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: T-Mobil **Date:** 2000-Feb-10

Subject: Refinement of EUIC according to 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.

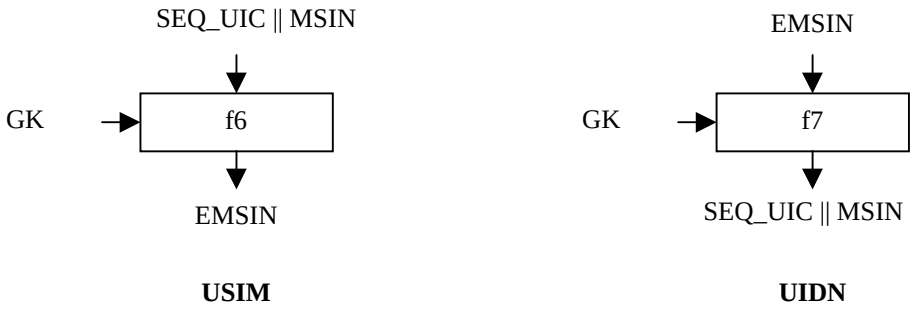

Figure A.1: Encryption and decryption of the permanent user identity

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

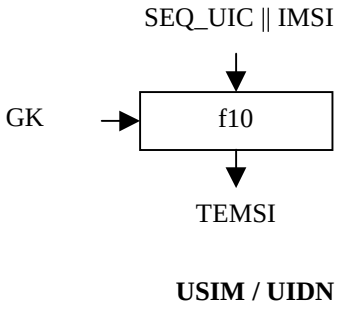

Figure A.2: Calculation of the Temporary Encrypted Mobile Subscriber Identity

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