3GPP TR 24.801 V8.1.0 (2008-12)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Core Network and Terminals;
3GPP System Architecture Evolution;
CT WG1 Aspects
(Release 8)

Keywords
SAE, LTE

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document discusses and describes the CT1 aspects of the 3GPP System Architecture Evolution (SAE) towards a higher-data-rate, lower-latency, packet-optimized system that supports multiple access technologies.

In particular, these CT1 aspects include the Non-Access-Stratum (NAS) functions to be performed by the User Equipment (UE) in idle mode, the NAS signalling procedures between the UE and the evolved packet core network (EPC) via the E-UTRAN, and the layer 3 signalling procedures between the UE and the EPC via non-3GPP access networks.

The present document also considers the requirements on the NAS between the UE and the core network which arise from specific services like MBMS and network functions like security, QoS, and mobility within the E-UTRAN or between the E-UTRAN and other 3GPP or non-3GPP access networks.

The present document is intended as a holding place for CT1 SAE material until it stabilises sufficiently to be moved to appropriate 3GPP technical specifications.

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".

[3] 3GPP TS 23.203: "Policy and charging control architecture".

[4] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[5] 3GPP TS 33.102: "3G security; Security architecture".

[6] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[7] 3GPP TS 23.003: "Numbering, addressing and identification".

[8] IETF RFC 4306 (December 2005): "Internet Key Exchange (IKEv2) Protocol".

[9] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[10] IETF Internet-Draft, draft-ietf-netlmm-proxymip6-00.txt (April 2007): "Proxy Mobile IPv6".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[11] IETF Internet-Draft, draft-ietf-mip6-nemo-v4traversal-05.txt (July 2007): "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[12] 3GPP TS 23.402: "Architecture Enhancements for non-3GPP accesses".

[13] 3GPP TR 29.803: "3GPP System Architecture Evolution: CT WG4 aspects (Stage3)".

[14] 3GPP TS 24.234: "3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3".

[15] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description".

[16] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC) protocol specification".

[17] 3GPP TS 36.413: "Evolved Universal Terrestrial Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[18] IETF RFC 4877 (April 2007): "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture".

[19] Void.

[20] IETF Internet-Draft, draft-ietf-mip6-bootstrapping-split-07.txt (June 2007): "Mobile IPv6 bootstrapping in split scenario".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[21] IETF RFC 2782 (February 2000): "A DNS RR for specifying the location of services (DNS SRV)".

[22] 3GPP TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".

[23] IETF Internet-Draft, draft-ietf-mip4-rfc3344bis-05.txt (July 2007): "IP Mobility Support for IPv4, revised".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[24] IETF RFC 2794 (January 2000): "Mobile IP Network Access Identifier Extension for IPv4".

[25] IETF RFC 3775 (June 2004): "Mobility Support in IPv6".

[26] IETF RFC 3748 (June 2004): "Extensible Authentication Protocol (EAP)".

[27] IETF RFC 4301 (December 2005): "Security Architecture for the Internet Protocol".

[28] IETF RFC 4555 (June 2006): "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[29] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[30] IETF RFC 4862 (September 2007): "IPv6 Stateless Address Autoconfiguration".

[31] IETF RFC 3736 (April 2004): "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[32] 3GPP TR 29.804: "3GPP Evolved Packet System: CT WG3 Aspects (Stage3)".

[33] IETF RFC 4861 (September 2007): "IPv6 Neighbor Discovery for IP version 6 (IPv6)".

[34] IETF RFC 2131 (March 1997): "Dynamic Host Configuration Protocol".

[35] IETF RFC 4039 (March 2005): "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[36] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[37] 3GPP TS 24.305: " Selective Disabling of 3GPP User Equipment Capabilities (SDoUE) Management Object (MO)".

[38] 3GPP TS 27.007: "AT command set for User Equipment (UE)".

[39] IETF RFC 3633 (December 2003): "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6".

[40] 3GPP TS 33.401: "3GPP System Architecture Evolution; Security architecture".

[41] IETF RFC 5026 (October 2007): "Mobile IPv6 bootstrapping in split scenario".

[42] IETF RFC 4303 (December 2005): "IP Encapsulating Security Payload (ESP)".

[43] IETF Internet-Draft, draft-ietf-mip6-hiopt-10.txt (January 2008): "DHCP Option for Home Information Discovery in MIPv6".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[44] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[45] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[46] 3GPP TS 24.303: "Mobility Management based on DSMIPv6; User Equipment (UE) to network protocols; Stage 3".

[47] 3GPP TS 22.011: "Service accessibility".

[48] 3GPP TS 24.304: "Mobility management based on Mobile IPv4; User Equipment (UE) – Foreign Agent interface; Stage 3".

[49] 3GPP TS 23.272: "Circuit Switched Fallback in Evolved Packet System; Stage 2".

[50] 3GPP TS 29.018: "Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR) Gs interface layer 3 specification".

[51] 3GPP TS 23.216: " Single Radio Voice Call Continuity (SRVCC); Stage 2".

[52] OMA-ERELD-DM-V1_2: "Enabler Release Definition for OMA Device Management".

[53] OMA-TS-DM_Protocol-V1_2: "OMA Device Management Protocol, Version 1.2".

[54] OMA-TS-DM_Notification-V1_2: "OMA Device Management Notification Initiated Session, Version 1.2".

[55] OMA-TS-DM_Security-V1_2: "OMA Device Management Security, Version 1.2".

[56] OMA-TS-DM-FUMO-V1_0: "Firmware Update Management Object, Version 1.0".

[57] 3GPP TS 24.167: "3GPP IMS Management Object (MO)".

[58] 3GPP TS 24.216: "Communication Continuity Management Object (MO)".

[59] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[60] IEEE P802.21/D12.0 (June 2008): "Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services", IEEE LAN/MAN Standards committee of IEEE Computer Society.

[61] IETF Internet-Draft, draft-ietf-mipshop-mstp-solution-04.txt (May 2008): "Mobility Services Framework Design".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[62] IETF RFC 4346 (April 2006): "The Transport Layer Security (TLS) Protocol (Version 1.1)".

[63] IETF RFC 4366 (April 2006): "Transport Layer Security (TLS) Extensions".

[64] IETF RFC 4282 (December 2005): "The Network Access Identifier".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Aggregate Maximum Bit Rate: The maximum bit rate that limits the aggregate bit rate of a set of non-GBR bearers of a UE. Definition derived from 3GPP TS 23.401 [2].

The label **(E-UTRAN only)** indicates this subclause or paragraph applies only if E-UTRAN is used as current radio access network.

EMM context: An EMM context is established in the UE and the MME when an attach procedure is successfully completed.

EMM-CONNECTED mode: A UE is in EMM-CONNECTED mode when a NAS signalling connection between UE and network is established. The term EMM-CONNECTED mode used in the present document corresponds to the term ECM-CONNECTED state used in 3GPP TS 23.401 [2].

EMM-IDLE mode: A UE is in EMM-IDLE mode when no NAS signalling connection between UE and network exists. The term EMM-IDLE mode used in the present document corresponds to the term ECM-IDLE state used in 3GPP TS 23.401 [2].

Evolved packet core network: the successor to the 3GPP Release 7 packet-switched core network, developped by 3GPP within the framework of the 3GPP System Architecture Evolution (SAE).

Evolved packet system: The evolved packet system (EPS) or evolved 3GPP packet-switched domain consists of the evolved packet core network and the evolved universal terrestrial radio access network. Definition derived from 3GPP TS 23.401 [2].

Dedicated bearer: An EPS bearer that is associated with uplink packet filters in the UE and downlink packet filters in the PDN GW where the filters only match certain packets. Definition derived from 3GPP TS 23.401 [2].

Default bearer: An EPS bearer that is used associated with "match all" uplink and downlink packet filters in the UE and the PDN GW, respectively. Definition derived from 3GPP TS 23.401 [2].

GBR bearer: An EPS bearer that uses dedicated network resources related to a Guaranteed Bit Rate (GBR) value, which are permanently allocated at EPS bearer establishment/modification. Definition derived from 3GPP TS 23.401 [2].

Initial NAS message: A NAS message is considered as an initial NAS message, if this NAS message can trigger the establishment of a NAS signalling connection. For instance, the ATTACH REQUEST message is an initial NAS message.

Label: A label is a scalar that is used as a reference to node-specific parameters that control bearer level packet forwarding treatment that have been pre-configured by the operator owning the node. Definition derived from 3GPP TS 23.401 [2].

Last Visited Registered TAI: A TAI which is contained in the TAI list that the UE registered to the network and which identifies the tracking area last visited by the UE.

Linked Bearer Identity: This identity indicates to which default bearer the additional bearer resource is linked.

MME area: An area containing tracking areas served by an MME.

NAS signalling connection: is a peer to peer S1 mode connection between UE and MME. A NAS signalling connection consists of the concatenation of an RRC connection via the "LTE-Uu" interface and an S1AP connection via the S1 interface. The UE considers the NAS signalling connection established when the RRC connection has been established successfully. The UE considers the NAS signalling connection released when the RRC connection has been released.

Non-access stratum protocols: The protocols between UE and MSC or SGSN that are not terminated in the UTRAN, and the protocols between UE and MME that are not terminated in the E-UTRAN. Definition derived from 3GPP TS 21.905 [1].

Non-GBR bearer: An EPS bearer that uses network resources that are not related to a Guaranteed Bit Rate (GBR) value. Definition derived from 3GPP TS 23.401 [2].

PDN address: an IP address assigned to the UE by the Packet Data Network Gateway (PDN GW).

Procedure Transaction Identity: An identity which is dynamically allocated by the UE for the UE requested bearer resource activation, modification and deactivation procedures. The procedure transaction identity is released when the procedure is completed.

The label **(S1 mode only)** indicates this subclause or paragraph applies only to a system which operates in S1 mode, i.e. with a functional division that is in accordance with the use of an S1 interface between the radio access network and the core network. In a multi-access system this case is determined by the current serving radio access network.

TAI list: A list of TAIs that identify the tracking areas that the UE can enter without performing a tracking area update procedure.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.401 [2] apply:

MME pool area

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

AMBR	Aggregate Maximum Bit Rate
ARP	Allocation Retention Priority
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
ECM	EPS Connection Management
EMM	EPS Mobility Management
EPC	Evolved Packet Core Network
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
ESM	EPS Session Management
FA	Foreign Agent
GBR	Guaranteed Bit Rate
GUMMEI	Globally Unique MME Identifier
GUTI	Globally Unique Temporary Identifier
HRPD	High Rate Packet Data
ISR	Idle mode Signalling Reduction
LBI	Linked Bearer Identity
M-TMSI	M-Temporary Mobile Subscriber Identity
MBR	Maximum Bit Rate
MME	Mobility Management Entity
MMEC	MME Code
OC	Overflow Counter

PDN GW	Packet Data Network Gateway
PTI	Procedure Transaction Identity
RRQ	Registration Request
RRP	Registration Reply
S-TMSI	S-Temporary Mobile Subscriber Identity
S1AP	S1 Application Protocol
SAE	System Architecture Evolution
SDF	Service Data Flow
SMC	Security Mode Command
SN	Sequence Number
TAC	Tracking Area Code
TAI	Tracking Area Identity
TFT	Traffic Flow Template

4 Network selection procedures

Editor's note: This clause will contain a description of the procedures for network selection, i.e. access technology selection and PLMN selection. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

4.1 Concepts

Editor's note: This subclause will contain a description of concepts, general principles, working assumptions agreed by CT1, etc. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

As per 3GPP TS 22.011 [44] PLMN selection defines a UE based procedure, whereby candidate PLMNs are selected, one at a time, for attempted registration.

E-UTRAN is a new access technology for PLMN selection procedures different from GERAN and UTRAN (see 3GPP TS 22.011 [44]).

New forbidden lists are needed to be specified for E-UTRAN: "forbidden tracking areas for roaming" and "forbidden tracking areas for regional provision of service". These lists will contain one or more tracking area identities rather than location area identities. The handling of these new lists is similar to the "forbidden location areas for roaming" and "forbidden location areas for regional provision of service" lists.

Editor's note: The current requirement for the "forbidden location areas for roaming" and "forbidden location areas for regional provision of service" of having at least 10 entries will be further investigated for the new tracking area related lists since it comes from the times when the memory in the ME was limited, and this is not the case any longer.

The existing "forbidden PLMNs" and the "forbidden PLMNs for GPRS service" lists are also used for E-UTRAN.

Editor's note: The use of the reject cause value #14 "GPRS services not allowed in this PLMN" is under discussion in SA1, and therefore the need of the associated "forbidden PLMNs for GPRS service" list for E-UTRAN may need to be re-considered.

The existing concept of ranking the available candidate PLMNs in automatic PLMN selection is extended to cover also cdma2000® 1xRTT and cdma2000® HRPD Radio Access Technologies.

In PLMN selection procedures a multi mode UE that supports both 3GPP and 3GPP2 radio access technologies shall consider all candidate PLMNs across all supported 3GPP and 3GPP2 RATs.

Once the PLMN selection has been performed, the UE shall follow the signalling procedures defined for the selected RAT.

NOTE: cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA).

4.2 Procedures

Editor's note: This subclause will contain a detailed description of the procedures for network selection.

4.2.1 General

For 3GPP and 3GPP2 access technologies the Radio Access Technology identifier (RAT) associated with each entry in the "User controlled PLMN selector with Access Technology", "Operator controlled PLMN selector with Access Technology" and "HPLMN selector with Access Technology" data files can indicate any combination of the values: GSM, GSM COMPACT, UTRAN, E-UTRAN, cdma2000® 1xRTT and cdma2000® HRPD access technologies.

Any signalling procedures after PLMN selection are defined in the specifications related with the radio access technology of the selected PLMN.

4.2.2 Procedures for 3GPP radio access networks

The same procedures for PLMN selection applicable for the GSM and UTRAN access technologies as described in 3GPP TS 22.011 [47] and 3GPP TS 23.122 [22] also apply for E-UTRAN.

4.2.3 Procedures for non-3GPP access networks

4.2.3.1 Procedures for access networks defined by 3GPP2

New Radio Access Technology codes for cdma2000® 1xRTT and cdma2000® HPRD access technologies will be defined so that they can be used in the same PLMN selection procedures that are already applicable for the GSM and UTRAN access technologies as described in 3GPP TS 22.011 [47] and 3GPP TS 23.122 [22].

4.2.3.2 Procedures for other non-3GPP access networks

Editor's note: Currently there are no requirements available.

5 UE NAS mobility functions in EMM-IDLE and EMM-CONNECTED mode

Editor's note: This clause will contain a description of aspects of intra E-UTRAN mobility in IDLE and CONNECTED mode relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

5.1 General

5.1.1 Registration areas in the EPS

5.1.1.1 General

Within the EPS, a registration area is defined as a set of tracking areas and each of these tracking areas consists of one or more cells that cover a geographical area. Tracking areas cannot overlap each other. Within the EPS, the concept of "registration to multiple tracking areas" applies:

- A tracking area is identified by a TAI which is broadcast in the cells of the tracking area. The TAI is constructed from a TAC and a PLMN identifier. In case of a shared network, a single TAC and multiple PLMN identifiers are broadcast.

Editor's note: The structure and coding of the TAC is FFS.

- In order to reduce the tracking area update signalling within the EPS, the MME can assign several tracking areas to the UE. These tracking areas construct a list of tracking areas which is identified by a TAI list

- The UE considers itself registered to a list of tracking areas and does not need to trigger tracking area update other than periodic tracking area update as long as it stays in one of the tracking areas of the list of tracking areas received from the MME.

Editor's note: the maximum number of tracking areas which can be allocated per UE needs to be defined.

- The UE will consider the TAI list as valid, until it receives a new TAI list in the next normal tracking area update or periodic tracking area update or it is commanded by the network to delete the complete TAI list or it is detached from the EPS. If the tracking area update request or attach procedure via E-UTRAN is accepted or the TAI list is reallocated by the MME, the MME shall provide at least one entry in the TAI list. If the new and the old TAI list are identical, the MME does not need to provide the new TAI list to the UE during tracking area update or GUTI reallocation procedures.

- The TAI list can be reallocated by the MME.

- The UE shall take the current TAI provided by the EPS system as last visited registered TAI if the TAI is within the TAI list that the UE is registered to the network. If there is an old last visited registered TAI stored by the UE, the old last visited registered TAI is replaced by the new last visited registered TAI, that is, the UE shall delete the old last visited registered TAI and store the new last visited registered TAI into its non volatile memory.

- When the UE is detached from the EPS, the TAI list in the UE is invalid; except for the last visited registered TAI, the TAI list can be deleted by the UE.

- The MME allocates only one temporary identity (GUTI) to the UE, even if the UE is registered to more than one tracking area.

- The MME stores the GUTI and TAI list in its EMM Context for the UE.

- The MME can initiate paging of the UE in all cells of all tracking areas the UE is registered to.

- A TAI list assigned by an MME to a UE shall only contain tracking areas served by this MME.

5.1.1.2 Open issues for tracking area update procedure

1) When designing tracking area related operations in CT1, the balance between resource consumption for tracking area update and resource consumption for paging should be taken into account.

2) When designing the TAI and TAI list, CT1 should define an efficient encoding scheme for the TAI list,

3) CT1 needs to study whether the periodic update timers for tracking area update in EPS and for periodic routing area update in GPRS can have different values, related values, or the same value.

5.1.2 GUTI and S-TMSI handling

A globally unique temporary user identity for E-UTRA based services, the Globally Unique Temporary Identity (GUTI), is used for identification within the signalling procedures. In the paging and service request procedures, a shortened form of the GUTI, the S-Temporary Mobile Subscriber Identity (S-TMSI), is used to enable more efficient radio signalling. The purpose of the GUTI and S-TMSI is to provide identity confidentiality, i.e., to protect a user from being identified and located by an intruder. The structure of the GUTI and its derivatives will be specified in 3GPP TS 23.003 [7]. The GUTI has two main components, the Globally Unique MME Identifier (GUMMEI) that uniquely identifies the MME that allocated the GUTI and the M-Temporary Mobile Subscriber Identity (M-TMSI) that provides for an unambiguous identity of the UE within this MME.

The MME is responsible for allocating the GUTI to the UE. The allocation of the GUTI can be performed during attach, tracking area updating and GUTI reallocation procedures. The MME uses the S-TMSI for paging purposes.

A UE supporting E-UTRA includes a valid GUTI, if any is available, in the attach and tracking area updating request messages. In the service request message, the UE includes a valid S-TMSI as user identity. The MME may assign a new GUTI for a particular UE at successful attach, tracking area updating and GUTI reallocation procedures.

If a new GUTI is assigned by the MME, the UE and the MME handle the GUTI as follows:

- Upon receipt of a mobility management message containing a new GUTI the UE considers the new GUTI as valid and the old GUTI as invalid.
- The MME considers the old GUTI as invalid as soon as an acknowledgement for an attach, tracking area updating or GUTI reallocation procedure is received.

Usually, the GUTI reallocation is performed at least at each time the UE moves to a new tracking area not included in the TAI list assigned to the UE. However, this is left to the network operator's policies.

5.1.3 IP address allocation

Editor's note: The content of this subclause has been moved to 3GPP TS 24.301 [44]. Therefore this subclause is discontinued and no longer updated.

Editor's note: The text within this subclause shall be transferred to a technical specification.

5.1.3.1 General

The UE can configure an IP address during the attach procedure and/or through an IETF-based IP address allocation mechanism once the default bearer is established.

The following IETF-based IP address/prefix allocation methods are specified in this specification:

a) /64 IPv6 prefix allocation via IPv6 stateless address autoconfiguration;

b) IPv4 address allocation and IPv4 parameter configuration via DHCPv4;

c) IPv6 parameter configuration via stateless DHCPv6;

d) shorter than /64 IPv6 prefix delegation via DHCPv6.

5.1.3.2 IP address allocation via NAS signalling

If available, the UE shall include the capability of the IP stack associated with the UE (i.e. support of IPv4, IPv6 or IPv4/IPv6) in a PDN address allocation IE. If the UE wants to be allocated an IPv4 address for the default bearer during the attach procedure, the UE shall include a PDN address allocation IE requesting an IPv4 address in the ATTACH REQUEST message or PDN CONNECTIVITY REQUEST message.

If the UE knows that an IPv6 address for the default bearer needs to be configured, the UE shall include, in the ATTACH REQUEST message or PDN CONNECTIVITY REQUEST message, the PDN address allocation IE requesting an IPv6 prefix.

The UE may also include in the same PDN address allocation IE both the request of an IPv4 address and the indication that it will configure an IPv6 prefix.

If the UE does not request any IP address during the default bearer activation procedure and does not have any information about the capability supported by the IP stack, the PDN address allocation IE will not contain any information.

Editor's note: It is FFS if in this case the UE shall send an (empty) PDN address allocation IE anyway.

On receipt of the ATTACH REQUEST or PDN CONNECTIVITY REQUEST message sent by the UE, the network when allocating an IP address shall take into account the request received from the UE, UE's IP version capability, UE's subscription data and the policies of the home and visited network. When an IPv4 address is allocated during the default bearer activation procedure, the MME shall include in the ATTACH ACCEPT message or PDN CONNECTIVITY ACCEPT message a PDN address IE with the allocated IPv4 address.

If the PDN address allocation IE includes a request for IPv6 prefix that the UE will perform the IPv6 stateless address autoconfiguration, the MME shall include a PDN address IE with the allocated IPv6 prefix and interface identifier in the ATTACH ACCEPT message or PDN CONNECTIVITY ACCEPT message. The IPv6 prefix shall be ignored by the UE. The interface identifier shall be used to configure the link-local address. The UE shall use the IPv6 prefix received in the Router Advertisement for the stateless IPv6 address configuration. The IPv6 prefix in the PDN address IE and the one in the Router Advertisement shall be the same.

NOTE: The MME can assign both an IPv4 address and an IPv6 prefix to the same default bearer.

Editor's note: How the static IP address allocation is handled in the UE and in the network is FFS.

5.1.3.3 IPv6 stateless address allocation

The IPv6 stateless address configuration procedure is defined in IETF RFC 4862 [30]. This subclause provides some specific handling which shall apply in the context of this specification.

After a default bearer has been established, the UE may send a Router Solicitation message to trigger the network to send a Router Advertisement (see IETF RFC 4861 [33]). The PDN GW (or the Serving GW if S5-PMIP reference point is used) shall periodically send Router Advertisement messages as soon as the default bearer has been established.

Editor's note: The timers used by the UE to send the Router Solicitation messages and by the network to send the Router Advertisement messages are FFS.

To indicate to the MS that stateless address autoconfiguration shall be performed, the Router Advertisement shall have the M flag ("Managed Address Configuration" flag) cleared. The O flag ("Other Configuration" flag) may be set if additional parameters can be provided via DHCPv6 (see subclause 5.1.3.5).

One prefix is included in the Router Advertisement. The Prefix Information Option which contains the prefixes shall have the A flag ("Autonomous Address-Configuration" flag) set and the L flag ("On-Link" flag) cleared.

Editor's note: It is FFS if more than one prefix can be included in the Router Advertisement.

Editor's note: The lifetime of the prefix included in the Router Advertisement is FFS.

When creating a global IPv6 address, the UE may use any interface identifier. There is no restriction on the value of the interface identifier, since the prefixes are uniquely allocated to the UE. As the PDN GW guarantees that the prefixes in the Router Advertisements are unique, the UE shall not perform the Duplicate Address Detection procedure.

5.1.3.4 IPv4 address allocation via DHCPv4

If the UE wants to configure the IPv4 address and additional IPv4 parameters that were not provided during the attach procedure (e.g. the DNS server address), the UE shall send a DHCPDISCOVER message and use DHCPv4 as specified in IETF RFC 2131 [34].

Editor's note: The type of identifier used by the UE in the DHCP protocol (e.g. client identifier) is FFS.

If the IPv4 address was provided during the attach procedure and the UE needs additional parameters which were not provided, the UE shall use DHCPv4 for configuring the remaining additional IPv4 parameters.

The PDN GW shall reply with the options requested by the UE.

Editor's note: It is FFS if the PDN GW acts as DHCPv4 Relay or DHCPv4 server.

The UE may use the Rapid Commit option as specified in IETF RFC 4039 [35]. If the DHCPv4 server supports the option and is configured to use it, a two message exchange is executed. If the UE sends a DHCPDISCOVER with the Rapid Commit option but this is not accepted by the DHCPv4 server, the rules specified in IETF RFC 2131 [34] shall be followed.

5.1.3.5 IPv6 parameter configuration via stateless DHCPv6

If the O flag ("Other Configuration" flag) is set in the Router Advertisement (see IETF RFC 4861 [33]) and the UE needs to configure additional IP parameters (e.g. the DNS server address) that were not provided during the attach

procedure or the IPv6 address allocation procedure, the UE shall send a DHCPv6 Information-Request message including the options it wishes to receive, as specified in IETF RFC 3736 [31].

The PDN GW shall reply with the options requested by the UE. Any interaction between the PDN GW and any external DHCPv6 server are specified in 3GPP TR 29.804 [32].

Editor's note: The details of this procedure when S5-PMIP is used are FFS.

5.1.3.6 IPv6 prefix delegation via DHCPv6

At any time, after the establishment of the default bearer and the IP address allocation procedure described in subclauses 5.1.3.2, 5.1.3.3 and 5.1.3.4 , based on operator's policy, the UE may request and be provided with additional /64 or shorter prefixes. Prefix delegation shall be performed using DHCPv6 as defined in IETF RFC 3633 [39].

The UE shall act as requesting router as defined in IETF RFC 3633 [39]. If S5-GTP is used, the PDN GW shall act as delegating router as specified in IETF RFC 3633 [39]; if S5-PMIP is used, the Serving GW shall act as delegating router.

Editor's note: it is FFS if an additional PDN connection is established for the delegated prefix.

5.1.4 Relationship between the EMM and the GMM entity in the UE

If we consider a model of two "linked" state machines for EMM and GMM in the UE (see fig. 5.1.4.1), the following requirements for a communication between EMM and GMM can be derived from 3GPP TS 23.401 [2] and 3GPP TS 24.008 [4]:

In a network not using idle mode signalling reduction:

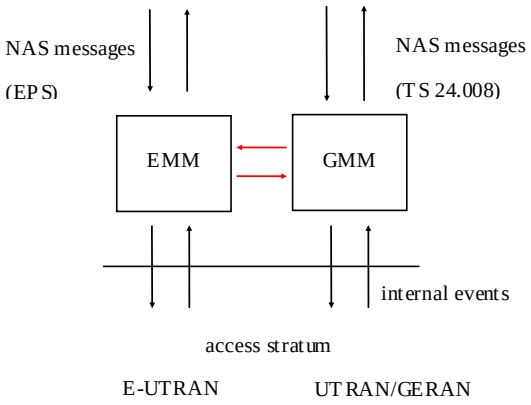
- When either of the two entities EMM and GMM in the UE enters main state REGISTERED or DEREGISTERED, the other entity in the UE shall also enter main state REGISTERED or DEREGISTERED, respectively, regardless whether the change of state is triggered by a successful attach or detach procedure or is a result of any other EMM or GMM procedure.

- There is no requirement to inform the other state machine also of a change to one of the "transient" states REGISTERED-INITIATED, DEREGISTERED-INITIATED, SERVICE-REQUEST-INITIATED, and TRACKING-AREA-UPDATING-INITIATED or ROUTING-AREA-UPDATING-INITIATED.

Editor's note: The requirements for a communication between EMM and GMM when the network is using idle mode signalling reduction are FFS.

NOTE 1: It is not intended to provide a detailed specification of the interface between EMM and GMM.

NOTE 2: The model used in this subclause does not exclude an implementation of EMM and GMM in a single, common state machine.



NOTE: For the sake of simplicity, other NAS protocol entities in the UE (e.g. session management) and the interactions of EMM and GMM with those entities are not included in this figure.

Figure 5.1.4.1: Linked state machines for EMM and GMM in the UE

5.2 UE NAS mobility functions in EMM-IDLE mode

Editor's note: This subclause will contain a description of UE NAS mobility functions in EMM-IDLE mode.

In EMM-IDLE mode a UE with a valid USIM inserted will:

- perform cell selection/reselection according to 3GPP TS 36.304 [29] and PLMN selection according to 3GPP TS 23.122 [22];
- when not attached to the EPS:
  - perform the attach procedure in order to receive services that require registration in the EPS;
- when attached to the EPS:
  - perform tracking area updating when entering a tracking area not in the list of assigned tracking areas, in order to maintain the registration and enable the MME to keep track of the UE;
  - perform periodic tracking area updating to periodically notify the EPC that the UE is available;
  - answer to paging from the MME by performing a service request procedure;
  - perform the service request procedure in order to establish the radio bearers when uplink user data is to be sent;

Editor's note: The use of the service request procedure in order to establish only a NAS signalling connection (without establishing the radio bearers), when session management signalling is to be sent, is FFS.

  - perform detach when the UE is switched off, the USIM is removed from the UE, or the EPS capability of the UE is disabled.

In EMM-IDLE mode a UE without valid USIM inserted will:

- perform cell selection/reselection according to 3GPP TS 36.304 [29], but not PLMN selection.

Editor's note: The support of emergency services by a UE without valid USIM is FFS.

5.3 UE NAS mobility functions in EMM-CONNECTED mode

Editor's note: This subclause will contain a description of UE NAS mobility functions in EMM-CONNECTED mode.

In EMM-CONNECTED mode a UE with a valid USIM inserted will:

- perform GUTI reallocation when requested by the MME;
- respond to identification requests from the MME;
- perform authentication when requested by the MME;
- initiate the ciphering and integrity protection for NAS signalling when requested by the MME;
- not perform periodic tracking area updating;
- when attached to the EPS:
  - perform tracking area updating when after handover the UE detects that it has entered a tracking area not in the assigned list of tracking areas;
  - perform the service request procedure in order to establish the radio bearers when uplink user data is to be sent;
  - perform detach when the UE is switched off, the USIM is removed from the UE, the EPS capability of the UE is disabled, or when requested by the MME.

Editor's note: The support of GUTI reallocation, identification request and tracking area updating by a UE using emergency services without valid USIM is FFS.

5.4 Reject causes for EMM procedures

Editor's note: this section contains temporary information on reject cause values to be used for EMM procedures, in order to help for further specification of the EMM procedures for the case they are rejected by the network. These information were derived from the study of the GMM cause values used for the attach, routing area update, detach and service request procedure as specified in 3GPP TS 24.008 [4], for the case these procedures are not accepted by the network. Some other reject causes may be necessary, such as causes for protocol errors or causes for abnormal cases such as failure of e.g. IP address allocation, but these are not defined in the current version of the present document.

5.4.1 Reject cause values for EMM procedures

The cause values below, defined in 3GPP TS 24.008 [4], are applicable in EPS:

#3 (Illegal MS);

#6 (Illegal ME);

#7 (GPRS services not allowed);

#8 (GPRS services and non-GPRS services not allowed);

#9 (MS identity cannot be derived by the network);

#10 (Implicitly detached);

#11 (PLMN not allowed);

#14 (GPRS services not allowed in this PLMN).

The new causes listed below shall be defined for EPS:

#12 (Tracking area not allowed);

This cause is sent to the UE if it requests tracking area updating in a tracking area where the HPLMN determines that the UE, by subscription, is not allowed to operate.

#13 (Roaming not allowed in this tracking area);

This cause is sent to a UE which requests tracking area updating in a tracking area of a PLMN which by subscription offers roaming to that UE, but not in that tracking area.

#15 (No suitable cells in tracking area);

This cause is sent to the UE if it requests tracking area updating in a tracking area where the UE, by subscription, is not allowed to operate, but when it should find another allowed tracking area or location area in the same PLMN.

Editor's note: it is FFS whether other new causes need to be created in EPS.

The cause values listed below, defined in 3GPP TS 24.008 [4], are not applicable to EPS:

#2 (IMSI unknown in HLR);

#40 (No PDP context activated).

