3GPP TSG SA WG 3 Meeting #12
Stockholm, Sweden, 11-14 April 2000

***Document* S3-000268**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

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:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: SA#7 *list expected approval meeting # here ↑*	for approval	X	strategic		*(for SMG use only)*
	for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM	X	ME	X	UTRAN / Radio		Core Network	X

Source: Siemens Atea **Date:** 11 April 2000

Subject: Removal of enhanced user identity confidentiality

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	X

Reason for change: Decision taken by the SA#6.

Clauses affected: 3.2, 3.3, 5.1.1, 6.2, Annex B

Other specs affected:

Other 3G core specifications	X	→ List of CRs:	CR against 33.103 CR against 33.105
Other GSM 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.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

‖	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK
~~f6~~	~~Encryption function used to encrypt the IMUI~~
~~f7~~	~~Decryption function used to decrypt the IMUI ($=f6^{-1}$)~~
K	Long-term secret key shared between the USIM and the AuC

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
~~EMSI~~	~~Encrypted Mobile Subscriber Identity~~
~~EMSIN~~	~~Encrypted MSIN~~
$D_{SK(X)}$(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
~~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
~~MSIN~~	~~Mobile Station Identity Number~~
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
~~TEMSI~~	~~Temporary Encrypted Mobile Subscriber Identity used for paging instead of IMSI~~
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
UICC	UMTS IC Card
~~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

5.1.1 User identity confidentiality

The following security features related to user identity confidentiality are provided:

- **user identity confidentiality:** the property that the permanent user identity (IMUI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;
- **user location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **user untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

To achieve these objectives, the user is normally identified by a temporary identity by which he is known by the visited serving network, or by an encrypted permanent identity. To avoid user traceability, which may lead to the compromise of user identity confidentiality, the user should not be identified for a long period by means of the same temporary or encrypted identity. To achieve these security features, in addition it is required that any signalling or user data that might reveal the user's identity is ciphered on the radio access link.

Clause 6.1 describes a mechanism that allows a user to be identified on the radio path by means of a temporary identity by which he is known in the visited serving network. This mechanism should normally be used to identify a user on the radio path in location update requests, service requests, detach requests, connection re-establishment requests, etc..

~~Clause 6.2 describes a mechanism that allows a user to be identified on the radio path in case he is not known in the visited serving network by a temporary identity. It provides a transparent channel between the USIM and the user's HE that provides the user's HE with the option to implement a mechanism that allows identification by means of an encrypted permanent identity. The serving network then has to forward the encrypted permanent identity to the user's HE for decryption and receives the user's permanent identity from the user's HE. A possible mechanism that makes use of symmetric key encryption using group keys is included in Annex B. Alternatively, the user's HE environment has the option to let the user identify himself by means of its permanent identity in cleartext. Either of both mechanisms should be used to identify a user on the radio path, whenever the user is not known by a temporary identity in the serving network.~~

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 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 TMSI by which the user identifies itself on the radio path.

The mechanism is illustrated in Figure 4.

