

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 for approval (only one box should be marked with an X)
list TSG meeting no. here ↑ 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 ME UTRAN Core Network

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
- 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	<input type="checkbox"/>	→ 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	<input type="checkbox"/>	→ List of CRs:
MS test specifications	<input type="checkbox"/>	→ List of CRs:
BSS test specifications	<input type="checkbox"/>	→ List of CRs:
O&M specifications	<input type="checkbox"/>	→ 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
$D_{SK(X)}(\text{data})$	Decryption of "data" with Secret Key of X used for signing
<u>EMSI</u>	<u>Encrypted Mobile Subscriber Identity</u>
<u>EMSIN</u>	<u>Encrypted MSIN</u>
$E_{KSXY(i)}(\text{data})$	Encryption of "data" with Symmetric Session Key #i for sending data from X to Y
$E_{PK(X)}(\text{data})$	Encryption of "data" with Public Key of X used for encryption
<u>GI</u>	<u>Group Identifier</u>
<u>GK</u>	<u>Group Key</u>
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
<u>MSIN</u>	<u>Mobile Station Identity Number</u>
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
<u>TEMSI</u>	<u>Temporary Encrypted Mobile Subscriber Identity used for paging instead of IMSI</u>
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
<u>UIDN</u>	<u>User Identity Decryption Node</u>
USIM	User Services Identity Module
VLR	Visitor Location Register
X	Network Identifier
<u>XEMSI</u>	<u>Extended Encrypted Mobile Subscriber Identity</u>
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 (~~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 ~~IMSI~~ from the ~~TMUI-TMSI~~ by which the user identifies itself on the radio path.

The mechanism is illustrated in Figure 4.

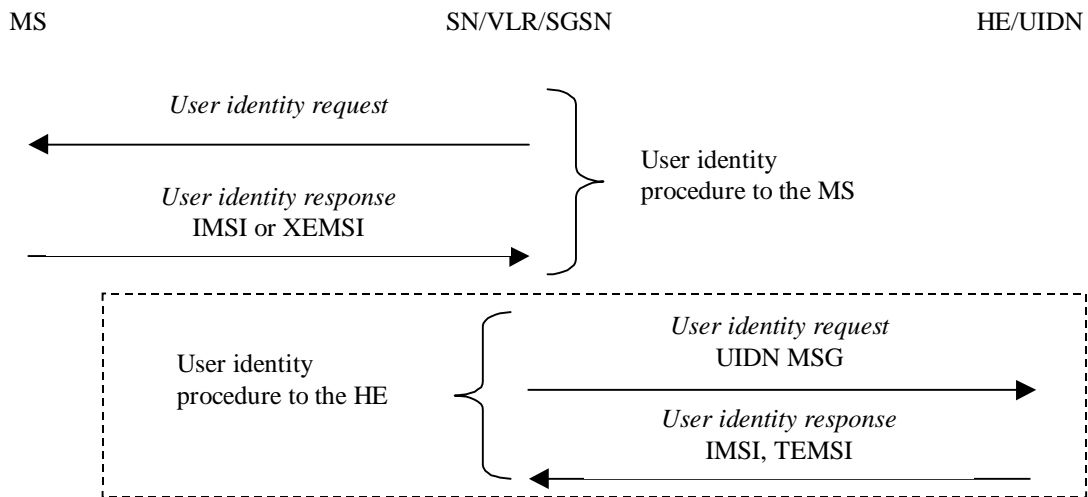


Figure 4: Identification by the permanent identity

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.

