMSI and SQN_{UIC} with cryptographic algorithm f10 and the group key GK.

   The SQN_{UIC} prevents traceability attacks and synchronizes the derivation of TEMSI in the USIM and HE.

~~The user sends XEMSI in a response to the SN/VLR/SGSN consisting of UIDN address and UIDN message. The UIDN message itself consists of group key GI and encrypted IMSI EMSI. that includes the MCC || MNC and the first three digits of the user's MSIN that identify an HLR within the user's HE core network.~~

~~Note: Alternatives are~~

~~— to define a single network element within each HE which performs all decryption related to EMUI, or~~

~~— that all gateway MSCs are able to decrypt EMUI and route the message to the correct HLR~~

3. Upon receipt of that response the SN/VLR/SGSN ~~should~~ resolves the ~~user's HE/HLR~~UIDN ~~address~~ ADR from XEMSI ~~MCC ||MNC || HLR id~~ and forwards ~~UIDN message~~EMSI ~~the group identity GI and the user's EMUI~~ to the user's HE/~~HLR~~UIDN.

4. Upon receipt the HE/~~HLR~~ UIDN
   - retrieves the group identity GI contained in EMSI.
   - retrieves the group key GK associated with the group identity GI.
   - ~~The HE/HLR~~ UIDN ~~then~~ decrypts ~~EMUI~~ EMSIN with the deciphering algorithm f7 ($f7 = f6^{-1}$) and the group key GK and retrieves SQN_{UIC} and ~~IMUI~~IMSIN.
   - constructs the user's IMSI according to the following rule: $IMSI := MCC_{UIDN\_ADR} || MNC_{UIDN\_ADR} || MSIN$ $(UIDN\_ADR := MCC_{UIDN\_ADR} || MNC_{UIDN\_ADR} || MSIN_{UIDN\_ADR})$.
   - calculates TEMSI as $TEMSI := f10_{GK} (SQN_{UIC} || IMSI)$~~$SQN_{UIC}$ is no longer used~~.
   - ~~The HE/HLR~~ UIDN ~~then~~ sends ~~the IMUI~~ IMSI and TEMSI in a response to the visited SN/VLR/SGSN.

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** **005r2** Current Version: 3.1.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG: SA #7 *list TSG meeting no. here ↑*

for approval **X** *(only one box should be marked with an X)*

for information

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

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

Subject: Refinement EUIC (according to TS 33.102)

3G Work item: Security

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

F	Correction	**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 ($=f6^{-1}$)
f8	Integrity algorithm
f9	Confidentiality algorithm
f10	Deriving function used to compute TEMSI
K	Long-term secret key shared between the USIM and the AuC

3.3 Abbreviations

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

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
EMSI	Encrypted Mobile Subscriber Identity
ECK	Network Wide Cipher Key
ECKC	Network Cipher Key Component for UE
ECKCpeer	Network Cipher Key Component for peer UE
EMSI	Encrypted Subscriber identity
EMSIN	Encrypted MSIN
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_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
MSIN	Mobile Station Identity Number
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
SEQ_{UIC}	Sequence number
SN	Serving Network
TE	Terminal Equipment
TEMSI	Temporary Encrypted Mobile Subscriber Identity used for paging instead of IMSI
Text1	Optional Data Field
Text2	Optional Data Field
Text3	Public Key algorithm identifier and Public Key Version Number (eventually included in Public Key Certificate)
TMSI	Temporary Mobile Subscriber Identity
TVP	Time Variant Parameter
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UIDN	User Identity Decryption Node
UN	User Name
USIM	User Services Identity Module
VLR	Visited Location Register
X	Network Identifier
XEMSI	Extended Encrypted Mobile Subscriber Identity
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.