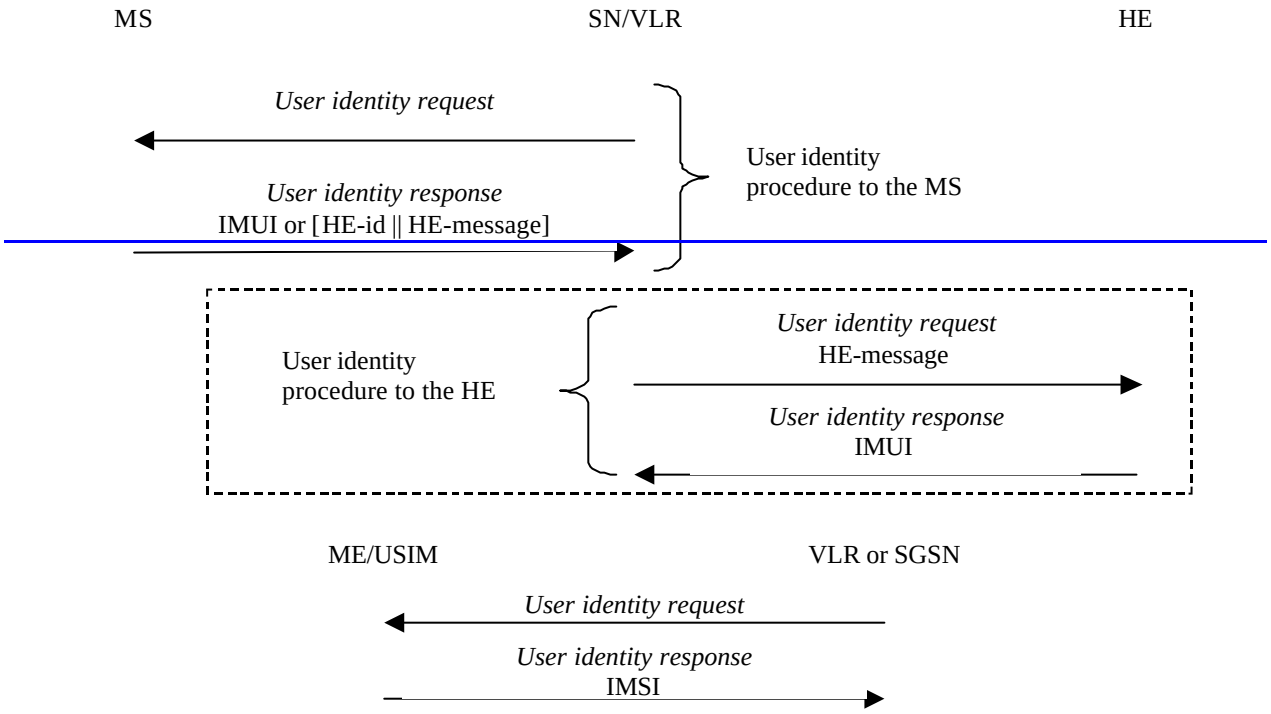


Figure 4: Identification by the permanent identity

The mechanism is initiated by the visited ~~SN/~~VLR or SGSN that requests the user to send its permanent identity. ~~According to the user's preferences, his~~ The user's response ~~may~~ contains ~~either 1)~~ the ~~IMSA~~ 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) and a 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].~~

~~In case the response contains the IMSI in cleartext, the procedure is ended successfully.~~ This ~~variant~~ represents a breach in the provision of user identity confidentiality.

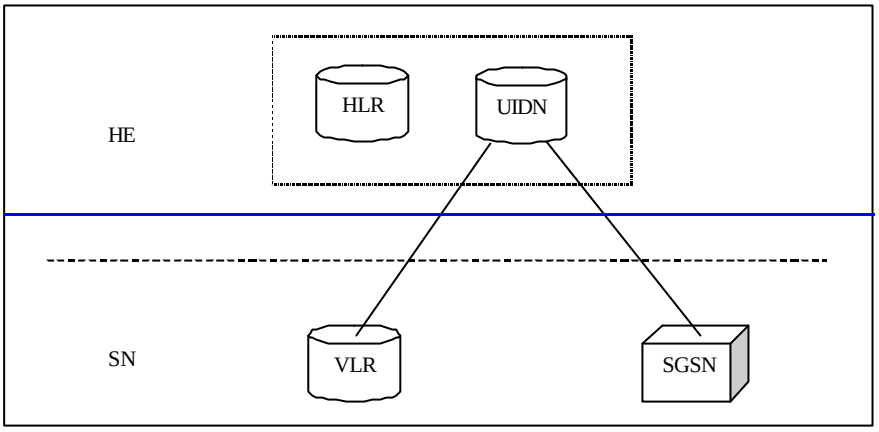
~~In case the response contains the XEMSI, the visited SN/VLR/SGSN forwards the EMSI to the user's UIDN/HE in a request to send the user's IMSI and TEMSI (Temporary EMSI). The user's UIDN/HE then derives the IMSI from EMSI, calculates TEMSI and sends the IMSI and TEMSI back to the SN/VLR/SGSN. Annex B describes an example mechanism that makes use of group keys to encrypt the IMSI and to calculate the TEMSI and provides details on 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 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 of the IMSI contained in EMSI from the UIDN;~~
- ~~calculation of the TEMSI for the circuit/packet switched domain;~~
- ~~most recently derived TEMSI.~~

