3GPP TSG SA WG3 Security — S3#11 **S3-000110**

22-24 February, 2000

Mainz, Germany

Source: **T-Mobil**

Title: **Related CRs and documents on EUIC from other groups**

Document for: **Information**

Agenda Item:

The following 4 documents were provided by T-Mobil for information and have been input to the SA WG3 meeting by the Secretary (Maurice Pope).

RAN WG2 document: Introduction of EUIC

T WG3 CR to 33.102: Alignment of Enhanced User Identity Confidentiality feature with S3 requirements

CN WG1 CR to 24.008: Introduction of a new code point within the mobile identity IE, encrypted IMSI

SA WG2 CR to 23.060: Introduction of Enhanced User Identity Confidentiality

3GPP TSG-RAN WG2 Meeting #11 **TSGR2#11(00)0xxx**
Torino, Italy, February 28th – March 3rd, 2000

Agenda Item: x.x

Source: T-Mobil

Title: Introduction of EUIC
(Enhanced User Identification Confidentiality)

Document for: Discussion and Decision

Introduction

During TSG SA#6 it became apparent that the full R'99 security features as defined and specified by SA3 are not fully implemented into the current set of 3GPP specifications. Therefore it is allowed to include open issues for R'99 until TSG SA#7 [Tdoc TSGS#6(99)622].

One open issue is the Enhanced User Identification Confidentiality (EUIC) for which actually work is done e.g. in SA3 and CN1. They adopt their specifications to use the EUIC feature for Release 99.

It is also necessary to modify the RAN specification TS 25.331 due to implementation of this feature.

This Change Request to TS 25.331 proposes the modification of the UE identity in the way that a new UE identification (Extended Encrypted Mobile Subscriber Identity – XEMSI) and a temporary UE identity (Temporary Encrypted Mobile Subscriber Identity – TEMSI) is introduced that allows to identify and page an UE with an encrypted identity and not with its IMSI in clear form.

3GPP TSG-RAN WG2 Meeting #11
Torino, Italy, February 28th – March 3rd, 2000

Document R2-000xxx

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.

25.331	CR	xxx	Current Version:	3.1.0

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

For submission to:	TSG-RAN#7	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	X	ME	X	UTRAN / Radio	X	Core Network	X

Source: T-Mobil **Date:** Feb. 11, 2000

Subject: Inclusion of Enhanced User Identification Confidentiality (EUIC)

Work item:

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

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

Reason for change: Implementation of Enhanced User Identification Confidentiality (EUIC) in 3GPP specifications due to decision made in SA#6.

Clauses affected: 3.2, 8.5.1, 9.1, 10.1.16, 10.1.xx, 10.2.3.16, 10.2.3.25

Other specs affected:			
Other 3G core specifications		→ List of CRs:	23.003, 23.012, 23.018, 23.060, 24.008, 29.002, 31.102, 33.102, 33.103, 33.105
Other GSM core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
		→ 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 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in [1] apply.

3.2 Abbreviations

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

ACK	Acknowledgement
AICH	Acquisition Indicator CHannel
AM	Acknowledged Mode
AS	Access Stratum
ASN.1	Abstract Syntax Notation.1
BCCH	Broadcast Control Channel
BCFE	Broadcast Control Functional Entity
BER	Bite Error Rate
BLER	BLock Error Rate
BSS	Base Station Sub-system
C	Conditional
CCPCH	Common Control Physical CHannel
CCCH	Common Control Channel
CN	Core Network
CM	Connection Management
CPCH	Common Packet CHannel
C-RNTI	Cell RNTI
DCA	Dynamic Channel Allocation
DCCH	Dedicated Control Channel
DCFE	Dedicated Control Functional Entity
DCH	Dedicated Channel
DC-SAP	Dedicated Control SAP
DL	Downlink
DRAC	Dynamic Resource Allocation Control
DSCH	Downlink Shared Channel
DTCH	Dedicated Traffic Channel
EUIC	Enhanced User Identification Confidentiality
FACH	Forward Access Channel
FAUSCH	Fast Uplink Signalling Channel
FDD	Frequency Division Duplex
FFS	For Further Study
GC-SAP	General Control SAP
ID	Identifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IE	Information element
IP	Internet Protocol
ISCP	Interference on Signal Code Power
LAI	Location Area Identity
L1	Layer 1
L2	Layer 2
L3	Layer 3
M	Mandatory
MAC	Media Access Control
MCC	Mobile Country Code
MM	Mobility Management

MNC	Mobile Network Code
MS	Mobile Station
NAS	Non Access Stratum
Nt-SAP	Notification SAP
NW	Network
O	Optional
ODMA	Opportunity Driven Multiple Access
PCCH	Paging Control Channel
PCH	Paging Channel
PDCP	Packet Data Convergence Protocol
PDSCH	Physical Downlink Shared Channel
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
PNFE	Paging and Notification Control Functional Entity
PRACH	Physical Random Access CHannel
P-TMSI	Packet Temporary Mobile Subscriber Identity
PUSCH	Physical Uplink Shared Channel
QoS	Quality of Service
RAB	Radio access bearer
RB	Radio Bearer
RAI	Routing Area Identity
RACH	Random Access CHannel
RB	Radio Bearer
RFE	Routing Functional Entity
RL	Radio Link
RLC	Radio Link Control
RNTI	Radio Network Temporary Identifier
RNC	Radio Network Controller
RRC	Radio Resource Control
RSCP	Received Signal Code Power
RSSI	Received Signal Strength Indicator
SAP	Service Access Point
SCFE	Shared Control Function Entity
SF	Spreading Factor
SHCCH	Shared Control Channel
SIR	Signal to Interference Ratio
SSDT	Site Selection Diversity Transmission
S-RNTI	SRNC - RNTI
tbd	to be decided
TDD	Time Division Duplex
TEMSI	Temporary Encrypted Mobile Subscriber Identity
TF	Transport Format
TFCS	Transport Format Combination Set
TFS	Transport Format Set
TME	Transfer Mode Entity
TMSI	Temporary Mobile Subscriber Identity
Tr	Transparent
Tx	Transmission
UE	User Equipment
UL	Uplink
UM	Unacknowledged Mode
UMTS	Universal Mobile Telecommunications System
UNACK	Unacknowledgement
URA	UTRAN Registration Area
U-RNTI	UTRAN-RNTI
USCH	Uplink Shared Channel
UTRAN	UMTS Terrestrial Radio Access Network
XEMSI	Extended Encrypted Mobile Subscriber Identity

8.5 General procedures

8.5.1 Selection of initial UE identity

The purpose of the IE "Initial UE identity" is to provide a unique UE identification at the establishment of an RRC connection. The type of identity shall be selected by the UE according to the following.
If the variable SELECTED_CN in the UE has the value "GSM-MAP", the UE shall choose "UE id type" in the IE "Initial UE identity" with the following priority:

1. TMSI (GSM-MAP): The TMSI (GSM-MAP) shall be chosen if available. The IE "LAI" in the IE "Initial UE identity" shall also be present when TMSI (GSM-MAP) is used, for making it unique.

2. P-TMSI (GSM-MAP): The P-TMSI (GSM-MAP) shall be chosen if available and no TMSI (GSM-MAP) is available. The IE "RAI" in the IE "Initial UE identity" shall in this case also be present when P-TMSI (GSM-MAP) is used, for making it unique.

3. TEMSI (GSM-MAP): The TEMSI (GSM-MAP) shall be chosen if neither TMSI (GSM-MAP) nor P-TMSI (GSM-MAP) is available.

4. XEMSI (GSM-MAP): The XEMSI (GSM-MAP) shall be chosen if no TMSI (GSM-MAP), P-TMSI (GSM-MAP) or TEMSI (GSM-MAP) is available.