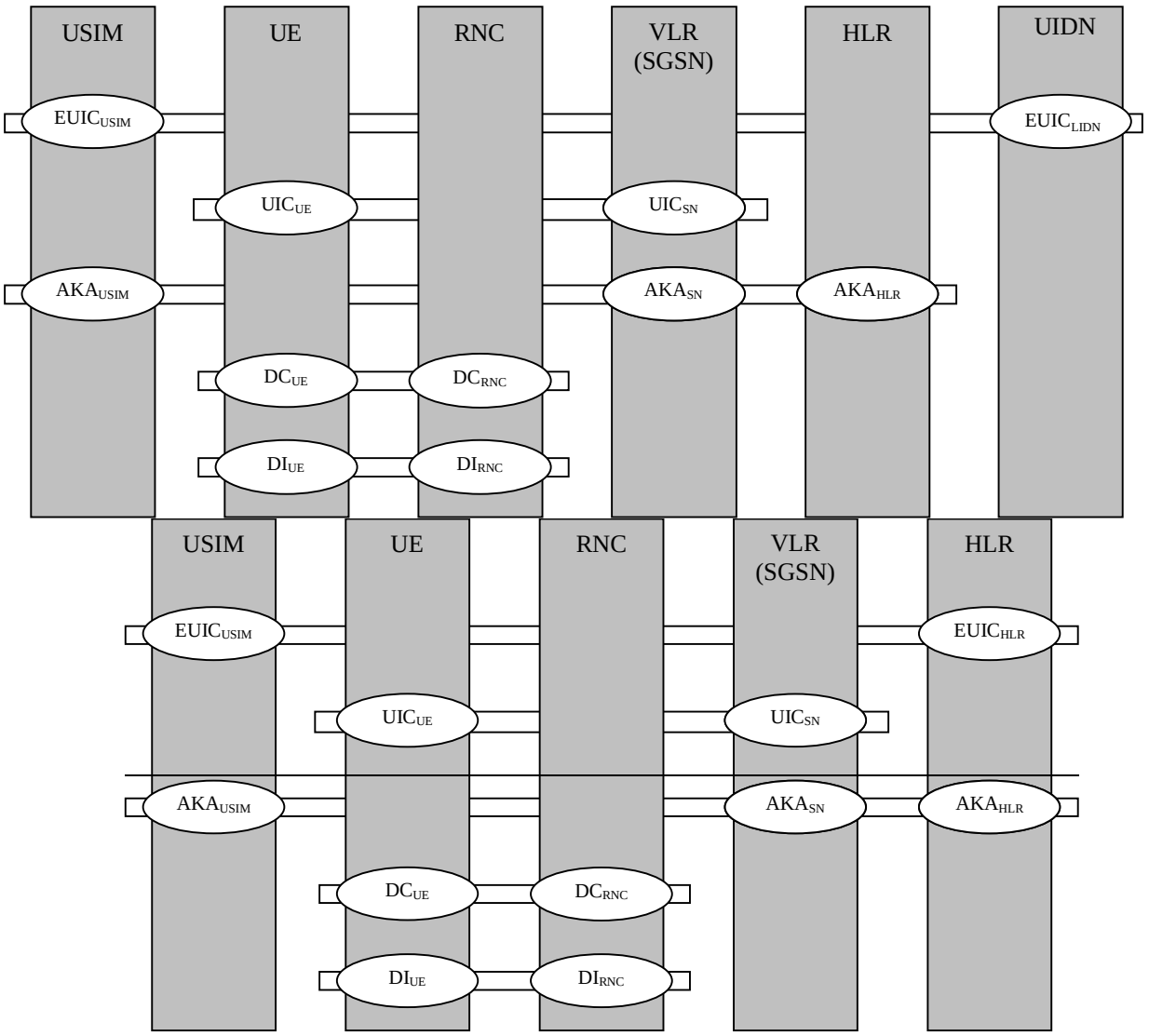


Figure 1: UMTS functional security architecture

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:

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 ($EUIC_{USIM}$)

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

b) GK: the group key used to encrypt the ~~I~~MSIN and SQN_{UIC};

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

~~d)~~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[1] bits	Optional
SQN_{UIC}	Counter	1 per user	Updated when protocol for EUIC is executed	32 bits	Optional
GI	Group Identity	1 per user	Permanent	32 bits	Optional
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
~~HLR id~~UIDN_ADR	~~Suba~~Address of UIDN according to E.164~~entitiy which can perform~~	1 per user	Permanent	~~3~~ 15 digits	Optional

[1] 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/AuC~~USIM:

– f6: the user identity encryption function;

– f10: TEMSI calculation function.