5.4.2 Applicability of reject causes to EMM procedures

The table 5.4.2.1 below indicates which reject cause values can be used for each EMM procedure.

Table 5.4.2.1: proposed reject causes for EMM procedures

	Attach	Tracking Area Update	Detach	Service Request
#3 - Illegal MS	X	X	X	X
#6 - Illegal ME	X	X	X	X
#7 - GPRS services not allowed	X	X	X	X
#8 - GPRS services and non-GPRS services not allowed	X		X	
#9 - MS identity cannot be derived by the network		X		X
#10 - Implicitly detached		X		X
#11 - PLMN not allowed	X	X	X	X
#12 – Tracking area not allowed	X	X	X	X
#13 - Roaming not allowed in this tracking area	X	X	X	X
#14 - GPRS services not allowed in this PLMN	X	X	X	
#15 - No suitable cells in tracking area	X	X	X	X

5.4.3 Interactions with GERAN/UTRAN

For a multi-mode UE (GERAN/UTRAN/E-UTRAN), reception of some reject cause values when attached to the EPS shall lead the UE to take the actions as defined in 3GPP TS 24.008 [4] for these reject causes and the corresponding GMM procedure. The reject causes for which such behaviour is required are:

#3 (Illegal MS);

#6 (Illegal ME);

#7 (GPRS services not allowed);

#8 (GPRS services and non-GPRS services not allowed);

#11 (PLMN not allowed);

#12 (Tracking area not allowed);

#13 (Roaming not allowed in this tracking area);

#14 (GPRS services not allowed in this PLMN);

#15 (No suitable cells in tracking area).

Editor's note: it is FFS whether other cause values need to be added to the list.

6 NAS signalling procedures between UE and MME

Editor's note: The content of this subclause has been moved to 3GPP TS 24.301 [44]. Therefore this subclause is discontinued and no longer updated.

Editor's note: This clause will contain a description of the NAS protocol between UE and MME, including security, QoS and MBMS aspects. The text within this section should be readily transferable to a technical specification. For NAS signalling procedures for 3GPP access via E-UTRAN the existing 3GPP TS 24.008 [4] procedures will be used as a model as much as possible.

6.1 General

Editor's note: This subclause will contain general information, the state model for the UE and the MME, and an overview of the signalling procedures used between UE and MME.

6.1.1 Integrity checking of signalling messages in the UE

Integrity protected signalling is mandatory for the NAS messages once the NAS security mode control procedure has been successfully completed in the network and the UE. Integrity protection of all NAS signalling messages is the responsibility of the NAS layer. It is the network which activates integrity protection.

Except the messages listed below, no NAS signalling messages shall be processed by the receiving EMM entity or forwarded to the ESM entity, unless the NAS security mode control procedure has been successfully completed.

- EMM messages:
  - IDENTITY REQUEST (if requested identification parameter is IMSI)

Editor's note: whether the TRACKING AREA UPDATE ACCEPT message can be processed without integrity protection is FFS.

Editor's note: This list of messages will need to be completed based on SA3 requirements.

Once integrity protection is activated, the receiving EMM or ESM entity in the UE shall not process any NAS signalling messages unless they have been successfully integrity checked by the NAS layer. If NAS signalling messages, having not successfully passed the integrity check, are received, then the NAS layer in the UE shall discard that message. If any NAS signalling message is received, as not integrity protected even though the integrity protection has been activated in the UE by the network, then the NAS layer shall discard this message.

Editor's note: The integrity protection handling for emergency calls is FFS.

6.2 Mobility management procedures

Editor's note: This subclause will contain a detailed description of the signalling procedures used between UE and MME.

6.2.1 Overview

6.2.1.1 General

This clause describes the procedures used for mobility management for EPS services (EMM) at the radio interface (reference point "LTE-Uu").

The main function of the mobility management sublayer is to support the mobility of a user equipment, such as informing the network of its present location and providing user identity confidentiality.

A further function of the mobility management sublayer is to provide connection management services to the session management (SM) sublayer.

Editor's note: The existence of other protocol entities to which the EMM sublayer provides connection management services is FFS.

All the EMM procedures described in this clause can only be performed if a NAS signalling connection has been established between the UE and the network. Else, the EMM sublayer has to initiate the establishment of a NAS signalling connection (see 3GPP TS 36.331 [16]).

Editor's note: The relationship between the EMM entity described in this TR and the GMM entity in 3GPP TS 24.008 [4] is FFS.

6.2.1.2 Types of EMM procedures

Depending on how they can be initiated, three types of EMM procedures can be distinguished:

1) EMM common procedures:

   An EMM common procedure can always be initiated whilst a NAS signalling connection exists. The procedures belonging to this type are:

   Initiated by the network:

   - GUTI reallocation;
   - authentication and security mode;

Editor's note: The inclusion of the security mode procedure for NAS signalling in the authentication procedure is FFS.

   - identification;
   - EMM information.

2) EMM specific procedures:

   At any time only one UE initiated EMM specific procedure can be running. The procedures belonging to this type are:

   Initiated by the UE and used to attach the IMSI in the network for EPS services and to establish an EMM context and a default bearer:

   - attach.

   Initiated by the UE or the network and used to detach the IMSI in the network for EPS services and to release an EMM context and all bearers:

- detach.

Initiated by the UE when an EMM context has been established:

- normal tracking area updating;
- periodic tracking area updating.

The tracking area updating procedure can be used to request also the resource reservation for sending data.

3) EMM connection management procedures:

Initiated by the UE and used to establish a secure connection to the network or to request the resource reservation for sending data, or both:

- service request.

The service request procedure can only be initiated if no UE initiated EMM specific procedure is ongoing.

Initiated by the network and used to request the establishment of a NAS signalling connection or to prompt the UE to re-attach if necessary as a result of a network failure:

- paging procedure.

6.2.1.3 EMM sublayer states

6.2.1.3.1 General

In the following subclauses, the EMM protocol of the UE and the network is described by means of two different state machines. In subclause 6.2.1.3.2, the states of the EMM entity in the UE are introduced. The behaviour of the UE depends on an EPS update status that is described in subclause 6.2.1.3.3. The states for the MME side are described in subclause 6.2.1.3.4.

NOTE: The names for the EMM sublayer states in the present document can be different from the names used in stage 2 specifications (e.g. 3GPP TS 36.300 [15]). E.g. the state LTE_DETACHED in 3GPP TS 36.300 corresponds to EMM-DEREGISTERED in the present document, and the states LTE_IDLE and LTE_ACTIVE correspond to the combinations EMM-REGISTERED / EMM-IDLE mode and EMM-REGISTERED / EMM-CONNECTED mode, respectively.

Editor's note: For UEs supporting both E-UTRAN and UTRAN/GERAN the relationship between the EMM state machine and the GMM state machine is FFS.

6.2.1.3.2 EMM sublayer states in the UE

6.2.1.3.2.1 General

In the following subclauses, the possible EMM states of an EMM entity in the UE are described. Subclause 6.2.1.3.2.2 summarizes the main states of an EMM entity. The substates that have been defined are described in subclause 6.2.1.3.2.3 and subclause 6.2.1.3.2.4.

It should be noted, however, that this subclause does not include a description of the detailed behaviour of the UE in the single states and does not cover abnormal cases. A detailed description of the behaviour of the UE is given in subclause 6.2.2. For the behaviour of the UE in abnormal cases refer to the description of the elementary EMM procedures in subclauses 6.2.4, 6.2.5, 6.2.6 and 6.2.7.

6.2.1.3.2.2 Main states

6.2.1.3.2.2.1 EMM-NULL

The EPS capability is disabled in the UE. No EPS mobility management function shall be performed in this state.

6.2.1.3.2.2.2 EMM-DEREGISTERED

In the state EMM-DEREGISTERED, no EMM context has been established and the UE location is unknown to an MME and hence it is unreachable by an MME. In order to establish an EMM context, the UE shall start the attach procedure (see subclause 6.2.5.1).

6.2.1.3.2.2.3 EMM-REGISTERED-INITIATED

A UE enters the state EMM-REGISTERED-INITIATED after it has started the attach procedure and is waiting for a response from the MME (see subclause 6.2.5.1).

6.2.1.3.2.2.4 EMM-REGISTERED

In the state EMM-REGISTERED an EMM context has been established in the UE. When the UE is in EMM-IDLE mode, the UE location is known to the MME with an accuracy of a list of tracking areas containing a certain number of tracking areas. When the UE is in EMM-CONNECTED mode, the UE location is known to the MME with an accuracy of a cell. The UE may initiate sending and receiving user data and signalling information and reply to paging. Additionally, tracking area updating procedure is performed (see subclause 6.2.5.3).

6.2.1.3.2.2.5 EMM-DEREGISTERED-INITIATED

A UE enters the state EMM-DEREGISTERED-INITIATED after it has requested release of the EMM context by starting the detach procedure and is waiting for a response from the MME (see subclause 6.2.5.2).

6.2.1.3.2.2.6 EMM-TRACKING-AREA-UPDATING-INITIATED

A UE enters the state EMM-TRACKING-AREA-UPDATING-INITIATED after it has started the tracking area updating procedure and is waiting for a response from the MME (see subclause 6.2.5.3).

6.2.1.3.2.2.7 EMM-SERVICE-REQUEST-INITIATED

A UE enters the state EMM-SERVICE-REQUEST-INITIATED after it has started the service request procedure and is waiting for a response from the MME (see subclause 6.2.6.1).

6.2.1.3.2.3 Substates of state EMM-DEREGISTERED

The state EMM-DEREGISTERED is subdivided into a number of substates as described in this subclause. Valid subscriber data are available for the UE before it enters the substates, except for the EMM-DEREGISTERED.NO-IMSI substate.

6.2.1.3.2.3.1 EMM-DEREGISTERED.NORMAL-SERVICE

The substate EMM-DEREGISTERED.NORMAL-SERVICE is chosen in the UE, if the EPS update status is EU1 or EU2, in the meantime a cell has been selected and the PLMN or tracking area is not in the forbidden list.

6.2.1.3.2.3.2 EMM-DEREGISTERED.LIMITED-SERVICE

The substate EMM-DEREGISTERED.LIMITED-SERVICE is chosen in the UE, if the EPS update status is EU3, and a selected cell is in the forbidden PLMN or in a forbidden tracking area.

6.2.1.3.2.3.3 EMM-DEREGISTERED.ATTEMPTING-TO-ATTACH

The substate EMM-DEREGISTERED.ATTEMPTING-TO-ATTACH is chosen in the UE, if the EPS update status is EU2, and a previous attach was rejected.

6.2.1.3.2.3.4 EMM-DEREGISTERED.PLMN-SEARCH

The substate EMM-DEREGISTERED.PLMN-SEARCH is chosen in the UE, if the UE with a valid USIM is switched on.

6.2.1.3.2.3.5 EMM-DEREGISTERED.NO-IMSI

The substate EMM-DEREGISTERED.NO-IMSI is chosen in the UE, if the UE is switched on without a valid USIM inserted.

6.2.1.3.2.3.6 EMM-DEREGISTERED.ATTACH-NEEDED

Valid subscriber data are available for the UE and for some reason an attach must be performed as soon as possible. This state can be entered if the access class is blocked due to access class control.

Editor's note: it is FFS whether other access control mechanism than the one described in 3GPP TS 36.304 will apply in EPS and will have impact on this state.

6.2.1.3.2.3.7 EMM-DEREGISTERED.NO-CELL-AVAILABLE

No E-UTRAN cell can be selected. This substate is entered after a first intensive search failed when in substate EMM-DEREGISTERED.PLMN-SEARCH. Cells are searched for at a low rhythm. No EPS services are offered.

6.2.1.3.2.4 Substates of state EMM-REGISTERED

The state EMM-REGISTERED is subdivided into a number of substates as described in this subclause.

6.2.1.3.2.4.1 EMM-REGISTERED.NORMAL-SERVICE

The substate EMM-REGISTERED.NORMAL-SERVICE is chosen by the UE as the primary substate when the UE entering the state EMM-REGISTERED.

6.2.1.3.2.4.2 EMM-REGISTERED.ATTEMPTING-TO-UPDATE

The EMM-REGISTERED.ATTEMPTING-TO-UPDATE substate is chosen by the UE if the tracking area updating procedure failed due to a missing response from the network. No EMM procedure except the TAU shall be initiated by the UE in this substate. No data shall be sent or received.

6.2.1.3.2.4.3 EMM-REGISTERED.LIMITED-SERVICE

The substate EMM-REGISTERED.LIMITED-SERVICE is chosen in the UE, if the cell the UE selected is known not to be able to provide normal service.

6.2.1.3.2.4.4 EMM-REGISTERED.PLMN-SEARCH

The substate EMM-REGISTERED.PLMN-SEARCH is chosen in the UE, while the UE is searching for PLMNs.

6.2.1.3.2.4.5 EMM-REGISTERED.UPDATE-NEEDED

The UE has to perform a tracking area updating procedure, but its access class is not allowed in the cell due to access class control. The procedure will be initiated as soon as access is granted, for example due to a cell-reselection or due to change of the access classes allowed in the current cell. No EMM procedure except tracking area updating shall be initiated by the UE in this substate.

Editor's note: it is FFS whether other access control mechanism than the one described in 3GPP TS 36.304 will apply in EPS and will have impact on this state.

6.2.1.3.2.4.6 EMM-REGISTERED.NO-CELL-AVAILABLE

E-UTRAN coverage has been lost. In this substate, the UE shall not initiate any EMM procedures except for cell and PLMN reselection.

6.2.1.3.3 EPS update status

In order to describe the detailed UE behaviour, the EPS update (EU) status pertaining to a specific subscriber is defined as:

EU1: UPDATED

The last attach or tracking area updating attempt was successful.

EU2: NOT UPDATED

The last attach or tracking area updating attempt failed procedurally, i.e. no response was received from the MME.

EU3: ROAMING NOT ALLOWED

The last attach or tracking area updating attempt was correctly performed, but the answer from the MME was negative (because of roaming or subscription restrictions).

6.2.1.3.4 EMM sublayer states in the MME

6.2.1.3.4.1 EMM-DEREGISTERED

In the state EMM-DEREGISTERED, the MME has no EMM context or the EMM Context is marked as detached. The UE is detached. The MME may answer to an attach procedure initiated by the UE (see subclause 6.2.5.1).

6.2.1.3.4.2 EMM-COMMON-PROCEDURE-INITIATED

The MME enters the state EMM-COMMON-PROCEDURE-INITIATED, after it has started a common EMM procedure (see subclause 6.2.4) and is waiting for a response from the UE.

6.2.1.3.4.3 EMM-REGISTERED

In the state EMM-REGISTERED, an EMM context has been established in the MME.

6.2.1.3.4.4 EMM-DEREGISTERED-INITIATED

The MME enters the state EMM-DEREGISTERED-INITIATED after it has started a detach procedure and is waiting for a response from the UE (see subclause 6.2.5.1).

6.2.2 Behaviour of the MS in EMM-DEREGISTERED state and EMM-REGISTERED state

6.2.2.1 General

6.2.2.2 UE behaviour in state EMM-DEREGISTERED

6.2.2.2.1 General

The state EMM-DEREGISTERED in entered in the UE, when:

- the detach is performed either by the UE or by the MME (see subclause 6.2.5.2);
- the attach request is rejected by the MME (see subclause 6.2.5.1);
- the UE is switched on; or
- when all EPS bearer contexts belonging to the UE are released.

Editor's note: the details of the last scenario (detach after release of all EPS bearer contexts) are FFS.

Editor's note: Other conditions are FFS.

6.2.2.2.2 Primary substate selection

6.2.2.2.3 Detailed description of UE behaviour in state EMM-DEREGISTERED

6.2.2.2.3.1 NORMAL-SERVICE

The UE shall perform an attach procedure.

6.2.2.2.3.2 LIMITED-SERVICE

The UE shall perform an attach procedure when entering a cell which provides normal service.

6.2.2.2.3.3 ATTEMPTING-TO-ATTACH

6.2.2.2.3.4 PLMN-SEARCH

No specific action is required.

6.2.2.2.3.5 NO-IMSI

The UE shall only perform cell selection according to 3GPP TS 36.304 [29].

6.2.2.2.3.6 ATTACH-NEEDED

The UE shall start the attach procedure, if still needed, as soon as the access is allowed in the selected cell for one of the access classes of the UE.

6.2.2.2.3.7 NO-CELL-AVAILABLE

The UE shall perform cell selection according to 3GPP TS 36.304 [29] and choose an appropriate substate when a cell is found.

6.2.2.2.4 Substate when back to state EMM-DEREGISTERED from another EMM state

When returning to state EMM-DEREGISTERED, the UE shall select a cell as specified in 3GPP TS 36.304 [29].

The substate depends on the result of the cell selection procedure, the outcome of the previously performed EMM specific procedures, on the EPS update status of the UE, on the tracking area data stored in the UE and on the presence of the USIM:

- If no cell has been found, the substate is NO-CELL-AVAILABLE, until a cell is found.
- If no USIM is present or if the inserted USIM is considered invalid by the UE, the substate shall be NO-IMSI.
- If the selected cell is in a tracking area where the UE is allowed to roam, the substate shall be NORMAL-SERVICE.
- If an attach shall be performed (e.g. network requested re-attach), the substate shall be ATTEMPTING-TO-ATTACH.
- If a PLMN reselection (according to 3GPP TS 23.122 [22]) is needed, the substate shall be PLMN-SEARCH.
- If the selected cell is in a tracking area where the UE is not allowed to roam, the substate shall be LIMITED-SERVICE.

6.2.2.3 UE behaviour in state EMM-REGISTERED

6.2.2.3.1 General

The state EMM-REGISTERED is entered at the UE, when:

- the attach procedure is performed by the UE (see subclause 6.2.5.1).

6.2.2.3.2 Detailed description of UE behaviour in state EMM-REGISTERED

6.2.2.3.2.1 NORMAL-SERVICE

The UE shall perform normal and periodic tracking area updating (see subclause 6.2.5.3).

6.2.2.3.2.2 ATTEMPTING-TO-UPDATE

6.2.2.3.2.3 LIMITED-SERVICE

6.2.2.3.2.4 PLMN-SEARCH

6.2.2.3.2.5 UPDATE-NEEDED

The UE shall:

- not send any user data nor signalling information;
- perform cell selection/reselection according to 3GPP TS 36.304 [29]; and
- enter the appropriate new substate depending on the EPS update status as soon as the access is allowed in the selected cell for one of the access classes of the UE.

6.2.2.3.2.6 NO-CELL-AVAILABLE

The UE shall perform cell selection/reselection according to 3GPP TS 36.304 [29].

6.2.3 General on elementary EMM procedures for EPS services

6.2.4 EMM common procedures

6.2.4.1 GUTI reallocation procedure

6.2.4.1.1 General

The purpose of the GUTI reallocation procedure is to allocate a GUTI and optionally to provide a new TAI list to a particular UE.

The reallocation of a GUTI is performed by the unique procedure defined in this subclause. This procedure can only be initiated by the MME in state EMM-REGISTERED.

The GUTI can also be implicitly reallocated at attach or tracking area updating procedures. The implicit reallocation of a GUTI is described in the subclauses which specify these procedures (see subclause 6.2.5.1 and 6.2.5.3).

NOTE 1: The GUTI reallocation procedure is usually performed in ciphered mode.

NOTE 2: Normally, the GUTI reallocation will take place in conjunction with another mobility management procedure, e.g. as part of tracking area updating.

6.2.4.1.2 GUTI reallocation initiation by the network

The MME shall initiate the GUTI reallocation procedure by sending a GUTI REALLOCATION COMMAND message to the UE and starting the timer T3450.

The GUTI REALLOCATION COMMAND message shall include a GUTI and may include a TAI list.

6.2.4.1.3 GUTI reallocation completion by the UE

Upon receipt of the GUTI REALLOCATION COMMAND message, the UE shall store the GUTI and the TAI list, and send a GUTI REALLOCATION COMPLETE message to the MME. The UE considers the new GUTI as valid and the old GUTI as invalid (see subclause 5.1.2). If the UE receives a new TAI list in the GUTI REALLOCATION COMMAND message, the UE shall consider the new TAI list as valid and the old TAI list as invalid; otherwise, the UE shall consider the old TAI list as valid

6.2.4.1.4 GUTI reallocation completion by the network

Upon receipt of the GUTI REALLOCATION COMPLETE message, the MME shall stop the timer T3450 and consider the new GUTI as valid and the old GUTI as invalid (see subclause 5.1.2).

Editor's note: The abnormal cases in the UE and on the network side need to be defined.

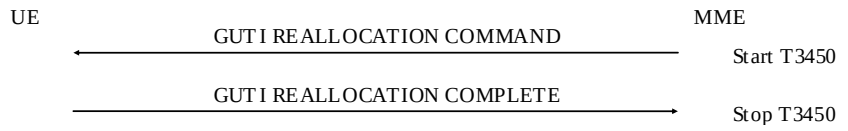


Figure 6.2.4.1.4.1: GUTI reallocation procedure

6.2.4.2 Authentication and security mode procedure

6.2.4.2.1 Authentication and key agreement

6.2.4.2.1.1 General

The purpose of the EPS authentication and key agreement (AKA) procedure is to provide mutual authentication between the user and the network (see 3GPP TS 33.401 [40]). The cases where the EPS AKA procedure should be used are defined in 3GPP TS 33.401 [40].

The EPS AKA procedure is always initiated and controlled by the network. However, there is the possibility for the UE to reject the EPS authentication challenge sent by the network.

The UE shall only support the EPS authentication challenge if a USIM is present.

An EPS security context is established in the UE and the network when an EPS authentication challenge is performed. After a successful EPS authentication, the resulting CK and IK are transformed into a key, K_{ASME}, which is the basis for the EPS key hierarchy, which is stored both in the network and the UE.

6.2.4.2.1.2 Authentication initiation by the network

The network initiates the authentication procedure by sending an AUTHENTICATION REQUEST message to the UE and starts the timer T3460. The AUTHENTICATION REQUEST message contains the parameters necessary to calculate the response parameters (see 3GPP TS 33.401 [40]). In an EPS AKA run, the AUTHENTICATION REQUEST message also contains the key set identifier allocated to the K_{ASME}, which may be computed from the given parameters.

6.2.4.2.1.3 Authentication response by the UE

The UE shall be ready to respond upon an AUTHENTICATION REQUEST message at any time whilst a NAS signalling connection exists. With exception of the cases described in subclause 6.2.4.2.1.6, it shall process the challenge information and send back an AUTHENTICATION RESPONSE message to the network.

In an EPS authentication challenge, the new K_{ASME} calculated from the challenge information shall overwrite the previous K_{ASME}.

The USIM will provide the mobile station with the authentication response, based upon the authentication challenge given from the ME. An EPS authentication challenge will result in the USIM passing a RES to the ME.

Editor's note: It is FFS how to avoid synchronisation failure during the authentication procedure.

6.2.4.2.1.4 Authentication completion by the network

6.2.4.2.1.4.1 Authentication response received by the network

Upon receipt of the AUTHENTICATION RESPONSE message, the network stops the timer T3460 and checks the validity of the response (see 3GPP TS 33.401 [40]).

Upon receipt of the AUTHENTICATION FAILURE message, the network stops the timer T3460. In the Synch failure case, the core network may renegotiate with the HSS/AuC and provide the UE with new authentication parameters.

6.2.4.2.1.4.2 EPS key identification

The security parameters for authentication and ciphering are tied together in sets. In an EPS authentication challenge, from a challenge parameter RAND, the authentication response parameter RES and the K_{ASME} can be computed given the secret key associated to the IMSI. In addition, a UMTS ciphering key, a UMTS integrity key and a GSM ciphering key can be computed from the K_{ASME} by means of a conversion function.

In order to allow start of ciphering and integrity protection on a NAS signalling connection without authentication, the Key Set Identifiers (KSIs) are introduced. The KSI is managed by the network in the way that the AUTHENTICATION REQUEST message contains the KSI allocated to the K_{ASME}.

If an authentication procedure has been completed successfully and a KSI is stored in the network, the network shall include a different KSI in the AUTHENTICATION REQUEST message when it initiates a new authentication procedure.

The mobile station stores the KSI with the K_{ASME}, EPS NAS ciphering key and the EPS NAS integrity key and indicates to the network in the initial NAS message which KSI the stored K_{ASME} has.

When the deletion of the KSI is described this also means that the associated K_{ASME}, EPS NAS ciphering key and the EPS NAS integrity key shall be considered as invalid (i.e. the established EPS NAS security context is no longer valid).

In S1 mode, the network may choose to start ciphering and integrity with the stored EPS NAS ciphering key and EPS NAS integrity key (under the restrictions given in 3GPP TS 33.401 [40]) if the stored KSI and the one given from the mobile station are equal.

NOTE: In some specifications the term ciphering key sequence number might be used instead of the term Key Set Identifier (KSI).

6.2.4.2.1.5 Authentication not accepted by the network

If authentication fails, because the response is not valid, the network may distinguish between the two different ways of identification used by the mobile station:

- the GUTI was used;
- the IMSI was used.

If the GUTI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the mobile station then differs from the one the network had associated with the GUTI, the authentication should be restarted with the correct parameters. If the IMSI provided by the UE is the expected one (i.e. authentication has really failed), the network should proceed as described below.

If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION REJECT message should be transferred to the mobile station.

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the USIM to EU3 ROAMING NOT ALLOWED, delete from the USIM the stored GUTI, TAI list, last visited registered TAI and KSI. The USIM shall be considered as invalid until switching off the mobile station or the UICC containing the USIM is removed.

If the AUTHENTICATION REJECT message is received, the mobile station shall abort any EMM signalling procedure, stop any of the timers T3410, 3417 or T3430 (if running) and enter state EMM_DEREGISTERED.

6.2.4.2.1.6 Authentication not accepted by the UE

In an EPS authentication challenge, the authentication procedure is extended to allow the UE to check the authenticity of the core network. Thus allowing, for instance the UE the possibility for detection of a false base station.

Following a EPS authentication challenge, the UE may reject the core network, on the grounds of an incorrect AUTN parameter (see 3GPP TS 33.102 [5]). This parameter contains two possible causes for authentication failure:

a) MAC code failure:

   If the UE considers the MAC code (supplied by the core network in the AUTN parameter) to be invalid, it shall send an AUTHENTICATION FAILURE message to the network, with the reject cause 'MAC failure'. The UE shall then follow the procedure described in subclause tbd.

Editor's note: It is FFS in which subclause this procedure referred to in the above paragraph will be described.

b) SQN failure:

   If the UE considers the SQN (supplied by the core network in the AUTN parameter) to be out of range, it shall send a AUTHENTICATION FAILURE message to the network, with the reject cause 'Synch failure' and a re-synchronization token AUTS provided by the USIM (see 3GPP TS 33.102 [5]). The UE shall then follow the procedure described in subclause tbd.

Editor's note: It is FFS in which subclause this procedure referred to in the above paragraph will be described.

A UE with a USIM shall reject the authentication challenge if no Authentication Parameter AUTN IE was present in the AUTHENTICATION REQUEST message (i.e. a GSM authentication challenge has been received when the UE expects an EPS authentication challenge). In such a case, the UE shall send the AUTHENTICATION FAILURE message to the network, with the reject cause "GSM authentication unacceptable". The UE shall then follow the procedure described in subclause tbd.

Editor's note: It is FFS in which subclause this procedure referred to in the above paragraph will be described.

If the UE returns an AUTHENTICATION_FAILURE message to the network, the UE shall delete any previously stored RAND and RES and shall stop timer T3418, if running.

6.2.4.2.2 Security mode setup command and algorithm negotiation

6.2.4.2.2.1 General

The purpose of the NAS security mode command procedure is to provide NAS signalling security between the UE and the MME, which performs integrity and replay protection as well as enciphering and deciphering of NAS signalling messages.

6.2.4.2.2.2 NAS security mode setup command initiation by the network

6.2.4.2.2.3 NAS security mode setup command accepted by the UE

6.2.4.2.2.4 NAS security mode setup command completion by the network

6.2.4.2.2.5 NAS security mode setup command not accepted by the UE

6.2.4.3 Identification procedure

6.2.4.3.1 General

The identification procedure is used by the network to request a particular UE to provide specific identification parameters, e.g. the International Mobile Subscriber Identity (IMSI) or the International Mobile Equipment Identity (IMEI) (see 3GPP TS 23.003 [7]).

6.2.4.3.2 Identification initiation by the network

The network shall initiate the identification procedure by sending an IDENTITY REQUEST message to the UE and start the timer T3470. The IDENTITY REQUEST message shall include the requested identification parameters in the Identity type information element.

Editor's note: Whether the timer T3470 is the same as the one specified for 2G/3G (i.e. T3370) is FFS.

Editor's note: The Identity type IE needs to be defined.

6.2.4.3.3 Identification response by the UE

A UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in EMM-CONNECTED mode.

Upon receipt of the IDENTITY REQUEST message the UE shall send an IDENTITY RESPONSE message to the network. The IDENTITY RESPONSE message shall contain the identification parameters as requested by the network.

6.2.4.3.4 Identification completion by the network

Upon receipt of the IDENTITY RESPONSE the network shall stop the timer T3470.

Editor's note: The abnormal cases in the UE and on the network side need to be defined.

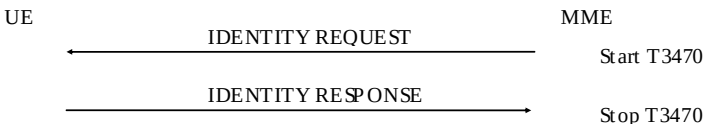


Figure 6.2.4.3.4.1: Identification procedure

6.2.4.4 EMM information procedure

6.2.5 EMM specific procedures

6.2.5.1 Attach procedure

6.2.5.1.1 General

The attach procedure is used to attach for packet services in EPS. With a successful attach procedure, a context is established for the UE in the MME, and a default bearer is established between the UE and the PDN GW, thus enabling always-on IP connectivity to the UE. The network may also initiate the activation of dedicated bearers as part of the attach procedure.

In a shared network, the UE shall choose one of the PLMN identities broadcast in the cell for the attach procedure. The selected network shall be indicated by the UE to the eNodeB.

During the attach procedure the UE may also obtain the home agent IPv4 and IPv6 addresses.

6.2.5.1.2 Attach procedure initiation

In state EMM-DEREGISTERED, the UE initiates the attach procedure by sending an ATTACH REQUEST message to the MME, starting timer T3410 and entering state EMM-REGISTERED-INITIATED. The UE shall include in the ATTACH REQUEST message a valid GUTI together with the last visited registered TAI, if available. If there is no valid GUTI available, the UE shall include the IMSI in the ATTACH REQUEST message. The UE shall also indicate the UE network capability, attach type, and NAS key set identifier.

If available, the UE shall also include information about the IP address allocation in the PDN address allocation IE as specified in subclause 5.1.3. The UE may also indicate the DRX parameter and the protocol configuration options.

If the UE wants to keep the connection(s) to the PDN GW to which it has connected via non-3GPP access, the UE shall indicate "handover attach" in the Attach type IE. Otherwise, the UE shall indicate "initial attach" in the Attach type IE.

Editor's note: It is FFS whether the UE provides the APN information in the ATTACH REQUEST message.

If a valid NAS security context exists, the UE shall include a message authentication code and a NAS message sequence number for uplink in the ATTACH REQUEST message.

If the UE is configured to use DSMIPv6, the UE may include a request for obtaining the IPv6 address of the home agent in the Protocol configuration options IE in the ATTACH REQUEST message. The UE may also include a request for obtaining the IPv4 address of the home agent.

6.2.5.1.3 EMM common procedure initiation

The network may initiate EMM common procedures, e.g. the identification, authentication and security mode procedures, depending on the received information such as IMSI, GUTI and KSI.

