3GPP TSG SA #6 **Tdoc TSG SA SP-99586**
Nice, FRANCE
15th - 17th December 1999

Source: TSG SA WG3

Subject: R99 CRs to 33.103
Agenda item: 5.3.3

This document contains CRs to 33.103 version 3.0.0 agreed by SA WG3 to be presented to SA#6 for approval.

CR	REV	CAT	SUBJECT	WG_DOC	3G_PHASE
001	1	C	Refinement of Enhanced User Identity Confidentiality	S3-99456	99
002	1	D	Corrections to figure 1	S3-99390	99
004		C	Change length of KSI (and other miscellaneous	S3-99415	99

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**	**001 r1**	Current Version:	3.0.0

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

For submision to TSG SA#6 *list TSG meeting no. here* ↑ for approval **X** for information *(only one box should 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: *(at least one should be marked with an X)* USIM **X** ME [ ] UTRAN [ ] Core Network **X**

Source: TSG SA WG3 **Date:** 1999-11-18

Subject: Refinement of Enhanced User Identity Confidentiality

3G Work item: Enhanced User Identity Confidentiality

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: This CR incorporates changes proposed to 33.102 related to refinement and clarification of enhanced user identity confidentiality mechanism.

Clauses affected: 3.3; 4.2.1; 6.2.1

Other specs affected:

Other 3G core specifications	**X**	→ List of CRs:	CR 33.102-022r1
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.

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 to Y
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption
ECK	Network Wide Cipher Key
ECKC	Network Cipher Key Component for UE
ECKCpeer	Network Cipher Key Component for peer UE
EMSI	Encrypted Subscriber identity
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
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
Text1	Optional Data Field
Text2	Optional Data Field
Text3	Public Key algorithm identifier and Public Key Version Number (eventually included in Public Key Certificate)
TMSI	Temporary Mobile Subscriber Identity
TTP	Trusted Third Party
~~TVP~~	~~Time Variant Parameter~~
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UN	User Name
USIM	User Services Identity Module
VLR	Visited Location Register
X	Network Identifier
XMAC	Expected message authentication code for user authentication
XMAC-I	Expected message authentication code for data integrity
XRES	Expected Response
XUR	Expected User Response
Y	Network Identifier

4.2 User services identity module

4.2.1 Enhanced User Identity Confidentiality (~~EUIF~~$_{USIM}$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) $SQN_{UIC/~~MS~~}$: a counter that is equal to the highest SQN_{UIC} generated and sent by the USIM to the HE/HLR/AuC;

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

c) GI: a group identifier that identifies the group the user refers to as well as the GK;

d) HLR-id consists of the first 3 digits of MSIN as a subaddress of HLR the user is related to;

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

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
GK	Group key	1 per user group the user belongs to	Permanent	128[1] bits	Optional
$SQN_{UIC/~~MS~~}$	Counter	1 per user	Updated when protocol for EUIC is executed	32 bits	Optional
G~~MS~~I	Group Identity	1 per user	Permanent	32 bits	Optional
HLR-id	Sub~~A~~address of entitiy which can perform decryption (first 3 digits of MSIN)	1 per user	Permanent	3 digits	Optional

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

– f6: the user identity encryption function.~~—~~

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

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

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

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

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:

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

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

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
~~$SQN_{UIC/HE}$~~	~~Counter~~	~~1 per user~~	~~Updated when protocol for EUIC is executed~~	~~32~~	~~Optional~~

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

– f7: the user identity decryption function.~~—~~

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

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

3GPP TSG-S3

The Hague, Netherlands
26 - 27 October 1999

Document S3-99390

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** **002r1** Current Version: 3.0.0

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

For submision to TSG *list TSG meeting no. here ↑*

for approval [X]
for information [ ]

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

Source: S3 **Date:** 25/10/99

Subject: Corrections to Figure 1 (UMTS functional security architecture)

3G Work item:

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	
D	Editorial modification	X

Reason for change: To correct DI_{UE} and clarify VLR as distinct from SN.

Clauses affected:

Other specs Affected:

Other 3G core specifications	[ ]	→ List of CRs:
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.

4.1 Functional network architecture

Figure 1 shows the functional security architecture of UMTS.