For a summary of the data elements and cryptographic function of the $EUIC_{HE}$ 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
f10	TEMSI calculation 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 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}).

f) KSI: key set identifier.

g) $THRESHOLD_C$: 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) $HFN_{MS:}$ 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.

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[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	3 bits	Mandatory
$THRESHOLD_C$	Threshold value for ciphering	1	Permanent	32 bits	Optional
CK	Cipher key	1	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	1	Updated when AKA protocol is executed	128 bits	Mandatory
$HFN_{MS:}$	Initialisation value for most significant part for COUNT-C and for COUNT-I	1	Updated when connection is released	25 bits	Mandatory
AMF	Authentication Management Field (indicates the algorithm and key in use)	1	Updated when AKA protocol is executed	16 bits	Mandatory
$RAND_G$	GSM authentication parameter from conversion function	***1***	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
SRES	GSM authentication parameter from conversion function	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
Kc	GSM cipher Key	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional

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

[2] 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

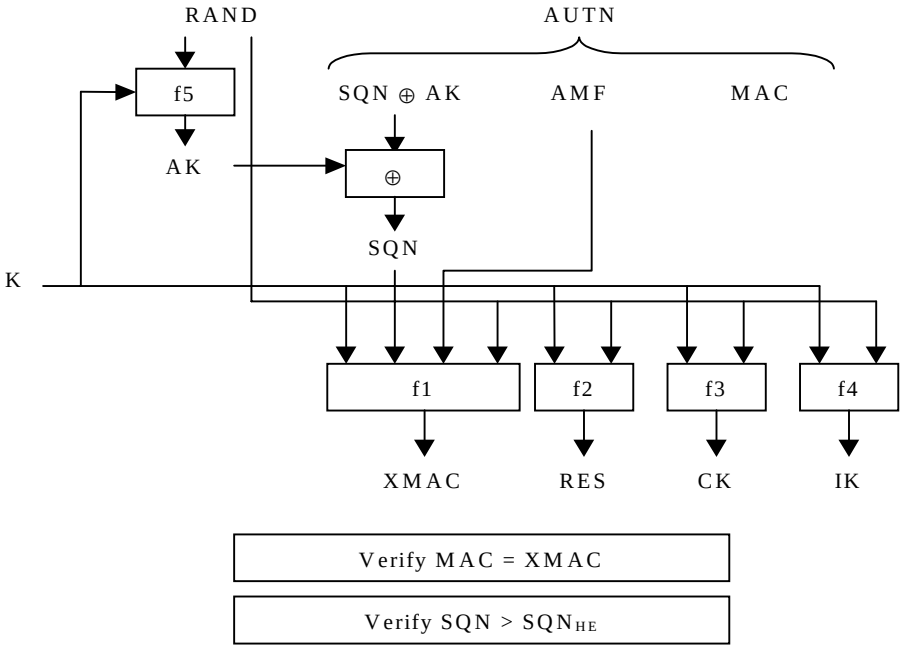


Figure 2: User authentication function in the USIM

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

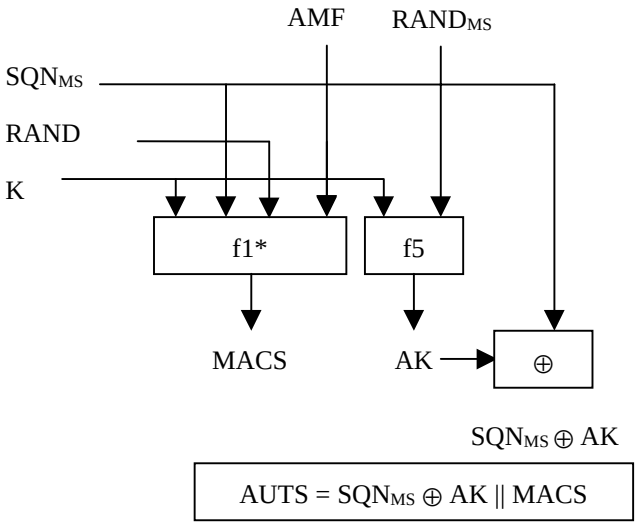


Figure 3: Generation of a token for re-synchronisation AUTS

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$_{UE}$)

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

The UE shall store the following data elements:

– TMUI-CS: a temporary identity allocated by the CS core network;

– LAI: a location area identifier;

– the TMUI-PS: a temporary identity allocated by the PS core network;

– the RAI: a routing area identifier

Table 5: UE – User Identity Confidentiality – Data elements

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

4.3.2 Data confidentiality (DC_{UE})

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

The UE shall store the following data elements:

a) UEA-MS: the ciphering capabilities of the UE;
b) CK: the cipher key;
c) UEA: the selected ciphering function;

In addition, when in dedicated mode:

d) COUNT-C_{UP}: a time varying parameter for synchronisation of ciphering for the uplink;
e) COUNT-C_{DOWN}: a time varying parameter for synchronisation of ciphering for the downlink;
f) BEARER: a logical channel identifier.
g) DIRECTION: An indication of the direction of transmission uplink or downlink to ensure a different cipher is applied

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

Table 6: UE – Data Confidentiality – Data elements

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

The following cryptographic functions shall be implemented on the UE:

– f8: access link encryption function.

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

4.3.4 Enhanced user identity confidentiality ($EUIC_{UE}$)

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

