3GPP TSG SA WG 3 (Security) meeting #10
Antwerp, 19—21 January, 2000

S3-000081

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**		Current Version:	3.3.1

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

For submission to TSG	SA #7	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 ☒ ME ☒ UTRAN □ Core Network ☒
(at least one should be marked with an X)

Source: T-Mobil **Date:** 2000-Jan-18

Subject: Refinement EUIC

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: Clarification needed after meeting with N2 experts

Clauses affected: 2.1, 3.3, 6.2 and annex B

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.

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
$E_{KSXY(i)}$(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
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
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.

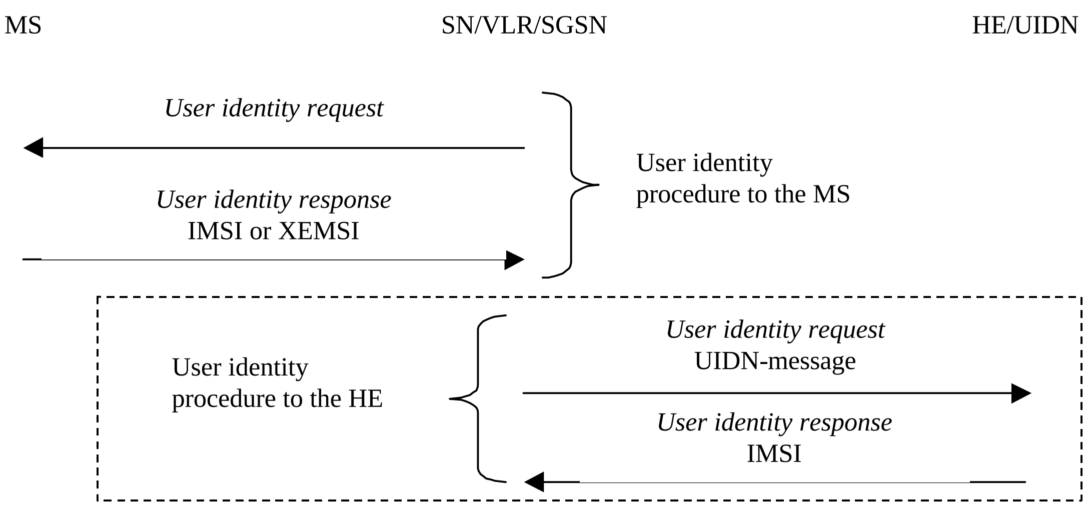


Figure 4: Identification by the permanent identity

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 (UIDN, see below) address and a UIDN-message. For details concerning the structure of the XEMSI see [26]. UIDN address shall ~~exist~~consist 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 to the user's UIDN/HE in a request to send the user's ~~IMUI~~IMSI. The user's UIDN/HE then derives the ~~IMUI~~ IMSI from the ~~HE~~UIDN-message and sends the ~~IMUI~~ IMSI back to the SN/VLR/SGSN. Annex B describes an example mechanism that makes use of group keys to encrypt the ~~IMUI~~IMSI and provides details on the UIDN-message.

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 by this home network node.

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

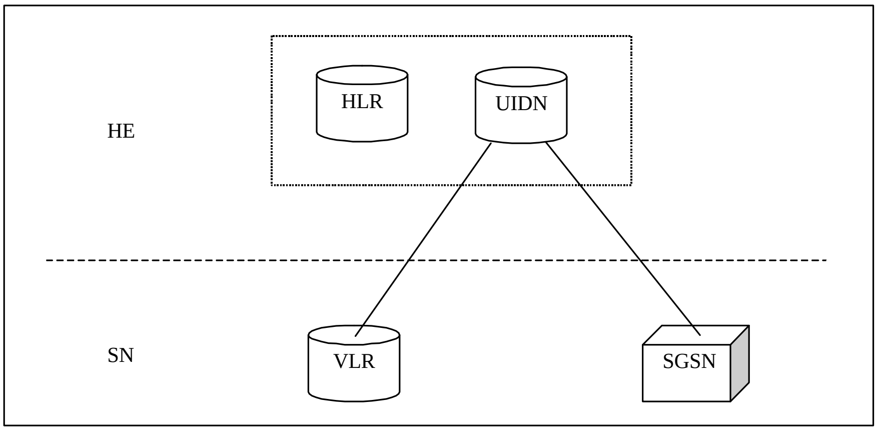


Figure 5: Core Network Architecture for Enhanced User Identity Confidentiality

The interface between the VLR and the UIDN is used by the VLR to request the decryption of the EIMSI contained in the UIDN-message from the UIDN for the circuit switched domain.