5. IMSI (GSM-MAP): The IMSI (GSM-MAP) shall be chosen if available and no XEMSI (GSM-MAP), TEMSI (GSM-MAP), TMSI (GSM-MAP) or P-TMSI (GSM-MAP) is available.
   If a UE supports the EUIC feature and the feature is activated the IMSI shall never be chosen.

6. IMEI: The IMEI shall be chosen when none of the above ~~three~~ five conditions are fulfilled.

When being used, the IEs "TMSI (GSM-MAP)," "P-TMSI (GSM-MAP)", "TEMSI (GSM-MAP)", "XEMSI (GSM-MAP)", "IMSI (GSM-MAP)", "LAI" and "RAI" shall be set equal to the values of the corresponding identities stored in the USIM or SIM.

9 Protocol states

9.1 RRC States and State Transitions including GSM

Figure 46 shows the RRC states in Connected Mode, including transitions between UTRAN connected mode and GSM connected mode for PSTN/ISDN domain services, and between UTRAN connected mode and GSM/GPRS packet modes for IP domain services. It also shows the transitions between Idle Mode and UTRAN Connected Mode and further the transitions within UTRAN connected Mode.

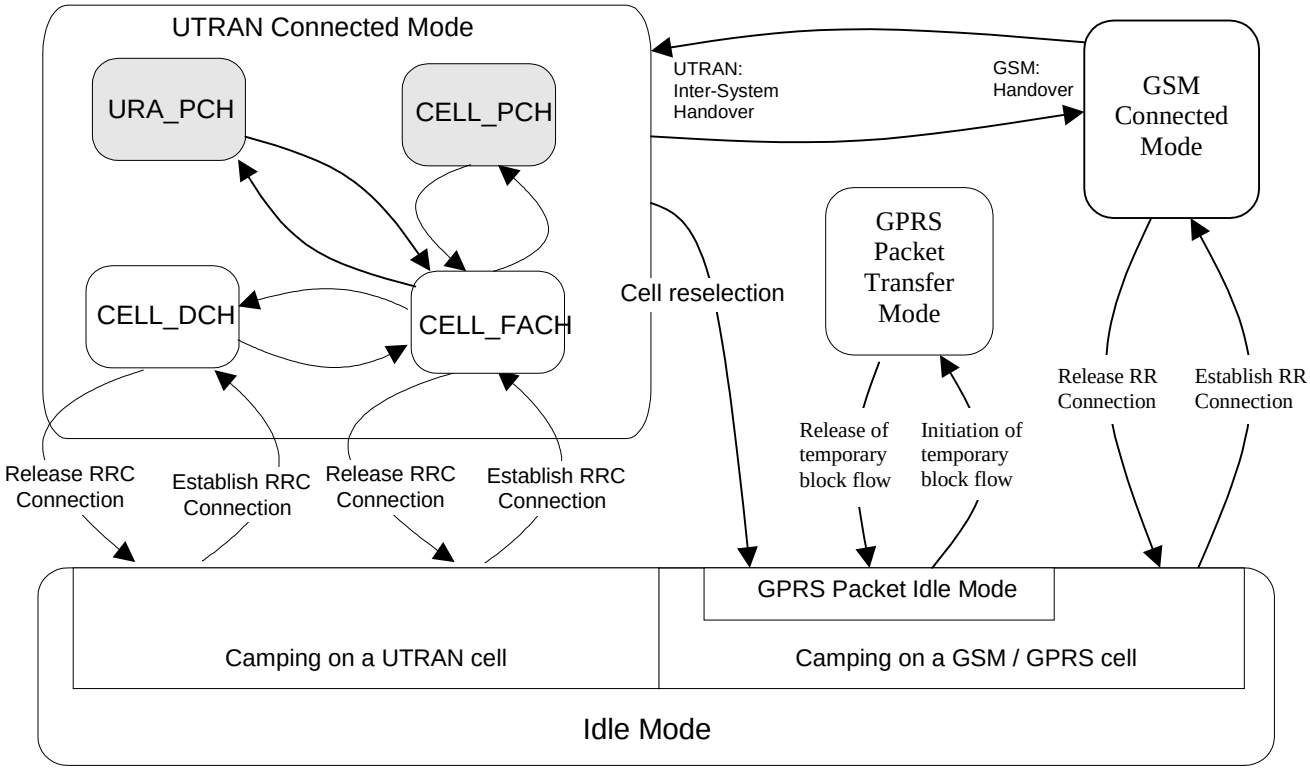


Figure 46: RRC States and State Transitions including GSM
[[1]: The indicated division within Idle Mode is only included for clarification and shall not be interpreted as states.]

It shall be noted that not all states may be applicable for all UE connections. For a given QoS requirement on the UE connection, only a subset of the states may be relevant.
After power on, the UE stays in Idle Mode until it transmits a request to establish an RRC Connection. In Idle Mode the connection of the UE is closed on all layers of the access stratum. In Idle Mode the UE is identified by non-access stratum identities such as IMSI, XEMSI, TEMSI, TMSI and P-TMSI. In addition, the UTRAN has no own information about the individual Idle Mode UEs, and it can only address e.g. all UEs in a cell or all UEs monitoring a paging occasion. The UE behaviour within this mode is described in [4].
The UTRAN Connected Mode is entered when the RRC Connection is established. The UE is assigned a radio network temporary identity (RNTI) to be used as UE identity on common transport channels.
NOTE: The exact definition of RRC connection needs further refinement.

The RRC states within UTRAN Connected Mode reflect the level of UE connection and which transport channels that can be used by the UE.

For inactive stationary data users the UE may fall back to PCH on both the Cell and URA levels. That is, upon the need for paging, the UTRAN shall check the current level of connection of the given UE, and decide whether the paging message shall be sent within the URA, or should it be sent via a specific cell.

10.1.16 PAGING TYPE 2

This message is used to page an UE in connected mode, when using the DCCH for CN originated paging.

RLC-SAP: AM

Logical channel: DCCH

Direction: UTRAN → UE

Information Element	Presence	Multi	IE type and reference	Semantics description
Message Type	M			
UE information elements				
Integrity check info	O			
CN Information elements				
CN domain identity	M			
Paging Record Type Identifier	M		Enumerated (IMSI (GSM-MAP), TEMSI (GSM-MAP), TMSI (GSM-MAP)/ P-TMSI, IMSI (DS-41), TMSI (DS-41))	
UE Information elements				
Paging cause	M			

10.2.1.xx XEMSI (GSM-MAP)

This IE contains an Extended Encrypted Mobile Subscriber Identity, used towards a GSM-MAP type of core network.

Information Element/Group name	Presence	Range	IE type and reference	Semantics description
XEMSI (GSM-MAP)	M		Bitstring (192)	Setting specified in [TS 23.003]

10.2.1.xx TEMSI (GSM-MAP)

This IE contains a Temporary Encrypted Mobile Subscriber Identity, used towards a GSM-MAP type of core network.

Information Element/Group name	Presence	Range	IE type and reference	Semantics description
TEMSI (GSM-MAP)	M			Setting specified in [TS 23.003]

10.2.3.16 Initial UE identity

This information element identifies the UE at a request of an RRC connection.