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
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

4.4 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	***1 per logical channel***	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_{UP}: a time varying parameter for synchronisation of data integrity in the uplink direction;

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

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

g) FRESH: an MS challenge;

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

Table12: UE – Data Integrity – Data elements

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

The following cryptographic functions shall be implemented on the UE:

– f9: access link integrity function.

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

Table 13: UE – Data Integrity – Cryptographic functions

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

4.5 SN (or MSC/VLR or SGSN)

4.5.1 User identity confidentiality (UIC_{SN})

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

The VLR shall store the following data elements:

– TMUI-CS: a temporary identity allocated by the CS core network;

– LAI: a location area identifier;

Table 14: VLR – User Identity Confidentiality – Data elements

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

Equivalently, the SGSN shall store the following data elements:

– TMUI-PS: a temporary identity allocated by the PS core network;

– RAI: a routing area identifier

~~□~~

Table 15: SGSN – User Identity Confidentiality – Data elements

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

4.5.2 -Enhanced user identity confidentiality ($EUIC_{SN}$)

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 VLR~~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

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
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

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

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
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

~~4.5.2~~4.5.3 Authentication and key agreement (AKA_{SN})

The VLR (equivalently the SGSN) shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored in the VLR (and SGSN):

a) AV: Authentication vectors;

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

Table 16: Composition of an authentication vector

Symbol	Description	Multiplicity	Length
RAND	Network challenge	1	128
XRES	Expected response	1	32-128
CK	Cipher key	1	128
IK	Integrity key	1	128
AUTN	Authentication token	1 that consists of:	112-144
SQN or SQN ⊕ 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 ($EUIC_{HE}$)~~

~~For UMTS users with EUIC, the HLR/AuC has to store additional data and have additional function implemented to decrypt the permanent user identity (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 $EUIC_{HE}$ function see Table 2.~~

~~Table19: 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~~4.6.1 Authentication and key agreement (AKA_{he})

The HLR/AuC shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

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

a) K: a permanent secret key;

b) SQN_{HE}: a counter used to generate SQN from;

c) AV: authentication vectors computed in advance;

Table 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.