6.2.5.1.4 Attach accepted by the network

If the attach request is accepted by the network, the MME shall send an ATTACH ACCEPT message to the UE. The network may also initiate the activation of dedicated bearers towards the UE by invoking the dedicated bearer context activation procedure (see subclause 10.3.3.2).

The MME shall assign and include the TAI list the UE is registered to in the ATTACH ACCEPT message. The UE, receiving an ATTACH ACCEPT message, shall delete its old TAI list and store the received TAI list.

Upon receiving the ATTACH ACCEPT message, the UE shall stop timer T3410, reset the attach attempt counter and tracking area update attempt counter, enter state EMM-REGISTERED and set the EPS update status to EU1 UPDATED.

The GUTI reallocation may be part of the attach procedure. When the ATTACH REQUEST message includes the IMSI or when the MME considers the GUTI provided by the UE is invalid, the MME shall allocate a new GUTI to the UE. The MME shall include in the ATTACH ACCEPT message the new assigned GUTI together with the assigned TAI list. In this case the MME shall start timer T3450 and enter state EMM-COMMON-PROCEDURE-INITIATED as described in subclause 6.2.4.1.

If the ATTACH ACCEPT message contains a GUTI, the UE shall use this GUTI as the new temporary identity. The UE shall delete its old GUTI and store the new assigned GUTI. If no GUTI has been included by the MME in the ATTACH ACCEPT message, the old GUTI, if any available, shall be kept.

The MME shall allocate an EPS bearer identity for the default EPS bearer context activated for the UE and shall include the EPS bearer identity IE in the ATTACH ACCEPT message.

The MME shall include in the ATTACH ACCEPT message the PDN address assigned to the UE by the PDN GW, if available, in the PDN address information IE. This address shall be used for the default bearer and any dedicated bearer established towards the same PDN.

The MME may include an IPv6 address of the PDN GW in the ATTACH ACCEPT message, for further use with host based mobility. In addition to the IPv6 address, the MME may also include an IPv4 address of the PDN GW.

Editor's note: The conditions under which a PDN GW address is delivered by the MME are FFS. Whether this IP address is delivered only if host based mobility is used or in any case is FFS. Whether this depends on UE IP version capabilities is FFS.

If the PDN address information is included in the ATTACH ACCEPT message, the MME shall also include the APN IE in order to provide to the UE the APN for which the activated default bearer is associated.

The UE, when receiving the ATTACH ACCEPT message, shall send an ATTACH COMPLETE message to the network, containing the EPS bearer identity.

Upon receiving an ATTACH COMPLETE message, the MME shall stop timer T3450 and consider the GUTI sent in the ATTACH ACCEPT message as valid.

6.2.5.1.5 Attach not accepted by the network

If the attach cannot be accepted by the network, the MME shall send an ATTACH REJECT message to the UE including an appropriate reject cause value.

Upon receiving the ATTACH REJECT message, the UE shall stop timer T3410, enter state EMM-DEREGISTERED and take corresponding actions based on the reject cause value received.

Editor's note: The reject cause values as well as the actions the UE takes and the substates of the state EMM-DEREGISTERED (see subclause 6.2.1.3.2.3) the UE enters as a result of receiving different reject causes are FFS.

6.2.5.2 Detach procedure

6.2.5.2.1 General

The detach procedure is used:

- by the UE to inform the network that it does not want to access the EPS any longer; and
- by the network to inform the UE that it does not have access to the EPS any longer.

The detach procedure shall be invoked by the UE if the UE is switched off, the USIM card is removed from the UE or the EPS capability of the UE is disabled.

If the detach procedure is performed, the EPS bearer context(s) for this particular UE are deactivated locally without peer-to-peer signalling between the UE and the MME.

6.2.5.2.2 UE initiated detach procedure

6.2.5.2.2.1 UE initiated detach procedure initiation

The detach procedure is initiated by the UE by sending a DETACH REQUEST message. The Detach type IE included in the message indicates whether detach is due to a "switch off" or not.

If the detach is not due to switch off and the UE is in the state EMM-REGISTERED, timer T3421 shall be started in the UE after the DETACH REQUEST message has been sent. The UE shall then enter the state EMM-DEREGISTERED-INITIATED.

If the UE is to be switched off, the UE shall try for a period of 5 seconds to send the DETACH REQUEST message. During this period, the UE may be switched off as soon as the DETACH REQUEST message has been sent.

6.2.5.2.2.2 UE initiated detach procedure completion

When the DETACH REQUEST message is received by the network, the network shall send a DETACH ACCEPT message to the UE, if the Detach type IE does not indicate "switch off". Otherwise, the procedure is completed when the network receives the DETACH REQUEST message.

The network and the UE shall deactivate the EPS bearer context(s) for this UE locally without peer-to-peer signalling between the UE and the MME.

The UE, when receiving the DETACH ACCEPT message, shall stop timer T3421.

The UE is marked as inactive in the network for EPS services. State EMM-DEREGISTERED is entered in the UE and the network.

6.2.5.2.2.3 Abnormal cases in the UE

6.2.5.2.3 Network initiated detach procedure

6.2.5.2.3.1 Network initiated detach procedure initiation

The network initiates the detach procedure by sending a DETACH REQUEST message to the UE. The network may include an EMM cause IE to specify the reason for the detach request. The network shall start timer T3422, deactivate the EPS bearer context(s) for the UE locally and enter state EMM-DEREGISTERED-INITIATED.

6.2.5.2.3.2 Network initiated detach procedure completion by the UE

When receiving the DETACH REQUEST message and the Detach type IE indicates "re-attach required", the UE shall deactivate the EPS bearer context(s) including the EPS default bearer context locally without peer-to-peer signalling between the UE and the MME. The UE shall then send a DETACH ACCEPT message to the network and enter state EMM-DEREGISTERED. The UE shall, after the completion of the detach procedure, initiate an attach procedure.

When receiving the DETACH REQUEST message and the Detach type IE indicates "re-attach not required", the UE shall deactivate the EPS bearer context(s) including the EPS default bearer context locally without peer-to-peer signalling between the UE and the MME. The UE shall then send a DETACH ACCEPT message to the network and enter state EMM-DEREGISTERED.

6.2.5.2.3.3 Network initiated detach procedure completion by the network

The network shall, upon receipt of the DETACH ACCEPT message, stop timer T3422 and enter state EMM-DEREGISTERED.

6.2.5.2.3.4 Abnormal cases on the network side

6.2.5.3 Tracking area updating procedure

6.2.5.3.1 General

The tracking area updating procedure is always initiated by the UE and is used for the following purposes:

- normal tracking area updating to update the registration of the actual tracking area of a UE in the network;
- periodic tracking area updating to periodically notify the availability of the UE to the network;
- Iu mode to S1 mode intersystem change and A/Gb mode to S1 mode intersystem change.

Editor's note: Other purposes of using the tracking area updating procedure will be added if identified.

Editor's note: The impact of idle mode signalling reduction on this procedure is FFS.

During the tracking area updating procedure, the MME may initiate an authentication procedure and setup security mode.

In a shared network, the UE shall select one of the PLMN identities received on the broadcast channel for the tracking area updating procedure. The selected network shall be indicated by the UE to the E-UTRAN.

A UE initiating the tracking area updating procedure in EMM-IDLE mode may request the network to re-establish the radio and S1 bearers for all active EPS bearer contexts during the procedure.

The periodic tracking area updating procedure is controlled in the UE by timer T3412. When timer T3412 expires, the periodic tracking area updating procedure is started. Start and reset of timer T3412 is described in subclause 6.2.5.3.2.

6.2.5.3.2 Handling of the periodic tracking area update timer

Periodic tracking area updating is used to periodically notify the availability of the UE to the network. The procedure is controlled in the UE by the periodic tracking area update timer T3412. The value of timer T3412 is sent by the network to the UE in the ATTACH ACCEPT message and the TRACKING AREA UPDATE ACCEPT message. The UE shall apply this value in all tracking areas of the list of tracking areas assigned to the UE, until a new value is received.

The timer T3412 is reset and started with its initial value, when the UE goes from EMM-CONNECTED to EMM-IDLE mode. The timer T3412 is stopped when the UE enters EMM-CONNECTED mode.

When timer T3412 expires, the periodic tracking area updating procedure shall be started and the timer shall be set to its initial value for the next start.

If the UE is in another state than EMM-REGISTERED.NORMAL-SERVICE when the timer expires the periodic tracking area updating procedure is delayed until the UE returns to EMM-REGISTERED.NORMAL-SERVICE.

Editor's note: Whether T3412 can be sent in the TRACKING AREA UPDATE ACCEPT message without integrity protection is FFS.

Editor's note: The impacts of idle mode signalling reduction on T3412 handling are FFS.

6.2.5.3.3 Tracking area updating procedure initiation

The UE in state EMM-REGISTERED shall initiate the tracking area updating procedure by sending a TRACKING AREA UPDATE REQUEST message to the MME,

i) when the UE detects entering a tracking area that is not in the list of tracking areas that the UE previously registered in the MME;

ii) when the periodic tracking area updating timer T3412 expires.

After sending the TRACKING AREA UPDATE REQUEST message to the MME, the UE shall start timer T3430 and enter state EMM-TRACKING-AREA-UPDATING-INITIATED.

In the TRACKING AREA UPDATE REQUEST message the UE shall include a GUTI and the last visited registered TAI, the update type indicating the type of the tracking area updating. If a UE in EMM-IDLE mode has uplink user data pending when it initiates the tracking area updating procedure, it may also set an "active" flag in the TRACKING AREA UPDATE REQUEST message to indicate the wish to establish the user plane to the network.

The UE may set a follow-on request pending indicator in the TRACKING AREA UPDATE REQUEST message, to indicate its wish to keep the NAS signalling connection after the completion of the tracking area updating procedure. Only one of the two indicators, "active" flag and follow-on request pending indicator, shall be set in the message.

When the tracking area updating procedure is initiated in EMM-IDLE mode, the UE may also include an EPS bearer context status IE in the TRACKING AREA UPDATE REQUEST message, indicating which EPS bearer contexts are active in the UE.

Editor's note: It is FFS whether the EPS bearer context status IE is an optional or a mandatory parameter.

6.2.5.3.4 Tracking area updating procedure accepted by the network

If the tracking area update request has been accepted by the network, the MME shall send a TRACKING AREA UPDATE ACCEPT message to the UE. If the MME assigns a new GUTI for the UE, a GUTI shall be included in the TRACKING AREA UPDATE ACCEPT message. In this case, the MME shall start timer T3450 and enter state EMM-COMMON-PROCEDURE-INITIATED as described in subclause 6.2.4.1. The MME may include a new TAI list for the UE in the TRACKING AREA UPDATE ACCEPT message.

Editor's note: It is FFS whether other information such as the "equivalent PLMNs" and a "list of emergency numbers" are included in the TRACKING AREA UPDATE ACCEPT message.

If an EPS bearer context status IE is included in TRACKING AREA UPDATE REQUEST message, the MME shall deactivate all those EPS bearer contexts locally (without peer-to-peer signalling between the MME and the UE) which are active on the network side, but are indicated by the UE as being inactive. Additionally, the MME shall include an EPS bearer context status IE in the TRACKING AREA UPDATE ACCEPT message, indicating which EPS bearer contexts are active in the MME.

In a shared network the MME shall indicate the PLMN identity of the operator that has accepted the tracking area update request in the TRACKING AREA UPDATE ACCEPT message.

Editor's note: How this PLMN identity is encoded in the TRACKING AREA UPDATE ACCEPT message is FFS.

If the "active" flag is included in the TRACKING AREA UPDATE REQUEST message, the MME shall re-establish the radio and S1 bearers for all active EPS bearer contexts.

Upon receiving a TRACKING AREA UPDATE ACCEPT message, the UE shall stop timer T3430, reset the routing area updating attempt counter, enter state EMM-REGISTERED and set the EPS update status to EU1 UPDATED. If the message contains a GUTI, the UE shall use this GUTI as new temporary identity for EPS services and shall store the new GUTI. If no GUTI was included by the MME in the TRACKING AREA UPDATE ACCEPT message, the old GUTI shall be used. If the UE receives a new TAI list in the TRACKING AREA UPDATE ACCEPT message, the UE shall consider the new TAI list as valid and the old TAI list as invalid; otherwise, the UE shall consider the old TAI list as valid.

If an EPS bearer context status IE is included in the TRACKING AREA UPDATE ACCEPT message, the UE shall deactivate all those EPS bearers contexts locally (without peer-to-peer signalling between the UE and the MME) which are active in the UE, but are indicated by the MME as being inactive.

If the network wishes to maintain the NAS signalling connection (for example, if the UE has indicated "follow-on request pending" in the TRACKING AREA UPDATE REQUEST message) the network shall indicate "follow-on proceed" in the TRACKING AREA UPDATE ACCEPT message. If the network wishes to release the NAS signalling connection, the network shall indicate "no follow-on proceed" in the TRACKING AREA UPDATE ACCEPT message. The UE shall act according to the follow-on proceed flag provided by the network.

If the TRACKING AREA UPDATE ACCEPT message contained a GUTI, the UE shall return a TRACKING AREA UPDATE COMPLETE message to the MME to acknowledge the received GUTI.

Upon receiving a TRACKING AREA UPDATE COMPLETE message, the MME shall stop timer T3450, and shall consider the GUTI sent in the TRACKING AREA UPDATE ACCEPT message as valid.

6.2.5.3.5 Tracking area updating procedure not accepted by the network

If the tracking area updating cannot be accepted by the network, the MME sends a TRACKING AREA UPDATE REJECT message to the UE including an appropriate reject cause value.

Upon receiving the TRACKING AREA UPDATE REJECT message, the UE shall stop timer T3430 and take corresponding actions depending on the reject cause value received.

Editor's note: The reject cause values as well as the actions the UE takes and the substates of the state EMM-DEREGISTERED (see subclause 6.2.1.3.2.3) the UE enters as a result of receiving different reject causes are FFS.

6.2.6 EMM connection management procedures

6.2.6.1 Service request procedure

6.2.6.1.1 General

The purpose of the service request procedure is to transfer the EMM mode from EMM-IDLE to EMM-CONNECTED mode and establish the radio and S1 bearers when uplink user data is to be sent.

This procedure is used when:

- the network has downlink signalling pending; or
- the UE or the network has user data pending and the UE is in EMM-IDLE mode; or
- the UE in EMM-CONNECTED mode has uplink user data to be sent and the corresponding user plane radio bearers are not established.

The service request procedure is initiated by the UE, however, for the downlink transfer of signalling or user data in EMM-IDLE mode, the trigger is given by the network by means of the paging procedure (see subclause 6.2.6.2).

The service type can take either of the following values: "data" or "paging response". Each of the values shall be selected according to the criteria to initiate the service request procedure.

The UE shall invoke the service request procedure when:

a) the UE receives a paging request from the network in EMM-IDLE mode. In this case, the service type shall be set to "paging response".

b) the UE, in EMM-IDLE or EMM-CONNECTED mode, has pending user data to be sent and no radio bearer is established. In this case, the service type shall be set to "data".

Editor's note: Additional criteria for initiating the Service request procedure as well as other values of the service type are FFS.

Editor's note: The interaction of this procedure with other MM procedures is FFS.

6.2.6.1.2 Service request procedure initiation

The UE initiates the service request procedure by sending a SERVICE REQUEST message to the MME, starts the timer T3417, and enters the state EMM-SERVICE-REQUEST-INITIATED and EMM-CONNECTED mode. The message SERVICE REQUEST shall contain the S-TMSI and the service type.

Upon receipt of the SERVICE REQUEST message, the MME may initiate the authentication procedure.

6.2.6.1.3 Service request procedure accepted by the network

If the SERVICE REQUEST message was sent by the UE in EMM-IDLE mode with service type "data", the indication from the lower layers that the access stratum security is set up shall be treated as a successful completion of the procedure.

If the SERVICE REQUEST message was sent by the UE in EMM-CONNECTED mode with service type "data", the indication from the lower layers that the user plane radio bearer is set up shall be treated as a successful completion of the procedure.

If the SERVICE REQUEST message was sent by the UE with service type "paging response", the indication from the lower layers that the access stratum security is set up shall be treated as a successful completion of the procedure.

If the SERVICE REQUEST message was sent by the UE with service type "paging response", the network will establish the radio and S1 bearers for all activated EPS bearer contexts if it wants to transfer data.

Upon successful completion of the procedure, the UE shall stop the timer T3417 and enter the EMM-REGISTERED state.

6.2.6.1.4 Service request procedure not accepted by the network

If the service request cannot be accepted, the network shall return a SERVICE REJECT message to the UE.

On receipt of the SERVICE REJECT message, the UE shall stop the timer T3417. In addition, the UE shall then take different actions depending on the received reject cause value.

6.2.6.2 Paging procedure

6.2.6.2.1 General

The paging procedure is used by the network to request the establishment of a NAS signalling connection to the UE.

Editor's note: the use of the paging procedure for other purposes is FFS.

6.2.6.2.2 Paging for EPS services through E-UTRAN using S-TMSI

The network shall initiate the paging procedure for EPS services using S-TMSI when NAS signalling messages or user data is pending to be sent to the UE when no NAS signalling connection exists.

To initiate the procedure the EMM entity in the network requests the lower layer to start paging (see 3GPP TS 36.300 [15], 3GPP TS 36.413 [17]) and starts a timer for this paging procedure. Upon reception of a paging indication, the UE shall respond to the paging with a SERVICE REQUEST message with service type "paging response" (see 3GPP TS 23.401 [2] and 3GPP TS 36.413 [17]).

The network shall stop the timer for the paging procedure when a response is received from the UE.

6.2.7 Receiving an EMM STATUS message by an EMM entity

The purpose of the sending of the EMM STATUS message is to report at any time certain error conditions detected upon receipt of EMM protocol data. The EMM STATUS message can be sent by both the MME and the UE.

On receipt of an EMM STATUS message no state transition and no specific action shall be taken as seen from the radio interface, i.e. local actions are possible. The local actions to be taken by the MME or the UE on receipt of an EMM STATUS message are implementation dependent.

6.3 Session management and bearer control procedures

Editor's note: This subclause will contain a detailed description of the signalling procedures used between UE and MME, as far as they are under CT1's responsibility.

6.4 Handling of unknown, unforeseen, and erroneous protocol data

6.5 Message functional definitions and contents

6.5.1 Overview

This clause defines the structure of the messages of the Layer 3 (L3) protocols defined in the present document. These are standard L3 messages as defined in 3GPP TS 24.007 [36].

Each definition given in the present clause includes:

a) a brief description of the message direction and use, including whether the message has:

1. Local significance, i.e. relevant only on the originating or terminating access;
2. Access significance, i.e. relevant in the originating and terminating access, but not in the network;
3. Dual significance, i.e. relevant in either the originating or terminating access and in the network; or
4. Global significance, i.e. relevant in the originating and terminating access and in the network.

b) a table listing the Information Elements (IE) known in the message and the order of their appearance in the message. All IEs that may be repeated are explicitly indicated (The V and LV formatted IEs, which compose the imperative part of the message, occur before the T, TV, and TLV formatted IEs which compose the non-imperative part of the message, see 3GPP TS 24.007 [36]). In a (maximal) sequence of consecutive IEs with half octet length, the first IE with half octet length occupies bits 1 to 4 of octet N, the second IE bits 5 to 8 of octet N, the third IE bits 1 to 4 of octet N+1 etc. Such a sequence always has an even number of elements.

For each information element the table indicates:

1. The Information Element Identifier (IEI), in hexadecimal notation, if the IE has format T, TV, or TLV. If the IEI has half octet length, it is specified by a notation representing the IEI as a hexadecimal digit followed by a "-" (example: B-).

NOTE: The same IEI may be used for different information element types in different messages of the same protocol.

2. The name of the information element (which may give an idea of the semantics of the element). The name of the information element followed by "IE" or "information element" is used in this technical report as reference to the information element within a message.
3. The name of the type of the information element (which indicates the coding of the value part of the IE), and generally, the referenced subclause of subclause 6.6 of the present document describing the value part of the information element.
4. The presence requirement indication (M, C, or O) for the IE as defined in 3GPP TS 24.007 [36].

Editor's note: The presence indication in the table of this document indicates whether the information needs, always, to be present or not in a particular message.

5. The format of the information element (T, V, TV, LV, TLV) as defined in 3GPP TS 24.007 [36].

6. The length of the information element (or permissible range of lengths), in octets, in the message, where "?" means that the maximum length of the IE is only constrained by link layer protocol. This indication is non-normative.

c) subclauses specifying, where appropriate, conditions for IEs with presence requirement C or O in the relevant message which together with other conditions specified in the present document define when the information elements shall be included or not, what non-presence of such IEs means, and - for IEs with presence requirement C - the static conditions for presence and/or non-presence of the IEs (see 3GPP TS 24.007 [36]).

6.5.2 EPS Mobility Management (EMM) messages

Editor's note: The detailed encoding of the information elements in all messages is FFS. It is assumed that existing information elements in other specifications, e.g. 3GPP TS 24.008 [4], will be reused when possible.

Editor's note: In the following tables the presence indication for information elements reflects the logical requirement for mandatory or optional inclusion in a message. For reasons of coding efficiency CT1 can decide e.g. to specify an information element as mandatory IE, although in the table it is indicated as optional. The order of sequence of information elements is FFS.

6.5.2.1 Attach request

This message is sent by the UE to the network in order to perform an attach procedure. See table 6.5.2.1.1.

Message type: ATTACH REQUEST

Significance: dual

Direction: UE to network

Table 6.5.2.1.1: ATTACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 6.6.2	M	V	1/2
	Skip indicator	Skip indicator 6.6.3	M	V	1/2
	Attach request message identity	Message type 6.6.4	M	V	1
	Old GUTI or IMSI	FFS	M	FFS	FFS
	UE network capability	FFS	M	FFS	FFS
	Attach type	FFS	M	FFS	FFS
	NAS key set identifier	FFS	M	FFS	FFS
FFS	Last visited registered TAI	FFS	O	FFS	FFS
FFS	Message authentication code	FFS	O	FFS	FFS
FFS	NAS message sequence number for uplink	FFS	O	FFS	FFS
FFS	PDN address allocation	FFS	O	FFS	FFS
FFS	DRX parameter	FFS	O	FFS	FFS
FFS	Protocol configuration options	Protocol configuration options 6.6.5.2.2	O	TLV	3 - 253

6.5.2.2 Attach accept

This message is sent by the network to the UE to indicate that the corresponding attach request has been accepted. See table 6.5.2.2.1.

Message type: ATTACH ACCEPT

Significance: dual

Direction: network to UE

Table 6.5.2.2.1: ATTACH ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Attach accept message identity	Message type 10.4	M	V	1
	Periodic TA update timer	FFS	M	V	FFS
	TAI list	FFS	M	LV	FFS
	EPS default bearer identity	FFS	M	FFS	FFS
	Access point name	Access point name 6.6.5.2.1	M	TLV	3 - 102
	Message authentication code	FFS	M	FFS	FFS
	NAS message sequence number for downlink	FFS	M	FFS	FFS
FFS	GUTI	FFS	O	FFS	FFS
FFS	PDN address information	FFS	O	FFS	FFS
FFS	Session management configuration	FFS	O	FFS	FFS
FFS	Protocol configuration options	Protocol configuration options 6.6.5.3.1	O	TLV	3 - 253

6.5.2.3 Attach complete

This message is sent by the UE to the network in response to an ATTACH ACCEPT message. See table 6.5.2.3.1.

Message type: ATTACH COMPLETE

Significance: dual

Direction: UE to network

Table 6.5.2.3.1: ATTACH COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Attach complete message identity	Message type 10.4	M	V	1
	EPS default bearer identity	FFS	M	FFS	FFS
	Message Authentication Code	FFS	M	FFS	FFS
	NAS message sequence number for uplink	FFS	M	FFS	FFS

6.5.2.4 Attach reject

This message is sent by the network to the UE to indicate that the corresponding attach request has been rejected. See table 6.5.2.4.1.

Message type: ATTACH REJECT

Significance: dual

Direction: network to UE

Table 6.5.2.4.1: ATTACH REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Attach reject message identity	Message type 10.4	M	V	1
	EMM cause	FFS	M	V	FFS
FFS	Message authentication code	FFS	O	FFS	FFS
FFS	NAS message sequence number for downlink	FFS	O	FFS	FFS

6.5.2.5 Detach request (UE originating detach)

This message is sent by the UE to request the release of an EMM context. See table 6.5.2.5.1.

Message type: DETACH REQUEST

Significance: dual

Direction: UE to network

Table 6.5.2.5.1: DETACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 6.6.2	M	V	1/2
	Skip indicator	Skip indicator 6.6.3	M	V	1/2
	Detach request message identity	Message type 6.6.4	M	V	1
	Detach type	Detach type 6.6.5.3.2	M	V	1/2
	Spare half octet	Spare half octet 6.5.5.2.2	M	V	1/2
	GUTI	FFS	M	FFS	FFS
	NAS message sequence number for uplink	FFS	M	FFS	FFS
	Message Authentication Code	FFS	M	FFS	FFS

Editor's note: The need of inclusion of the KSI in the DETACH REQUEST is FFS.

6.5.2.6 Detach request (UE terminated detach)

This message is sent by the network to request the release of an EMM context. See table 6.5.2.6.1.

Message type: DETACH ACCEPT

Significance: dual

Direction: network to UE

Table 6.5.2.6.1: DETACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 6.6.2	M	V	1/2
	Skip indicator	Skip indicator 6.6.3	M	V	1/2
	Detach request message identity	Message type 6.6.4	M	V	1
	Detach type	Detach type 6.6.5.3.2	M	V	1/2
	Spare half octet	Spare half octet 6.5.5.2.2	M	V	1/2
	NAS message sequence number for downlink	FFS	M	FFS	FFS
	Message Authentication Code	FFS	M	FFS	FFS
FFS	EMM cause	FFS	O	TV	FFS

6.5.2.7 Detach accept (UE originating detach)

This message is sent by the network to indicate that the detach procedure has been completed. See table 6.5.2.7.1.

Message type: DETACH ACCEPT

Significance: dual

Direction: network to UE

Table 6.5.2.7.1: DETACH ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 6.6.2	M	V	1/2
	Skip indicator	Skip indicator 6.6.3	M	V	1/2
	Detach accept message identity	Message type 6.6.4	M	V	1
	NAS message sequence number for downlink	FFS	M	FFS	FFS
	Message Authentication Code	FFS	M	FFS	FFS

6.5.2.8 Detach accept (UE terminated detach)

This message is sent by the UE to indicate that the detach procedure has been completed. See table 6.5.2.8.1.

Message type: DETACH ACCEPT

Significance: dual

Direction: UE to network

Table 6.5.2.8.1: DETACH ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 6.6.2	M	V	1/2
	Skip indicator	Skip indicator 6.6.3	M	V	1/2
	Detach accept message identity	Message type 6.6.4	M	V	1
	NAS message sequence number for uplink	FFS	M	FFS	FFS
	Message Authentication Code	FFS	M	FFS	FFS

6.5.3 EPS Session Management (ESM) messages

6.6 General message format and information elements coding

6.6.1 Overview

Within the protocols defined in the present document, every message is a standard L3 message as defined in 3GPP TS 24.007 [36]. This means that the message consists of the following parts:

a) protocol discriminator;

b) message type;

c) other information elements, as required.

Editor's note: It is for further study whether the EPS bearer identity and the PTI are used for the addressing of EPS Session Management (ESM) messages.

This organization is illustrated in the example shown in figure 6.6.1.1.

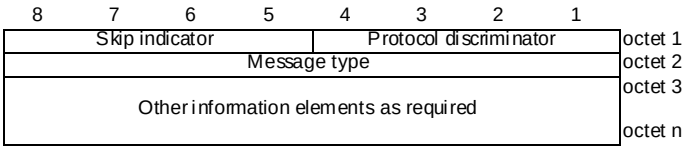


Figure 6.6.1.1: General message organization example

Unless specified otherwise in the message descriptions of subclause 6.6, a particular information element shall not be present more than once in a given message.

When a field extends over more than one octet, the order of bit values progressively decreases as the octet number increases. The least significant bit of the field is represented by the lowest numbered bit of the highest numbered octet of the field.

6.6.2 Protocol Discriminator

The Protocol Discriminator (PD) and its use are defined in 3GPP TS 24.007 [36].

6.6.3 Skip indicator

Bits 5 to 8 of the first octet of every EPS Mobility Management (EMM) message contain the skip indicator. A message received with the skip indicator different from 0000 shall be ignored. A message received with the skip indicator encoded as 0000 shall not be ignored (unless it is ignored for other reasons). A protocol entity sending an EMM message shall encode the skip indicator as 0000.

6.6.4 Message Type

The message type IE and its use are defined in 3GPP TS 24.007 [36]. Table 6.6.4.1 defines the value part of the message type IE used in the EMM protocol.

Table 6.6.4.1: Message types for EPS mobility management

Bits 8	7	6	5	4	3	2	1	
0	1	-	-	-	-	-	-	Mobility management messages
0	1	0	0	0	0	0	1	Attach request
0	1	0	0	0	0	1	0	Attach accept
0	1	0	0	0	0	1	1	Attach complete
0	1	0	0	0	1	0	0	Attach reject
0	1	0	0	0	1	0	1	Detach request
0	1	0	0	0	1	1	0	Detach accept
0	1	0	0	1	0	0	0	Tracking area update request
0	1	0	0	1	0	0	1	Tracking area update accept
0	1	0	0	1	0	1	0	Tracking area update complete
0	1	0	0	1	0	1	1	Tracking area update reject
0	1	0	0	1	1	0	0	Service Request
0	1	0	0	1	1	1	0	Service Reject
0	1	0	1	0	0	0	0	GUTI reallocation command
0	1	0	1	0	0	0	1	GUTI reallocation complete
0	1	0	1	0	0	1	0	Authentication request
0	1	0	1	0	0	1	1	Authentication response
0	1	0	1	0	1	0	0	Authentication reject
0	1	0	1	1	1	0	0	Authentication failure
0	1	0	1	0	1	0	1	Identity request
0	1	0	1	0	1	1	0	Identity response
0	1	0	1	1	1	0	1	Security mode command
0	1	0	1	1	1	1	0	Security mode complete
0	1	0	1	1	1	1	1	Security mode reject
0	1	1	0	0	0	0	0	EMM status
0	1	1	0	0	0	0	1	EMM Information

6.6.5 Other information elements

6.6.5.1 General

The different formats (V, LV, T, TV, TLV) and the four categories of information elements (type 1, 2, 3, and 4) are defined in 3GPP TS 24.007 [36].

The first octet of an information element in the non-imperative part contains the IEI of the information element. If this octet does not correspond to an IEI known in the message, the receiver shall determine whether this IE is of type 1 or 2 (i.e. it is an information element of one octet length) or an IE of type 4 (i.e. that the next octet is the length indicator indicating the length of the remaining of the information element) (see 3GPP TS 24.007 [36]).

This allows the receiver to jump over unknown information elements and to analyse any following information elements.

The information element definitions which are common for the EMM and ESM protocols are described in subclause 6.6.5.2.

The information elements of the EMM or ESM protocols can be defined by reference to an appropriate specification, e.g., "see 10.5.6.3 in 3GPP TS 24.008 [4]".

6.6.5.2 Common information elements

6.6.5.2.1 Access point name

See subclause 10.5.6.1 in 3GPP TS 24.008 [4].

6.6.5.2.2 Spare half octet

This element is used in the description of EMM and ESM messages when an odd number of half octet type 1 information elements are used. This element is filled with spare bits set to zero and is placed in bits 5 to 8 of the octet unless otherwise specified.

6.6.5.3 EPS Mobility Management (EMM) information elements

6.6.5.3.1 Protocol configuration options

See subcause 10.5.6.3 in 3GPP TS 24.008 [4].

6.6.5.3.2 Detach type

The purpose of the Detach type information element is to indicate the type of detach.

The Detach type is a type 1 information element.