Information Element/Group name	Presence	Range	IE type and reference	Semantics description
CHOICE UE id type	M			
>IMSI (GSM-MAP)			IMSI (GSM-MAP)	
>XEMSI (GSM-MAP)			XEMSI (GSM-MAP)	
>TEMSI (GSM-MAP)			TEMSI (GSM-MAP)	
>TMSI (GSM-MAP)			TMSI (GSM-MAP)	
>P-TMSI (GSM-MAP)			P-TMSI (GSM-MAP)	
>IMEI			IMEI	
>ESN (DS-41)			TIA/EIA/IS-2000-4	
>IMSI (DS-41)			TIA/EIA/IS-2000-4	
>IMSI and ESN (DS-41)			TIA/EIA/IS-2000-4	
>TMSI (DS-41)			TIA/EIA/IS-2000-4	
LAI (GSM-MAP)			TS 24.008	
RAI (GSM-MAP)			TS 24.008	

CHOICE *UE Id Type*	Condition under which the given *UE Id Type* is used
IMSI(GSM-MAP)	See section 8.5.1
XEMSI (GSM-MAP)	See section 8.5.1
TEMSI (GSM-MAP)	See section 8.5.1
TMSI(GSM-MAP)	See section 8.5.1
P-TMSI(GSM-MAP)	See section 8.5.1
IMEI	See section 8.5.1
ESN (DS-41)	See section 8.5.1
IMSI (DS-41)	See section 8.5.1
IMSI and ESN (DS-41)	See section 8.5.1
TMSI (DS-41)	See section 8.5.1

10.2.3.25 Paging record

Information Element/Group name	Presence	Range	IE type and reference	Semantics description
Paging originator	M		Enumerated (UTRAN,CN)	
Paging cause	C isCN			
CN domain identity	C isCN			
CHOICE CN Identity	C idleMode			
>IMSI (GSM-MAP)			IMSI (GSM-MAP)	
>TEMSI (GSM-MAP)			TEMSI (GSM-MAP)	
>TMSI (GSM-MAP)			TMSI (GSM-MAP)	
>P-TMSI (GSM-MAP)			P-TMSI (GSM-MAP)	
>IMSI (DS-41)			TIA/EIA/IS-2000-4	
>TMSI (DS-41)			TIA/EIA/IS-2000-4	
U-RNTI	C connected Mode			

Condition	Explanation
IsCN	This information element is included where the page is originated from the CN.
IdleMode	This IE is included for UE not having RRC Connection.
ConnectedMode	This IE is included for UE having RRC Connection.

CHOICE CN *Identity*	Condition under which the given *Identity* is chosen
IMSI	For idle mode pages
TEMSI	For idle mode pages
TMSI	For idle mode pages
P-TMSI	For idle mode pages
IMSI(DS-41)	For idle mode pages
TMSI(DS-41)	For idle mode pages

3GPP TSG-T3 #13
Tokyo, Japan, 21.-24. 2. 2000

Document T3-00-xxxx
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:	3.0.0

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

For submission to:	TSG-T #7	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: (U)SIM [X] ME [X] UTRAN / Radio [ ] Core Network [ ]
(at least one should be marked with an X)

Source: T-Mobil **Date:**

Subject: Enhanced User Identity Confidentiality

Work item:

Category:

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

(only one category shall be marked with an X)

Reason for change: Alignment of Enhanced User Identity Confidentiality feature with S3 requirements

Clauses affected:

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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3G TS 21.111: "USIM and IC Card Requirements".

[2] 3G TS 22.011: "Service accessibility".

[3] 3G TS 22.024: "Description of Charge Advice Information (CAI)".

[4] 3G TS 22.030: "Man-Machine Interface (MMI) of the Mobile Station (MS)".

[5] 3G TS 23.038: "Alphabets and language".

[6] 3G TS 23.040: "Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[7] 3G TS 23.060 : "General Packet Radio Service (GPRS); Service description; Stage 2".

[8] 3G TS 23.073: "Support of Localised Service Area (SoLSA)".

[9] 3G TS 24.008: "Mobile Radio Interface Layer 3 specification".

[10] 3G TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[11] 3G TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[12] 3G TS 31.111: "USIM Application Toolkit (USAT)".

[13] 3G TS 33.102: "3G Security Architecture".

[14] 3G TS 33.103: "3G Security; Integration Guidelines".

[15] 3G TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[16] 3G TS 23.041: "Technical realization of Short Message Service Cell Broadcast (SMSCB)".

[16] 3G TS 23.003: "Numbering, adressing and identification".

[17] GSM 02.07: "Mobile Stations (MS) features".

[18] GSM 11.11: "Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface".

[19] ISO 639 (1988): "Code for the representation of names of languages".

[20] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".

[21] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers ".

[22] ITU-T Recommendation E.164: "Numbering plan for the ISDN era".

[23] ITU-T Recommendation T.50: "International Alphabet No. 5". (ISO 646: 1983, "Information processing - ISO 7-bits coded characters set for information interchange".)

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

ADM: Access condition to an EF which is under the control of the authority which creates this file

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
f1*	A message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa.
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 to encipher the IMSI
f10	Encryption function used to compute TEMSI

3.3 Abbreviations

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

3GPP	3rd Generation Partnership Project
AC	Access Condition
ADF	Application Dedicated File
AID	Application IDentifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AoC	Advice of Charge
AuC	Authentication Centre
AUTN	Authentication token
BDN	Barred Dialling Number
CCP	Capability Configuration Parameter
CK	Cipher key
CS	Circuit switched
DF	Dedicated File
DO	Data Object
EF	Elementary File
EMUI	Encrypted Mobile User Identity
EUIC	Enhanced User Identity Confidentiality
FCI	File Control Information
FFS	For Further Study
GK	User group key
GMSI	Group Identity
GSM	Global System for Mobile communications
HE	Home Environment
ICC	Integrated Circuit Card

ID	IDentifier
IK	Integrity key
IMSI	International Mobile Subscriber Identity
K	USIM Individual key
KSI	Key Set Identifier
K_C	Cryptographic key used by the cipher A5
LSB	Least Significant Bit
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MCC	Mobile Country Code
MF	Master File
MMI	Man Machine Interface
MNC	Mobile Network Code
MODE	Indication packet switched / circuit switched mode
MSB	Most Significant Bit
NEV	NEVer
NPI	Numbering Plan Identifier
OFM	Operational Feature Monitor
PIN	Personal Identification Number
PS	Packet switched
RAND	Random challenge
$RAND_{MS}$	Random challenge stored in the USIM
RES	User response
RFU	Reserved for Future Use
RST	Reset
SDN	Service dialling number
SE	Security Environment
SFI	Short EF Identifier
SQN	Sequence number
SRES	Signed RESponse calculated by a USIM
SW	Status Word
TEMSI	Temporary encrypted user identity (IMSI)
TLV	Tag Length Value
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
XRES	Expected user RESponse
XEMSI	Extended encrypted user identity (MSIN)

4.2.41 EF_{GMSI} (Group Identity)

This EF contains the group identity of the mobile subscriber. This group identity references a group key GK, stored in the USIM, which is used for enhanced user identity confidentiality (enciphering of the IMSI).

Identifier: '6FC2'	Structure: transparent	Optional
File size: 4 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	Group Identity	M	4 bytes

- Group Identity GMSI
  Coding:
  the least significant bit of GMSI is the least significant bit of the 4th byte. The most significant bit of GMSI is the most significant bit of the first byte.

4.2.42 $EF_{UIDNADR}$ (User Identity Decryption Node Adress)

This EF contains User Identity Decryption Node Adress UIDN_ADR used to locate the node for decryption of user identities. This file is required if service n°26 (EUIC) is available.

Identifier: '6FC4'	Structure: transparent	Optional
File size: 40 ?? bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 40	User Identity Decryption Node Adress	M	40 bytes

- User Identity Decryption Node Adress
  Coding:
  the least significant bit of UIDN_ADR is the least significant bit of the 40th byte. The most significant bit of UIDN_ADR is the most significant bit of the first byte. Unused digits are padded with 'FF'.

