3GPP TSG SA WG 3 (Security) meeting #13
Yokohama (Japan), 24—26 May, 2000

Document **S3-000335**
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.

33.103	**CR**	**xxx**	Current Version:	3.2.0

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

For submission to:	SA #8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		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 [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: Ericsson **Date:** 2000-05-19

Subject: Removal of EUIC from 33.103

Work item: Security

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

F	Correction	X
A	Corresponds to a correction in an earlier release	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Release:

Phase 2	
Release 96	
Release 97	
Release 98	
Release 99	X
Release 00	

Reason for change: As per SA#7 decision, EUIC is not a R99 feature. EUIC is therefore removed from 33.103.

Clauses affected: 4.2.1, 4.3.4, 4.5.2, 4.7.

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
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.

4.2.1 Enhanced User Identity Confidentiality ($EUIC_{USIM}$)

For UMTS users with EUIC, the USIM has to store additional data and have additional functions implemented to encrypt the permanent user identity (IMSI). We describe the requirements as regards data storage and algorithm implementation for an example mechanism in annex B of 3G TS 33.102.

The following data elements need to be stored on the USIM:

a) SQN_{UIC}: a counter that is equal to the highest SQN_{UIC} generated and sent by the USIM to the HE/UIDN;

b) GK: the group key used to encrypt the MSIN and SQN_{UIC};

c) GI: a group identifier that identifies the group the user refers to as well as the GK;

d) TEMSI: a temporary identity used for paging instead of IMSI;

d) UIDN_ADR: address of UIDN according to E.164.

Table 1: USIM – Enhanced User Identity Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
GK	Group key	1 per user group the user belongs to	Permanent	128 bits (Note 1)	Optional
SQN_{UIC}	Counter	1 per user	Updated when protocol for EUIC is executed	32 bits	Optional
GI	Group Identity	1 per user	Permanent	32 bits	Optional
TEMSI	Temporary identity used for paging instead of IMSI	1 per user	Updated when a new identity request has been performed	As per IMSI	Optional
UIDN_ADR	Address of UIDN according to E.164	1 per user	Permanent	15 digits	Optional

NOTE 1: The table entry is for the example secret key mechanism given in annex B of 33.102

The following cryptographic functions need to be implemented in the USIM:

- f6: the user identity encryption function;
- f10: TEMSI calculation function.

For a summary of the data elements and cryptographic function of the $EUIC_{HE}$ function see table 2.

Table 2: USIM – Enhanced User Identity Confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f6	User identity encryption function	1	Permanent	Proprietary	Optional
f10	TEMSI calculation function	1	Permanent	Proprietary	Optional

4.3.4 Enhanced user identity confidentiality ($EUIC_{UE}$)

The UE shall support the UMTS mechanism for enhanced user identity confidentiality described in 6.2 of 3G TS 33.102.

The UE shall store the following data elements:

- the TEMSI: a temporary identity used for paging instead of IMSI.

Table 9a: UE – User Identity Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
TEMSI	Temporary identity used for paging instead of IMSI	1 per user	Updated when a new identity request has been performed	As per IMSI	Optional

4.5.2 Enhanced user identity confidentiality ($EUIC_{SN}$)

The VLR (equivalently the SGSN) shall support the UMTS mechanism for enhanced user identity confidentiality described in 6.2 of 3G TS 33.102.

The VLR shall store the following data elements:

- the TEMSI: a temporary identity used for paging instead of IMSI.

Table 15a: VLR – User Identity Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
TEMSI	Temporary identity used for paging instead of IMSI	1 per user	Updated when a new identity request has been performed	As per IMSI	Optional

Equivalently, the SGSN shall store the following data elements:

- the TEMSI: a temporary identity used for paging instead of IMSI.

Table 15b: SGSN – User Identity Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
TEMSI	Temporary identity used for paging instead of IMSI	1 per user	Updated when a new identity request has been performed	As per IMSI	Optional

4.7 Enhanced user identity confidentiality ($EUIC_{HE}$)

For UMTS users with EUIC, the UIDN has to store additional data and have additional function implemented to decrypt the permanent user identity (IMSI) and to calculate the paging identity TEMSI to be used instead of IMSI. We describe the requirements as regards data storage and algorithm implementation for the example mechanism in annex B of 3G TS 33.102.

The following data elements need to be stored on the UIDN:

a) GK: the group key used to decrypt the IMSI and SQN_{UIC};

b) GI: a group identifier that identifies the group the user refers to as well as the GK;

c) TEMSI: a temporary identity used for paging instead of IMSI;

d) IMSI: the IMSI of the user the feature is applied to.

Table 21a: UIDN – Enhanced User Identity Confidentiality – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
GK	Group key	1 per user group	Permanent	128	Optional
GI	Group Identity	1 per user	Permanent	32 bits	Optional
TEMSI	Temporary identity used for paging instead of IMSI	1 per user	Updated when a new identity request has been performed	As per IMSI	Optional
IMSI	IMSI	1 per user	Permanent	64 bits	Optional

The following cryptographic functions need to be implemented in UIDN:

- f7: the user identity decryption function.
- f10: TEMSI calculation function.

For a summary of the data elements and cryptographic function of the $EUIC_{HE}$ function see table 2.

Table 21b: UIDN – Enhanced User Identity Confidentiality – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f7	User identity decryption function	1	Permanent	Proprietary	Optional
f10	TEMSI calculation function	1	Permanent	Proprietary	Optional