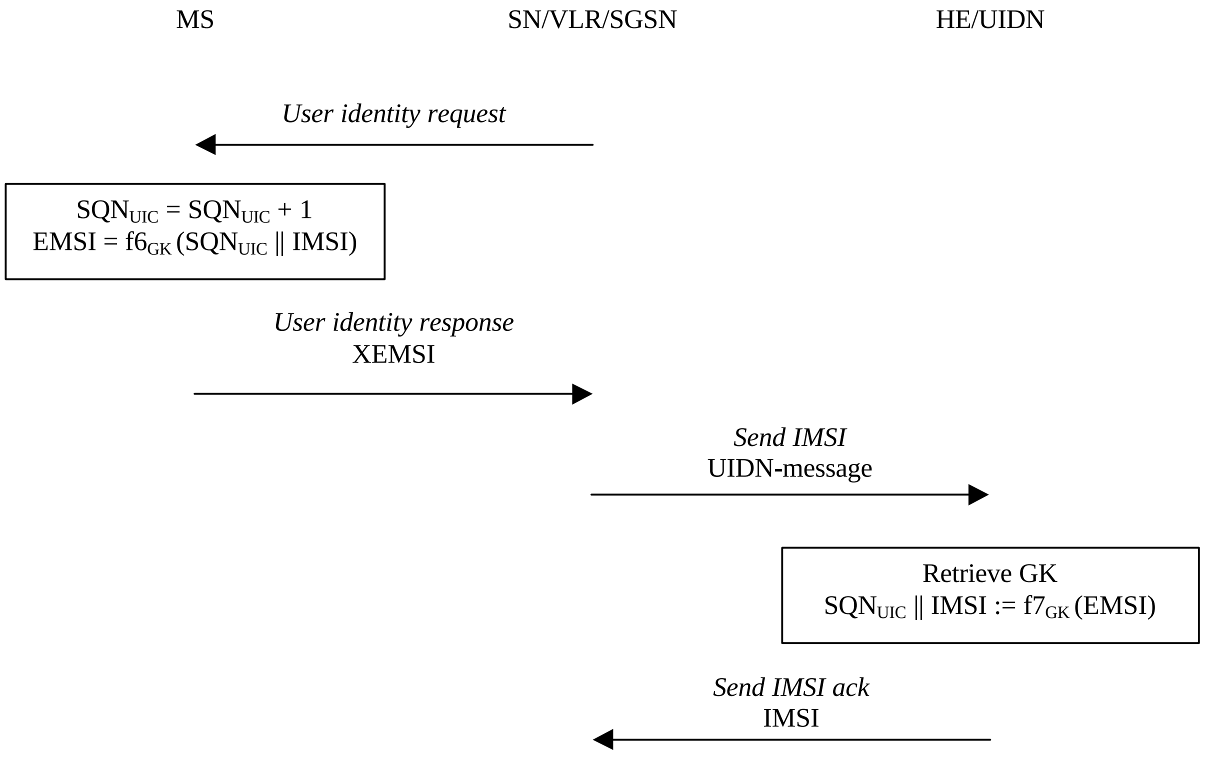
The interface between the SGSN and the UIDN is used by the SGSN to request the decryption of the EIMSI contained in the UIDN-message from the UIDN for the packet switched domain.

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

XEMSI := UIDN-address || UIDN-message
UIDN-address := UIDN’s global title (according to 6.2)
UIDN-message := GI||EMSI

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

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

Upon receipt the user increments SQN_{UIC} as a time variant parameter. The user encrypts SQN_{UIC} and the ~~IMUI~~ IMSI with enciphering algorithm f6 and his group key GK. The SQN_{UIC} prevents traceability attacks. 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~~

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

Upon receipt the HE/~~HLR~~ UIDN retrieves the group key GK associated with the group identity GI. The HE/~~HLR~~ UIDN then decrypts ~~EMUI~~ EMSI with the deciphering algorithm f7 (f7 = f6^{-1}) and the group key GK and retrieves SQN$_{UIC}$ and ~~IMUI~~IMSI. SQN$_{UIC}$ is no longer used. The HE/~~HLR~~ UIDN then sends the ~~IMUI~~ IMSI in a response to the visited SN/VLR/SGSN.