3GPP TSG SA WG3 (Security) meeting #10 *S3-000082*
Antwerp, 19-21 January 2000

DRAFT 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 33.105 CR 007 Current Version: V3.2.0

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

Source:	TSG SA WG3	**Date:**	21-01-2000
Subject:	Enhanced user confidentiality		
3G Work item:	Security		

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

Reason for change:	Align with TS33.102 (Security Architecture), descriptions and figures on the enhanced user confidentiality have been corrected.
Clauses affected:	3.3, Annex A

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:	

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
CK	Cipher key
EMS~~U~~I	Encrypted Mobile Subscriber~~User~~ Identity
GK	User group key
IK	Integrity key
IMS~~U~~I	International Mobile Subscriber~~User~~ 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
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
UE	User equipment
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**Error! Reference source not found.** illustrates the use of the encryption function f6 to encrypt the IMS~~U~~I and the sequence for user identity confidentiality (SEQ_UIC) into an EMS~~U~~I and the use of the decryption function f7 to decrypt the EMS~~U~~I and retrieve the SEQ_UIC and the IMS~~U~~I.

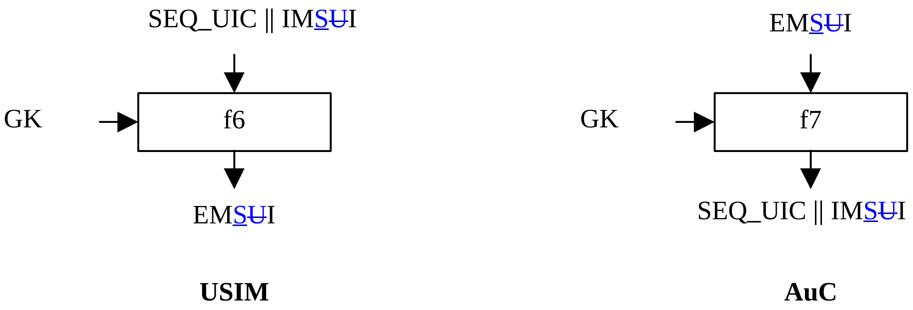

Figure A: Encryption and decryption of the permanent user identity

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.

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.

A.3 Allocation

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

A.4 Extent of standardisation

The functions f6 and f7 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 in less than X11 ms.

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

A.6 Type of algorithm

A.6.1 f6

f6: the user identity encryption function f6: (GK; SEQ_UIC || IMS~~U~~I) → EMS~~U~~I

f6 should be a block cipher.

A.6.2 f7

f7: the user identity decryption function

f7: (GK; EMS~~U~~I) → SEQ_UIC || IMS~~U~~I

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 || IMS~~U~~I and all valid y = GK.

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.

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 IMS~~U~~I

IMS~~U~~I: the international mobile subscriber~~user~~ identity

IMS~~U~~I[0], IMS~~U~~I[1], …, IMS~~U~~I[X15-1]

The length of the IMS~~U~~I is X15bits. The IMS~~U~~I is the permanent identity of the user, stored in the USIM and in the AuC.

A.7.4 EMS~~U~~I

EMS~~U~~I: the encrypted mobile subscriber~~user~~ identity

EMS~~U~~I[0], EMS~~U~~I[1], …, EMS~~U~~I[X16-1]

The length of the EMS~~U~~I is X16 bits.