4.2.43~~2~~ $EF_{Hiddenkey}$ (Key for hidden phone book entries)

This EF contains the hidden key that has to be verified by the ME in order to display the phone book entries that are marked as hidden. The hidden key can consist of 4 to 8 digits.

Identifier: '6FC3'	Structure: transparent	Optional
File size: 4 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	PIN
DEACTIVATE	ADM
ACTIVATE	ADM

Bytes	Description	M/O	Length
1 to 4	Hidden Key	M	4 bytes

- Hidden Key

Coding:

the hidden key is coded on 4 bytes using BCD coding. The minimum number of digits is 4. Unused digits are padded with 'FF'.

NOTE: The phone book entries marked as hidden are not scrambled by means of the hidden key. The are stored in plain text in the phone book.

4.2.4~~3~~ Files required for 2G Access

...

4.2.4~~3~~.1 EF_{Kc} (Ciphering key Kc)

...

4.2.4~~3~~.2 EF_{KcGPRS} (GPRS Ciphering key KcGPRS)

...

4.2.4~~3~~.3 $EF_{LOCIGPRS}$ (GPRS location information)

...

4.2.4~~3~~.4 EF_{LOCI2G} (Location Information for 2G access)

...

4.2.4~~3~~.5 EF_{BCCH} (Broadcast Control Channels)

...

5.2.1 Authentication algorithms computation

The ME selects a USIM application and uses the INTERNAL AUTHENTICATE command (see 7.1.1). The response is sent to the ME (in case of the T=0 protocol when requested by a subsequent GET RESPONSE command).

~~5.2.2 IMSI request~~

~~The ME performs the reading procedure with EF_{IMSI}.~~

5.2.3 Access control information request

The ME performs the reading procedure with EF_{ACC}.

5.2.4 HPLMN search period request

The ME performs the reading procedure with EF_{HPLMN}.

5.2.5 Location information

Request: The ME performs the reading procedure with EF_{LOCI}.
Update: The ME performs the updating procedure with EF_{LOCI}.

In the case when updating EF_{LOCI} with data containing the TMSI value and the card reports the error '92 40' (Memory Problem), the ME shall terminate 3G operation.

5.2.6 Cipher and Integrity key

Request: The ME performs the reading procedure with EF_{Keys}.
Update: The ME performs the updating procedure with EF_{Keys}.

5.2.7 Forbidden PLMN

Request: The ME performs the reading procedure with EF_{FPLMN}.
Update: The ME performs the updating procedure with EF_{FPLMN}.

5.2.8 LSA information

Request: The ME performs the reading procedure with EF_{SAI}, EF_{SLL} and its associated LSA Descriptor files.
Update: The ME performs the updating procedure with EF_{SLL}.

5.2.9 User Identity Request

The ME selects a USIM and checks service n°26 ~~no. 26~~ (Enhanced user identity confidentiality). If service n°26 ~~no. 26~~ is not available then the ME performs the reading procedure with EF_{IMSI}.

Otherwise the ME uses the Encipher ~~IMSI~~ User Identity function to encipher the MSIN with cryptographic function f6(see 7.2.1). Then the ME uses the Encipher User Identity function to encipher the IMSI with cryptographic function f10(see 7.2.1) to obtain the TEMSI. In both cases ~~T~~the response is received by the ME (in case of the T=0 protocol when requested by a subsequent GET RESPONSE command).

NOTE: The TEMSI is used by the serving network to page a particular user.

Then the ME performs the reading procedures ~~with EF_{GMSI}~~ to obtain the group identity ~~out of EF_{GMSI}~~, and with $EF_{UIDNADR}$ to obtain the User Identity Decryption Node Adress UIDN_ADR. The ME concatenates UIDN_ADR ~~,the HE id,~~ the group identity ~~GMSI~~ and the enciphered ~~I~~MSIN to obtain XEMSI and sends that to the network.

5.2.10 GSM Cipher key

Request: The ME performs the reading procedure with EF_{Kc}.
Update: The ME performs the updating procedure with EF_{Kc}.

7 USIM Commands

…

7.2 Encipher ~~IMSI~~User Identity

7.2.1 Command description

The function is used during the procedure for identification of the user via the radio access path. It operates in two modes:

- ~~by means of the~~ encipher~~ed~~ the permanent user identity (IMSI) (see TS 23.003 [..]).

- encipher the MSIN which is a part of the IMSI (see TS 23.003 [..]).

For the execution of the command the USIM uses the group key GK and the sequence number $SEQ_{UIC/UE}$ which are stored internally in the USIM.

Each time the command is invoked in the first mode (to encipher the IMSI), ~~T~~the USIM increments the internal sequence number $SEQ_{UIC/UE}$ that holds the value from the last execution of 'Encipher User Identity~~IMSI~~'.

Next the USIM computes the enciphered IMSI as $f6_{GK}$ ($SEQ_{UIC/UE}$ || ~~I~~MSIN), or the enciphered MSIN as $f10_{GK}$ ($SEQ_{UIC/UE}$ || MSIN), ~~-~~which is then returned in the command response.

The function is related to a particular USIM and shall not be executable unless the USIM or any sub-directory has been selected as the Current Directory and a successful PIN verification procedure has been performed (see clause 5).

Input:
- none

Output:
- enciphered IMSI or MSIN.

7.2.2 Command parameters and data

Code	Value
CLA	As defined in 3G TS 31.101
INS	'2A'
P1	See below~~'00'~~
P2	'00'
Lc	not present
Data	not present
Le	Length of EMSI (L1)

Parameter P1 specifies the command mode as follows:

Coding of the reference control P1

Coding b8-b1	Meaning
'XXXXXXX0'	Encipher MSIN with f6
'XXXXXXX1'	Encipher IMSI with f10

Parameter Le specifies the expected length of the response. This is depending on the further specification of functions f6 and f10.

Command parameters/data:

none

Response parameters/data:

Byte(s)	Description	Length
1	Length of encrypted ~~IMSI~~Identity (L1)	1
2 to (L1+1)	Encrypted Identity~~IMSI~~	L1

The most significant bit of the encrypted Identity ~~IMSI~~ is coded on bit 8 of byte 2.

7.3.2 Status Words of the Commands

The following table shows for each command the possible status conditions returned (marked by an asterisk *). Status conditions of GSM and USIM applications are on the left and right sides of the table, respectively.

Commands and status words

AUTHENTICATE	ENCIPHER ~~IMSI~~USer	
		90 00
		91 XX
*	*	9F XX
		61XX#
		93 00
		92 0X
*	*	65 81
		94 00
		94 02
		94 04
*		94 08
		98 02
*	*	69 82
		98 08
		98 10
		98 40
		98 50
*		98 62
*	*	67 XX
*	*	6B XX
		6D XX
*	*	6E XX
*	*	6F XX
		62 81
		62 83
		62 82
		62 84
		62 00
		63 CX
		69 81
*	*	69 84
*	*	69 85
		69 86
		6A 81
		6A 82
		6A 83
		6A 84
		6A 85
*	*	6A 86
		6A 87
*	*	6A 88
		6C XX

3GPP/SMG Meeting #11
Umea, Sweden, 28th February – 3rd March 2000

Document N1-000280
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.

24.008	**CR**	**122rev1**	Current Version:	3.2.1

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

For submission to: *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	X	Core Network	X

Source: T-Mobil **Date:** 11.02.00

Subject: Introduction of a new code point within the mobile identity IE, encrypted IMSI

Work item: Security

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

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

Reason for change: This CR is necessary to introduce Enhanced User Identity Confidentiality according the WI security.
A new code point , named XEMSI will be introduced. This code point address the encrypted IMSI and the necessary routing information.