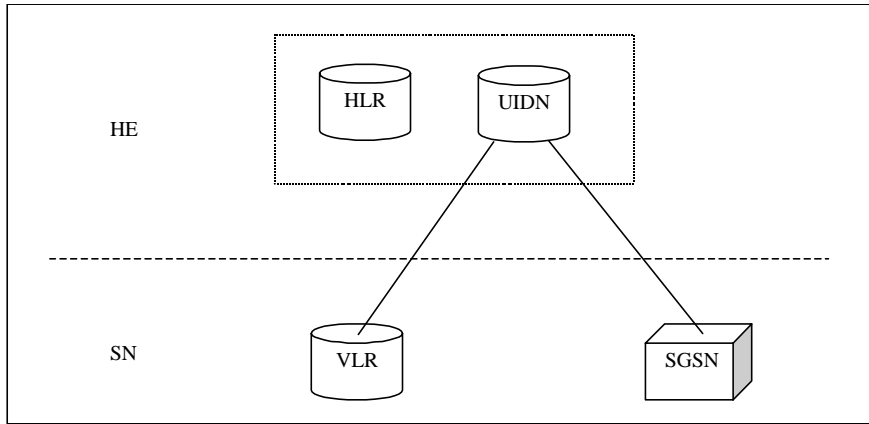


Figure 5: Core Network Architecture for Enhanced User Identity Confidentiality

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

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

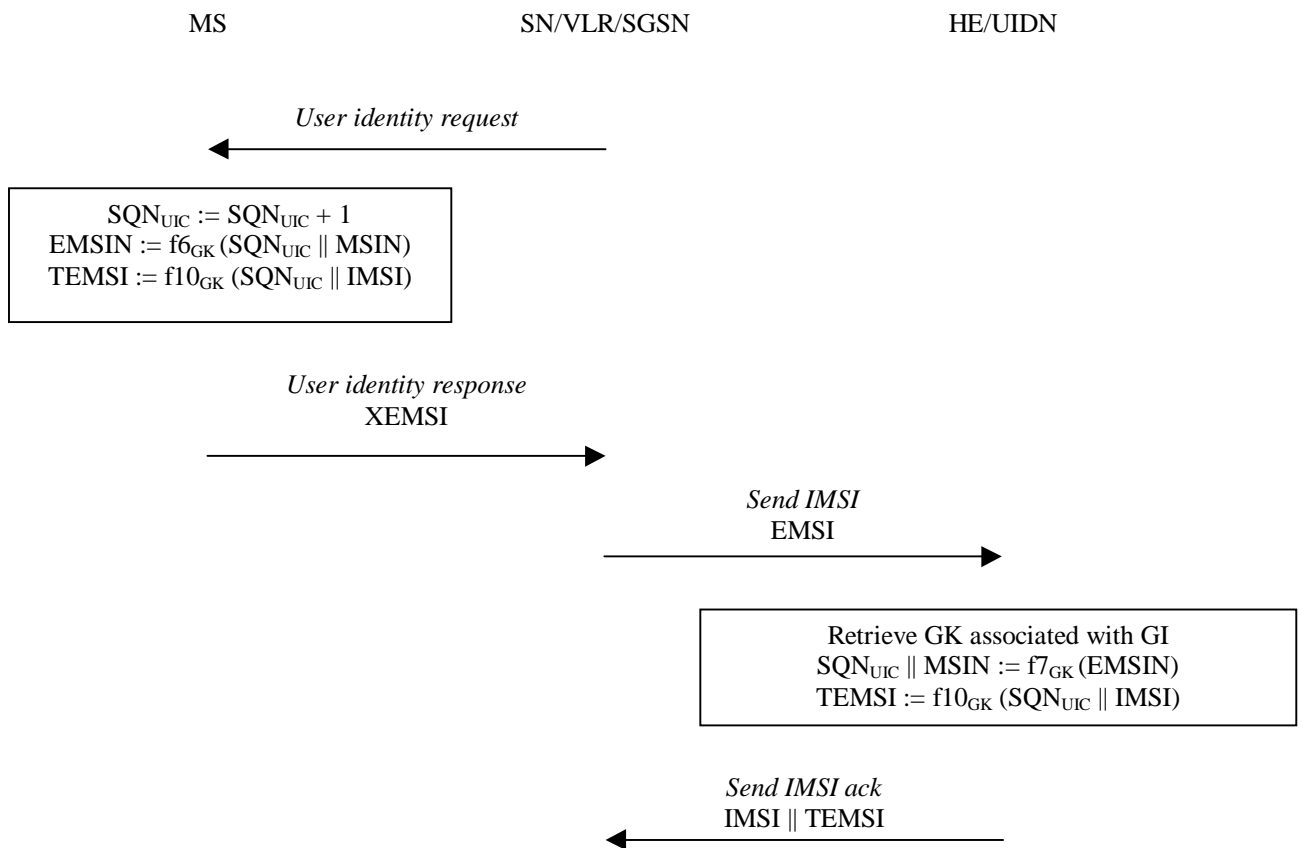
The interface between the SGSN and the UIDN is used by the SGSN to request the decryption of the EIMSI contained in the UIDN message from the UIDN for the packet switched domain.

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_{UEC} as a time variant parameter. ~~The user~~
 - encrypts SQN_{UEC} 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_{UEC} with cryptographic algorithm f10 and the group key GK.
- The SQN_{UEC} 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/HLRUIDN 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/HLRUIDN.
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-EM SIN with the deciphering algorithm f_7 ($f_7 = f_6^{-1}$) and the group key GK and retrieves SQN_{UIC} and ~~IMUI~~ MSIN.
 - constructs the user's IMSI according to the following rule: $IMSI := MCC_{UIDN_ADR} || MNC_{UIDN_ADR} || MSIN_{UIDN_ADR}$
($UIDN_ADR := MCC_{UIDN_ADR} || MNC_{UIDN_ADR} || MSIN_{UIDN_ADR}$).
 - calculates TEMSI as $TEMSI := f_{10_{GK}}(SQN_{UIC} || IMSI)$ ~~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.