The Detach type information element is coded as shown in figure 6.6.5.3.2.1 and table 6.6.5.3.2.1.

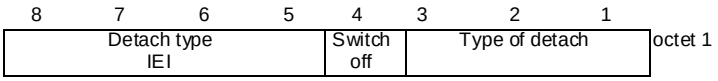


Figure 6.6.5.3.2.1: Detach type information element

Table 6.6.5.3.2.1: Detach type information element

Type of detach (octet 1)

In the network to UE direction:
Bits
3 2 1
0 0 1 re-attach required
0 1 0 re-attach not required

All other values are interpreted as "re-attach not required" in this version of the protocol.

In the UE to network direction the bits 1 to 3 are spare. The UE shall set these bits to zero.

Switch off (octet 1)

In the UE to network direction:
Bit
4
0 normal detach
1 switch off

In the network to UE direction bit 4 is spare. The network shall set this bit to zero.

6.6.5.4 EPS Session Management (ESM) information elements

6.7 List of system parameters

6.7.1 General

The description of timers in the following tables should be considered a brief summary.

6.7.2 Timers of EPS mobility management

Table 6.7.1.1: EPS mobility management timers – UE side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T3412	Default (duration FFS) NOTE 1	EMM-REGISTERED	In EMM-REGISTERED, when EMM-CONNECTED mode is left.	When entering state EMM-DEREGISTERED or when entering EMM-CONNECTED mode.	Initiation of the periodic TAU procedure
NOTE 1: The value of this timer is used if the network does not indicate another value in an EMM signalling procedure.					

Table 6.7.1.2: EPS mobility management timers – network side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3450	6s	EMM-COMMON-PROC-INIT	ATTACH ACCEPT sent with GUTI TAU ACCEPT sent with GUTI GUTI REALLOC COMMAND sent	ATTACH COMPLETE received TAU COMPLETE received GUTI REALLOC COMPLETE received	Retransmission of the same message type, i.e. ATTACH ACCEPT, TAU ACCEPT or GUTI REALLOC COMMAND
T3470	6s	EMM-COMMON-PROC-INIT	IDENTITY REQUEST sent	IDENTITY RESPONSE received	Retransmission of IDENTITY REQUEST
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.					

7 Access to the EPC via non-3GPP access networks

Editor's note: The contents of this clause have been moved to 3GPP TS 24.302 [45]. Therefore this clause is discontinued and no longer updated.

7.1 General

Editor's note: This subclause will contain general information about the access to the EPC via non-3GPP access networks. Among other things this subclause will specify criteria that need to be fulfilled (e.g. with regard to the authentication and authorization procedure) to consider a non-3GPP access network as trusted or untrusted.

Editor's note: The definition of "trusted" and "untrusted" access network is FFS.

7.1.1 User identification

The user identification shall be either the root NAI, or the decorated NAI as defined in 3GPP TS 23.003 [7], when the UE accesses the EPC via non-3GPP access networks, and gets authentication, authorization and accounting services from the EPC.

User identification in non-3GPP accesses may require additional identities that are out of the scope of 3GPP.

7.2 Access authentication and authorization in a trusted non-3GPP access network

Editor's note: This subclause will contain a description of the access authentication and authorization procedures needed when the UE attaches to a trusted non-3GPP access network (reference point S2a or S2c). Section 6.1.1 of 3GPP TS 24.234 [14] can be considered as a basis for this subclause.

7.2.1 General

Editor's note: This subclause will contain general information about the access to the EPC via trusted non-3GPP access networks.

7.2.2 UE procedures

7.2.3 3GPP AAA server procedures

Editor's note: It is assumed that within the present report, like in 3GPP TS 24.234 [14], no distinction needs to be made between roaming and non-roaming scenarios. I.e. within the scope of this report, the Ta* and Wd* reference points defined in 3GPP TS 23.402 [12] are considered to coincide. The Wd* reference point between 3GPP AAA proxy and 3GPP AAA server will be described by CT4 in 3GPP TR 29.803 [13].

7.3 Access authentication and authorization and tunnel management in an untrusted non-3GPP access network

Editor's note: This subclause will contain a description of the access authentication and authorization procedures and tunnel management procedures needed when the UE attaches to an untrusted non-3GPP access network (reference point S2b or S2c).

7.3.1 General

In order to attach to the evolved packet core network (EPC) via untrusted non-3GPP IP access, the UE first needs to be configured with a local IP address from the untrusted non-3GPP access network. Once the UE is configured with a local IP address, the UE shall select the Evolved Packet Data Gateway (ePDG) as described in subclause 7.3.3.2.1 and shall initiate the IPsec tunnel establishment procedure as described in subclause 7.3.3.2.2.

7.3.2 Access authentication and authorization

Editor's note: This subclause will contain a description of the access authentication and authorization procedures needed when the UE attaches to an untrusted non-3GPP access network (reference point S2b or S2c). Section 6.1.1 of 3GPP TS 24.234 [14] can be considered as a basis for this subclause.

7.3.2.1 General

Authentication signalling for untrusted non-3GPP access to the EPC shall be executed between the UE and the 3GPP AAA server in the EPC to ensure mutual authentication of the user and the EPC.

Authorization of EPC access shall be performed by the 3GPP AAA server upon successful user authentication.

Access authentication signalling shall be based on IETF protocols, for e.g., Extensible Authentication Protocol (EAP) as specified in IETF RFC 3748 [26].

Editor's note: The choice of an authentication protocol is FFS.

7.3.2.2 UE procedures

7.3.2.3 3GPP AAA server procedures

Editor's note: It is assumed that within the present report, like in 3GPP TS 24.234 [14], no distinction needs to be made between roaming and non-roaming scenarios. I.e. within the scope of this report, the Wa* and Wd* reference points defined in 3GPP TS 23.402 [12] are considered to coincide. The Wd* reference point between 3GPP AAA proxy and 3GPP AAA server will be described by CT4 in 3GPP 3GPP TR 29.803 [13].

7.3.3 Tunnel management procedures

Editor's note: This subclause will describe the tunnel management procedures. Section 8 of 3GPP TS 24.234 [14] can be considered as a basis for this subclause. The need of additional procedures or parameters is FFS.

7.3.3.1 General

The purpose of tunnel management procedures is to define the procedures for establishment or disconnection of an end-to-end tunnel between the UE and the ePDG. The tunnel establishment procedure is always initiated by the UE, whereas the tunnel disconnection procedure can be initiated by the UE or the ePDG.

The tunnel is an IPsec tunnel (see IETF RFC 4301 [27]) established via an IKEv2 protocol exchange [8] between the UE and the ePDG. The UE may indicate support for MOBIKE [28]. The security mechanisms for tunnel setup using IPsec and IKEv2 are specified in 3GPP TS 33.234 [9].

7.3.3.2 UE procedures

7.3.3.2.1 Selection of the ePDG

The UE shall support the implementation of standard DNS mechanisms in order to retrieve the IP address(es) of the ePDG.

The procedure used by the UE to select an ePDG is the same as the procedure described in 3GPP TS 24.234 [14] for the selection of the PDG.

When building a Fully Qualified Domain Name (FQDN) for the DNS request, the UE shall include both W-APN Network Identifier (NI) and W-APN Operator Identifier (OI). If the user did not provide a value for W-APN OI, then the UE shall use the HPLMN ID or VPLMN ID as the W-APN OI, depending on internal configuration. The structure of the W-APN is defined in 3GPP TS 23.003 [7].

In roaming case, if the UE has selected VPLMN ID for W-APN Operator Identifier (OI) and the DNS query fails, the UE shall build an FQDN with W-APN Operator Identifier (OI) set to HPLMN ID and shall perform a new DNS query to resolve the W-APN.

Upon reception of a DNS response containing one or more IP addresses of ePDGs, the UE shall select an IP address of ePDG with the same IP version as its local IP address.

7.3.3.2.2 Tunnel establishment

Once the ePDG has been selected, the UE shall initiate the IPsec tunnel establishment procedure using the IKEv2 protocol as defined in IETF RFC 4306 [8].

The UE shall send an IKE_SA_INIT request message to the selected ePDG in order to setup an IKE connection. Upon receipt of an IKE_SA_INIT response, the UE shall send an IKE_AUTH request message to the ePDG, including the type of IP address (IPv4 or IPv6 or both) that needs to be configured in an IKEv2 CFG_REQUEST Configuration Payload. If the UE requests for both IPv4 and IPv6 address, it shall send two configuration attributes in the CFG_REQUEST Configuration Payload, one for the IPv4 address and the other for the IPv6 address.The IKE_AUTH request message shall contain in "IDr" payload the W-APN that was used in the DNS query for ePDG selection and in the "IDi" payload the NAI. The IKE_AUTH request message may contain in a notify payload an indication that MOBIKE is supported by the UE.

7.3.3.2.3 Tunnel modification

This procedure is used if MOBIKE as defined in IETF RFC 4555 [28] is supported by the UE.

When there is a change of local IP address for the UE, the UE shall update the IKE security association with the new address, and shall update the IPsec security association associated with this IKE security association with the new address. The UE shall then send an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification to the ePDG.

If, further to this update, the UE receives an INFORMATIONAL request with a COOKIE2 notification present, the UE shall copy the notification to the COOKIE2 notification of an INFORMATIONAL response and send it to the ePDG.

7.3.3.3 3GPP AAA server procedures

7.3.3.4 ePDG procedures

7.3.3.4.1 Tunnel establishment

Upon receipt of an IKE_AUTH request message from the UE requesting the establishment of a tunnel, the ePDG shall proceed with authorization and authentication. The procedure is the same as described in 3GPP TS 33.234 [9].

The ePDG shall proceed with IPsec tunnel setup completion and relay in the IKEv2 Configuration Payload (CFG_REPLY) of the final IKE_AUTH response message the remote IP address assigned to the UE. If the UE requested both an IPv4 and an IPv6 address, both are allocated to the UE via a single CFG_REPLY Configuration Payload containing two configuration attributes, one for the IPv4 address, the other for the IPv6 address, else only the IP address of the requested IP version is allocated. An IPsec tunnel is now established between the UE and the ePDG.

Editor's note: In case of IPv6, it is FFS whether an IPv6 address or an IPv6 prefix is allocated to the UE.

Editor's note: The implications of the IP mobility mode selection procedure on this section are FFS.

7.3.3.4.2 Tunnel modification

When receiving an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification, the ePDG shall check the validity of the IP address and update the IP address in the IKE security association with the values from the IP header. The ePDG shall reply with an INFORMATIONAL response.

The ePDG may initiate a return routability check for the new address provided by the UE, by including a COOKIE2 notification in an INFORMATIONAL request and send it to the UE. When the ePDG receives the INFORMATIONAL response from the UE, it shall check that the COOKIE2 notification payload is the same as the one it sent to the UE. If it is different, the ePDG shall close the IKE security association by sending an INFORMATIONAL request message including a "DELETE" payload.

If no return routability check is initiated by the ePDG, or if a return routability check is initiated and is successfully completed, the ePDG shall update the IPsec security associations associated with the IKE security association with the new address.

8 Mobility management based on mobile IP

Editor's note: This clause will contain a description of the CT1 aspects of mobility management based on mobile IP. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

8.1 General

Editor's note: This subclause will contain general information about mobility management based on mobile IP.

Editor's note: One of the questions to be answered is when and based on which criteria (e.g. trusted or untrusted non-3GPP access or 3GPP access) which of the mobility modes is used (MIPv4 FA mode, PMIPv6 or DSMIPv6).

8.2 Mobility management based on MIPv4 foreign agent mode

Editor's note: The content of this subclause has been moved to 3GPP TS 24.304 [48]. Therefore this subclause is discontinued and no longer updated.

Editor's note: This subclause will contain a description of the CT1 aspects of mobility management using MIPv4 in foreign agent (FA) mode. According to 3GPP TS 23.402 [12] the UE can select this protocol for trusted non-3GPP access (reference point S2a). (For an alternative protocol for reference point S2a see subclause 8.3.)

8.2.1 General

This subclause specifies the procedures for Mobile IPv4 FA mode over S2a reference point based on 3GPP TS 23.402 [12]. The scope of the subclause is limited to the communication between the UE and the FA. The messages exchanged between the FA and the home agent are in the scope of 3GPP TR 29.803 [13].

8.2.2 Mobile IP initial attach

Editor's note: This subclause will describe the procedures related to the PDN GW address discovery, the home address assignment and the bootstrapping of a security association between the UE and the PDN GW via the FA.

8.2.2.1 General

The Mobile IPv4 initial attach is performed by the UE to establish a Mobile IPv4 connection with the node acting as home agent. The initial attach involves the following procedures:

- **Discovery of the home agent address.** The UE needs to discover the IPv4 address of the node acting as home agent.
- **Discovery of the foreign agent care-of address.** The UE needs to discover the IPv4 care-of address provided by the foreign agent.
- **IPv4 home address assignment.** The UE needs to be assigned an IPv4 address to be used as home address in Mobile IPv4 FA mode. The home agent is responsible of assigning the home address to the UE.
- **Security association establishment.** The UE needs to establish a security association with the node acting as home agent in order to secure the Mobile IPv4 signalling. This procedure usually consists in a shared key verification and is performed via Mobile IPv4 signalling.

Editor's note: Details of the security association establishment are FFS.

8.2.2.2 UE procedures

When the UE has attached to the non-3GPP access network, it may send a Mobile IPv4 Agent Solicitation as specified in draft-ietf-mip4-rfc3344bis [23].

As soon as it receives a Mobile IPv4 Agent Advertisement from a foreign agent, the UE selects one care-of address included in the Mobility Agent Advertisement Extension and sends a Registration Request (RRQ) to the foreign agent as specified in [23] with the care-of address included in the Care-of Address field of the RRQ message. The source address shall be the unspecified address (i.e. 0.0.0.0). The Home Address field shall include the unspecified address. Bits S (simultaneous binding) and D (decapsulation by mobile node) shall be cleared, while bit T (reverse tunneling) shall be set to request reverse tunnelling. The UE shall also include the NAI extension as specified in IETF RFC 2794 [24].

If the UE already knows the IP address of the PDN GW (e.g. when the PDN GW address is pre-configured) the UE shall include that IP address in the Home Agent field.

If the UE does not know the IP address of the PDN GW, it shall include the unspecified address in the Home Agent field.

Editor's note: It is FFS how the RRQ is authenticated and which extensions shall be included by the UE.

When the UE receives a Registration Reply from the foreign agent, it shall perform the validity checks and process the message as specified in draft-ietf-mip4-rfc3344bis [23]. After receiving a successful Registration Reply, the UE shall store the home agent address and the home address and may start sending data using the home address.

8.2.2.3 Foreign agent procedures

When the foreign agent receives a Mobile IPv4 Agent Solicitation it shall send to the UE a Mobile IPv4 Agent Advertisement as specified in draft-ietf-mip4-rfc3344bis [23]. The Mobile IPv4 Agent Advertisement shall include only the Mobility Agent Advertisement Extension.

The foreign agent should send an unsolicited Mobile IPv4 Agent Advertisement when it receives a trigger that a new UE has attached to its link. In this case the destination address of the Mobile IPv4 Agent Advertisement shall be the "limited broadcast" address (i.e. 255.255.255.255).

For both solicited and unsolicited Mobile IPv4 Agent Advertisements, the following bits in the Mobility Agent Advertisement Extension shall be set: R (registration required), F (foreign agent) and T (reverse tunneling) (see draft-ietf-mip4-rfc3344bis [23]). At least one care-of address is included in the Mobility Agent Advertisement Extension.

When the foreign agent receives a RRQ from the UE, it shall process it as specified in draft-ietf-mip4-rfc3344bis [23] and 3GPP TS 29.803 [13].

If the RRQ is accepted by the network, the foreign agent shall send to the UE a Registration Reply (RRP) as specified in draft-ietf-mip4-rfc3344bis [23].

Editor's note: It is FFS how the RRP is authenticated and which extensions shall be included by the foreign agent.

8.2.3 Mobile IP handover

8.2.3.1 General

A MIPv4 handover occurs when the UE changes access between trusted non-3GPP accesses. A change in the local point of attachment will trigger a MIPv4 handover procedure. In this case the UE has already an established binding at the PDN GW/home agent, and the handover procedure will update the care-of address (FA IP address) of its binding.

8.2.3.2 UE procedures

The UE may detect a movement, based on the ICMP Lifetime field of the router advertisements: if the lifetime of an agent advertisement has expired, and the UE has not received another Agent Advertisement message from the same FA, then the UE will need to attempt to register with a new FA, and this means that the UE has moved.

Another method for the UE to discover that it had moved is based on the advertised prefix: a change in the advertised prefix may lead the UE to think that it has moved and to register with the newly advertised prefix. This method is only used when all mobility agents use the prefix length extension in their agent advertisements.

NOTE: the UE can also detect the movement based on an indication from the layer 1 and layer 2.

Upon detecting movement, the UE will register with the new FA as specified in draft-ietf-mip4-rfc3344bis [23].

This time in the registration message from the UE, the home address is known, along with the IP address of the home agent.

8.2.3.3 Foreign agent procedures

The FA shall respond to agent solicitations sent by the UE, by addressing them to the unicast layer 2 and layer 3 addresses.

When the FA receives a RRQ from the UE, it shall process it as specified in draft-ietf-mip4-rfc3344bis [23] and 3GPP TS 29.803 [13].

The FA will relay the MIP RRQ to the home agent IP address found in the registration message.

If the network accepts the RRQ, the FA shall send to the UE a Registration Reply (RRP) as specified in draft-ietf-mip4-rfc3344bis [23].

Editor's note: It is FFS how the RRP is authenticated and which extensions shall be included by the FA.

8.2.4 Mobile IP deregistration

8.2.4.1 General

The mobile IP deregistration is either due to a detach or a return home event.

When the UE returns home, it will need to deregister from the home agent. This may occur when the UE returns to the 3GPP network. In this scenario, the UE will de-register from the PDN-GW acting as a home agent.

8.2.4.2 UE procedures

When the UE discovers that it is back home, based on the agent advertisements received: if the agent advertisement has the H bit set, and the prefix advertised is the same as the UE home address, then the UE is home, and it needs to de-register from its home agent.

In case of UE deregistration, the UE sends a MIP RRQ to the home agent, with a Lifetime field set to 0 to indicate that it needs to de-register from the home agent. The MIP RRQ will be handled as specified in draft-ietf-mip4-rfc3344bis [23].

The UE receives a MIP RRP from the home agent, once the deregistration request is accepted.

8.2.4.3 Foreign agent procedures

When the FA receives a RRQ with a Lifetime field set to 0 from the UE, it shall process it as specified in draft-ietf-mip4-rfc3344bis [23] and 3GPP TS 29.803 [13].

The FA will relay the MIP RRQ to the home agent IP address found in the registration message.

If the network accepts the RRQ, the FA shall send to the UE a Registration Reply (RRP) as specified in draft-ietf-mip4-rfc3344bis [23].

Editor's note: It is FFS how the RRP is authenticated and which extensions shall be included by the FA.

In case of return home event, the deregistration procedure occurs between the UE and the home agent, which FA is not involved.

8.3 Mobility management based on PMIPv6

Editor's note: This subclause is a placeholder for CT1 aspects of mobility management based on PMIPv6. According to 3GPP TS 23.402 [12] this protocol can be used in the network for trusted and untrusted non-3GPP access (reference point S2a or S2b, respectively). Currently no direct impact on the UE and correspondingly no CT1 aspects are identified.

8.4 Mobility management based on DSMIPv6

Editor's note: The content of this subclause has been moved to 3GPP TS 24.303 [46]. Therefore this subclause is discontinued and no longer updated.

Editor's note: This subclause will contain a description of the CT1 aspects of mobility management using DSMIPv6. According to 3GPP TS 23.402 [12] the UE can select this protocol for trusted and untrusted non-3GPP access and 3GPP access (reference point S2c).

8.4.1 Mobile IP initial attach

Editor's note: This subclause will describe the procedures related to the PDN GW address discovery, the home address assignment and the bootstrapping of a security association between the UE and the PDN GW when S2c reference point is used.

8.4.1.1 General

The DSMIPv6 initial attach is performed by the UE to establish a DSMIPv6 connection with the node acting as home agent. This is also known as the bootstrapping procedure as the UE establishes the security association with the home agent. The initial attach involves the following tasks:

- **Discovery of the home agent address.** The UE needs to discover the IPv6 address as well as the IPv4 address of the home agent.
- **Security association establishment.** The UE needs to establish an IPsec security association with the home agent in order to secure the DSMIPv6 signalling. IKEv2 (IETF RFC 4877 [18]) is used to establish this security association.
- **IPv6 home address assignment.** The UE needs to be assigned an IPv6 address to be used as home address in DSMIPv6. The home agent is responsible of assigning the home address to the UE.
- **IPv4 home address assignment.** Optionally, a dual-stack UE can also request to be assigned an IPv4 home address to be used for IPv4-only applications. The home agent is responsible of assigning the IPv4 home address to the UE.
- **Initial binding registration.** The UE sends a Binding Update message to perform its initial registration with the PDN GW.

NOTE: In this subclause the terms of home agent and PDN GW are interchangeable.

8.4.1.2 UE procedures

8.4.1.2.1 Discovery of the home agent address

8.4.1.2.1.1 General

The first procedure the UE needs to perform for DSMIPv6 registration is the discovery of the node acting as the home agent.

The UE can discover the IP address of the PDN GW in one of the four following ways:

- via DNS;
- via attach procedure for E-UTRAN access;
- via IKEv2 during tunnel setup to ePDG for untrusted non-3GPP accesses;
- via DHCPv6.

Editor's note: It is FFS under which conditions the above methods can be used.

8.4.1.2.1.2 Home agent address discovery based on DNS

A UE performing PDN GW discovery based on DNS shall support the implementation of standard DNS mechanisms. As specified in draft-ietf-mip6-bootstrapping-split [20], the UE shall perform either a DNS lookup based on the home agent name or a DNS query for a SRV record.

In the former case the UE constructs a DNS request, by setting the QNAME to the configured FQDN. If a home agent has both an IPv4 and an IPv6 address, the corresponding DNS record should be configured with both 'AAAA' and 'A' records. Accordingly the DNS reply will contain 'AAAA' and 'A' records.

Editor's note: It is FFS how the FQDN is constructed from available information. The APN and well-known strings (e.g. "homeagent") may be used for this purpose.

Alternatively the UE performs a DNS query for a SRV record, as specified in RFC 2782 [21]. For this purpose it constructs a request with QTYPE set to SRV and QNAME based on a concatenation of the string specified in draft-ietf-mip6-bootstrapping-split [20] and an FQDN including the Network Identifier and the Operator Identifier.

Editor's note: The exact method to construct the QNAME in case QTYPE is set to SRV is FFS.

8.4.1.2.1.3 Home agent address discovery based on protocol configuration options

The UE may request the IP address of the home agent using the Protocol configuration options IE during the attach procedure for E-UTRAN access or the additional PDN connectivity procedure. The details of this procedure for the case of attach for E-UTRAN access are described in subclause 6.2.5.1.

8.4.1.2.1.4 Home agent address discovery based on IKEv2 signalling

8.4.1.2.1.5 Home agent address discovery based on DHCPv6

A UE performing home agent discovery based on DHCPv6 shall support the implementation of stateless DHCPv6 as specified in IETF RFC 3736 [31] and the DHCPv6 options as specified in draft-ietf-mip6-hiopt [43].

In order to discover the address of the home agent the UE shall send an Information-Request message including the Home Network Identifier Option.

If the UE wants to connect to a home agent in VPLMN for default connectivity, the UE shall set the id-type to 0.

If the UE wants to connect to a home agent for a specific target PDN it shall set the id-type to 1. In this case the UE shall then include the identifier of the requested PDN in the Home Network Identifier field.

Editor's note: It is FFS how the target PDN is constructed from available information and encoded into the Home Network Identifier field. The APN and well-known strings (e.g. "homeagent") may be used for this purpose.

The home agent information is provided to the UE within a Home Network Information Option as described in draft-ietf-mip6-hiopt [43]. This option shall include either the home agent address or the home agent FQDN. In the latter case the UE shall perform a DNS query with the received home agent FQDN as described in subclause 8.4.1.2.1.2.

Editor's note: This procedure is applicable when the UE is in a 3GPP access since the PDN GW acts as DHCPv6 server. It is FFS if it is applicable also when the UE is attached to a non-3GPP access.

8.4.1.2.2 Security association establishment and IPv6 home address assignment

The UE shall support the IKEv2 protocol (see IETF RFC 4306 [8]) for negotiating the IPsec security association to secure DSMIPv6 signalling and shall support EAP over IKEv2 as described in IETF RFC 4306 [8] to perform authentication with an AAA server.

The UE shall support IPsec ESP (see IETF RFC 4303 [42]) in order to provide authentication of Binding Update and Binding Acknowledgement messages as specified in IETF RFC 4877 [18].

The UE shall initiate the security association establishment procedure by sending the IKE_SA_INIT request message defined in IETF RFC 4306 [8] to the home agent. On receipt of an IKE_SA_INIT response, the UE shall send an IKE_AUTH request message including the MN-NAI in the IDi payload and the indication of the target PDN the UE wants to connect to.

Editor's note: It is FFS how the target PDN is encoded (e.g. W-APN or another identifier) and in which IKEv2 payload this information is included (e.g. IDr).

EAP-AKA over IKEv2 shall be used to authenticate UE in the IKE_AUTH exchange, while public key signature based authentication with certificates shall be used to authenticate the home agent.

During the IKEv2 exchange, the UE shall request the allocation of an IPv6 home prefix through the Configuration Payload in the IKE_AUTH. Since in EPS a unique IPv6 prefix is assigned to the UE, the UE shall include a MIP6_HOME_PREFIX attribute in the CFG_REQUEST message as described in IETF RFC 5026 [41]. The UE shall then auto-configure a home address from the IPv6 prefix received from the home agent and shall run a CREATE_CHILD_SA exchange to create the security association for the new home address. In the CREATE_CHILD_SA exchange the UE shall include the home address and the appropriate selectors in the TSi (Traffic Selector-initiator) payload to negotiate the IPsec security association for protecting the Binding Update and Binding Acknowledgement messages as specified in IETF RFC 4877 [18].

8.4.1.2.3 Initial binding registration and IPv4 home address assignment

After establishing the security association and obtaining the home address, the UE shall send a Binding Update message as specified in IETF RFC 3775 [25] and draft-ietf-mip6-nemo-v4traversal [11] in order to register its home address and care-of address at the PDN GW.

If there is IPv6 connectivity in the foreign network, the UE shall send the Binding Update message to the IPv6 address of the home agent. In this Binding Update message the H (home registration) and A (acknowledge) bits shall be set.

Editor's note: It is FFS if the Alternate Care-of Address option can be used by the UE to indicate a care-of address different from the source address of the IPv6 packet.

If there is only IPv4 connectivity in the foreign network, the UE shall send the Binding Update as follows (see draft-ietf-mip6-nemo-v4traversal [11]):

- The IPv6 packet, with the IPv6 home address as the Source Address field of the IPv6 header, shall be encapsulated in UDP.
- The UE shall include the IPv4 care-of address as the Source Address field of the IPv4 header and the home agent IPv4 address as the Destination Address field of the IPv4 header.
- The UE shall include the IPv4 Care-of Address option containing the IPv4 care-of address.
- The UE shall set the H (home registration) and A (acknowledge) bits.
- If the UE has an IPv4 home address, the UE shall include an IPv4 Home Address option with this IPv4 home address, and if the UE requests an IPv4 home address, the UE shall include an IPv4 Home Address option with the unspecified address in the Binding Update message, as defined in draft-ietf-mip6-nemo-v4traversal [11].

When the UE receives the Binding Acknowledgement from the PDN GW, it shall validate it based on the rules described in IETF RFC 3775 [25] and draft-ietf-mip6-nemo-v4traversal [11]. If the Binding Acknowledgement contains a successful status code, the UE shall create an entry for the registered home address in its Binding Update List and may start sending packets containing its IPv6 home address: the formats of the data packets depend on the connectivity type available in the access network and are specified in IETF RFC 3775 [25] and draft-ietf-mip6-nemo-v4traversal [11].

If the Binding Acknowledgment contains an IPv4 Address Acknowledgement option indicating success, the UE shall create two entries in its Binding Update List, one for the IPv6 home address and another for the IPv4 home address. The UE may then send data traffic either with the IPv6 home address or with the IPv4 home address. The details of the data packets formats based on the connectivity type available in the access network are specified in IETF RFC 3775 [25] and draft-ietf-mip6-nemo-v4traversal [11]. If the Binding Acknowledgement contains the NAT Detection option, the UE shall tunnel data packets in UDP and IPv4 as described in draft-ietf-mip6-nemo-v4traversal [11].

8.4.1.3 PDN GW procedures

8.4.1.3.1 Security association establishment and IPv6 home address assignment

The home agent shall support the IKEv2 protocol (see IETF RFC 4306 [8]) for negotiating the IPsec security association to secure DSMIPv6 signalling and shall support EAP over IKEv2 as described in IETF RFC 4306 [8] to perform UE authentication with an AAA server.

The home agent shall support IPsec ESP (see IETF RFC 4303 [42]) in order to provide authentication of Binding Update and Binding Acknowledgement messages as specified in IETF RFC 4877 [18].

The home agent shall complete the IKE_SA_INIT exchange as specified in IETF RFC 4306 [8].

Editor's note: It is FFS which identity is used by the home agent in this exchange and how it relates with the target PDN indicated by the UE.

Upon successful authorization and authentication, the home agent shall accept the security association establishment request by sending the IKE_AUTH response message with the CFG_REPLY payload including the IPv6 prefix allocated to the UE in the MIP6_HOME_PREFIX attribute. This prefix information shall include the prefix length as specified in IETF RFC 5026 [41].

8.4.1.3.2 Initial binding registration and IPv4 home address assignment

When the PDN GW receives a Binding Update message from the UE, it shall validate it as described in IETF RFC 3775 [25]. If the PDN GW accepts the Binding Update message, it shall create a new entry in its Binding Cache for UE, marking it as a home registration. The lifetime of this Binding Cache entry is set based on operator's policies. The PDN GW shall not perform a Duplicate Address Detection on the IPv6 home address of the UE because of the uniqueness of the IPv6 prefix assigned by the PDN GW to the UE. Then the PDN GW shall send a Binding Acknowledgement as specified in IETF RFC 3775 [25].

If the Binding Update contains an IPv4 Home Address option with the unspecified IPv4 address, the PDN GW shall assign an IPv4 home address to the UE, including an IPv4 Address Acknowledgement option in the Binding Acknowledgement message, as specified in draft-ietf-mip6-nemo-v4traversal [11].

If in the received Binding Update the IPv4 care-of address in the IPv4 Care-of Address option is not the same as the IPv4 address in the Source Address in the outer IPv4 header then a NAT was in the path. This information shall be included in the Binding Acknowledgement within a NAT Detection option with the F bit set.

The PDN GW shall send the Binding Acknowledgement message over UDP over IPv4, if the Binding Update message is received over UDP over IPv4.

When the Binding Cache entry is created for the UE, the PDN GW shall tunnel all packets destined to the IPv6 home address and all packets destined to the IPv4 home address (if present) to the UE's care-of address. The tunnelling method depends on the type of care-of address and is specified in draft-ietf-mip6-nemo-v4traversal [11] and IETF RFC 3775 [25].

8.4.2 Mobile IP handover

Editor's note: This subclause will describe the procedures needed when the UE performs a Mobile IP handover over S2c reference point.

8.4.2.1 General

The DSMIPv6 handover procedure is performed by the UE to update its care-of address at the PDN GW after a movement between two different accesses which implies a change of the local IP address (e.g. a movement from a 3GPP to a non-3GPP access). When this procedure takes place, the UE has already a valid registration at the home agent, which implies that the PDN GW has an entry in its Binding Cache for that UE and a security association to secure DSMIPv6 signalling is in place between the UE and the PDN GW.