Clauses affected: 10.5.1.4, 10.5.3.4, 10.5.5.9, 4.7.9.1.2

Other specs affected:				
Other 3G core specifications		→ List of CRs:	23.003, 23.012, 23.018, 25.331, 29.002, 31.102, 33.103,33.105
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.

10.5.1.4 Mobile Identity

The purpose of the *Mobile Identity* information element is to provide either the international mobile subscriber identity, IMSI, the temporary mobile subscriber identity, TMSI/P-TMSI, the international mobile equipment identity, IMEI ~~or~~ the international mobile equipment identity together with the software version number, IMEISV ,the extended encrypted IMSI (XEMSI) or the Temporary encrypted mobile subscriber identity TEMSI .

The IMSI shall not exceed 15 digits, the TMSI/P-TMSI is 4 octets long, the TEMSI is 8 octets long, and the IMEI is composed of 15 digits, the IMEISV is 16 digits. The XEMSI is composed of an UIDN ADDR (max. 15 digits, coded as E.164 address) and an encrypted IMSI (presented by a Octet String with 1 to 12 octets) (see TS 23.003).

For packet paging the network shall select the mobile identity type with the following priority:

1- P-TMSI: The P-TMSI shall be used if it is available.

2- IMSI: The IMSI/TEMSI shall be used in cases where no P-TMSI is available.

If a mobile user supports encrypted IMSI (XEMSI) then the TEMSI will be used instead of the IMSI. For all other transactions except emergency call establishment, emergency call re-establishment, mobile terminated call establishment, the identification procedure, the GMM identification procedure, the GMM authentication and ciphering procedure and the ciphering mode setting procedure, the mobile station and the network shall select the mobile identity type with the following priority:

1- TMSI: The TMSI shall be used if it is available.

2- IMSI: The IMSI/XEMSI shall be used in cases where no TMSI is available.

For mobile terminated call establishment the mobile station shall select the same mobile identity type as received from the network in the PAGING REQUEST message. If a mobile user supports encrypted IMSI (XEMSI) then the XEMSI will be used instead of the IMSI.

For emergency call establishment and re-establishment the mobile station shall select the mobile identity type with the following priority:

1- TMSI: The TMSI shall be used if it is available.

2- IMSI: The IMSI/XEMSI shall be used in cases where no TMSI is available.

3- IMEI: The IMEI shall be used in cases where no SIM is available or the SIM is considered as not valid by the mobile station or no IMSI or TMSI is available.

In the identification procedure and in the GMM identification procedure the mobile station shall select the mobile identity type which was requested by the network. If a mobile user supports encrypted IMSI (XEMSI) then the XEMSI will be used instead of the IMSI.

In the ciphering mode setting procedure and in the GMM authentication and ciphering procedure the mobile shall select the IMEISV.

The *Mobile Identity* information element is coded as shown in figure 10.5.4/TS 24.008 and table 10.5.4/TS 24.008.

The *Mobile Identity* is a type 4 information element with a minimum length of 3 octet and 24 ~~11~~ octets length maximal. Further restriction on the length may be applied, e.g. number plans.

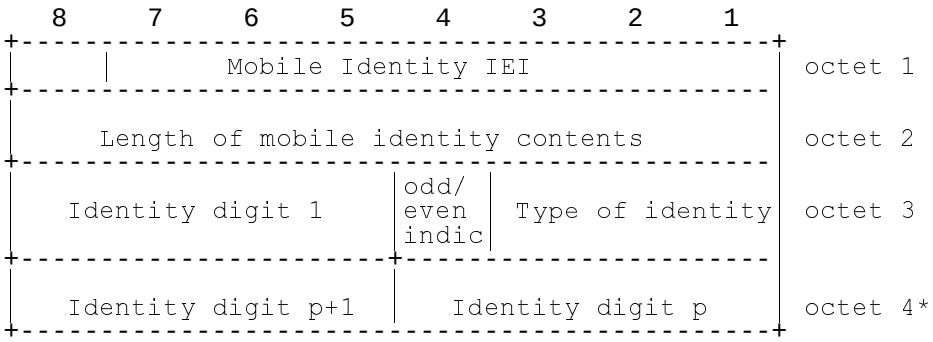


Figure 10.5.4/TS 24.008 *Mobile Identity* information element (TMSI/P-TMSI/TEMSI, IMSI, IMEI, IMEISV)

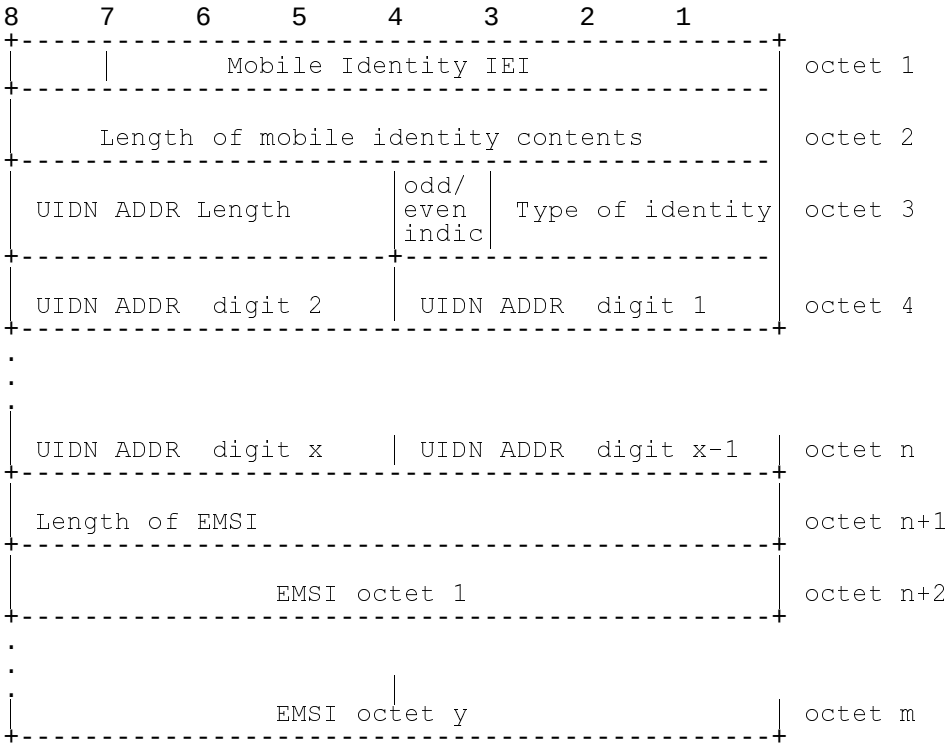


Figure 10.5.x/TS24.008 Mobile Identity information element (XEMSI)

Table 10.5.4/TS 24.008: *Mobile Identity* information element

Type of identity (octet 3)
Bits
3 2 1
0 0 1 IMSI
0 1 0 IMEI
0 1 1 IMEISV
1 0 0 TMSI/P-TMSI
1 0 1 XEMSI note 2)
1 1 0 TEMSI
0 0 0 No Identity note 1)

All other values are reserved.

Odd/even indication (octet 3)
Bit
4
0 even number of identity digits and also when the TMSI/P-TMSI is used
1 odd number of identity digits

Identity digits (octet 3 etc)
For the IMSI, IMEI , UIDN ADDR and IMEISV this field is coded using BCD coding. If the number of identity digits is even then bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111".

If the mobile identity is the TMSI/P-TMSI/TEMSI then bits 5 to 8 of octet 3 are coded as "1111" and bit 8 of octet 4 is the most significant bit and bit 1 of the last octet the least significant bit. The coding of the TMSI/P-TMSI is left open for each administration.

NOTE 1: This can be used in the case when a fill paging message without any valid identity has to be sent on the paging subchannel.