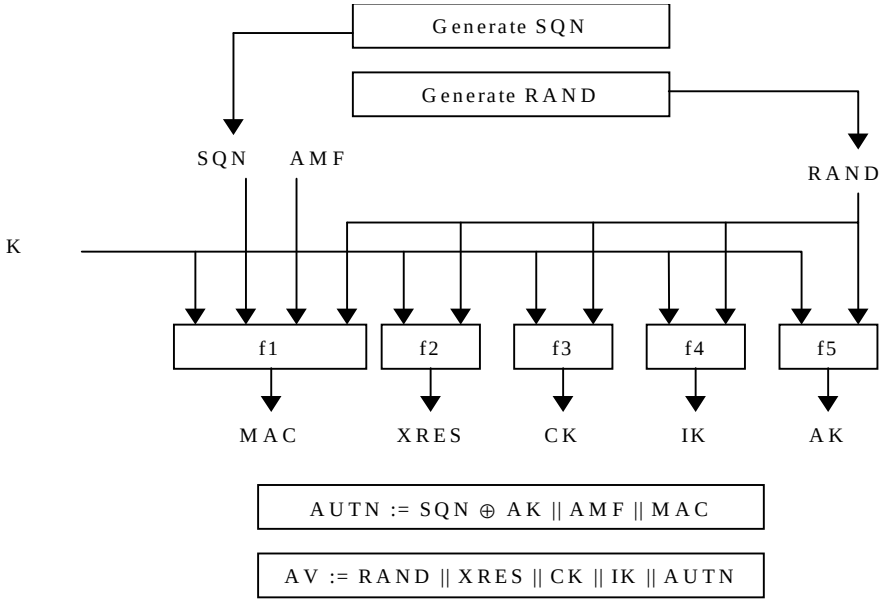


Figure 4: Generation of an authentication vector

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 ($EUIC_{HE}$)

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:

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;

c) TEMSI: a temporary identity used for paging instead of IMSI;

d) IMSI: the IMSI of ~~that~~ the user~~s~~ the feature is applied ~~for~~to.

Table ??: UIDN – 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
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
IMSI	IMSI	1 per user	Permanent	64 bits	Optional

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 $EUIC_{HE}$ function see Table 2.

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

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

f10	TEMSI calculation function	1	Permanent	Proprietary	Optional

3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.105 **CR** **008** Current Version: 3.2.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

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

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

Source: SA WG3 **Date:** 2000-Feb-10

Subject: Refinement of EUIC for consistency with 33.102

3G Work item: Security

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

F	Correction	**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

Clauses affected: 3.3, Annex A, Annex C

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, 33.103
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.

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AK	Anonymity key
AuC	Authentication Centre
AUTN	Authentication token
COUNT-C	Time variant parameter for synchronisation of ciphering
COUNT-I	Time variant parameter for synchronisation of data integrity
CK	Cipher key
~~EMUI~~	~~Encrypted Mobile User Identity~~
EMSIN	Encrypted Mobile Station Identification Number
GK	User group key
IK	Integrity key
~~IMUI~~IMSI	International Mobile ~~User Identity~~Station Identity
IPR	Intellectual Property Right
MAC	Medium access control (sublayer of Layer 2 in RAN)
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MSIN	Mobile Station Identification Number
PDU	Protocol data unit
RAND	Random challenge
RES	User response
RLC	Radio link control (sublayer of Layer 2 in RAN)
RNC	Radio network controller
SEQ_UIC	Sequence for user identity confidentiality
SDU	Signalling data unit
SQN	Sequence number
TEMSI	Temporary encrypted mobile subscriber identity
UE	User equipment
UIDN	User Identity Decryption Node
USIM	User Services Identity Module
XMAC-A	Expected MAC used for authentication and key agreement
XMAC-I	Expected MAC used for data integrity of signalling messages
XRES	Expected user response