The procedure involves the exchange of a Binding Update and a Binding Acknowledgement between the UE and the PDN GW. For the handover procedure the UE does not need to discover the PDN GW address or set up a security association with it, as these steps are part of the initial attach procedure described in subclause 8.4.1 which is assumed to be already performed.

8.4.2.2 UE procedures

Following a change of access, the UE configures a new IP address on the target access system. The details of IP address configuration can be access specific.

Editor's note: It is FFS how the UE detects a movement. It is FFS how the IP address can be configured while in the source access system (i.e. optimized handover).

If the access network supports IPv6, as soon as the UE has configured a new IPv6 address, it shall send a Binding Update to the PDN GW including the newly configured IP address as the care-of address. The UE shall always include the IPv6 home address in the Binding Update as specified in IETF RFC 3775 [25].

Editor's note: It is FFS if the Alternate Care-of Address option can be used in the Binding Update.

If the IPv6 prefix assigned to the UE in the target access network and the DSMIPv6 home network prefix are the same, the UE shall send a Binding Update with the Lifetime field set to 0 in order to remove the binding at the home agent, as specified in IETF RFC 3775 [25]. The UE may preserve the IKEv2 session in order to avoid re-establishing the session when the next handover occurs. If there is not a safe assumption that the UE will remain in the home link (e.g. switching off the non-3GPP radio interface in case of a dual radio terminal), the UE should preserve the IKEv2 session.

If the UE has been assigned also an IPv4 home address and wants to update also the binding for it, it shall include the IPv4 Home Address option including the assigned IPv4 home address.

If the UE does not have an IPv4 home address but wants to configure one, it shall include the IPv4 Home Address option with the unspecified address.

If the access network supports only IPv4, as soon as the UE has configured a new IPv4 care-of address, the UE shall send a Binding Update tunnelled in UDP as specified in draft-ietf-mip6-nemo-v4traversal [11].

8.4.2.3 PDN GW procedures

When the PDN GW receives a Binding Update from the UE, it shall update the Binding Cache entry related to the home address included in the Binding Update.

If the Binding Update is an IPv6 packet, the PDN GW shall update the Binding Cache entry with the care-of address is in the Source Address of the IPv6 header.

If the Binding Update outer header is an IPv4 header, the PDN GW shall update the Binding Cache entry with the care-of address in the IPv4 Care-of Address option.

If in the received Binding Acknowledgment the IPv4 care-of address in the IPv4 Care-of Address option is not the same as the IPv4 address in the Source Address in the outer IPv4 header then a NAT was in the path. This information shall be included in the Binding Acknowledgement within a NAT Detection option with the F bit set.

The PDN GW shall send the Binding Acknowledgement message over UDP over IPv4, if the Binding Update message is received over UDP over IPv4.

If the Binding Update contains an IPv4 Home Address option with an IPv4 home address previously assigned, the PDN GW shall update also the Binding Cache entry related to the IPv4 home address to the UE. In any case, the Binding Acknowledge shall always contain the IPv6 home address of the UE in the routing header.

If the Binding Update contains an IPv4 Home Address option with the unspecified IPv4 address, the PDN GW shall assign an IPv4 home address to the UE, including an IPv4 Address Acknowledgement option in the Binding Acknowledgement message. In any case, the Binding Acknowledge shall always contain the IPv6 home address of the UE in the routing header.

If the Lifetime field in the Binding Update is set to 0, the PDN GW shall process the message based on IETF RFC 3775 [25], removing the associated Binding Cache entry and sending the Binding Acknowledge message with the Status field set to 0 (Binding Update accepted).

8.4.3 Mobile IP detach

Editor's note: This subclause will describe the procedures needed when the Mobile IP connection over S2c reference point is released.

8.4.3.1 General

The DSMIPv6 detach is performed by the UE to close the DSMIPv6 session and the respective IKEv2 session or by the network to inform the UE that it does not have access to a specific PDN through DSMIPv6 any longer. After the DSMIPv6 detach procedure, the UE still has IP connectivity provided by the access network.

There are two explicit detach procedures:

- **UE-initiated detach procedure:** in this case the UE performs a DSMIPv6 de-registration with the PDN GW and closes the IKEv2 session.
- **PDN GW-initiated detach procedure:** in this case the PDN GW informs the UE that the DSMIPv6 binding is no more valid. The UE-initiated detach procedure shall then take place.

8.4.3.2 UE procedures

To detach from a specific PDN to which it is connected through a DSMIPv6 session, the UE shall send a Binding Update with the Lifetime field set to 0 as specified in IETF RFC 3775 [25].

The UE shall use the procedures defined in the IKEv2 protocol in IETF RFC 4306 [8] to remove the IPsec security associations associated with the DSMIPv6 registration. The UE shall close the security associations associated with the DSMIPv6 registration and instruct the home agent to do the same by sending the INFORMATIONAL request message including a DELETE payload. The Protocol ID in the DELETE payload shall be set to "1" (IKE) to indicate that all IPsec ESP security associations that were negotiated within the IKEv2 exchange shall be deleted.

Editor's note: In the PDN GW-initiated detach procedure the message used by the PDN GW to inform the UE that a detach procedure occurs and the need for the UE to acknowledge are FFS.

8.4.3.3 PDN GW procedures

When the PDN GW receives a Binding Update with the Lifetime field set to 0, it shall delete any existing entry for the home address included in the Binding Update. Then the PDN GW shall send a Binding Acknowledgement as specified in IETF RFC 3775 [25].

On receipt of the INFORMATIONAL request message including a DELETE payload indicating that the UE is deleting the IPsec security associations associated with the DSMIPv6 registration, the PDN GW shall close the IKE security association, and all IPsec ESP security associations that were negotiated within it towards the UE.

Editor's note: In the PDN GW-initiated detach procedure the message used by the PDN GW to inform the UE that a detach procedure occurs is FFS.

9 Inter-system mobility between E-UTRAN and other access networks

Editor's note: This clause will contain a description of the aspects of inter-system mobility between E-UTRAN and other access networks that are relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

9.1 General

Editor's note: This subclause will contain general information about inter-system mobility between E-UTRAN and other access networks.

9.2 Inter-system mobility between E-UTRAN and GERAN/UTRAN

Editor's note: This subclause will contain a description of aspects of inter-system mobility between E-UTRAN and GERAN/UTRAN relevant for CT1.

9.2.1 General

9.2.2 Mobility management

9.2.2.1 S1 mode to Iu mode inter-system change

When a UE registered with an MME performs S1 mode to Iu mode inter-system change for the first time, it shall initiate the routeing area update procedure (see 3GPP TS 24.008 [4]) by indicating the GUMMEI in the old RAI IE and the M-TMSI in the old P-TMSI IE. (The mapping of the GUMMEI and M-TMSI to the old RAI IE and old P-TMSI IE is defined in 3GPP TS 23.401[2], annex H.)

Editor's note: Impacts of the stage 3 work related to idle mode signalling reduction on the other IEs to be included in the routeing area update is FFS.

9.2.2.2 S1 mode to A/Gb mode inter-system change

When a UE registered with an MME performs S1 mode to A/Gb mode inter-system change for the first time, it shall initiate the routeing area update procedure (see 3GPP TS 24.008 [4]) by indicating the GUMMEI in the old RAI IE and the M-TMSI in the TLLI. (The mapping of the GUMMEI and M-TMSI to the old RAI IE and TLLI IE is defined in 3GPP TS 23.401[2], annex H.)

Editor's note: Impacts of the stage 3 work related to idle mode signalling reduction on the other IEs to be included in the routeing area update is FFS.

9.2.2.3 Idle mode signalling reduction

Editor's note: The following section is to describe ISR effect from CT1's point of view. As there are still some open issues about ISR in SA2, the analysis below may need to be updated.

The network shall inform the UE of the ISR status via NAS signalling. E.g. the TAU accept or RAU accept message shall indicate to the UE whether ISR is activated or not. If ISR is activated:

- The UE shall maintain an internal update type status and provide TIN (Temporary Identity used in Next update) in the TAU/RAU request according to the internal update type status.
- If the UE holds valid TMSI information of the access system, the UE indicates it as additional TMSI information in the TAU/RAU request message, regardless whether the TIN is identical with the additional TMSI.
- The UE shall maintain two independent periodic update timers for the two RATs. An extra mechanism in the core network will prevent the MME or SGSN from marking the UE as implicitly detached due to the expiration of the mobile reachable timer, when the UE misses a periodic update in one RAT while it is camping in the other RAT.
- The ISR capability of the UE shall be included in the UE Network Capability IE.

9.2.3 Session management

9.2.3.1 EPS bearer context enhancements for a GERAN/UTRAN capable UE

If inter-system mobility from E-UTRAN to GERAN/UTRAN is supported by the UE and the network, the EPS bearer context will include not only EPS specific information (see subclause 10.3.5), but also some GERAN/UTRAN specific information.

Editor's note: The detailed information needed in the UE and the network for the support of inter-system change from E-UTRAN to GERAN/UTRAN is FFS.

9.2.3.2 Activation of a primary PDP context in GERAN/UTRAN at initial attach

When a UE performs initial attach to UTRAN/GERAN, it executes the normal attach procedure as defined in 3GPP TS 24.008 [4]. When the UE needs an IP address, it initiates the PDP context activation procedure as defined in 3GPP TS 24.008 [4].

9.2.3.3 Mapping between EPS bearer contexts and PDP contexts

9.2.3.3.1 General

In this subclause the rules to apply when mapping between EPS bearer contexts and PDP contexts are described. This mapping needs to be performed at handover when the UE moves from E-UTRAN to GERAN/UTRAN or the other way around.

Editor's note: The definition of the rules to apply is FFS.

Editor's note: Additional constraints and mapping rules for the combination dual stack EPS bearer context and pre-Rel8 PDP context is FFS.

9.3 Inter-system mobility between E-UTRAN and non-3GPP access networks

Editor's note: This subclause will contain a description of aspects of inter-system mobility between E-UTRAN and non-3GPP access networks, as far as relevant for CT1 and not already covered by clause 8.

9.3.1 General

9.3.2 IP mobility mode selection

Editor's note: The contents of this subclause have been moved to 3GPP TS 24.302 [45]. Therefore this subclause is discontinued and no longer updated.

9.3.2.1 General

The purpose of the IP mobility mode selection procedure is to select the mobility protocol, namely DSMIPv6 or PMIPv6, when the UE moves from 3GPP system to non-3GPP system.

Editor's note: it is FFS whether the IP mobility mode section procedure is also needed when the UE moves from non-3GPP system to 3GPP system

9.4 Inter-system optimized handover between E-UTRAN and cdma2000® HRPD networks

Editor's note: So far, there has been no impacts identified on CT1 specified NAS protocols for optimized inter-system handover from E-UTRAN to cdma2000® HRPD network as described above and any impacts in the other direction is FFS. If in the course of further work performed in other WGs, any specific impacts are identified then appropriate actions need to be taken to specify them in the appropriate specifications within CT WG1.

Editor's note: Impacts from security aspects (work being performed in SA WG3) and possible impacts on network selection aspects are FFS.

9.4.1 General

The purpose of the procedure is to minimise the total service interruption time experienced at the UE, by allowing the UE to attach (in the case of E-UTRAN) or to perform a session configuration or connection establishment (in the case of cdma2000® HRPD) in the target access system before leaving the source access system.

The general mechanism used for optimized handover is to tunnel target specific network access signalling between the source and target access networks.

The purpose of this tunnelling procedure is to remove the authentication, and session management signalling from the time sensitive process that occurs when/if the UE moves from one access to another access. If conditions subsequently warrant that a handover should occur, the UE is ready to connect to the target system.

See 3GPP TS 23.402 [12] for details on the cdma2000® HRPD – E-UTRAN optimized handover flows.

9.4.2 Optimized handover and idle mode mobility from E-UTRAN to cdma2000® HRPD

For handover from an E-UTRAN to a cdma2000® HRPD access network, both active mode and idle mode, the UE performs a pre-registration with a cdma2000® HRPD access and core network over a tunnelling protocol, if the source system provides the UE with sufficient information. If conditions subsequently warrant that a handover should occur for an active UE, the E-UTRAN will send a message the UE to initiate handover procedures, resulting in the handover signalling (connection request / traffic channel allocation) being performed over the tunnelling interface. Once the UE receives the traffic channel allocation, it switches to the cdma2000® HRPD access. If conditions subsequently warrant and the UE is in idle mode, the UE switches to the cdma2000® HRPD access and connects to the target system.

The cdma2000® HRPD messages exchanged between the UE and the target cdma2000® HRPD access and core network are tunnelled over the E-UTRAN access and the S101 reference point. The tunnelling function that carries that signalling occurs below the NAS level and is the responsibility of RAN2 (for RRC) and RAN3 (for S1AP), from a 3GPP perspective. The signalling messages are delivered to the cdma2000® HRPD access network via the S101 tunnelling reference point which is the responsibility of CT4. The stage 2 specification 3GPP TS 23.402 [12] provides the end-to-end specification.

Therefore there are no impacts on CT1 specified protocols for handover from E-UTRAN to cdma2000® HRPD.

9.4.3 Optimized handover and idle mode mobility from cdma2000® HRPD to E-UTRAN

Editor's note: This subclause will contain a procedural description of the optimized HO aspects, including the Pre-registration towards E-UTRA network, while attached to HRPD network. These procedures are exchanged between the UE and MME.

For optimized handover from a cdma2000® HRPD access network to an E-UTRAN, both active mode and idle mode, the UE performs an attach procedure with the target EPS over the tunnelling protocol. Once the attach procedure is completed, the UE switches to the E-UTRAN and starts the service request or tracking area updating procedure.

The E-UTRAN attach messages exchanged between the UE and the target MME are tunnelled over the cdma2000® HRPD access and the S101 reference point. The tunnelling protocol over the cdma2000® HRPD access should be specified by 3GPP2. The signalling messages are delivered to the target MME via the S101 tunnelling reference point which is the responsibility of CT4.

Editor's note: It is FFS if the NAS attach messages over S101 are different from the NAS attach messages over S1-MME. This difference, if any, should be specified in CT1.

10 SAE impact on services, network functions and capabilities

10.1 Security

Editor's note: This clause will contain a description of security aspects relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

10.1.1 Security for E-UTRA

10.1.1.1 General

Security for the NAS signalling is terminated in the UE and in the MME. The security protection for the NAS signalling includes ciphering and integrity protection.

Security for the user plane, as well as for AS signalling, is terminated in the UE and in the E-UTRAN.

The keys for NAS signalling security and user plane security are agreed between MME and UE by means of an authentication and key agreement procedure.

According to the current working assumptions in SA3:

- the UMTS AKA mechanism will be used for authentication and key agreement between MME and UE. This mechanism achieves mutual authentication by the user and the network. For a description of the UMTS AKA mechanism and its use for UTRA security see 3GPP TS 33.102 [5];
- for E-UTRA security the UE shall have a UICC inserted and an activated USIM application. E-UTRA security is based on the existing USIM application.

10.1.1.2 NAS security mode command set-up procedure for E-UTRA

In order to provide NAS signalling security there is a NAS security function in both the UE and the MME that performs integrity/replay protection as well as enciphering/deciphering of NAS signalling messages.

Editor's note: It is FFS whether the NAS security function is an integral part of the NAS protocol layer, a lower sublayer of the NAS protocol layer or a separate protocol layer below the NAS protocol layer.

There are separate security mode command (SMC) set-up procedures for the Access Stratum (AS) between UE and eNodeB and for the Non-Access Stratum (NAS) between UE and MME. The message signalling flow in figure 10.1.1.2.1 shows the NAS security mode command set-up procedure on a high level in case of e.g. power on/attach or tracking area updating.

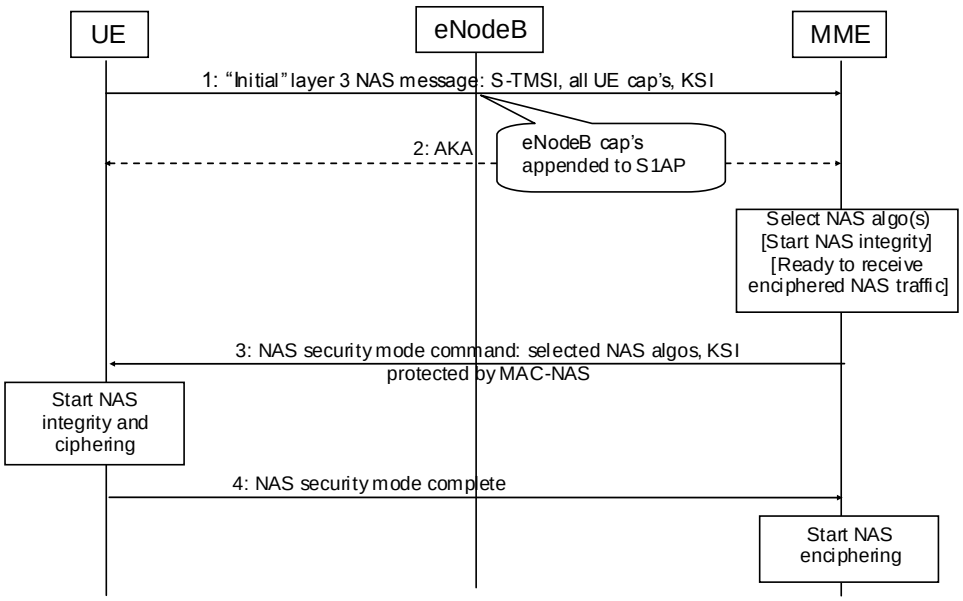


Figure 10.1.1.2.1: NAS security mode command set-up procedure for E-UTRA

Editor's note: The exact outline of the NAS security mode command procedure is FFS. It should be studied whether the UMTS AKA and the SMC set-up procedures could be combined in order to save message round trips and to reduce the time for the UE to get access to the system.

Before step 3 the MME selects the NAS ciphering algorithm to be used, based on information on supported NAS algorithms received from both the UE and the eNodeB (appended by S1AP). At that stage the MME also prepares for the receipt of ciphered NAS signalling messages and starts the NAS integrity protection function which applies to the NAS Security Mode Command message in step 3. When this message is received by the UE, the UE starts integrity and ciphering/deciphering. This means that the Security Mode Complete message in step 4 is both integrity protected and ciphered. When the MME receives this message, it starts the ciphering function.

Other functions related to E-UTRA security and the NAS security mode command procedure in particular that need to be considered are, e.g.:

- NAS encryption/integrity algorithm change at MME relocation (this may need to be handled due to different MMEs being at varying "upgrade" levels);
- Renewal of NAS ciphering key and NAS integrity key triggered by the network (SQN wraparound or keys been too long in UE);
- Renewal of entire key hierarchy based on AKA re-run;
- Activation of new keys (when to start using the new keys); and
- Detection/repair of NAS ciphering key and NAS integrity key out of synch errors or SQN out of synch errors.

10.1.1.3 Input parameters for NAS encryption and integrity algorithms

The same input parameters as were used for UTRA, though slightly modified, will be used for E-UTRA. These parameters are:

- NAS BEARER ID A constant value of the same length as the AS BEARER ID parameter (only included for alignment with AS input parameters)

- NAS COUNT 32 bits (the CT1 working assumption is that the NAS COUNT consists of an 8 bit Sequence number and a 16 bit Overflow counter that is padded with leading zeroes to provide a 32 bit input parameter to the security algorithm)
- DIRECTION 1 bit
- LENGTH The maximum size of NAS messages will be less than 2^{16} octets

The uniqueness property sought from the input parameters is that no two different NAS messages transmitted between the UE and MME shall have the same input parameters to the security algorithms using the same key.

Of the parameters described above, it is clear that the NAS COUNT is required to ensure that each message has a unique input for any given direction (the NAS protocol is a bi-directional channel). Since the same NAS COUNT may appear in both the uplink and the downlink, it is equally clear that the DIRECTION bit is required. The NAS COUNT parameter is built up from two parts, the Overflow Counter (OC) and the Sequence Number (SN). The SN is the part that is carried with each security protected unit and is increased for each new security protected unit. The OC is kept locally by each peer, and is increased when the SN wraps around.

Under the assumption that there can be only one NAS signalling channel per UE, the NAS COUNT and DIRECTION would be sufficient to uniquely identify any given NAS. Therefore, the use of a BEARER ID input parameter will not be necessary from NAS point of view, but for alignment with AS input parameters, a NAS BEARER ID is defined, but is always constant. The length of the NAS BEARER ID parameter shall be the same as it is for the AS.

Editor's note: Which constant value for the NAS BEARER ID to use is left to SA3 to decide upon.

It is required that the NAS COUNT shall be reset to zero if and only if an AKA has been run and a Security Mode Control procedure is performed. An implication of this is that a new AKA must be run when the NAS COUNT is approaching the wraparound point.

The COUNT parameters used in UTRAN and in E-UTRAN PDCP for the AS are 32 bits long. Since the user plane in E-UTRAN can be expected to generate vastly more data than the NAS layer, using a 24-bit value range for NAS COUNT is sufficient.

NOTE: Only the SN part of NAS COUNT needs to be transmitted together with the NAS message, so there is no loss of bandwidth of having a large NAS COUNT. The size of the SN part of the NAS COUNT needs to be large enough to accommodate the expected message loss and message re-ordering. That is, if the SN is, e.g., 8 bits long, the NAS layer can tolerate a loss of 255 NAS messages in a row, or NAS messages re-ordered by 255 packets if an appropriate windowing mechanism is used.

Since EPS is going to be an "all IP network", an upper bound on the length of the NAS messages is the total length of an IP datagram. For IPv4 this length is 2^{16} octets (including the header) if one wish to avoid fragmentation. This is clearly more than what is required for NAS messages, including transport overhead, and far less than what will be regarded as insecure (considering the state of modern encryption algorithms).

10.1.2 Security for non-3GPP access

10.1.2.1 Security for untrusted non-3GPP access

10.2 Quality of service and bearer control (E-UTRAN only)

Editor's note: This clause will contain a description of QoS and bearer control aspects relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

10.2.1 EPS bearer concept

The overall EPS bearer concept is described in 3GPP TS 23.401 [2] and 3GPP TS 23.402 [12]. An EPS bearer is a logical aggregate of one or more service data flows (SDFs), described in 3GPP TS 23.203 [3], running between a UE and a PDN GW for S5/S8 based on GTP or running between a UE and a S-GW for S5/S8 based on PMIP. Basically, there are two types of EPS bearers:

- dedicated bearers
- default bearers.

A dedicated bearer can either be a GBR bearer or a non-GBR bearer. A default bearer can only be a non-GBR bearer.

The EPS bearer concept for E-UTRA is similar to the PS bearer concept from 3GPP Rel-7. Though, one exception is that the notion of a RAB (radio access bearer) does not exist any longer in case of E-UTRA. For S5/S8 based on GTP-u, there is a one-to-one mapping between a radio bearer (RB), an S1 bearer and an S5/S8 bearer for a specific EPS bearer. For S5/S8 based on PMIP, there is a one-to-one mapping between a radio bearer (RB) and a S1 bearer for a specific EPS bearer.

10.2.2 QoS concept

In Rel-7, the possibility for operator controlled QoS was introduced where the network can initiate bearers for services requiring specific QoS by requesting PDP contexts to be established by the network-initiated secondary PDP context activation procedure. Also, the concept of uplink packet filters was introduced. For Rel-8, the EPC/E-UTRAN QoS profile is simplified to only contain a few number of parameters compared to the current Rel-99 UMTS QoS profile. Depending on the type of service to be supported a suitable QoS profile is chosen.

Editor's note: Signalling of QoS profiles and signalling for resource (bearer) establishment and resource reservation, including the direction of such signalling procedures, i.e. network initiated or UE initiated, is FFS.

For an overall description of the EPS QoS concept, refer to 3GPP TS 23.401 [2] and 3GPP TS 23.402 [12].

10.2.3 Bearer level QoS parameters

Each EPS bearer (GBR and non-GBR) is associated with the following bearer level QoS parameters:

- Label
- Allocation and Retention Priority (ARP).

Each GBR bearer is associated with the following bearer level QoS parameters:

- Guaranteed Bit Rate (GBR)
- Maximum Bit Rate (MBR).

For each PDN connection the set of non-GBR bearers between the UE and this PDN is associated with the following bearer level QoS parameter:

- Aggregate Maximum Bit Rate (AMBR).

10.3 Session management and bearer control procedures

10.3.1 General

The session management cooperates with the bearer control for the handling of the EPS bearer context(s) and EPS bearer(s) between UE and MME. The procedures for the handling of EPS bearer context(s) and EPS bearer(s) include procedures for activation, deactivation and modification of bearer context(s) or bearer(s). The EPS bearer context can be either a default bearer context or a dedicated bearer context.

A default EPS bearer context is established when the UE connects to a PDN. The default EPS bearer context remains established throughout the lifetime of connection to this PDN. A UE can also request to setup a new default EPS bearer context with an additional PDN by invoking the UE requested PDN connectivity procedure (see subclause 10.3.3.7). This results in another default EPS bearer context being established between the UE and this other PDN.

Editor's note: It is FFS whether a default bearer context can be established (or selected) in other procedure such as handover procedure from legacy network.

A dedicated EPS bearer context can be established to a PDN after the default EPS bearer context has been established. The dedicated EPS bearer context can be modified or released at any time. The establishment of a dedicated EPS bearer context can be initiated by the network.

The UE can request the network to allocate additional EPS bearer resources. The network decides whether to fulfil this request by activating a new dedicated EPS bearer context(s) or EPS bearer(s) or modifying existing ones. The UE uses a linked bearer identity (LBI) to indicate the PDN connection for which the additional bearer resources are requested.

Figure 10.3.1.1 defines two sublayers for a UE supporting E-UTRAN and UTRAN/GERAN:

- The CM sublayer includes the SM and ESM entities.
- The MM sublayer includes the GMM and EMM entities.

A UE supporting both E-UTRAN and UTRAN/GERAN needs to support some coordination between the contexts maintained by ESM and SM, i.e. EPS bearer contexts and PDP contexts. For EPS bearer contexts the network provides GERAN/UTRAN specific information to support this coordination (see subclause 9.2.2.1).

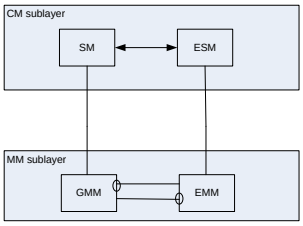


Figure 10.3.1.1: Protocol architecture of non-access-stratum supporting E-UTRAN and UTRAN/GERAN, UE side

10.3.2 Session management states

Editor's note: The content of this subclause has been moved to 3GPP TS 24.301 [44]. Therefore this subclause is discontinued and no longer updated.

10.3.2.1 General

In this subclause the possible states of EPS bearer contexts in the UE and on the network side are described. Each EPS bearer context is associated with an individual state.

Editor's note: For a UE supporting both E-UTRAN and UTRAN/GERAN the relationship between the ESM state machine described in the following subclauses and the SM state machine described in 3GPP TS 24.008 [4] is FFS.

10.3.2.2 EPS bearer context states in the UE

10.3.2.2.1 BEARER CONTEXT INACTIVE

No EPS bearer context exists.

10.3.2.2.2 BEARER CONTEXT ACTIVE

The EPS bearer context is active in the UE.

Editor's note: The need for an additional state for the activation of a default EPS bearer context is FFS.

Editor's note: It is FFS how the activation of default EPS bearer context(s) between the UE and multiple PDN GWs can be described by this state machine.

Editor's note: It is FFS how to describe the UE initiated EPS bearer resource allocation by this state machine.

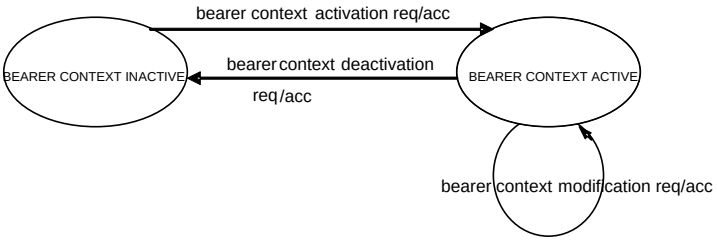


Figure 10.3.2.2.2.1: The bearer context states in the UE (overview)

10.3.2.3 EPS bearer context states in the network

10.3.2.3.1 BEARER CONTEXT INACTIVE

No EPS bearer context exists.

10.3.2.3.2 BEARER CONTEXT ACTIVE PENDING

The network has initiated an EPS bearer context activation towards the UE.

10.3.2.3.3 BEARER CONTEXT ACTIVE

The EPS bearer context is active in the network.

10.3.2.3.4 BEARER CONTEXT INACTIVE PENDING

The network has initiated an EPS bearer context deactivation towards the UE.

10.3.2.3.5 BEARER CONTEXT MODIFY PENDING

The network has initiated an EPS bearer context modification towards the UE.

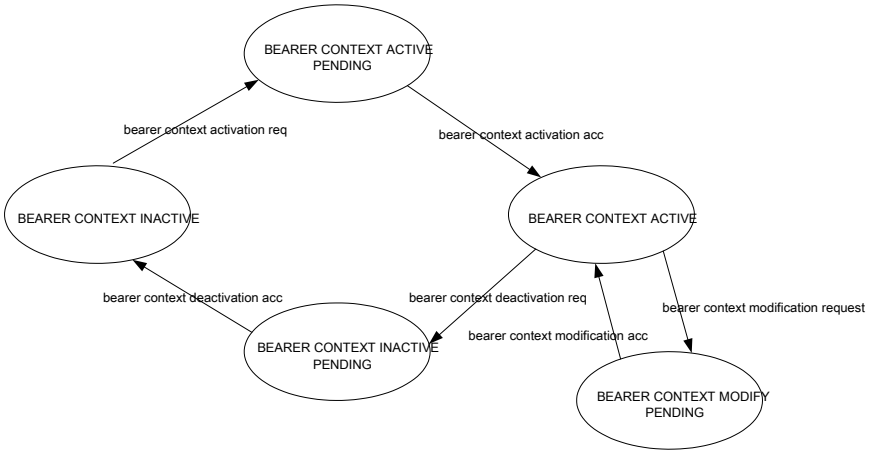


Figure 10.3.2.3.5.1: The bearer context states in the network (overview)

10.3.3 Session management procedures

Editor's note: The content of this subclause has been moved to 3GPP TS 24.301 [44]. Therefore this subclause is discontinued and no longer updated.

10.3.3.1 General

Unless explicitly stated otherwise, the procedures described in the following subclauses can only be executed whilst a NAS signalling exists between the UE and the MME.

Editor's note: Whether it is necessary to define different messages for the ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT and the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT as well as for the ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT and ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT is FFS.

10.3.3.2 Dedicated bearer context activation procedure

10.3.3.2.1 General

The purpose of the dedicated bearer context activation procedure is to establish an EPS bearer context with specific QoS and TFT between the UE and the EPC. The dedicated EPS bearer context activation procedure is initiated by the network, but may be requested by the UE by means of the UE requested bearer resource allocation procedure (see subclause 10.3.3.5). When initiated by the network, the dedicated bearer context activation procedure can be part of the attach procedure (see subclause 6.2.5.1.4), and if the attach procedure fails, the UE shall consider that the dedicated bearer activation has implicitly failed.

10.3.3.2.2 Dedicated bearer context activation initiated by the network

The MME shall initiate the dedicated bearer context activation procedure by sending an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message, which is piggybacked in the Radio Bearer Setup Request to the UE, and enter the state BEARER CONTEXT ACTIVE PENDING.

The ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message shall include an EPS bearer identity, an UL TFT, and the linked EPS bearer identity (LBI). The ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message shall also include a procedure transaction identity (PTI), if this procedure was initiated by a UE requested bearer resource allocation procedure (see subclause 10.3.3.5). If the UE supports GERAN or UTRAN or both, as indicated in the UE network capability IE (see subclause 6.2.5.1.2), the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message may also include the corresponding pre-Rel-8 QoS parameter values of a PDP context according to 3GPP TS 23.401 [2].