NOTE 2: The coding of the XEMSI within the identity digits is as following according 3G TS 23.003:

The UIDN ADDR is the E.164 address of the User Identity Decryption Node (UIDN) with a maximum length of 15 digits.

The EMSI (Encrypted IMSI) is an octet string with the minimum of 1 and the maximum length of 12 octets.

10.5.3.4 Identity type

The purpose of the *Identity Type* information element is to specify which identity is requested.

The *Identity Type* information element is coded as shown in figure 10.5.78/TS 24.008 and table 10.5.92/TS 24.008.

The *Identity Type* is a type 1 information element .

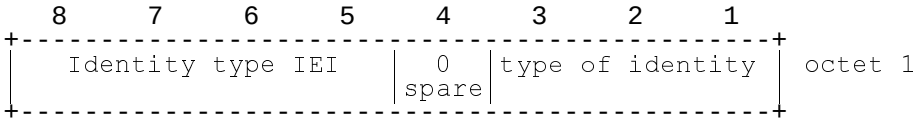


Figure 10.5.78/TS 24.008 *Identity Type* information element

Table 10.5.92/TS 24.008: *Identity Type* information element

Type of identity (octet 1) Bits 3 2 1	
0 0 1	IMSI
0 1 0	IMEI
0 1 1	IMEISV
1 0 0	TMSI
1 0 1	XEMSI see 10.5.1.4
1 1 0	TEMSI see 10.5.1.4
All other values are reserved.	

10.5.5.9 Identity type 2

The purpose of the *identity type 2* information element is to specify which identity is requested.

The *identity type 2* is a type 1 information element.

The *identity type 2* information element is coded as shown in figure 10.5.125/TS 24.008 and table 10.5.142/TS 24.008.

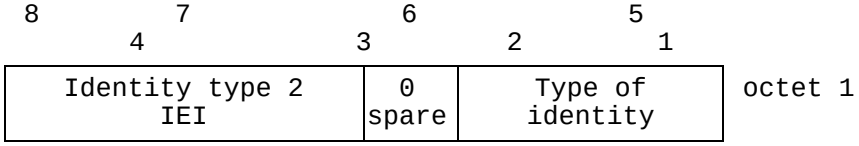


Figure 10.5.125/TS 24.008: *Identity type 2* information element

Table 10.5.142/TS 24.008: *Identity type 2* information element

Type of identity (octet 1) Bits 3 2 1	
0 0 1	IMSI
0 1 0	IMEI
0 1 1	IMEISV
1 0 0	TMSI
1 0 1	XEMSI see 10.5.1.4
1 1 0	TEMSI see 10.5.1.4

All other values are interpreted as *IMSI* by this version of the protocol.

4.7.9.1.2 Paging for GPRS services using IMSI

Paging for GPRS services using IMSI is an abnormal procedure used for error recovery in the network.

The network may initiate paging using IMSI if the P-TMSI is not available due to a network failure. If the mobile supports enhanced user identity confidentiality, than the TEMSI will be used instead of IMSI:

To initiate the procedure the GMM entity in the network requests the RR sublayer to start paging (see GSM 04.18, GSM 04.60 [75], TS 25.331 and TS 25.413).

Upon reception of a paging indication for GPRS services using IMSI/TEMSI, the MS shall locally deactivate any active PDP contexts and locally detach from GPRS. The local detach includes deleting any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number stored, setting the GPRS update status to GU2 NOT UPDATED and changing state to GMM-DEREGISTERED.

After performing the local detach, the MS shall then perform a GPRS attach or combined GPRS attach procedure. After performing the attach, a MS should activate PDP context(s) to replace any previously active PDP context(s).

NOTE: In some cases, user interaction may be required and then the MS cannot activate the PDP context(s) automatically.

NOTE: The MS does not respond to the paging except with the Attach Request. Hence timer T3313 in the network is not used when paging with IMSI/TIMSI.

NOTE: Paging without DRX parameters may require a considerable extension of the paging duration

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

3GPP TSG SA2 Meeting #11
Puerto Vallarta, Mexico, 24 – 28 January 2000

Document ***S2-000282~~xxx~~***

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

f) The VLR acknowledges with Insert Subscriber Data Ack (IMSI).

g) After finishing the inter-MSC location update procedures, the HLR responds with Update Location Ack (IMSI) to the new VLR.

h) The VLR responds with Location Update Accept (VLR TMSI) to the SGSN.

8) The SGSN selects Radio Priority SMS, and sends an Attach Accept (P-TMSI, VLR TMSI, P-TMSI Signature, Radio Priority SMS) message to the MS. P-TMSI is included if the SGSN allocates a new P-TMSI.

9) If P-TMSI or VLR TMSI was changed, the MS acknowledges the received TMSI(s) by returning an Attach Complete message to the SGSN.

10) If VLR TMSI was changed, the SGSN confirms the VLR TMSI re-allocation by sending a TMSI Reallocation Complete message to the VLR.

If the Attach Request cannot be accepted, the SGSN returns an Attach Reject (IMSI, Cause) message to the MS.

For an MS with GPRS-CSI defined, CAMEL interaction may be performed, see referenced procedure in 3G TS 23.078:

C1) CAMEL-GPRS-Attach-Request.

6.5.2 UMTS PS Attach Function

[It is an outstanding task to merge this subclause with "GPRS Attach Function".]

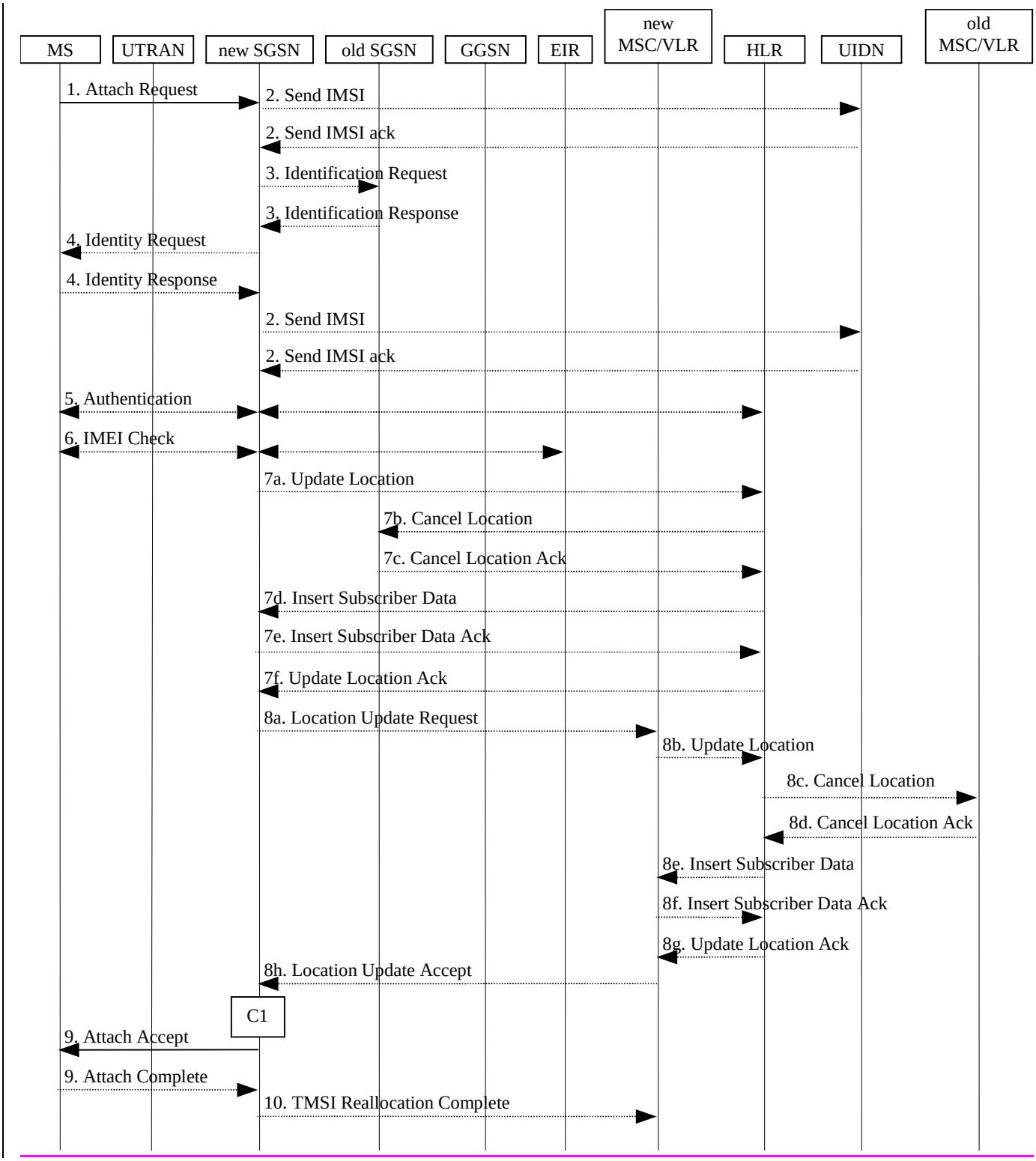
A PS-attached MS makes a CS attach via the SGSN with the combined RA / LA update procedure if the network operates in mode I. In network operates in mode II, or if the MS is not PS-attached, then the MS makes a normal CS attach. A CS-attached MS engaged in a CS connection shall use the (non-combined) PS Attach procedure when it performs a PS attach.