Annex A (informative): User identity confidentiality

A.1 Overview

Figure A.1 illustrates the use of the encryption function f6 to encrypt the ~~IMUI~~ MSIN and the sequence for user identity confidentiality (SEQ_UIC) into an ~~EMUI~~ EMSIN and the use of the decryption function f7 to decrypt the ~~EMUI~~ EMSIN and retrieve the SEQ_UIC and the ~~IMUI~~MSIN.

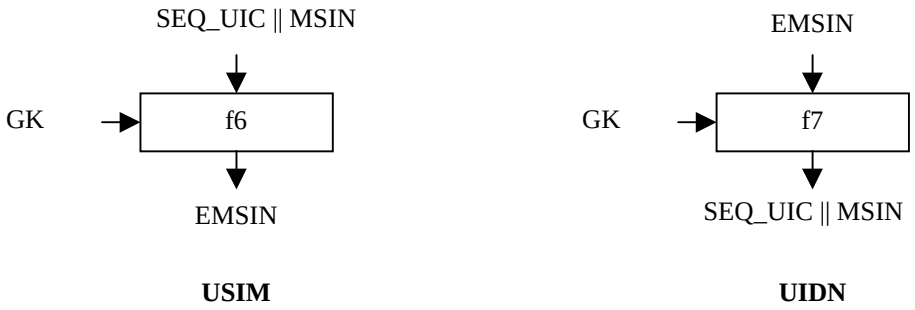


Figure A.1: Encryption and decryption of the permanent user identity

The mechanism for user identity confidentiality that is described in annex B of [1] requires the following cryptographic functions:

f6 the user identity encryption function;

f7 the user identity decryption function.

Figure A.2 describes the use of the one-way function f10 to calculate a paging-id for an user to avoid using the IMSI

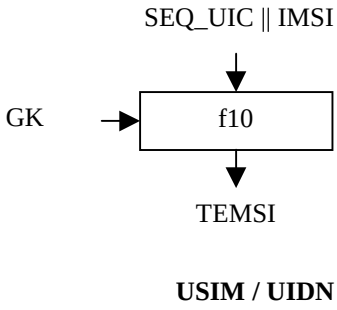


Figure A.2: Calculation of the Temporary Encrypted Mobile Subscriber Identity

A.2 Use

The functions f6 and f7 shall only be used to protect the confidentiality of the user identity when transmitted from USIM to ~~AuC~~UIDN

.

The function f10 shall only be used to derive a paging-id from the IMSI and the SEQ_UIC.

A.3 Allocation

The function f6 is allocated to the USIM. The function f7 is allocated to the ~~Authentication Centre~~UIDN.

The function f10 is allocated to the USIM and the UIDN

A.4 Extent of standardisation

The functions f6, ~~and~~ f7, and f10 are proprietary to the home environment.

A.5 Implementation and operational considerations

The function f6 shall be designed so that it can be implemented on an IC card equipped with a X1-bit microprocessor running at X2 MHz and with X3 kbits of memory and produce ~~EMUI~~ EMSIN in less than X11 ms.

The functions f7 shall be designed so that they can be implemented in software in the ~~AuC~~ UIDN on a X6-bit microprocessor running at X7 MHz and X8 kbits of memory and produce SEQ_UIC || ~~IMUI~~ EMSIN in less than X12 ms.

The function f10 shall be designed so that it can be implemented on an IC card equipped with a X1-bit microprocessor running at X2 MHz and with X3 kbits of memory and produce TEMSI in less than X11 ms.

A.6 Type of algorithm

A.6.1 f6

f6: the user identity encryption function

f6: (GK; SEQ_UIC || ~~IMUI~~MSIN) → ~~EMUI~~EMSIN

f6 should be a block cipher.