NOTE: The QoS is negotiated on layer 2 when the radio bearer is set up as part of the dedicated EPS bearer context activation procedure.

10.3.3.2.3 Dedicated bearer context activation accepted by the UE

Upon receipt of the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message, the UE shall first check the received UL TFT before taking it into use. Then the UE shall send an ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message, which is piggybacked in the Radio Bearer Setup Response to the MME, and enter the state BEARER CONTEXT ACTIVE. The ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message shall include the EPS bearer identity.

The LBI included in the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message indicates to the UE to which default bearer, IP address and PDN the dedicated bearer is linked.

If the PTI is included in the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message, the UE uses the PTI to identify the UE requested bearer resource allocation procedure to which the dedicated bearer context activation is related (see subclause 10.3.3.5).

The UE shall use the received UL TFT to apply mapping of uplink service data flows (SDFs) to the radio bearer.

Upon receipt of the ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message, the MME shall enter the state BEARER CONTEXT ACTIVE.

10.3.3.2.4 Dedicated bearer context activation not accepted by the UE

Upon receipt of the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message, the UE may reject the request from the MME by sending an ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message. The message shall include the EPS bearer identity and a cause value indicating the reason for rejecting the dedicated EPS bearer context activation request.

If the PTI indicated in the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST does not match with any PTI used in the UE, the UE shall respond with an ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT with the EPS bearer identity associated with this PTI.

Upon receipt of the ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message in state BEARER CONTEXT ACTIVE PENDING, the MME shall enter the state BEARER CONTEXT INACTIVE and abort the dedicated EPS bearer context activation procedure.

Editor's note: The reject cause values and the actions to be taken are FFS.

10.3.3.3 Dedicated bearer context modification procedure

10.3.3.3.1 General

The purpose of the dedicated bearer context modification procedure is to modify an EPS bearer context with a specific QoS and TFT. The dedicated bearer context modification procedure is initiated by the network in order to either modify the QoS, the TFT, or both.

NOTE: QoS between EPS and UE is negotiated on layer 2 (S1AP and RRC) and does not affect the ESM entity. This implies that there is only a single NAS procedure for both the dedicated bearer context modification with or without QoS update.

10.3.3.3.2 Dedicated bearer context modification initiated by the network

The MME shall initiate the dedicated bearer context modification procedure by sending a SESSION MANAGEMENT CONFIGURATION REQUEST message to the UE and enter the state BEARER CONTEXT MODIFY PENDING. The message shall include the EPS bearer identity and will be piggybacked in the Radio Bearer Modify Request if the modification updates the QoS or in the Downlink NAS Transport if the modification does not update the QoS.

The SESSION MANAGEMENT CONFIGURATION REQUEST message shall include an EPS bearer identity that identifies the EPS bearer context to be modified and a TFT.

The SESSION MANAGEMENT CONFIGURATION REQUEST message shall include also a procedure transaction identity (PTI), if this procedure was initiated by a UE requested bearer resource allocation procedure (see subclause 10.3.3.5), or a UE requested bearer resource release procedure (see subclause 10.3.3.6).

10.3.3.3.3 Dedicated bearer context modification accepted by the UE

Upon receipt of the SESSION MANAGEMENT CONFIGURATION REQUEST message, the UE shall first check the received TFT before taking it into use and then send a SESSION MANAGEMENT CONFIGURATION ACCEPT message to the MME. The message will be piggybacked in the Radio Bearer Modify Response if the modification updates the QoS or in the Uplink NAS Transport if the modification does not update the QoS.

NOTE: When the UE accepts the dedicated bearer context modification, the radio bearer may be modified with a new QoS.

If the PTI is included in the SESSION MANAGEMENT CONFIGURATION REQUEST message, the UE uses the PTI to identify the UE requested bearer resource allocation procedure (see subclause 10.3.3.5), or the UE requested bearer resource release procedure (see subclause 10.3.3.6) to which the dedicated bearer context modification is related.

The UE shall use the received TFT to apply mapping of uplink service data flows to the radio bearer.

Upon receipt of the SESSION MANAGEMENT CONFIGURATION ACCEPT message, the MME shall enter the state BEARER CONTEXT ACTIVE.

10.3.3.3.4 Dedicated bearer context modification not accepted by the UE

Upon receipt of the SESSION MANAGEMENT CONFIGURATION REQUEST message, the UE may reject the request from the MME by sending a SESSION MANAGEMENT CONFIGURATION REJECT message to the MME. The message shall include the EPS bearer identity and a cause value indicating the reason for rejecting the dedicated bearer context modification request.

If the PTI indicated in the SESSION MANAGEMENT CONFIGURATION REQUEST does not match with any PTI used in the UE, the UE shall respond with a SESSION MANAGEMENT CONFIGURATION REJECT with the EPS bearer identity associated with this PTI.

Upon receipt of the SESSION MANAGEMENT CONFIGURATION REJECT message in state BEARER CONTEXT MODIFY PENDING, the MME shall enter the state BEARER CONTEXT ACTIVE and abort the dedicated bearer context modification procedure.

Editor's note: The reject cause values and the actions to be taken are FFS.

10.3.3.4 Dedicated bearer context deactivation procedure

10.3.3.4.1 General

The purpose of the dedicated bearer context deactivation procedure is to deactivate a dedicated EPS bearer context. The dedicated bearer context deactivation procedure is initiated by the network.

10.3.3.4.2 Dedicated bearer context deactivation initiated by the network

If a NAS signalling connection exists when the MME initiates the dedicated bearer context deactivation, the ESM entity in the MME shall request the S1AP layer to deactivate the EPS bearer towards the UE by sending a SESSION MANAGEMENT CONFIGURATION REQUEST that includes a Deletion Indicator and the EPS bearer identity. The procedure transaction identity (PTI) shall also be included if the deactivation was a result of a UE initiated bearer resource release. This SESSION MANAGEMENT CONFIGURATION REQUEST to deactivate an EPS bearer context will be piggybacked in the RRC Radio Bearer Release Request message.

Editor's note: The details of the Deletion Indicator are FFS.

If no NAS signalling connection exists when the MME initiates the dedicated bearer context deactivation, the ESM entity in the MME shall locally deactivate the EPS bearer context towards the UE without any peer-to-peer ESM signalling between the MME and the UE.

NOTE: The EPS bearer context state(s) can be synchronized between the UE and the MME at the next EMM-IDLE to EMM-CONNECTED transition, e.g. during a service request or tracking area updating procedure.

10.3.3.4.3 Dedicated bearer context deactivation accepted by the UE

Upon receipt of the SESSION MANAGEMENT CONFIGURATION REQUEST message that includes a Deletion Indicator, the UE shall delete the EPS bearer context identified by the EPS bearer identity. After deactivating the identified EPS bearer context, the UE shall respond to the MME with the SESSION MANAGEMENT CONFIGURATION ACCEPT including in that message the EPS bearer identity of the EPS bearer context that has been deactivated.

The SESSION MANAGEMENT CONFIGURATION ACCEPT message will be piggybacked in the RRC message Radio Bearer Release Response.

If the EPS bearer identity indicated in the SESSION MANAGEMENT CONFIGURATION REQUEST does not point to an existing EPS bearer context the UE shall respond with a SESSION MANAGEMENT CONFIGURATION ACCEPT with the EPS bearer identity set to the received EPS bearer identity.

Editor's note: It is FFS what action the UE shall take if the PTI indicated in the SESSION MANAGEMENT CONFIGURATION REQUEST does not match with any PTI in use.

10.3.3.5 UE requested bearer resource allocation procedure

10.3.3.5.1 General

The purpose of the UE requested bearer resource allocation procedure is for a UE to request the allocation of bearer resources for new service data flows. If accepted by the network, this procedure invokes either the dedicated EPS bearer context activation procedure or the dedicated EPS bearer context modification procedure.

10.3.3.5.2 UE requested bearer resource allocation procedure initiation

In order to request the allocation of bearer resources for new service data flows, the UE shall send a BEARER RESOURCE ALLOCATION REQUEST message to the MME. This message shall contain the requested QoS characteristics, linked bearer identity (LBI), procedure transaction identity (PTI) and the specific uplink and downlink traffic flow template (TFT).

Editor's note: The SDF QoS parameters to be sent are FFS.

10.3.3.5.3 UE requested bearer resource allocation procedure accepted by the network

Upon receipt of the BEARER RESOURCE ALLOCATION REQUEST message, the MME checks whether the EPS bearer requested by the UE can be established.

If the bearer resource allocation requested is accepted by the network, the MME shall initiate either the dedicated EPS bearer context activation procedure or one of the dedicated EPS bearer context modification procedures.

10.3.3.5.4 UE requested bearer resource allocation procedure not accepted by the network

If the bearer resource allocation requested cannot be accepted by the network, the MME shall send a BEARER RESOURCE ALLOCATION REJECT message to the UE. The message shall contain the PTI and a cause value indicating the reason for rejecting the UE requested bearer resource allocation.

Editor's note: The reject cause values and the actions to be taken are FFS.

10.3.3.6 UE requested bearer resource release procedure

10.3.3.6.1 General

The purpose of the UE requested bearer resource release procedure is for a UE to request the release of bearer resources related to specific service data flows. If accepted by the network, this procedure invokes either the dedicated bearer context deactivation procedure or one of the dedicated bearer context modification procedures.

10.3.3.6.2 UE requested bearer resource release procedure initiation

In order to request the release of bearer resources for specific service data flows, the UE shall send a BEARER RESOURCE RELEASE REQUEST message to the MME. This message shall include the linked bearer identity (LBI), the procedure transaction identity (PTI) and uplink and downlink TFT. The TFT parameter describes the service data flows the UE asks to release the resources for.

10.3.3.6.3 UE requested bearer resource release procedure accepted by the network

Upon receipt of the BEARER RESOURCE RELEASE REQUEST message, the MME checks whether the requested bearer resource can be released.

If the bearer resource release requested is accepted by the network, the MME shall initiate either the dedicated bearer context deactivation procedure or one of the dedicated bearer context modification procedures.

10.3.3.6.4 UE requested bearer resource release procedure not accepted by the network

If the bearer resource release requested cannot be accepted by the network, the MME shall send a BEARER RESOURCE RELEASE REJECT message to the UE. The message shall contain the PTI and a cause value indicating the reason for rejecting the UE requested bearer resource release.

Editor's note: The reject cause values and the actions to be taken are FFS.

10.3.3.7 UE requested PDN connectivity procedure

10.3.3.7.1 General

The purpose of the UE requested PDN connectivity procedure is for a UE to request the setup of a default EPS bearer to an additional PDN in order to allow the UE simultaneous access to multiple PDNs. If accepted by the network, this procedure initiates the establishment of an additional default EPS bearer context.

10.3.3.7.2 UE requested PDN connectivity procedure initiation

In order to request connectivity to an additional PDN, the UE shall send a PDN CONNECTIVITY REQUEST message to the MME. This message shall include the requested APN, the procedure transaction identity (PTI) and, if available, information about the IP address allocation as specified in subclause 5.1.3.

10.3.3.7.3 UE requested PDN connectivity procedure accepted by the network

Upon receipt of the PDN CONNECTIVITY REQUEST message, the MME checks whether connectivity with the requested PDN can be established.

If connectivity with the requested PDN is accepted by the network, the MME shall initiate the establishment of an additional default EPS bearer context by sending a PDN CONNECTIVITY ACCEPT message, which is piggybacked in the Radio Bearer Setup Request to the UE. The message shall contain the EPS bearer identity, the PTI and may contain the allocated PDN address information.

Editor's note: The procedure for the UE to be assigned a PDN address outside the PDN connectivity procedure (e.g. via an IETF-based mechanism) is FFS.

The MME may include a Protocol configuration options IE in the PDN CONNECTIVITY ACCEPT message if the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

10.3.3.7.4 UE requested PDN connectivity procedure not accepted by the network

If connectivity with the requested PDN cannot be accepted by the network, the MME shall send a PDN CONNECTIVITY REJECT message to the UE. The message shall contain the PTI and a cause value indicating the reason for rejecting the UE requested PDN connectivity.

Editor's note: The reject cause values and the actions to be taken are FFS.

10.3.3.8 UE requested PDN disconnection procedure

10.3.3.8.1 General

The purpose of the UE requested PDN disconnection procedure is for a UE to request disconnection from one PDN. With this procedure, all EPS bearer contexts established towards this PDN, including the default EPS bearer context, are released.

10.3.3.8.2 UE requested PDN disconnection procedure initiation

In order to request PDN disconnection to a PDN, the UE shall send a PDN DISCONNECT REQUEST message to the MME.

10.3.3.8.3 UE requested PDN disconnection procedure accepted by the network

Upon receipt of the PDN DISCONNECT REQUEST message, the MME shall initiate the bearer context deactivation procedure by sending the DEACTIVATE EPS BEARER CONTEXT REQUEST message including the linked EPS bearer identity, the ESM cause set to #36 "regular deactivation".

On reception of DEACTIVATE EPS BEARER CONTEXT ACCEPT message from the UE, the MME releases all the resources reserved for the PDN in the network.

Editor's note: whether the PDN disconnection procedure can be rejected by the network is FFS.

10.3.4 Reject causes for ESM procedures

Editor's note: this section contains temporary information on reject cause values to be used for ESM procedures, in order to help for further specification of the ESM procedures for the case they are rejected by either the UE or the network. This information was derived from the study of the SM cause values used for the PDP context activation and PDP context modification procedure as specified in 3GPP TS 24.008 [4], for the case these procedures are not accepted by either the UE or the network. Some other reject causes may be necessary, such as causes for abnormal cases e.g. PTI mismatch, but these are not defined in the current version of the present document.

10.3.4.1 Reject cause values for ESM procedures

The cause values listed below, defined in 3GPP TS 24.008 [4], are applicable in EPS:

#8 (Operator Determined Barring);

#26 (Insufficient resources);

#27 (Missing or unknown APN);

#29 (User authentication failed);

#30 (Activation rejected by Serving GW or PDN GW);

#31 (Activation rejected, unspecified);

#32 (Service option not supported);

#33 (Requested service option not subscribed);

#34 (Service option temporarily out of order);

#37 (SDF QoS not accepted);

#41 (Semantic error in the TFT operation);

#42 (Syntactical error in the TFT operation);

#43 (Unknown EPS bearer context);

#44 (Semantic error in packet filter(s));

#45 (Syntactical error in packet filter(s));

#46 (EPS bearer context without TFT already activated);

#95-111 (Protocol errors);

#112 (APN restriction value incompatible with active EPS bearer context).

Editor's note: it is FFS whether any new causes need to be created in EPS.

The cause values listed below, defined in 3GPP TS 24.008 [4], are not applicable to EPS:

#28 (Unknown PDP address or PDP type);

#35 (NSAPI already used);

#48 (Activation rejected, Bearer Control Mode violation).

The cause value listed below, defined in 3GPP TS 24.008 [4], may be considered applicable to subsequent release(s) of EPS:

#40 (Feature not supported).

10.3.4.2 Applicability of reject causes to ESM procedures

The table 10.3.4.2.1 below indicates which reject cause values can be used for each ESM procedure.

Table 10.3.4.2.1: proposed reject causes for ESM procedures

	UE requested PDN connectivity	Default EPS bearer context activation	UE requested bearer resource allocation	Dedicated EPS bearer context activation	EPS bearer context modification
#8 - Operator Determined Barring	X				
#26 - Insufficient resources	X	X	X	X	X
#27 - Missing or unknown APN	X				
#29 - User authentication failed	X				
#30 - Activation rejected by Serving GW or PDN GW	X		X		
#31 - Activation rejected, unspecified	X	X	X	X	
#32 - Service option not supported	X		X		
#33 - Requested service option not subscribed	X		X		
#34 - Service option temporarily out of order	X		X		
#37 - SDF QoS not accepted			X		
#41 - Semantic error in the TFT operation		X	X	X	X
#42 - Syntactical error in the TFT operation		X	X	X	X
#43 - Unknown EPS bearer context			X	X	
#44 - Semantic errors in packet filter(s)		X	X	X	X
#45 - Syntactical errors in packet filter(s)		X	X	X	X
#46 - EPS bearer context without TFT already activated				X	X
#95-111 - Protocol errors	X	X	X	X	X
#112 – APN restriction value incompatible with active EPS bearer context	X				

10.3.5 EPS bearer context information

Each established EPS bearer will be described by a set of parameters in both the UE and the MME. This grouping of parameters is referred to as an EPS bearer context.

A PDN context can be defined as a grouping of one default EPS bearer context and zero, one or more dedicated EPS bearer contexts. A UE may have simultaneous connectivity with more than one PDN and thus more than one PDN context, see figure 10.3.5.1.

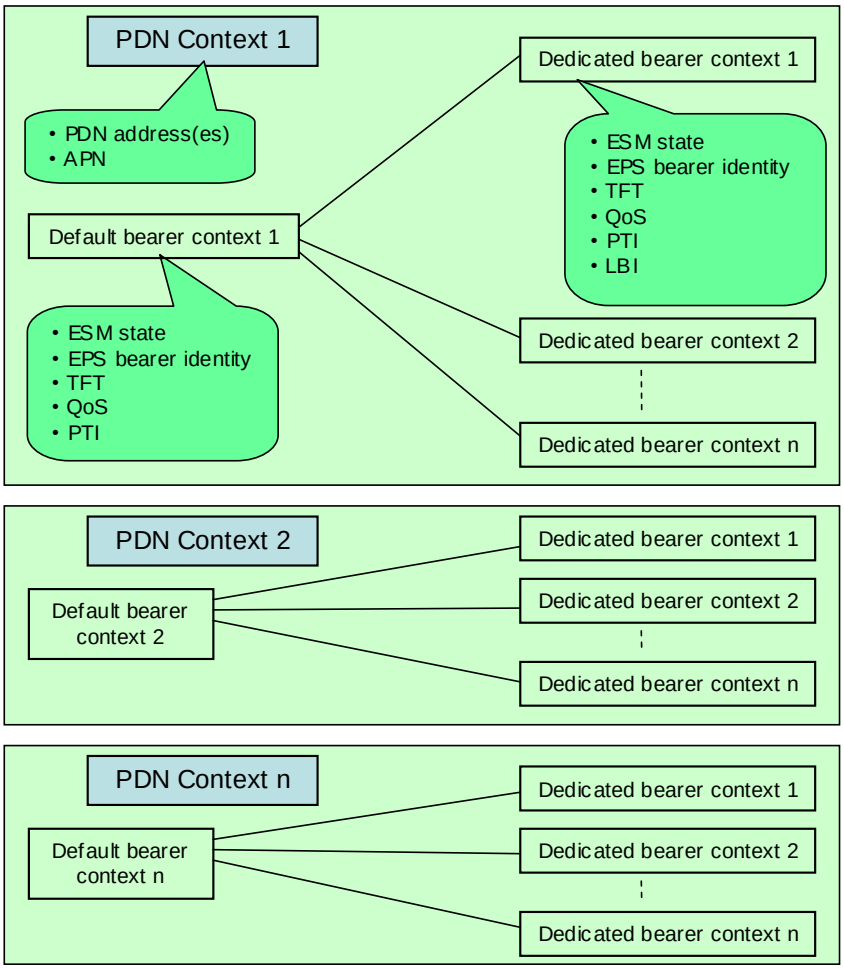


Figure 10.3.5.1: Relation between the PDN context and the default/dedicated EPS bearer contexts

The structure and content as well as the relationship between the PDN context and the default and dedicated EPS bearer contexts that are stored in the UE and MME are shown in the following tables.

NOTE: The tables describing the different types of contexts is not meant to define a specific data structure that has to be implemented by the UE and the MME in exactly that form, but to create a representation of the data that can be used in the further analysis of the EPS bearer concept.

Table 10.3.5.1: PDN context

Field	Description
PDN address(es)	One IPv4 address and/or one IPv6 prefix assigned to the UE
APN	Access point name

Editor's note: Whether the IPv4/IPv6 PDN address(es) need to be part of the PDN context in the MME is FFS.

Table 10.3.5.2: Default EPS bearer context

Field	Description
ESM state	Session management state
EPS bearer identity	EPS bearer identity
TFT	Traffic flow template
QoS	Quality of service
PTI	Procedure transaction identity (temporary parameter)

Table 10.3.5.3: Dedicated EPS bearer context

Field	Description
ESM state	Session management state
EPS bearer identity	EPS bearer identity
TFT	Traffic flow template
QoS	Quality of service
PTI	Procedure transaction identity (temporary parameter)
LBI	Linked bearer identity

Editor's note: The content in the tables above should not be seen as being complete. Other IEs needed to represent these contexts are FFS.

10.4 NAS signalling transport (E-UTRAN only)

In GPRS, procedures related to GMM, SM and RAB setup are performed independently of each other.

In EPS, in order to reduce the time and number of signalling necessary, there have been enhancements to these signalling flows, e.g. there are impacts on the attach and dedicated EPS bearer establishment procedures compared to GPRS.

For the attach procedure, at least the following messages should be considered for piggybacked transport in the radio bearer messages:

- Attach Accept (GUTI, etc.);
- Session Management Configuration (e.g. PDN Address).

For the dedicated EPS bearer establishment procedure, at least the following message should be considered for piggybacked transport in the radio bearer messages:

- Session Management Configuration (e.g. UL filter).

Editor's note: The lists of procedures and messages for each procedure to be considered for piggybacked transport are not intended to be complete.

10.5 MBMS

Editor's note: This clause will contain a description of MBMS aspects relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

10.6 SDoUE

Editor's note: This clause will contain a description of the aspects of "Selective disabling of UE capabilities (SDoUE)" relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

10.7 Network sharing

Editor's note: This clause will contain a description of network sharing aspects relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

10.8 Charging

Editor's note: This clause will contain a description of charging aspects relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

10.9 Trace

Editor's note: This clause will contain a description of trace aspects relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

10.10 Impact on the IM CN subsystem

10.10.1 Impact on 3GPP TS 24.229

New IP-CAN technologies are created, currently identified as EPS, and as new access technologies using mobile IP, for each of which the following will need to be studied and specified:

1) creation of a new annex within 3GPP TS 24.229 [6] for each new access technology, suitably referenced from subclause 3A and subclause 9.2.2 of 3GPP TS 24.229 [6]. This annex will detail the following (using the same layout as other access technology specific annexes):

   - specific procedures of the access technology signalling relating to access to the IM CN subsystem including:

     a) application of IP flows to signalling and media of the IM CN subsystem, and the creation of those required flows;

NOTE: If priority mechanisms are required for signalling flows, then these mechanisms will have to be defined elsewhere.

     b) mechanisms for obtaining the P-CSCF address;

     c) any constraints on modification of IP flows;

     d) any requirements for reestablishment of signalling IP flows;

     e) any requirements for session management procedures;

     f) any requirements for mobility management procedures;

     g) any requirements for cell selection and lack of coverage;

     h) requirements on IP flows for media, including activation, modification by the UE or the network;

     i) any special requirements for forked responses;

   - special provisions for the support of emergency calls in the IM CN subsystem, in particular in regard to allowing the UE to discover whether it is attached to the home network;

   - access technology specific usage of SIP including:

     a) whether the UE includes the P-Access-Network-Info header in requests and responses or not;

     b) how the P-CSCF detects that requests are destined for a PSAP in this specific access technology;

2) Assignment of new values in the P-Access-Network-Info header field;

3) Assignment of appropriate extensions to the access-network-charging-info parameter in the P-Charging-Vector header field;

4) Whether SigComp applies to this access technology or not;

5) Whether SIP signalling timer values are modified for this access technology or not.

10.11 Service continuity between E-UTRAN and the CS domain

Editor's note: This subclause will contain a description of the NAS aspects of service continuity between E-UTRAN and the CS domain ("single radio VCC") relevant for CT1.

10.12 Home cell deployments

10.12.1 General

10.12.1.1 Introduction

A home cell deployment is a single eNodeB used in a home or a small group of cells e.g. in a campus deployment. Typically, access to home cells is restricted to particular subscribers.

10.12.1.2 Working assumptions for all home cell deployment options

- Tracking area update reject messages alone cannot be used to control access to home cells.
- A UE must be prevented from attempting to access a home cell if the UE is not a member of the home cell.
- It is not practical to use a forbidden list to control access to home cells because of the need to allow for a very large number of home cells within a single network.
- A home cell must identify itself as a home cell by broadcasting a one bit flag.
- UE access to home cells will be controlled by a white list of home cell identifiers stored in the UE.

Editor's note: Subclauses of 10.12 from 10.12.2 onwards contain solution options for home cell deployments, with one self-contained option per subclause.

10.12.2 Option A

10.12.2.1 Introduction

A closed subscriber group (CSG) area is a tracking area that consists of a cell or group of cells to which access is restricted to a defined group of users. Idle and Active mobility procedures are optimized to avoid UE battery inefficiencies when a UE is not allowed to use a cell.

NOTE: A CSG is not limited to the deployment of a single cell in a home, it can also be a campus deployment of multiple cells.

10.12.2.2 Definitions related to CSGs

Allowed CSGs List: A list stored in the UE of TAIs that belong to CSG cells. A UE is able to access only those CSG cells that have a TAI in this list.

Closed Subscriber Group (CSG) area: A collection of one or more cells that have a common TAI and indicate that they are closed, i.e. CSG cells.

CSG area identity: The identifier of a Closed Subscriber Group. For Option A, the CSG area identity is the TAI of the CSG cell(s).

Current Registration Area: an area represented by the cells identified by the Mobility List stored in the UE.

Mobility List: A list stored in the UE of TAIs that belong to tracking areas and CSG cells that the UE can access without performing a tracking area updating procedure.

10.12.2.3 Abbreviations related to CSGs

CSG Closed Subscriber Group

10.12.2.4 Impact of CSGs on registration areas in the EPS

Within the EPS, a registration area is defined as a list of tracking areas and each of these tracking areas consists of one or more cells that cover a geographical area. A single cell can only belong to a single tracking area or a single Closed Subscriber Group (CSG). Tracking areas cannot overlap each other. CSGs cannot overlap each other. Within the EPS, the concept of "registration to multiple tracking areas" applies:

- A TAI or closed subscriber group identifier is broadcast in a cell, and in both cases is identified by a TAC and a PLMN identifier. In case of a shared network, a single TAC and multiple PLMN identifiers are broadcast.

- An indication is broadcast on each cell indicating whether the TAI is an identity of a tracking area or of a closed subscriber group.

Editor's note: The structure and coding of the TAI is FFS.

- In order to reduce the tracking area update signalling within the EPS, the MME can assign several tracking areas and CSGs to the UE.

- The EPC may indicate to the UE the identities of the CSGs to which it is subscribed. The UE shall treat all CSG cells where the UE does not belong to the associated CSG as though they are NOT a suitable cell as defined in 3GPP TS 23.122 [22].

Editor's note: To help with battery efficiency, the decision on what CSG TAs to provide to the UE could be based on the proximity of the UE to a subscribed CSG. Whether the UE location influences the provided CSG TAs is FFS.

- The working assumption is that the allowed CSG list shall be stored in the UICC and, as an implementation option, can be stored additionally in the ME. If stored in the ME, when the ME detects that the UICC has been changed, the CSG list will be deleted from the ME.

Editor's note: for the decision where to store the allowed CSG list the following points should be taken into account:

  - how quickly CSG cells must be found at power on;

  - whether it is required to maintain the list when moving the UICC between terminals;

  - whether EPS requires other modification of the UICC; and

  - the number of entries there will be in a white list.

- At switch-on the UE searches for a suitable cell in the manner described in 23.122 [22] and 25.304 [29]. This could result in the UE getting onto a TA of CSG cells correspond to the CSG list stored in the UICC or in the ME. Otherwise by cell reselection procedures, the UE can be manoeuvred to get onto TAs of CSG cells of its CSG list.

Editor's note: The manner by which the UE can be persuaded to perform cell reselection or be manoeuvred onto CSG TAs when and if CSG TAs are available is a cell selection/reselection is FFS, but this matter is the responsibility of RAN2 and not within the remit of CT1.

- The MME may as part of Attach and/or TAU procedures provide the UE with a TAI (or TAIs) identifying a CSG or non-CSG tracking area. If the TAI is a CSG area identity, the UE shall add this identity to the Allowed CSGs List.

- The UE considers itself registered to a list of tracking areas stored in its Mobility List and does not need to trigger tracking area update other than periodic tracking area update as long as it stays in the Current Registration Area i.e. a cell that has one of the TAIs in the Mobility List stored in the UE.

- The MME shall indicate to the UE whether or not a CSG to which the UE is subscribed belongs to the Current Registration Area assigned to the UE, and if it does the UE shall add this identity to its Mobility List, and the UE shall not trigger tracking area update when entering the CSG.

Editor's note: the maximum number of tracking areas and CSGs which can be allocated per UE needs to be defined.

- The MME shall derive the CSG TAI from the Cell Global ID of the serving cell included in the message containing the service request received from the eNodeB (e.g. S1AP Initial UE message). The MME shall check if the CSG TAI belongs to the ones subscribed by the UE. If the CSG TAI doesn't match with the subscribed ones, then the MME shall reject the network access initiated by the UE.

Editor's note: For this purpose, the definition of a new reject cause for the service request procedure should be investigated.

- The NAS may use the CSG TAI, extracted from the message received by the eNodeB carrying the service request message (e.g. S1AP Initial UE message), for charging purposes.

Editor's note: the maximum number of tracking areas and CSGs which can be allocated per UE needs to be defined.

- The UE will consider its Mobility List as valid, until it receives a new list from the network (e.g. in the next normal tracking area update or periodic tracking area update or it is commanded by the network to delete the Mobility List). If the tracking area update request is accepted, the MME shall provide at least one entry in the Mobility List.

- The UE will consider its Allowed CSGs List as valid until it receives a new list from the network (e.g. in the next normal tracking area update or periodic tracking area update) or it is commanded by the network to delete all TACs in the Allowed CSGs List.

Editor's note: Whether the UE will be provide the CSG TAI list solely by EMM procedures or by some other means is FFS.

- The MME allocates only one temporary identity (GUTI) to the UE, even if the UE has more than one TAI in its Mobility List.

- When necessary, the MME shall initiate paging of the UE in all cells of all tracking areas and all CSG area identities in the Current Registration Area. Cells having the same CSG area identity must be part of the same MME pool.

10.12.2.5 Option A open issues for tracking area update procedure

1) First time access to a CSG may require a forced tracking area update. The UE and network impact of this needs to be studied and reflected in the specifications, e.g. UE MMI dependencies, and limiting the frequency of forced updates.

2) Forbidden lists are cleared at power down. CT1 should decide whether the Allowed CSG List is to be cleared at power down. One possibility is to keep only the CSGs that are also in the Mobility List.

3) CT1 should decide whether the same solution applies to single-cell home and multiple-cell campus deployments.

4) It must be possible for subscribers to control whether they are added to a closed subscriber group.

10.12.2.6 Option A open issues for service request procedure

1) The signalling sent by the eNodeB to the MME tunnelling the service request procedure shall contain the Cell Global ID of the cell where the UE is trying to start a service request procedure.

2) The MME shall be able to check the CSG TAI received with the service request message with the subscribed CSG TAIs.

3) In case the access list is changed (e.g. due to subscription change), the procedure needed to align the access lists contained in the MME and in the UE is FFS.

10.12.3 Option B

10.12.3.1 Introduction

A Closed Subscriber Group (CSG) consists of a cell or group of cells to which access is restricted to a defined group of users. Idle and Active mobility procedures are optimized to avoid UE battery inefficiencies when a UE is not allowed to use a cell.

NOTE: A CSG is not limited to the deployment of a single cell in a home; it can also be, for example, a campus or office building area deployment of multiple cells.

10.12.3.2 Definitions related to CSGs

Closed Subscriber Group (CSG) area: A collection of one or more cells that have a common TAI. A tracking area either contains only CSG cells or only macro cells. Several CSGs can use the same TAI.