In the attach procedure, the MS shall provide its identity and an indication of which type of attach that is to be executed. The identity provided to the network shall be the MS's Packet TMSI (P-TMSI) or IMSI or EMSI (Encrypted Mobile Subscriber Identity) and UIDN (User Identity Decryption Node) address. P-TMSI and the RAI associated with the P-TMSI shall be provided if the MS has a valid P-TMSI. If the MS does not have a valid P-TMSI, then the MS shall provide its IMSI or EMSI and UIDN Address. The SGSN shall be able to request the decryption of an EMSI by the UIDN of the home network. The different types of attach are PS attach and combined PS / CS attach.

After having executed the PS attach, the MS is in the PMM-CONNECTED state and MM contexts are established in the MS and the SGSN. The MS may then activate PDP contexts as described in subclause "Activation Procedures".

An CS-attached MS that cannot operate in CS/PS mode of operation shall follow the normal CS detach procedure before it makes a PS attach. A PS-attached MS that cannot operate in CS/PS mode of operation shall perform a PS detach before it makes a CS attach.

The Combined PS / CS Attach procedure is illustrated in Figure 22. Each step is explained in the following list.


MS
UTRAN
new SGSN
old SGSN
GGSN
EIR
new MSC/VLR
HLR
UIDN
old MSC/VLR
1. Attach Request
2. Send IMSI
2. Send IMSI ack
3. Identification Request
3. Identification Response
4. Identity Request
4. Identity Response
2. Send IMSI
2. Send IMSI ack
5. Authentication
6. IMEI Check
7a. Update Location
7b. Cancel Location
7c. Cancel Location Ack
7d. Insert Subscriber Data
7e. Insert Subscriber Data Ack
7f. Update Location Ack
8a. Location Update Request
8b. Update Location
8c. Cancel Location
8d. Cancel Location Ack
8e. Insert Subscriber Data
8f. Insert Subscriber Data Ack
8g. Update Location Ack
8h. Location Update Accept
C1
9. Attach Accept
9. Attach Complete
10. TMSI Reallocation Complete

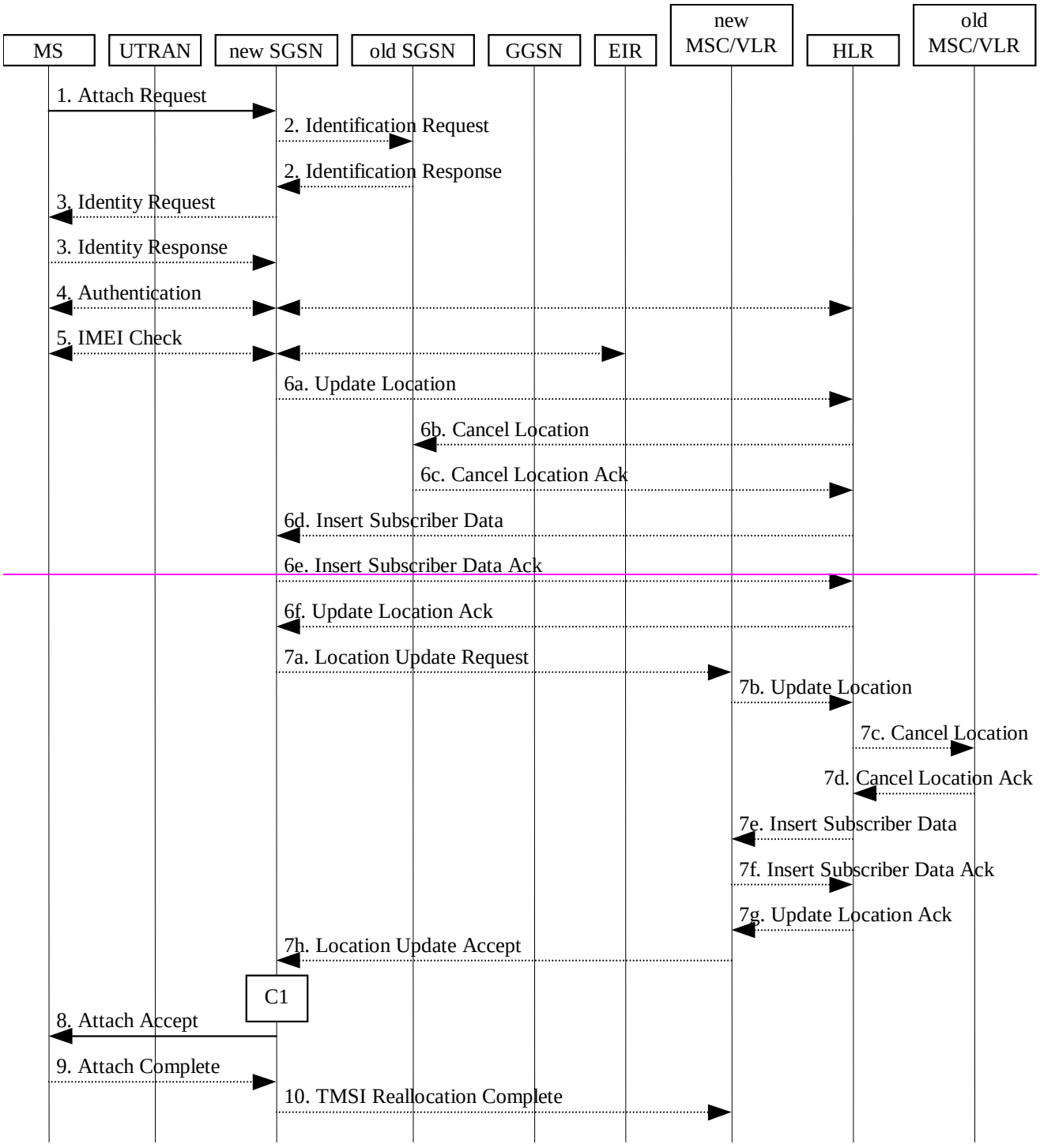


Figure 22: Combined PS / CS Attach Procedure

1) The MS initiates the attach procedure by the transmission of an Attach Request (IMSI or P-TMSI and old RAI or EMSI and UIDN Address), Core Network Classmark, KSI, Attach Type, old P-TMSI Signature, Follow on request) message to the SGSN. IMSI shall be included if the MS does not have a valid P-TMSI available. If the MS uses P-TMSI for identifying itself and if it has also stored its old P-TMSI Signature, then the MS shall include the old P-TMSI Signature in the Attach Request message. If the MS has a valid P-TMSI, then P-TMSI and the old RAI associated with P-TMSI shall be included. KSI shall be included if the MS has valid security parameters. Core Network Classmark is describe in subclause "Core Network Classmark". Follow on request shall be set by MS if there is pending uplink traffic (signalling or user data). The SGSN may use, as an implementation option, the follow on request indication to release or keep the Iu connection after the completion

of the PS Attach procedure. Attach Type indicates which type of attach that is to be performed, i.e., PS attach only, PS Attach while already CS attached, or combined PS / CS attach.