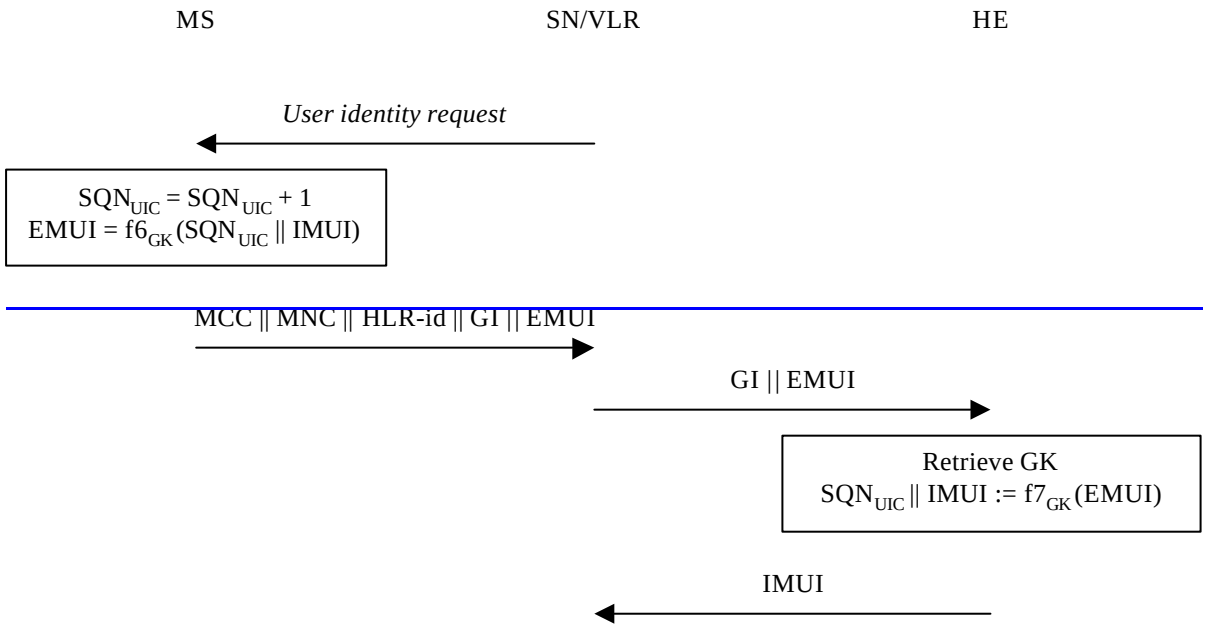
Annex B ~~(informative)~~: Void

~~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/UIDN.~~

~~The mechanism is illustrated in Figure B.1.~~



~~Figure B.1: Identification by means of the 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 USIM to send its XEMSI.~~

2) ~~Upon receipt the USIM:~~

   - ~~increments SQN_{UIC} as a time variant parameter;~~
   - ~~encrypts SQN_{UIC} and its MSIN with enciphering algorithm f6 and 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_{UIC} with cryptographic algorithm f10 and the group key GK.~~

   ~~The SQN_{UIC} prevents traceability attacks and synchronizes the derivation of TEMSI in the USIM and HE.~~

3) ~~Upon receipt of that response the SN/VLR/SGSN resolves the UIDN_ADR from XEMSI and forwards EMSI to the user's HE/UIDN.~~

4) Upon receipt the HE/UIDN:

- retrieves the group identity GI contained in EMSI;
- retrieves the group key GK associated with the group identity GI;
- decrypts EMSIN with the deciphering algorithm f7 (f7 = $f6^{-1}$) and the group key GK and retrieves SQN_{UIC} and MSIN;
- constructs the user's IMSI according to the following rule: IMSI := MCC_{UIDN_ADR} || MNC_{UIDN_ADR} || MSIN (UIDN_ADR := MCC_{UIDN_ADR} || MNC_{UIDN_ADR} || $MSIN_{UIDN\_ADR}$);
- calculates TEMSI as TEMSI := $f10_{GK}$ (SQN_{UIC} || IMSI);
- sends IMSI and TEMSI in a response to the visited SN/VLR/SGSN.

SQN_{UIC} is no longer used. The HE/HLR then sends the IMUI in a response to the visited SN/VLR.