CSG cell area identity: The identity of a CSG cell which consists of a TAI plus cell identity code.

Allowed CSGs list: A list stored in the UE of CSG cell area identity that belong to CSG cells. A UE is able to access only those CSG cells which have CSG cell area identities in this list.

10.12.3.3 Abbreviations related to CSGs

CSG Closed Subscriber Group

10.12.3.4 Impact of CSGs on registration areas in the EPS

Within the EPS, a registration area is defined as a set of tracking areas and each of these tracking areas consists of one or more cells that cover a geographical area. A single cell can only belong to a single tracking area or a single Closed Subscriber Group (CSG). Tracking areas cannot overlap each other. CSG areas cannot overlap each other. Within the EPS, the concept of "registration to multiple tracking areas" applies:

- A TAI and cell identity is broadcast in a cell. The TAI is identified by a PLMN identifier and a TAC. The CSG cell area identity consists of a TAI plus a cell identity code. In case of a shared network, a single TAC and cell identity and multiple PLMN identifiers are broadcast.
- An indication is broadcast on each cell indicating whether the cell belongs to a closed subscriber group or not.
- In order to reduce the tracking area update signalling within the EPS, the MME can assign several tracking areas to the UE by means of the TAI list (see subclause 5.1.1.1).
- The UE considers itself registered to a list of tracking areas stored and does not need to trigger tracking area update other than periodic tracking area update as long as it stays in the current registration area, i.e. a cell that has one of the TAIs in the TAI list stored in the UE (see subclause 5.1.1.1).
- The MME may indicate to the UE the identities of the CSGs to which it is subscribed. The UE shall treat all CSG cells where the UE does not belong to the associated CSG as though they are NOT a suitable cell as defined in 3GPP TS 23.122 [22]. However, the UE is anyhow allowed to camp on restricted CSG cell (limited service state) so that emergency calls can be made as defined in 3GPP TS 23.122 [22].
- The MME may provide the UE with a list of allowed CSG cells (Allowed CSGs list) in, for example, a similar way as today's Equivalent PLMN list or the TAI list (e.g., acceptance message of the attach/tracking area updating procedures).

Editor's note: the maximum number of CSG cells which can be allocated per UE needs to be defined.

- The UE will store the Allowed CSGs list either in the ME or in the USIM and it will consider its Allowed CSGs list as valid until it receives a new list in the next EMM procedure or it is commanded by the network to delete all entries in the Allowed CSGs list.
- A new NAS cause value, instead of forbidden TAI, may be used when a UE attempts to access a restricted cell. An eNodeB, which belongs to a CSG area, sends the CSG cell area identity, i.e., TAI plus (parts of) cell identity, to the MME whenever authorization needs to be checked in the MME. This may also be used for charging purposes.
- On receipt of a new cause value the UE removes CSG cell area identity (outdated information) from the stored Allowed GSGs list. This prevents non-allowed UEs from accessing cells indicated as restricted.
- Other alternative than a new NAS for case of erroneous access attempt to CSG cells may be the use of the service request procedure that allows to check the CSG cell area identity towards the user subscription. In case, the CSG cell area identity and the user subscription do not match, the MME rejects the service request procedure.
- When necessary, the MME shall initiate paging of the UE in all cells of all tracking areas and all CSG areas in the current registration area. Cells that belong to a CSG area must be part of the same MME pool.

10.12.3.5 Option B open issues for tracking area update procedure

1) It should be decided whether the Allowed CSG List is to be cleared at power down, is stored in the ME or USIM and in which way would be distributed to the UE.

Editor's note: The working assumption is that the allowed CSGs list shall be stored in the USIM and, as an implementation option, can be stored additionally in the ME. If the allowed CSGs list is stored and the ME detects that the USIM has been changed, the allowed CSGs list will be deleted from the ME.

2) It should be decided whether a new cause value or the service request procedure are used for preventing erroneous access attempts to CSG cells.

3) It must be possible for subscribers to control whether they are added to a CSG.

10.12.4 Option C

10.12.4.1 Introduction

A closed subscriber group (CSG) area consists of a physical area or areas containing a cell or group of cells to which access is restricted to a defined group of users. Idle and Active mobility procedures are optimized to avoid UE battery inefficiencies when a UE is not allowed to use a cell.

Generally, there is no one to one relationship between CSG id and TAI in the PLMN (e.g. the same TAI can be associated to cells belonging to different CSG ids and cells belonging to the same CSG id can be associated to different TAIs). The CSG area can be uniquely identified by the CSG id together with the associated TAIs.

NOTE: A CSG is not limited to the deployment of a single cell in a home; it can also be, for example, a campus or office building area deployment of multiple cells.

10.12.4.2 Definitions related to CSGs

Allowed CSG list: A list of CSG ids stored in the UE. A UE is able to access only those CSG cells that have a CSG id in this list.

Closed Subscriber Group (CSG) area: A collection of one or more cells that have a common CSG id.

CSG Mobility List: A list of TAIs of CSG cells provided to the UE where the UE can access those TAs without performing any EMM procedure (e.g. tracking area updating procedure). The TAI(s) in this CSG Mobility List is (are) part of the TAI list.

NOTE: The CSG Mobility List is not a physically separate list but is a logical list whose elements are taken from the TAI list. The CSG Mobility List is introduced to allow the analysis of the UE behaviour, but it is not intended to separate the TAIs belonging to the CSG Mobility List from other TAIs belonging to the TAI list in the EMM signalling messages, or to specify a different handling for these two lists of TAIs.

Current Registration Area: an area represented by the cells identified by the TAI list stored in the UE. The area represented by the cells identified by the CSG Mobility List is part of this area.

10.12.4.3 Abbreviations related to CSGs

CSG Closed Subscriber Group

10.12.4.4 Impact of CSGs on registration areas in the EPS

Within the EPS, a registration area is defined as a list of tracking areas and a list of Closed Subscriber Group (CSG) cells that cover a geographical area. A single cell can only belong to a single tracking area and can be associated to a single Closed Subscriber Group (CSG) area. Tracking areas cannot overlap each other. Within the EPS, the concept of "registration to multiple tracking areas" applies:

- A CSG id is broadcast in a cell. In case of a shared network, a single CSG id and multiple PLMN identifiers are broadcast.

Editor's note: The relationship between the CSG id and the Cell Global Id is FFS.

- An indication is broadcast on each cell indicating whether the cell belongs to a closed subscriber group or not ("one bit indicator" defined in RAN2).
- In order to reduce the tracking area update signalling within the EPS, the MME can assign several tracking areas to the UE.
- The UE shall treat all CSG cells where the UE does not belong to the associated CSG as though they are NOT a suitable cell as defined in 3GPP TS 23.122 [22].
- The UE is allowed to camp on a restricted CSG cell (limited service state) so that emergency calls can be made as defined in 3GPP TS 23.122 [22].

Editor's note: The technical solution for the support of the emergency call is FFS.

- The UE considers itself registered to a list of TAs stored in its TAI List and does not need to trigger tracking area update other than periodic tracking area update as long as it stays in a cell that has one of the TAs in the TAI List stored in the UE.
- The MME may as part of Attach and/or TAU and/or GUTI reallocation procedures provide the UE with one or more than one TAI related with the CSG id and additionally with TAIs not related to any CSG id. The UE shall update with these TAIs the content of the TAI List.
- The UE will store the Allowed CSG list either in the ME or in the USIM and it will consider its Allowed CSGs list as valid until it receives a new list from the network or it is commanded by the network to update one or more entries in the Allowed CSG list.
- In order to update the Allowed CSG List the following mechanisms can be used:
  - Manual update: based on the user interaction. The user can trigger at any time the UE to search for the CSG cell. The UE will update the Allowed CSG List according to the response to the Attach and TAU procedures. If the permissions for a UE to access to a HeNB are removed, then the CSG Id will be deleted from the Allowed CSG List contained in the UE at the receiption of the subsequent Service Reject sent by the network to avoid the UE access to the CSG cell; or
  - Application level update: based on the usage of OMA DM procedures. The OMA DM procedures defined in OMA-ERELD-DM-V1_2 [52] can be used to add/remove one or more CSG Id in the Allowed CSG List.

Editor's note: Other Application level mechanisms to update the Allowed CSG List are not excluded.

Editor's note: In case of OMA DM usage, the Allowed CSG List is stored in the ME. The procedures needed to exchange the Allowed CSG List between USIM and ME shall be discussed with CT6.

Editor's note: The procedures needed to remove a CSG Id from the Allowed CSG List, if the membership in the CSG is withdrawn while the UE is in EMM-connected mode, are FFS.

Editor's note: Both methods described above for updating the Allowed CSG List can be considered applicable to the cases of HNB and HeNB.

- At switch-on the UE searches for a suitable cell in the manner described in 23.122 [22] and 25.304 [29]. This can result in the UE getting onto a CSG cell belonging to the CSG list stored in the USIM or in the ME. Otherwise by cell reselection procedures, the UE can be manoeuvred to get onto CSG cells belonging to its CSG list.
- The NAS may use the CSG id and TAI, transported in the message received from the eNodeB carrying the attach request, tracking area update request or service request message (e.g. S1AP Initial UE message), for charging purposes.
- The MME shall be provided with the CSG id of the serving cell in the message containing the attach request, tracking area update request or service request received from the Home eNodeB (e.g. S1AP Initial UE message). The MME shall check if the CSG id belongs to the ones contained in the Allowed CSG List stored at MME. If the CSG id doesn't match with the subscribed ones, then the MME shall reject the network access initiated by the UE. A new reject cause is needed for Attach Reject, Service Reject and Tracking Area Update Reject messages if the MME decides the user is not allowed to access the selected CSG cell according to the white list.

Editor's note: The reaction of the MME when the UE initiates a detach procedure in a CSG cell the user is not allowed to access is FFS.

- The UE will consider its TAI List and therefore also its CSG Mobility List as valid, until it receives a new TAI list from the network (e.g. in the next normal tracking area update or periodic tracking area update or GUTI reallocation procedure).
- The MME allocates only one temporary identity (GUTI) to the UE, even if the UE has more than one TAI in its TAI List.
- When necessary, the MME shall initiate paging of the UE in all cells of all tracking areas contained in the TAI list. Cells having the same TAI must be part of the same MME pool.
- Paging optimization mechanisms should be adopted in order to avoid huge amounts of paging messages in the cells served by HeNBs. Possible approaches are as follows:
  - The MME sends the paging request message only to those HeNBs which have the TAI in the UE's registered TAI list and the CSG ID in the UE's CSG white list; or
  - the MME provides both the TAI and the UE's CSG white list to those HeNBs which have the TAI in the UE's registered TAI list, and each of the HeNBs decides whether its cell belongs to the CSG area and the paging is sent via the radio interface.

Editor's note: if the HeNB GW is adopted as an entity of CSG architecture, other approaches of paging optimization may be possible. This is FFS.

Editor's note: if multiple CSG IDs are supported by a HeNB is FFS.

10.12.4.5 Principles of access control for CSG cells

The CSG subscription information is permanently stored in HSS, and retrieved by the MME for access control during attach, detach, service request and tracking area updating procedures.

A new reject cause value is used to indicate that the UE is not allowed in the CSG for attach, service request and tracking area updating procedures. The MME includes the reject cause in the NAS signalling response.

Editor's note: the same principle is applied to the access control of 3G CSG cells. In this case, MSC/VLR and SGSN play the role of MME described in this section.

10.13 Access Control

Editor's note: This clause will contain a description of access control aspects relevant for CT1. None of the text within this section shall be transferred directly to any specification unless explicitly stated.

10.13.1 General

Due to problems in certain areas, network operators may decide to restrict access from some UEs (e.g., in case of congestion). In the case that a network operator decides to restrict access they may as an option allow restricted UEs to respond to paging messages and/or to perform location registrations.

10.13.2 Access Control

At subscription one or more access control classes are allocated to the subscriber and stored in the USIM. The information providing all authorized classes is broadcast as system information (together with a bit indicating whether emergency calls may be made). This information is modified dynamically and therefore the UE has to check the system information before each attempt to access. (See 3GPP TS 36.331 [16] and 3GPP TS 36.304 [29].)

When the UE sends an initial access message, the UE may access the network if Access Class stored in the USIM does not match the broadcasted SIB(Access Class Barred List). The UE may not access to the network if Access Class stored in the USIM matches the broadcasted SIB(Access Class Barred List).

10.13.3 Paging Permission with Access Control (PPAC)

10.14 Circuit Switched Fallback

Editor's note: This clause will contain a description of CS Fallback aspects relevant for CT1, based on stage 2 described in 3GPP TS 23.272 [49].

10.14.1 SGs reference point

The SGs reference point is the reference point between the MME and MSC server. The SGs reference point is used for the mobility management and paging procedures between the EPS and the CS domain, and these procedures are based on the Gs interface procedures as described in 3GPP TS 29.018 [50]. The mobile originating and mobile terminated SMS can also be delivered via the SGs reference point.

10.14.1.1 SGs implementation alternatives

Editor's note: This clause will contain a description of different alternatives for SGs implementation and recommendations.

10.14.1.1.1 Alternative 1: enhanced Gs interface

With this alternative, new parameters would be added to Gs interface layer 3 if required or new messages would be added to Gs interface layer 3. Protocol used on SGs would be an enhancement of BSSAP+, called "enhanced BSSAP+" below. In order to have MME as a pure IP node, enhanced BSSAP+ could be transported over IP-based SS7, as indicated in figure 10.14.1.1.1.1.

Fig. 10.14.1.1.1.1: Protocol architecture for alternative 1

10.14.1.1.2 Alternative 2: new SGs interface to be introduced using DIAMETER protocol

With this alternative, in the same way as for MME-HSS interface, DIAMETER could be adapted to the SGs interface. Since 3GPP related parameters, e.g. IMSI, are already defined in DIAMETER, the new SGs interface could reuse them.

Fig. 10.14.1.1.2.1: Protocol architecture for alternative 2

It should be noted that alternative 2 has impact on the MSC server, while stage 2 clearly indicates that the solution for CS fallback "should have no or minimum impacts on CS domain entities and UE as well as the user experience on CS Domain services." However, from MME point of view, this solution avoids the need to implement SS7 stack in the MME.

In addition to alternative 2, an enhanced BSSAP+ may run directly over SCTP and IP. This is alternative 2' as described in figure 10.14.1.1.2.2.

Fig. 10.14.1.1.2.2: Protocol architecture for alternative 2'

10.14.1.1.3 Alternative 3: introduction of an Interworking Function

With this alternative, a new IWF (Interworking Function) node would be introduced between the MME and the MSC server.

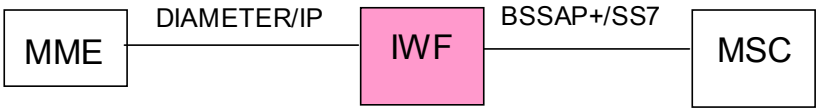


Fig. 10.14.1.1.3.1: Interworking Function

Several implementations are possible. If an operator wishes to deploy a pure IP based network, then the IWF could be collocated with MSC. On the other hand, if an operator wishes to avoid any impacts to existing MSCs, the IWF could be added to their network as a standalone node or could be collocated with MME. The following figures 10.14.1.1.3.2 and 10.14.1.1.3.3 illustrate possible implementations.

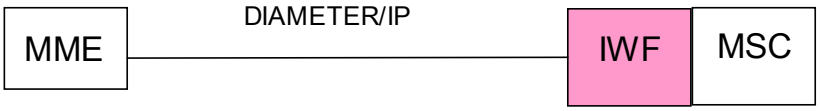


Fig. 10.14.1.1.3.2: Interworking Function implemented in the MSC

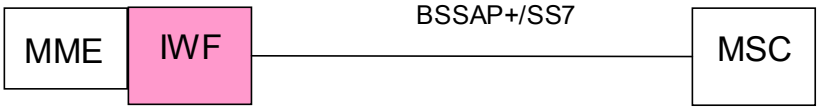


Fig. 10.14.1.1.3.3: Interworking Function implemented in the MME

Towards the MSC the IWF behaves like an SGSN so that there is no impact to the MSC to support the SGs interface.

IWF functionalities would include:

- Message Routing (e.g. translation SGSN Number → MME IP address);
- Connection Management (i.e. SCCP Class0 connectionless service <-> SCTP association);
- Gs Emulation (i.e. Parameter/Message conversion between BSSAP+ and SGs application).

The protocol architecture is described in figure 10.14.1.1.3.4.

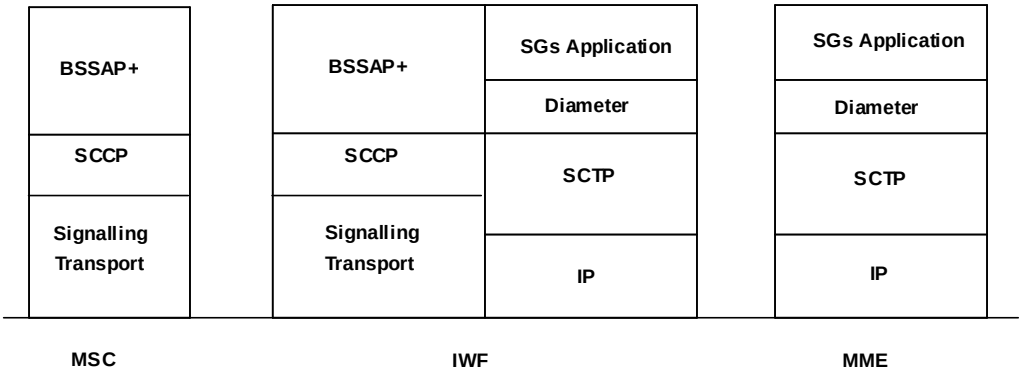
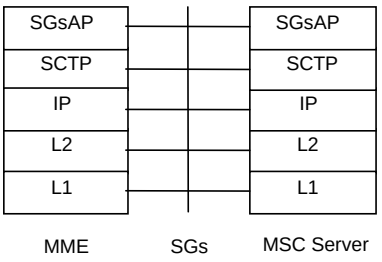


Fig. 10.14.1.1.3.4: Protocol architecture

10.14.1.1.4 Conclusion

The protocol stack agreed by SA2 for the SGs interface is shown in figure 10.14.1.1.4.1.



NOTE: **SGsAP:** This protocol is used to connect an MME to an MSC Server based on the BSSAP+.
Stream Control Transmission Protocol (SCTP): This protocol transfers signalling messages.

Fig. 10.14.1.1.4.1: Protocol architecture for the MME-MSC server interface

10.14.1.2 Specification work for SGs

SGs interface will be documented in a new TS which will cover the following aspects:

- description of procedures used on SGs. For SGs procedures which have an equivalent Gs procedure, the description of the Gs procedure will be reused as much as possible;
- definition of messages and IEs for SGsAP protocol;
- use of SCTP as the transport protocol for SGsAP messages.

Editor's note: for the use of SCTP, CT1 needs to investigate how much can be reused from other work in CT4.

10.14.2 Mobile originating call handling

The following impacts have been identified for the UE:

- Need for NAS to request a change of radio access technology due to a request for a CS call. Registration status for CS domain needs to be taken into account for this trigger;
- Possible changes to the NAS state machine: NAS has to wait for GERAN or UTRAN RAT selection to proceed with the mobile originating call establishment;
- Need for NAS actions upon failure to move the UE to GERAN or UTRAN. Such failures will be seen as a failure to establish the CS call;
- Upon reception from AS of an indication that GERAN or UTRAN has been selected, NAS needs to proceed with NAS procedures in order to establish CS call;
- Possible impacts on MM state machine to trigger MM connection establishment once location update procedure is successful.
- Impacts on EMM/ESM handling to resume the suspended EPS bearer contexts.

The following impacts have been identified for the MME:

- Possible impacts on NAS to trigger AS to indicate eNodeB to move UE to GERAN/UTRAN upon reception of service request with CS fallback indicator.
- Impacts on EMM/ESM handling upon reception of the suspend/resume indication (S1 UE Context Release Request with specific cause).

10.14.3 Mobile terminating call handling

The following impacts have been identified for the UE:

- NAS to handle a CS paging indication from AS (in EMM-IDLE mode) and NAS (in EMM-CONNECTED mode);
- Need for NAS actions upon failure to move the UE to GERAN or UTRAN. Such failures will be seen as a failure to establish the CS call;
- Upon reception from AS of an indication that GERAN or UTRAN has been selected, NAS needs to proceed with NAS procedures in order to establish CS call;
- Paging response in A/Gb mode may need to be specified in NAS or some coordination is required between NAS and AS for the paging response to be sent after the completion of the location update procedure;
- Some updates required to procedure for paging response in Iu mode;
- Impacts on the NAS handling for decision based on the CLI (Caller Line Identification).

Editor's note: it needs to be aligned with SA2 whether the CLI is revised and/or removed in the future.

- Impacts on EMM/ESM handling to resume the suspended EPS bearer contexts.

The following impacts have been identified for the MME:

- Possible impacts on NAS to trigger AS to indicate eNodeB to move UE to GERAN/UTRAN upon reception of service request with CS fallback indicator.
- Impacts on EMM/ESM handling upon reception of the suspend/resume indication (S1 UE Context Release Request with specific cause).

11 Decisions on the organization of normative specifications

Editor's note: This clause will contain the agreed conclusions about the creation of new Technical Specifications and the respective scope.

11.1 Specification work for 3GPP access

CT1 has reached the following agreements with regard to the specification work for 3GPP access:

1. A new TS is started for the specification work of EMM and ESM.
2. New protocol discriminators are allocated for the EMM and ESM protocols.
3. Both EMM and ESM re-use the 3GPP TS 24.007 [36] common protocol element structure. For ESM, necessary enhancements of the transaction model due to the introduction of the procedure transaction identifier will be investigated.
4. Both EMM and ESM re-use the 3GPP TS 24.007 [36] and the 3GPP TS 24.008 [4] clause 8 handling of erroneous and unforeseen data.
5. EMM and ESM re-use some of the information element definitions given by 3GPP TS 24.007 [36] and 3GPP TS 24.008 [4].

Some of the reasons for the above agreements are the fact that according to the network architecture, the terminating entity for the GMM and SM protocols is the SGSN on the network side, whereas the terminating entity for the EMM and ESM protocols is the MME. Both entities can be implemented on different physical nodes. Also, procedures for EMM and ESM differ from the ones specified for GMM and SM, though some of them show similarities. Several new identifiers have been introduced for EMM and ESM, different from the ones specified for GMM and SM. The identifiers are part of mandatory parts of messages and contexts stored in both network and terminal. Furthermore, re-using existing information element definitions by different specifications already exists in 3GPP and is done by means of references rather than duplicating specification text. It is also noted that the current L3 message structure has already been implemented, and therefore the message handling rules can to some degree be shared if EMM and ESM re-use the existing PDU encoding mechanism.

The aspects of EPS related to 3GPP accesses will be documented in different Technical Specifications:

- 3GPP TS 24.301 [44] on NAS protocol for the EPS; stage 3. This TS will be the stage 3 part of 3GPP TS 23.401 [2] and cover protocols for mobility management, session management, and control of NAS security. Furthermore, the TS would provide support of inter-system mobility between; E-UTRAN and GERAN/UTRAN, E-UTRAN and cdma2000®, and E-UTRAN and generic non-3GPP access.
- 3GPP TS 23.122 [22] on Non-Access-Stratum functions related to Mobile Station (MS) in idle mode. This existing TS will include enhancements of PLMN selection procedures to support access technology E-UTRA.
- 3GPP TS 24.008 [4] on Radio Interface Layer 3 specification; Core Network Protocols; stage 3. This existing TS will be modify to accommodate support of inter-system mobility between E-UTRAN and GERAN/UTRAN (impact on mobility management, session management, and security).

- 3GPP TS 24.007 [36] on Mobile radio interface signalling layer 3; General aspects. This existing TS will provide a description of new protocol principles (e.g. identifier for parallel session management transactions).

- 3GPP TS 24.305 [37] on Selective Disabling of 3GPP User Equipment Capabilities (SDoUE); Management Object (MO). This existing TS would include selective disabling of UE (SDoUE) for EPS procedures.

- 3GPP TS 27.007 [38] on AT command set for User Equipment (UE). This existing TS will provide support of E-UTRA in existing or new AT commands.

11.2 Specification work for non-3GPP access

The aspects of EPS related to non-3GPP access will be documented in three different Technical Specifications:

- 3GPP TS 24.302 [45] on access to EPC via non-3GPP access. This TS will cover the network selection procedures for non-3GPP access, the network selection procedures between 3GPP and non-3GPP access, the authentication and tunnel management procedures with trusted/untrusted networks, IP mobility mode selection, and, more in general, any procedure associated with accessing the EPC via non-3GPP accesses until the UE has gained IP connectivity.

- 3GPP TS 24.303 [46] on Dual-Stack Mobile IPv6. This TS will provide the specification of the procedures used via the S2c reference point and other related procedures, such as the home agent address discovery.

NOTE: Taking subclause 6.3 of 3GPP TS 23.402 [12] as a reference, the messages in the scope of 3GPP TS 24.303 will be those in step 4, 5 and 7. Messages before step 4 are independent of DSMIPv6 and therefore will not be documented in 3GPP TS 24.303. The same applies to the untrusted non-3GPP access; in subclause 7.3 of 3GPP TS 23.402 [12] steps 4, 5 and 6 will be specified in 3GPP TS 24.303.

- 3GPP TS 24.304 [48] on Mobile IPv4, UE to FA protocol. This TS will provide the specification of the exchange between the UE and the FA when Mobile IPv4 is used to access trusted non-3GPP networks.

The reason for structuring the procedures in this way is that the protocols DSMIPv6 and MIPv4 FA mode are independent of the specific underlying non-3GPP access network, and also the network entities terminating these protocols – home agent/PDN-GW for DSMIPv6, foreign agent for MIPv4 FA mode, and ePDG for trusted non-3GPP access – are logically independent of each other.

Based on this document plan, 3GPP TS 24.234 [14] will not include any EPS aspects as the topics related to untrusted non-3GPP accesses will be covered in 3GPP TS 24.hkl.

12 Agreed principles for the NAS message layout

12.1 Security functions in the NAS layer

When several EMM messages and/or ESM messages need to be transported in one step, typically in the case of linked ESM and EMM procedures, e.g. the ESM default EPS bearer context activation procedure and the EMM attach procedure, there shall be one single Sequence number IE and one single Message authentication code IE for the NAS message.

Figure 12.1.1 describes the security function (encryption (Encr) and integrity protection (Intgr)) flow.

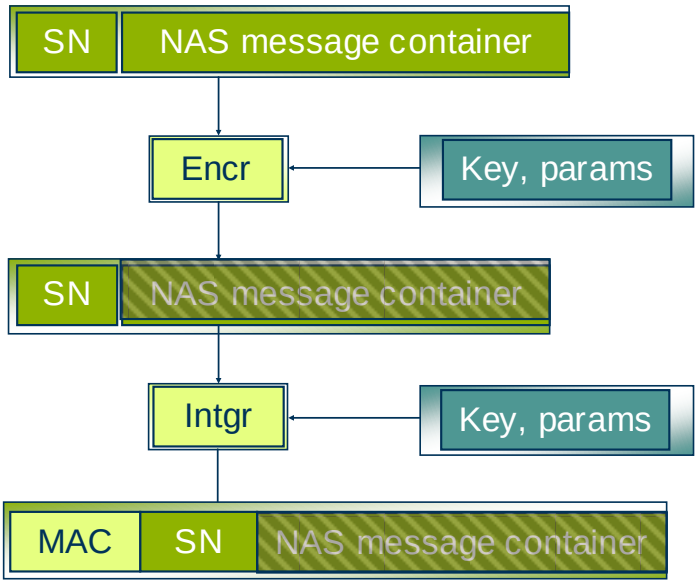


Figure 12.1.1: Encryption (Encr) and integrity protection (Intgr)) flow for NAS messages

The NAS message is first encrypted and then the encrypted NAS message and the SN are integrity protected by calculating the MAC.

12.2 NAS encryption algorithm input parameters

As an example the figure 12.2.1 below shows which input parameters are needed for the encryption algorithm. For the integrity protection algorithm a simular situation applies.

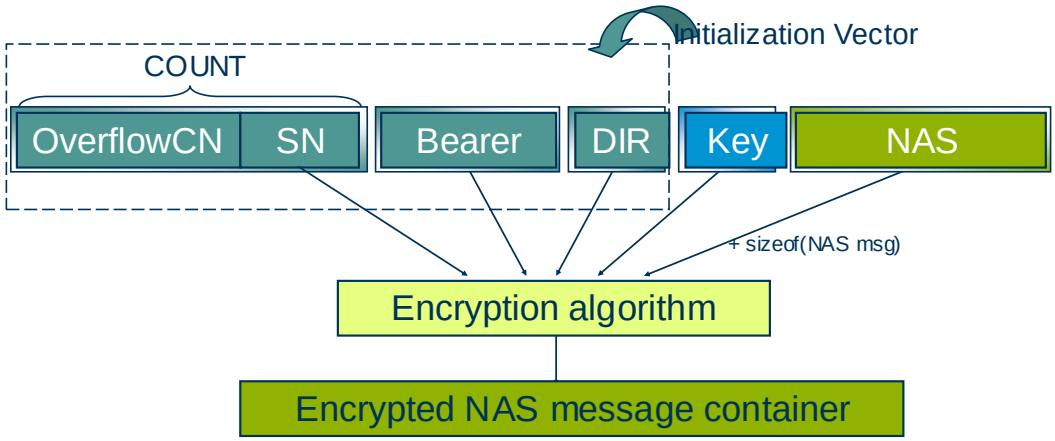


Figure 12.2.1: Input parameters for NAS encryption algorithm

OverflowCN = Overflow counter, kept locally in each peer. This overflow counter shall be incremented when the SN wraps around.

SN = Sequence Number, transferred together with the NAS message to the peer node

Bearer = A constant value of the same length as the AS BEARER ID parameter

DIR = Direction-bit, uplink or downlink

The only input parameter to the encryption algorithm transferred between peers is the SN parameter, and it shall be transferred unencrypted, but integrity protected.

12.3 General security header

The NAS messages shall be encrypted and integrity protected if a valid NAS security context exists and security functions are started. The following figure 12.3.1 shows the organization of the security header together with the NAS message:

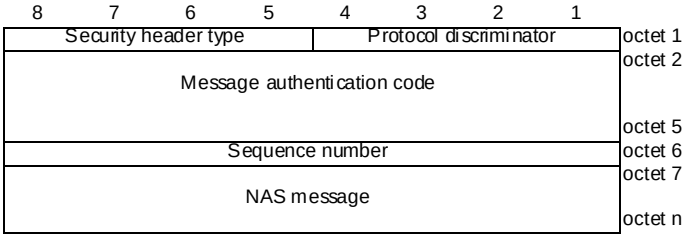


Figure 12.3.1: General security header

Editor's note: It is FFS how the NAS message IE is organized, i.e. concatenated or piggybacked.

12.4 Security header for service request

The structure of service request message does not comply with the structure of a standard layer 3 message.

NOTE: Because of the size restriction to 32 bits the message type is encoded as part of the security header type, and only parts of the sequence number and the message authentication code can be included.

The following figure 12.4.1 shows the structure of the security header for the service request message. The complete content of the service request message is encoded in the security header.

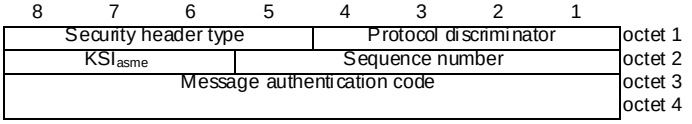


Figure 12.4.1: Security header for the SERVICE REQUEST message (Security header type = '11xx')

For the encoding of the parameters protocol discriminator and security header type see subclauses 12.5.1 and 12.5.2.