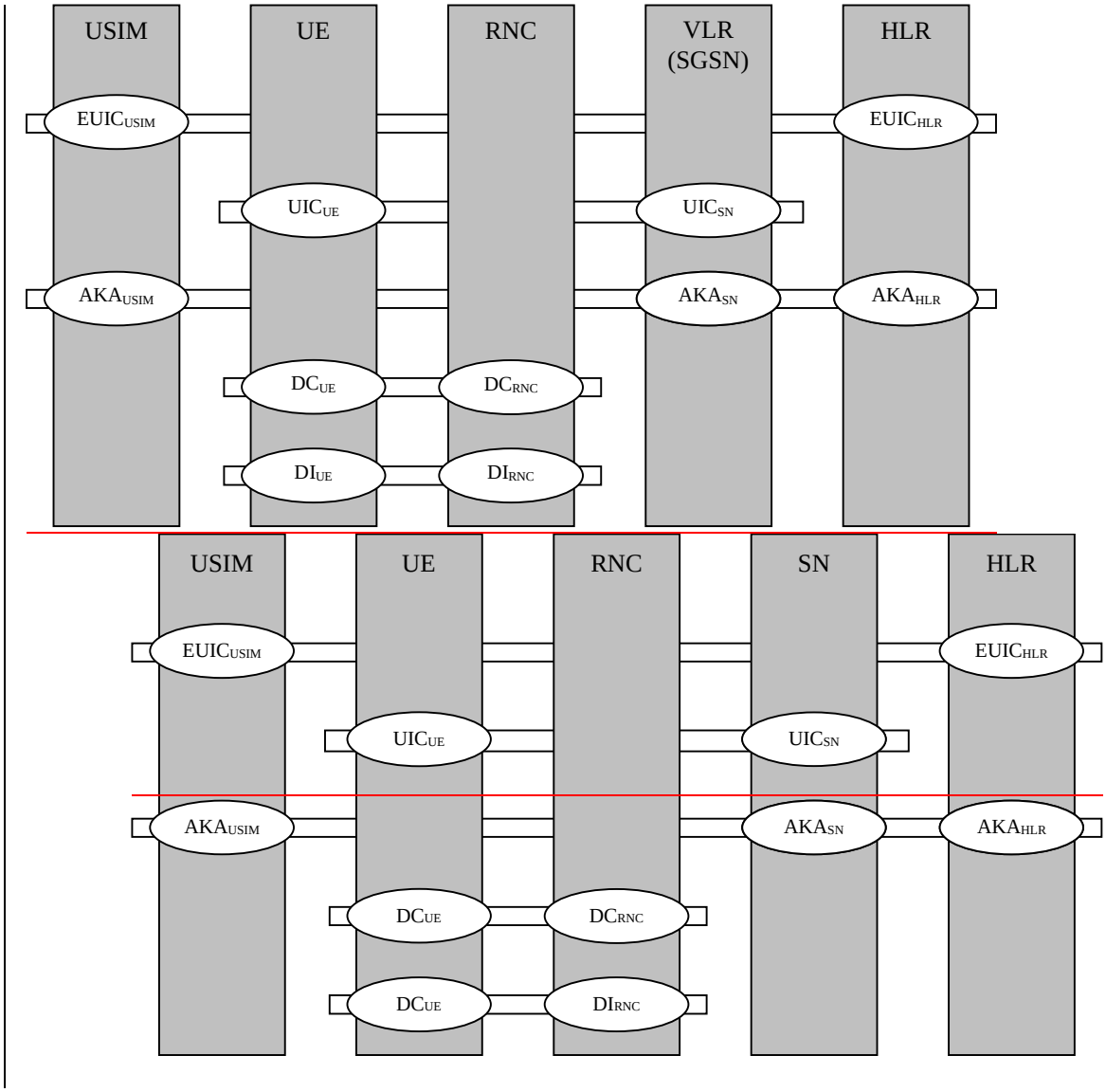

Figure 1: UMTS functional security architecture

The vertical bars represent the network elements:

In the user domain:

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

– UE (User Equipment);

In the serving network (SN) domain:

– RNC (Radio Network Controller);

– VLR (Visited Location Register), also the SGSN;

In the home environment (HE) domain:

– HLR/AuC.

The horizontal lines represent the security mechanisms:

– EUIC: mechanism for enhanced user identity confidentiality (optional, between user and HE);
– UIC: conventional mechanism for user identity confidentiality (between user and serving network);

- AKA: the mechanism for authentication and key agreement, including the functionality to trigger a re-authentication by the user, i.e., to control the access key pair lifetime;
- DC: the mechanism for data confidentiality of user and signalling data;
- DI: the mechanism for data integrity of signalling data.
- DEC: the mechanism for network-wide data confidentiality

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

TSG SA WG3 #8, **S3-99415**

3G CHANGE REQUEST

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

TS 33.103 **CR** **004** Current Version: V3.0.0

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

For submission to TSG SA#6 for approval [X] *(only one box should*
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 [X] ME [X] UTRAN [ ] Core Network [X]
(at least one should be marked with an X)

Source: Vodafone **Date:** 16-11-99

Subject: Change length of KSI, removal of SQN from AV, correction of AUTN and AV length and correction of group identity terminology

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: The length of KSI is changed to reach alignment with CKSN in GSM.

Clauses affected: Sections 4.2.1, 4.2.2, 4.5.2

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
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:

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

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

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

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

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

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

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

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

– f6: the user identity encryption function.

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

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

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

4.2.2 Authentication and key agreement (AKA_{USIM})

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

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

a) K: a permanent secret key;

b) SQN_{MS}: a counter that is equal to the highest sequence number SQN in an AUTN parameter accepted by the user.

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

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

e) $RAND_{MS}$: the random challenge which was received 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}).

---

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

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	~~4~~ 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

4.5.2 Authentication and key agreement (AKA_{SN})

The VLR (equivalently the SGSN) shall support the UMTS mechanism for authentication and key agreement described

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

in 6.3 of 3G TS 33.102.

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

a) AV: Authentication vectors;

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

Table 16: Composition of an authentication vector

Symbol	Description	Multiplicity	Length
~~SQN~~	~~Sequence number~~	~~1~~	~~32 64~~
RAND	Network challenge	1	128
XRES	Expected response	1	32-128
CK	Cipher key	1	128
IK	Integrity key	1	128
AUTN	Authentication token	1 that consists of:	~~96 128~~112-144
SQN or SQN ⊕ AK	~~Concealed s~~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 Authentication vectors	several per user, SN dependent	Depends on many things	~~544 640~~528-656	Mandatory
KSI	Key set identifier	1 per user	Updated when AKA protocol is executed	3~~4~~ bits	Mandatory
CK	Cipher key	1 per user	Updated when AKA protocol is	128 bits	Mandatory

			executed		
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