A.6.2 f7

f7: the user identity decryption function

f7: (GK; ~~EMUI~~EMSIN) → SEQ_UIC || ~~IMUI~~MSIN

f7 should be a block cipher and the inverse function of f6, in the sense that

x = f7(y; f6(y; x)), for all valid x = SEQ_UIC || ~~IMUI~~MSIN and all valid y = GK.

A.6.3 f10

f10: the paging-id function

f10: (GK; SQN_UIC || IMSI) -> TEMSI

f10 should be a one-way function.

A.7 Interface

A.7.1 GK

GK: the user group key

GK[0], GK[1], …, GK[X13-1]

The maximum length of the group key GK is X13 bits. The user group key GK is a long term secret key stored in several USIMs and in the ~~AuC~~UDIN.

A.7.2 SEQ_UIC

SEQ_UIC: the sequence for user identity confidentiality

SEQ_UIC[0], SEQ_UIC[1], …, SEQ_UIC[X14-1]

The length of SEQ_UIC is X14 bits. The SEQ_UIC is generated by the USIM and should be different each time so as to prevent traceability of a user.

~~A.7.3 IMUI~~A.7.3 IMSI

~~IMUI~~IMSI: the international mobile user identity

IMSI~~UI~~[0], IMSI~~UI~~[1], …, IMSI~~UI~~[X15-1]

The length of the IMUI is X15bits. The IMSI~~UI~~ is the permanent identity of the user, stored in the USIM and in the ~~AuC~~UIDN.

~~A.7.4 EMUI~~A.7.4 EMSIN

~~EMUI~~EMSIN: the encrypted mobile station identification number~~user identity~~

EMSIN~~UI~~[0], EMSIN~~UI~~[1], …, EMSIN~~UI~~[X16-1]

The length of the EMSIN~~UI~~ is X16 bits.

A.7.5 TEMSI

TEMSI: the temporary encrypted IMSI

TEMSI[0], TEMSI[1], ..., TEMSI[X22-1]

The length of the TEMSI is X22 bits.

Annex C:
Unspecified values

Reference	Meaning	Range	Source
X1	Bus width of the USIM processor (bit)		TSG T WG3
X2	Clock speed of the USIM processor (MHz)		TSG T WG3
X3	Memory size of the USIM (kbits)		TSG T WG3
X4	Response time for AK, MAC-A and RES (ms)		TSG SA WG2
X5	Response time for CK and IK (ms)		TSG SA WG2
X6	Bus width of the AuC processor (bit)		TSG CN
X7	Clock speed of the AuC processor (MHz)		TSG CN
X8	Memory size of the AuC (kbits)		TSG CN
X9	Response time for authentication vector in AuC (ms)		TSG SA WG2
X10	Length of sequence number (bits)	32—64	TSG SA WG3
X11	Response time for ~~EMUI~~ EMSIN computation in the USIM (ms)		TSG SA WG2
X12	Response time for SEQ_UIC || ~~IMUI~~ EMSIN in the ~~AuC~~ UIDN (ms)		TSG SA WG2
X13	Length of the group key (bits)	128	TSG SA WG3
X14	Length of SEQ_UIC (bits)	~~32~~24	TSG SA WG3
X15	Length of ~~IMUI~~ IMSI (bits)		TSG SA
X16	Length of ~~EMUI~~ EMSIN (bits)	~~128~~64	TSG SA WG3
X17	Number of gates required for hardware implementation of ciphering algorithm	10 000	TSG T WG3 TSG CN
X18	Length of the field LENGTH for ciphering (bits)		TSG RAN WG2
X19	Maximum length of a signalling message (bits)		TSG SA WG3 TSG RAN WG2
X20	Length of MAC-I (bits)	24	TSG SA WG3
X21	Length of RES and XRES (bits)	32-128	TSG SA WG3
X22	Length of TEMSI	as per IMSI	TSG SA WG3