2) If the MS identifies itself with an EMSI and UIDN Address, the SGSN shall request decryption of the EMSI from the UIDN. The SGSN shall send a Send IMSI (EMSI) towards the UIDN. If the UIDN provides in the Send IMSI Ack the IMSI of the serving subscriber, processing in the SGSN shall continue based on this identity. If the UIDN returns a Send IMSI negative response, then the SGSN shall reject the Attach Request.

3) If the MS identifies itself with P-TMSI and the SGSN has changed since detach, the new SGSN sends an Identification Request (P-TMSI, old RAI, old P-TMSI Signature) to the old SGSN to request the IMSI. The old SGSN responds with Identification Response (IMSI, Authentication vector). If the MS is not known in the old SGSN, the old SGSN responds with an appropriate error cause. The old SGSN also validates the old P-TMSI Signature and responds with an appropriate error cause if it does not match the value stored in the old SGSN.

~~3~~4) If the MS is unknown in both the old and new SGSN, the SGSN sends an Identity Request (Identity Type = IMSI) to the MS. The MS responds with Identity Response (IMSI or EMSI and UIDN Address). If the MS identifies itself with an EMSI and UIDN Address, the SGSN shall obtain the IMSI via the procedure defined in 2).

~~5~~4) The authentication functions are defined in the subclause "Security Function". If no MM context for the MS exists anywhere in the network, then authentication is mandatory. Ciphering procedures are described in subclause "Security Function". If P-TMSI allocation is going to be done, and if ciphering is supported by the network, ciphering mode shall be set.

~~6~~5) The equipment checking functions are defined in the subclause "Identity Check Procedures". Equipment checking is optional.

~~7~~6) If the SGSN number has changed since the GPRS detach, or if it is the very first attach, then the SGSN informs the HLR:

a) The SGSN sends an Update Location (SGSN Number, SGSN Address, IMSI) to the HLR.

b) The HLR sends Cancel Location (IMSI, Cancellation Type) to the old SGSN with Cancellation Type set to Update Procedure.

c) The old SGSN acknowledges with Cancel Location Ack (IMSI). If there are any ongoing procedures for that MS, the old SGSN shall wait until these procedures are finished before removing the MM and PDP contexts.

d) The HLR sends Insert Subscriber Data (IMSI, GPRS Subscription Data) to the new SGSN.

e) The new SGSN validates the MS's presence in the (new) RA. If due to regional subscription restrictions the MS is not allowed to attach in the RA, the SGSN rejects the Attach Request with an appropriate cause, and may return an Insert Subscriber Data Ack (IMSI, SGSN Area Restricted) message to the HLR. If subscription checking fails for other reasons, the SGSN rejects the Attach Request with an appropriate cause and returns an Insert Subscriber Data Ack (IMSI, Cause) message to the HLR. If all checks are successful then the SGSN constructs an MM context for the MS and returns an Insert Subscriber Data Ack (IMSI) message to the HLR.

f) The HLR acknowledges the Update Location message by sending an Update Location Ack to the SGSN after the cancelling of old MM context and insertion of new MM context are finished. If the Update Location is rejected by the HLR, the SGSN rejects the Attach Request from the MS with an appropriate cause.

~~8~~7) If Attach Type in step 1 indicated PS Attach while already CS attached, or combined PS / CS attach, then the VLR shall be updated if the Gs interface is installed. The VLR number is derived from the RA information. The SGSN starts the location update procedure towards the new MSC/VLR upon receipt of the first Insert Subscriber Data message from the HLR in step 6 d). This operation marks the MS as GPRS-attached in the VLR.

a) The SGSN sends a Location Update Request (new LAI, IMSI, SGSN Number, Location Update Type) message to the VLR. Location Update Type shall indicate CS attach if Attach Type indicated combined PS / CS attach. Otherwise, Location Update Type shall indicate normal location update. The VLR creates an association with the SGSN by storing SGSN Number.

b) If the LA update is inter-MSC, the new VLR sends Update Location (IMSI, new VLR) to the HLR.

c) If the LA update is inter-MSC, the HLR sends a Cancel Location (IMSI) to the old VLR.

d) The old VLR acknowledges with Cancel Location Ack (IMSI).

e) If the LA update is inter-MSC, the HLR sends Insert Subscriber Data (IMSI, GSM subscriber data) to the new VLR.

f) The VLR acknowledges with Insert Subscriber Data Ack (IMSI).

g) After finishing the inter-MSC location update procedures, the HLR responds with Update Location Ack (IMSI) to the new VLR.

h) The VLR responds with Location Update Accept (VLR TMSI) to the SGSN.

9~~8~~) The SGSN selects Radio Priority SMS, and sends an Attach Accept (P-TMSI, VLR TMSI, P-TMSI Signature, Radio Priority SMS) message to the MS. P-TMSI is included if the SGSN allocates a new P-TMSI.

10~~9~~) If P-TMSI or VLR TMSI was changed, the MS acknowledges the received TMSI(s) by returning an Attach Complete message to the SGSN.

11~~10~~) If VLR TMSI was changed, the SGSN confirms the VLR TMSI re-allocation by sending a TMSI Reallocation Complete message to the VLR.

If the Attach Request cannot be accepted, the SGSN returns an Attach Reject (IMSI, Cause) message to the MS.

For an MS with GPRS-CSI defined, CAMEL interaction may be performed, see referenced procedure in 3G TS 23.078:

C1) CAMEL-GPRS-Attach-Request.

6.6 Detach Function

The PS Detach procedure allows:

- an MS to inform the network that it does not want access the SGSN-based services any longer; and
- the network to inform an MS that it does not have access to the SGSN-based services any more.

The Detach function allows an MS to inform the network that it wants to make a PS and/or CS detach, and it allows the network to inform an MS that it has been PS-detached or CS-detached by the network.

The different types of detach are:

- CS detach;
- PS detach; and
- combined PS / CS detach (MS-initiated only).

The MS is detached either explicitly or implicitly:

- Explicit detach: The network or the MS explicitly requests detach.
- Implicit detach: The network detaches the MS, without notifying the MS, a configuration-dependent time after the mobile reachable timer expired, or after an irrecoverable radio error causes disconnection of the logical link.

In the explicit detach case, a Detach Request (Cause) is sent by the SGSN to the MS, or by the MS to the SGSN.

The MS can make a CS detach in one of two ways depending on if it is PS-attached or not:

- A PS-attached MS sends a Detach Request message to the SGSN, indicating a CS detach. This can be made in combination with PS detach.
- An MS that is not PS-attached makes the CS detach as already defined in GSM or UMTS.

In the MO Detach Request message there is an indication to tell if the detach is due to switch off or not. The indication is needed to know whether a Detach Accept message should be returned or not.