Editor's note: The encoding of the key set identifier KSI_{asme} is FFS.

In the parameter sequence number the UE shall include the 5 least significant bits of the NAS message sequence number (see subclause 12.5.3).

In the parameter message authentication code the UE shall include the 16 least significant bits of the message authentication code (see subclause 12.5.4).

12.5 Security header information elements

12.5.1 Protocol discriminator

This IE indicates the protocol discriminator of the message. The total size of this IE is 4 bits. The sender shall encode this IE as EMM protocol discriminator.

12.5.2 Security header type

The Security header type IE occupies parts of the first octet position that in other L3 messages are occupied by the Skip indicator (see 3GPP TS 24.007 [36]), and it includes control bits for the security header. The total size of the Security header type IE is 4 bits.

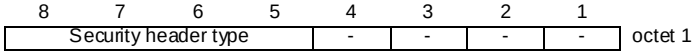


Figure 12.5.2.1: Security header type

The Security header type IE can take the values shown in Table 12.5.2.1.

Table 12.5.2.1: Security header type

Security header type (octet 1)				
8	**7**	**6**	**5**	
0	0	0	0	No security header included
0	0	0	1	General security header
1	1	0	0	Security header for the service request message
1	1	0	1	These values are not used in this version of the protocol.
	to			If received they shall be interpreted as '1100'.
1	1	1	1	
All other values are reserved.				

Editor's note: With this encoding, bits 5 and 6 can be used for future extensions of the service request message, e.g. for the introduction of a service type.

12.5.3 Sequence number

This IE includes the NAS message sequence number (SN). The SN IE shall be included in the security header if a valid NAS security context exists and security functions are started.

12.5.4 Message authentication code

The Message authentication code (MAC) information element contains the integrity protection information for the message. The algorithm to calculate the integrity protection information is specified in 3GPP TS 33.401 [40], and the integrity protection shall include all IEs in the security header, except the MAC IE itself, plus all the IEs in the NAS message IE. The MAC IE shall be included in the security header, if a valid NAS security context exists and security functions are started.

12.5.5 NAS message

This IE includes the EMM and/or ESM NAS message(s) according to the 3GPP TS 24.301 [44] which shall be transferred between the peers.

Editor's note: It is FFS how the NAS message is organized, i.e. how many NAS messages it can consists of and which type of NAS messages (EMM and/or ESM) it may consist of.

Annex A (informative): Proposed changes to 3GPP TS 23.122

A.1 Summary of changes

Editor's note: The following subclauses are a place holder for a draft CR to 3GPP TS 23.122 [22] until CT1 decides to send it to TSG CT plenary for approval. This annex includes only subclauses of 3GPP TS 23.122 [22] which need to be updated or added as new subclauses.

- Update of references to include references for E-UTRAN (3GPP TS 24.301 and 3GPP TS 36.304) and cdma2000® (3GPP2 C.S0016, C.S0011 and C.S0033-A).
- Update of definitions and text because of EPS and cdma2000®, e.g. addition of tracking area concept, enhancement of definitions of available PLMN and suitable cell.
- General description of idle mode (clause 2) needs to be generalised to avoid the exceptions in call initiation cases. The MM and AS procedures to deny the UEs access for outgoing calls do exist for various reasons, and none of those conditions is defined in the present document.
- Inclusion of E-UTRAN as a new access technology.
- Creation of new forbidden lists "forbidden TAs for roaming" and "forbidden TAs for regional provision of service".
- Subclause 4.4.4: a 3GPP – 3GPP2 multi mode MS may fall back to cdma2000® mode if no SIM is inserted, but cdma2000® credentials exist.
- Update of figures 2a, 2b and 3.
- New clause 6 describes the PLMN selection principles for 3GPP – 3GPP2 multi mode terminals.
- Indication of cdma2000® as a registered trademark of the Telecommunications Industry Association (TIA-USA).

A.2 First change

1 Scope

The present document gives an overview of the tasks undertaken by the Core network protocols of a Mobile Station (MS) when in idle mode, that is, switched on but typically not having a dedicated channel allocated. It also describes the corresponding network functions. The idle mode functions are also performed by a GPRS MS as long as no dedicated channel is allocated to the MS. The conditions when the idle mode functions are performed by an MS in the UTRA RRC connected mode states are specified in TS 25.331. The conditions when the idle mode functions are performed by an MS in the E-UTRAN are specified in 3GPP TS 36.304.

The present document defines the PLMN selection for a multi mode MS that supports both 3GPP and 3GPP2 systems. The common PLMN selection logic covers also PLMNs that are available in 3GPP2 system, but the present document makes no changes on the cdma2000® signalling towards networks that are available via 3GPP2 system.

This 3GPP TS outlines how the requirements of the 22 series Technical Specifications (especially 3GPP TS 22.011) on idle mode operation shall be implemented. Further details are given in 3GPP TS 24.008.

Clause 2 of this 3GPP TS gives a general description of the idle mode process. Clause 3 outlines the main requirements and technical solutions of those requirements. Clause 4 describes the processes used in idle mode. There is inevitably some overlap between these clauses.

NOTE: cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA).

Formatted: NO

1.1 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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] Void.

[2] 3GPP TS 22.001: "Principles of circuit telecommunication services supported by a Public Land Mobile Network (PLMN)".

[3] 3GPP TS 22.002: "Circuit Bearer Services (BS) supported by a Public Land Mobile Network (PLMN)".

[4] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)".

[5] 3GPP TS 22.004: "General on supplementary services".

[6] Void.

[7] Void

[8] Void.

[9] 3GPP TS 22.011: "Service accessibility".

[10] 3GPP TS 22.016: "International Mobile station Equipment Identities (IMEI)".

[11] Void.

[12] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".

[13] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".

[14] Void.

[15] 3GPP TS 22.041: "Operator Determined Barring (ODB)".

[16] 3GPP TS 22.081: "Line identification Supplementary Services; Stage 1".

[17] 3GPP TS 22.082: "Call Forwarding (CF) supplementary services - Stage 1".

[18] 3GPP TS 22.083: "Call Waiting (CW) and Call Holding (HOLD); Supplementary Services - Stage 1".

[19] 3GPP TS 22.084: "MultiParty (MPTY) Supplementary Services - Stage 1".

[20] 3GPP TS 22.085: "Closed User Group (CUG) Supplementary Services - Stage 1".

[21] 3GPP TS 22.086: "Advice of Charge (AoC) Supplementary Services - Stage 1".

[22] 3GPP TS 22.088: "Call Barring (CB) Supplementary Services - Stage 1".

[22A] 3GPP TS 23.003: "Numbering, addressing and identification".

[23] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification, Core Network Protocols - Stage 3".

[23A] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[24] 3GPP TS 45.002: "Multiplexing and multiple access on the radio path".

[25] 3GPP TS 45.008: "Radio subsystem link control".

[26] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service description, Stage 1".

[27] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description;Stage 2".

[28] 3GPP TS 43.064: "General Packet Radio Service (GPRS); Overall description of the GPRS Radio Interface; Stage 2".

[29] Void.

[30] Void.

[31] 3GPP TS 25.101: "UE Radio transmission and Reception (FDD)".

[32] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[33] 3GPP TS 25.331: "RRC Protocol Specification".

[34] 3GPP TS 44.018:"Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[35] 3GPP TS 43.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[36] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[37] Void.

[38] 3GPP TS 21.111: "USIM and IC card requirements".

[39] 3GPP TS 44.060: "General Packet Radio Service (GPRS);Mobile Station (MS) - Base Station System (BSS) interface;Radio Link Control/Medium Access Control (RLC/MAC) protocol".

[40] 3GPP TS 31.102: "Characteristics of the USIM Application".

[41] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[42] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[43] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol specification".

[44] 3GPP2 C.S0016: "Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards".

[45] 3GPP2 C.S0011: "Recommended Minimum Performance Standards for cdma2000 Spread Spectrum Mobile Stations".

[46] 3GPP2 C.S0033-A: "Recommended Minimum Performance Standards for cdma2000 High Rate Packet Data Access Terminal".

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: EX

1.2 Definitions and abbreviations

For the purposes of the present document, the abbreviations defined in 3GPP TR 21.905 [36] apply.

(A/Gb mode only): Indicates this clause applies only to GSM system. For multi system case this is determined by the current serving radio access network.

(Iu mode only): Indicates this clause applies only to UMTS system. For multi system case this is determined by the current serving radio access network.

Acceptable Cell: This is a cell that the MS may camp on to make emergency calls. It must satisfy criteria which is defined for A/Gb mode in 3GPP TS 43.022 and for Iu mode in 3GPP TS 25.304.

Access Technology: The access technology associated with a PLMN. The MS uses this information to determine what type of radio carrier to search for when attempting to select a specific PLMN (e.g., GSM, ~~UMTS~~UTRAN, ~~or~~ GSM COMPACT, or E-UTRAN). A PLMN may support more than one access technology.

Allowable PLMN: In the case of a MS operating in MS operation mode A or B, **t**his is a PLMN which is not in the list of "forbidden PLMNs" in the MS. In the case of a MS operating in MS operation mode C, this is a PLMN which is not in the list of "forbidden PLMNs" or in the list of "forbidden PLMNs for GPRS service" in the MS

Available PLMN: For GERAN A/Gb mode and GERAN Iu mode see 3GPP TS 43.022 [35]. For UTRAN~~UMTS~~ see 3GPP TS 25.304 [32], For E-UTRAN see 3GPP TS 36.304 [42]. For cdma2000® 1xRTT and cdma2000® HRPD see 3GPP2 C.S0016 [44].

Available PLMN/access technology combination**:** This is an available PLMN in a specific access technology.

Camped on a cell: The MS (ME if there is no SIM) has completed the cell selection/reselection process and has chosen a cell from which it plans to receive all available services. Note that the services may be limited, and that the PLMN may not be aware of the existence of the MS (ME) within the chosen cell.

Current serving cell: This is the cell on which the MS is camped.

CTS MS: An MS capable of CTS services is a CTS MS.

EHPLMN: Any of the PLMN entries contained in the Equivalent HPLMN list.

Equivalent HPLMN list: To allow provision for multiple HPLMN codes, PLMN codes that are present within this list shall replace the HPLMN code derived from the IMSI for PLMN selection purposes. This list is stored on the USIM and is known as the EHPLMN list. The EHPLMN list may also contain the HPLMN code derived from the IMSI. If the HPLMN code derived from the IMSI is not present in the EHPLMN list then it shall be treated as a Visited PLMN for PLMN selection purposes.

GPRS MS: An MS capable of GPRS services is a GPRS MS.

MS operation mode: See 3GPP TS 23.060 [27].

High quality signal: The high quality signal limit is used in the PLMN selection procedure. It is defined in the appropriate AS specification: 3GPP TS 43.022 [35] for the GSM radio access technology, 3GPP TS 25.304 [32] for the UMTS radio access technology (FDD or TDD mode), 3GPP TS 36.304 [42] for the E-UTRAN radio access technology. For 3GPP2 access technologies the high quality signal limit is defined in 3GPP2 C.S0011 [45] for cdma2000® 1xRTT and in 3GPP2 C.S0033-A [46] for cdma2000® HRPD.

Home PLMN: This is a PLMN where the MCC and MNC of the PLMN identity match the MCC and MNC of the IMSI. Matching criteria are defined in Annex A.

In A/Gb mode,...: Indicates this clause applies only to GSM System. For multi system case this is determined by the current serving radio access network.

In Iu mode,...: Indicates this clause applies only to UMTS System. For multi system case this is determined by the current serving radio access network.

Formatted: NotHighlight
Formatted: NotHighlight
Formatted: NotHighlight
Formatted: NotHighlight
Formatted: Font:(Default)TimesNew Roman
Formatted: Font:(Default)TimesNew Roman
Formatted: Font:(Default)TimesNew Roman
Formatted: NotHighlight
Formatted: Font:(Default)TimesNew Roman
Formatted: Font:(Default)TimesNew Roman
Formatted: Font:(Default)TimesNew Roman
Formatted: Font:(Default)TimesNew Roman
Formatted: Font:(Default)TimesNew Roman
Formatted: Font:(Default)TimesNew Roman

Localised Service Area (LSA): A localised service area consists of a cell or a number of cells. The cells constituting a LSA may not necessarily provide contiguous coverage.

Location Registration (LR): An MS which is IMSI attached to non-GPRS services only performs location registration by the Location Updating procedure. A GPRS MS which is IMSI attached to GPRS services or to GPRS and non-GPRS services performs location registration by the Routing Area Update procedure only when in a network of network operation mode I. Both location updating and routing are update procedures are performed independently by the GPRS MS when it is IMSI attached to GPRS and non-GPRS services in a network of network operation mode II or III (see 3GPP TS 23.060). An MS which is attached via the E-UTRAN performs location registration by the tracking area update procedure.

MS: Mobile Station. The present document makes no distinction between MS and UE.

Network Type: The network type associated with HPLMN or a PLMN on the PLMN selector (see 3GPP TS 31.102). The MS uses this information to determine what type of radio carrier to search for when attempting to select a specific PLMN. A PLMN may support more than one network type.

Registered PLMN (RPLMN): This is the PLMN on which certain LR outcomes have occurred (see table 1). In a shared network the RPLMN is the PLMN defined by the PLMN identity of the CN operator that has accepted the LR.

Registration: This is the process of camping on a cell of the PLMN and doing any necessary LRs.

Registration Area: A registration area is an area in which mobile stations may roam without a need to perform location registration. The registration area corresponds to location area (LA) for performing location updating procedure, ~~and it corresponds~~ to routing area for performing the GPRS attach or routing area update procedures, and to the tracking area (TA) for performing the attach or tracking area update procedure.

The PLMN to which a cell belongs (PLMN identity) is given in the system information transmitted on the BCCH (MCC + MNC part of LAI). In a shared network a cell belongs to all PLMNs given in the system information transmitted on the BCCH.

Selected PLMN: This is the PLMN that has been selected according to clause 3.1, either manually or automatically.

Shared Network: An MS considers a cell to be part of a shared network, when multiple PLMN identities are received on the BCCH.

SIM: Subscriber Identity Module (see 3GPP TS 21.111). The present document makes no distinction between SIM and USIM.

SoLSA exclusive access: Cells on which normal camping is allowed only for MS with Localised Service Area (LSA) subscription.

Suitable Cell: This is a cell on which an MS may camp. It must satisfy criteria which is defined for GERAN A/Gb mode or GERAN Iu mode in 3GPP TS 43.022 [35], ~~and~~ for ~~Iu mode~~UTRAN in 3GPP TS 25.304 [32], and for E-UTRAN in 3GPP TS 36.304 [42]. For 3GPP2 access technologies the criteria are defined in 3GPP2 C.S0011 [45] for cdma2000® 1xRTT and in 3GPP2 C.S0033-A [46] for cdma2000® HRPD.

Steering of Roaming: A technique whereby a roaming UE is encouraged to roam to a preferred roamed-to network by the HPLMN.

Visited PLMN: This is a PLMN different from the HPLMN (if the EHPLMN list is not present or is empty) or different from an EHPLMN (if the EHPLMN list is present).

Formatted: Not Highlight
Formatted: Not Highlight
Formatted: Not Highlight
Formatted: Font:(Default)Times New Roman
Formatted: Font:(Default)Times New Roman
Formatted: Font:(Default)Times New Roman
Formatted: Font:(Default)Times New Roman
Formatted: Font:(Default)Times New Roman

A.3 Next change

2 General description of idle mode

When an MS is switched on, it attempts to make contact with a public land mobile network (PLMN). The particular PLMN to be contacted may be selected either automatically or manually.

The MS looks for a suitable cell of the chosen PLMN and chooses that cell to provide available services, and tunes to its control channel. This choosing is known as "camping on the cell". The MS will then register its presence in the registration area of the chosen cell if necessary, by means of a location registration (LR), GPRS attach or IMSI attach procedure.

If the MS loses coverage of a cell, or find a more suitable cell, it reselects onto the most suitable cell of the selected PLMN and camps on that cell. If the new cell is in a different registration area, an LR request is performed.

If the MS loses coverage of a PLMN, either a new PLMN is selected automatically, or an indication of which PLMNs are available is given to the user, so that a manual selection can be made.

Registration is not performed by MSs only capable of services that need no registration.

The purpose of camping on a cell in idle mode is fourfold:

a) It enables the MS to receive system information from the PLMN.

b) If the MS wishes to initiate a call, it can do this by initially accessing the network on the control channel of the cell on which it is camped ~~(with the exceptions defined in 3GPP TS 43.022 clauses 3.5.3 and 3.5.4 and 3GPP TS 25.304)~~.

c) If the PLMN receives a call for the MS, it knows (in most cases) the registration area of the cell in which the MS is camped. It can then send a "paging" message for the MS on control channels of all the cells in the registration area. The MS will then receive the paging message because it is tuned to the control channel of a cell in that registration area, and the MS can respond on that control channel.

d) It enables the MS to receive cell broadcast messages.

If the MS is unable to find a suitable cell to camp on, or the SIM is not inserted, or if it receives certain responses to an LR request (e.g., "illegal MS"), it attempts to camp on a cell irrespective of the PLMN identity, and enters a "limited service" state in which it can only attempt to make emergency calls.

In A/Gb mode, if the CTS MS is in CTS mode only or in automatic mode with CTS preferred, it will start by attempting to find a CTS fixed part on which it is enrolled

The idle mode tasks can be subdivided into 4 processes:

- PLMN selection;
- Cell selection and reselection;
- Location registration;
- CTS fixed part selection (A/Gb mode only).

In A/Gb mode, to make this initial CTS fixed part selection, the MS shall be enrolled on at least one fixed part.

The relationship between these processes is illustrated in figure 1 in clause 5. The states and state transitions within each process are shown in figures 2 to 4 in clause 5.

3 Requirements and technical solutions

The following clauses list the main requirements of idle mode operation and give an outline of the technical solution.

3.1 PLMN selection and roaming

The MS normally operates on its home PLMN (HPLMN) or equivalent home PLMN (EHPLMN). However, a visited PLMN (VPLMN) may be selected, e.g., if the MS loses coverage. There are two modes for PLMN selection:

i) Automatic mode - This mode utilizes a list of PLMNs in priority order. The highest priority PLMN which is available and allowable is selected.

ii) Manual mode - Here the MS indicates to the user which PLMNs are available. Only when the user makes a manual selection does the MS try to obtain normal service on the VPLMN.

To prevent repeated attempts to have roaming service on a not allowed area (i.e. LA or TA), when the MS is informed that an area~~LA~~ is forbidden, the LA or TA is added to a list of "forbidden LAs for roaming" or "forbidden TAs for roaming" respectively which is stored in the MS. The~~i~~se lists, if existing, are~~is~~ deleted when the MS is switched off or when the SIM is removed. ~~Such area~~LA restrictions are always valid for complete location areas independent of possible subdivision into GPRS routing areas. The structure of the routing area identifier (see 3GPP TS 23.003 [22A]) supports area restriction on LA basis.

If a ~~"No Suitable Cells In Location Area"~~ message with cause value #15 (see 3GPP TS 24.008 [13A] and 3GPP TS 24.301 [23A]) is received by an MS, the~~n a~~ the MS shall take the following actions depending on the access technology in which the message was received:

GSM, GSM COMPACT or UTRAN:

The location area is added to the list of "forbidden LAs for roaming" which is stored in the MS. The MS shall then search for a suitable cell in the same PLMN but belonging to an LA or TA which is not in the "forbidden LAs for roaming" or "forbidden TAs for roaming" list respectively.

E-UTRAN:

The tracking area is added to the list of "forbidden TAs for roaming" which is stored in the MS. The MS shall then search for a suitable cell in the same PLMN but belonging to a TA or LA which is not in the "forbidden TAs for roaming" or "forbidden LAs for roaming" list respectively.

Formatted: B1

If a ~~"PLMN not allowed"~~ message with cause value "PLMN not allowed" is received by an MS in response to an LR request from a VPLMN, that VPLMN is added to a list of "forbidden PLMNs" in the SIM and thereafter that VPLMN will not be accessed by the MS when in automatic mode. A PLMN is removed from the "forbidden PLMNs" list if, after a subsequent manual selection of that PLMN, there is a successful LR. This list is retained when the MS is switched off or the SIM is removed. The HPLMN (if the EHPLMN list is not present or is empty) or an EHPLMN (if the EHPLMN list is present) shall not be stored on the list of "forbidden PLMNs".

In A/Gb mode, an ME not supporting SoLSA may consider a cell with the escape PLMN code (see 3GPP TS 23.073) to be a part of a PLMN belonging to the list of "forbidden PLMNs".

Optionally the ME may store in its memory an extension of the "forbidden PLMNs" list. The contents of the extension of the list shall be deleted when the MS is switched off or the SIM is removed.

If a ~~"GPRS services not allowed in this PLMN"~~ message with cause value "GPRS services not allowed in this PLMN" is received by an MS in response to an GPRS attach, GPRS detach, ~~or~~ routing area update, attach or tracking area update request (see 3GPP TS 24.008 [13A] and 3GPP TS 24.301 [23A]) from a VPLMN, that VPLMN is added to a list of "forbidden PLMNs for GPRS service" which is stored in the MS and thereafter that VPLMN will not be accessed by the MS for GPRS service when in automatic mode. This list is deleted when the MS is switched off or when the SIM is removed. A PLMN is removed from the list of "forbidden PLMNs for GPRS service" if, after a subsequent manual selection of that PLMN, there is a successful GPRS attach. The maximum number of possible entries in this list is implementation dependant, but must be at least one entry. The HPLMN (if the EHPLMN list is not present or is empty) or an EHPLMN (if the EHPLMN list is present) shall not be stored on the list of "forbidden PLMNs for GPRS service".

3.2 Regional provision of service

An MS may have a "regionally restricted service" where it can only obtain service on certain areas (i.e. LAs or TAs). If such an MS attempts to camp on a cell of an area~~LA~~ for which it does not have service entitlement, when it does an LR request, it will receive a~~n~~ ~~"LA not allowed"~~ message with cause value #12 (see 3GPP TS 24.008 [13A] and 3GPP TS 24.301 [23A]). In this case, the MS shall take the following actions depending on the access technology in which the message was received:

GSM, GSM COMPACT or UTRAN:

- The MS stores the forbidden LA identity (LAI) in a list of "forbidden LAs for regional provision of service", to prevent repeated access attempts on a cell of the forbidden LA. This list is deleted when the MS is switched off or the SIM is removed. The MS enters the limited service state.

E-UTRAN:

- The MS stores the forbidden TA identity (TAI) in a list of "forbidden TAs for regional provision of service", to prevent repeated access attempts on a cell of the forbidden TA. This list is deleted when the MS is switched off or the SIM is removed. The MS enters the limited service state.

In A/Gb mode, a cell may be reserved for SoLSA exclusive access (see 3GPP TS 24.008 and 3GPP TS 44.060). An MS is only allowed to camp normally on such a cell if it has a Localised Service Area subscription to the cell. Other MS may enter the limited service state.

NOTE: In A/Gb mode, in a SoLSA exclusive cell the MCC+MNC code is replaced by a~~n~~ unique escape PLMN code (see 3GPP TS 23.073), not assigned to any PLMN, in SI3 and SI4. An MS not supporting SoLSA may request for location update to an exclusive access cell. In this case the location attempt is rejected with the cause "PLMN not allowed" and the escape PLMN code is added to the list of the "forbidden PLMNs".

3.3 Borders between registration areas

If the MS is moving in a border area between registration areas, it might repeatedly change between cells of different registration areas. Each change of registration area would require an LR, which would cause a heavy signalling load and increase the risk of a paging message being lost. The access stratum shall provide a mechanism to limit this effect.

3.4 Access control

3.4.1 Access control

Due to problems in certain areas, Network Operators may decide to restrict access from some MSs (e.g., in case of congestion), and for this reason, a mechanism~~s~~ for common access control is provided. In A/Gb mode and Iu mode a~~nd~~ mechanism for domain specific access control is also~~are~~ provided (see 3GPP TS 43.022 and 3GPP TS 25.304).

In the case that a Network Operator decides to restrict access they may as an option allow restricted MSs to respond to paging messages and/or to perform location registrations. Mechanisms to allow this optional access are provided (see [3GPP TS 43.022 and] 3GPP TS 25.304).

3.4.2 Forbidden LA or TA for regional provision of service

When the MS is camped on a cell, the LA or TA of which belongs to the list of "forbidden LAs for regional provision of service" or "forbidden TAs for regional provision of service", the MS is not allowed to initiate establishment of a CM connection except for an emergency call; it may respond to paging. Also, the MS is not allowed to request GPRS services when camped on a cell of a LA or TA of which belongs to the list of "forbidden LAs for regional provision of service" or "forbidden TAs for regional provision of service".

A.4 Next change

4.3.3 List of states for location registration (figure 3)

The states are entered depending on responses to location registration (LR) requests. Independent update states exist for GPRS and for non-GPRS operation in MSs capable of GPRS and non-GPRS services.

L1 Updated - The MS enters this state if an LR request is accepted. The update status is set to "updated". The GPRS and the non-GPRS update state of a MS may enter "updated" as a result of combined signalling or as a result of individual signalling depending on the capabilities of the network.

Formatted: Font: 10 pt

L2 Idle, No IMSI - The MS enters this state if an LR request is rejected with cause:

a) IMSI unknown in HLR;

b) illegal ME;

c) illegal MS;

d) GPRS services and non-GPRS services not allowed,

or if there is no SIM. All update states of a MS enter this state regardless whether received by individual or combined signalling for events b) and c). Event a) has no influence on the GPRS update state. Events b) and c) result in "Roaming not allowed" for the GPRS and/or non-GPRS update status depending on the specific location registration procedure. Event d) results in "Roaming not allowed" for the GPRS update state.

If a SIM is present, the non-GPRS update status of the SIM is set to "Roaming not allowed".

L3 Roaming not allowed - The MS enters this state if it receives an LU reject message with the cause:

a) PLMN not allowed;

b) Location area not allowed;

c) Tracking area not allowed;

d~~e~~) Roaming not allowed in this location area.

e) Roaming not allowed in this tracking area;

f~~d~~) GPRS services not allowed in this PLMN;

g~~e~~) No Suitable Cells In Location Area;

h) No Suitable Cells In Tracking Area

Exept from event f~~d~~) all update states of the MS are set to "Roaming not allowed" regardless whether received by individual or combined signalling. Event f~~d~~) results in "Roaming not allowed" for the GPRS update state only. Event f~~d~~) has no influence on the non-GPRS update state. The behaviour of the MS in the roaming not allowed state is dependent on the LR reject cause as shown in table 2 in clause 5. Additionally:

- in automatic mode, "PLMN not allowed", ~~and~~ "R~~r~~oaming not allowed in this location area" and "Roaming not allowed in this tracking area" cause the Automatic Network Selection procedure of clause 4.4.3.1.1 to be started; it is also caused by "GPRS services not allowed in this PLMN" when received by a GPRS MS operating in MS operation mode C;
- in manual mode, "PLMN not allowed" and "R~~r~~oaming not allowed" cause the Manual Network Selection procedure of clause 4.4.3.1.2 to be started; it is also caused by "GPRS services not allowed in this PLMN" when received by a GPRS MS operating in MS operation mode C.

L4 Not updated - The MS enters this state if any LR failure not specified for states L2 or L3 occurs, in which cases the MS is not certain whether or not the network has received and accepted the LR attempt. The non-GPRS update status on the SIM and/or the GPRS update status are set to "not updated" depending on the specific location registration procedure and their outcome.

NOTE This clause does not describe all the cases. For more details refer to 3GPP TS 24.008 [23]

A.5 Next change

4.4.4 Abnormal cases

If there is no SIM in the MS, if there is an authentication failure, or if the MS receives an "IMSI unknown in HLR", "illegal ME" or "illegal MS" response to an LR request, then effectively there is no selected PLMN ("No SIM" state). In these cases, the states of the cell selection process are such that no PLMN selection information is used. No further attempts at registration on any PLMN are made until the MS is switched off and on again, or a SIM is inserted.

When in Automatic Network Selection mode and the MS is in the "not updated" state with one or more suitable cells to camp on; then after the maximum allowed unsuccessful LR requests (controlled by the specific attempt counters) the MS may continue (or start if it is not running) the user reselection procedure of 4.4.3.2 1.

A multi mode MS that also supports 3GPP2 access technology may fall back to 3GPP2 mode if no SIM is inserted.

4.4.5 Roaming not allowed in this LA or TA

If in either PLMN selection mode the LR response "Roaming not allowed in this LA" or "Roaming not allowed in this TA" is received:

The PLMN Automatic or Manual Mode Selection Procedure of clause 4.4.3.1 are followed, depending on whether the MS is in automatic or manual mode.

A.6 Next change

4.4.3.1.1 Automatic Network Selection Mode Procedure

The MS selects and attempts registration on other PLMN/access technology combinations, if available and allowable, in the following order:

i) either the HPLMN (if the EHPLMN list is not present or is empty) or the highest priority EHPLMN that is available (if the EHPLMN list is present) ;

ii) each PLMN/access technology combination in the "User Controlled PLMN Selector with Access Technology" data file in the SIM (in priority order);

iii) each PLMN/access technology combination in the "Operator Controlled PLMN Selector with Access Technology" data file in the SIM (in priority order);

iv) other PLMN/access technology combinations with received high quality signal in random order;

v) other PLMN/access technology combinations in order of decreasing signal quality.

When following the above procedure the following requirements apply:

a) An MS with voice capability shall ignore PLMNs for which the MS has identified at least one GSM COMPACT.

b) In A/Gb mode or GSM COMPACT, an MS with voice capability, or an MS not supporting packet services shall not search for CPBCCH carriers.

c) In ii and iii, the MS should limit its search for the PLMN to the access technology or access technologies associated with the PLMN in the appropriate PLMN Selector with Access Technology list (User Controlled or Operator Controlled selector list). An MS using a SIM without access technology information storage (i.e. the "User Controlled PLMN Selector with Access Technology" and the "Operator Controlled PLMN Selector with Access Technology" data files are not present) shall instead use the "PLMN Selector" data file, for each PLMN in the "PLMN Selector" data file, the MS shall search for all access technologies it is capable of and shall assume GSM access technology as the highest priority radio access technology.

d) In iv and v, the MS shall search for all access technologies it is capable of, before deciding which PLMN to select.

e) In ii, and iii, a packet only MS which supports GSM COMPACT, but using a SIM without access technology information storage (i.e. the "User Controlled PLMN Selector with Access Technology" and the "Operator Controlled PLMN Selector with Access Technology" data files are not present) shall instead use the "PLMN Selector" data file, for each PLMN in the "PLMN Selector" data file, the MS shall search for all access technologies it is capable of and shall assume GSM COMPACT access technology as the lowest priority radio access technology.

f) In i, the MS shall search for all access technologies it is capable of. No priority is defined for the preferred access technology and the priority is an implementation issue, but "HPLMN Selector with Access Technology" data file on the SIM may be used to optimise the procedure.

g) In i, an MS using a SIM without access technology information storage (i.e. the "HPLMN Selector with Access Technology" data file is not present) shall search for all access technologies it is capable of and shall assume GSM access technology as the highest priority radio access technology. A packet only MS which supports GSM COMPACT using a SIM without access technology information storage shall also assume GSM COMPACT access technology as the lowest priority radio access technology.

h) In v, the MS shall order the PLMN/access technology combinations in order of decreasing signal quality within each access technology. The order between PLMN/access technology combinations with different access technologies is an MS implementation issue.

NOTE 1: Requirements a) and b) apply also to requirement d), so a GSM voice capable MS should not search for GSM COMPACT PLMNs, even if capable of GSM COMPACT.

NOTE 2: Requirements a) and b) apply also to requirement f), so a GSM voice capable MS should not search for GSM COMPACT PLMNs, even if this is the only access technology on the "HPLMN Selector with Access Technology" data file on the SIM.

NOTE 3: High quality signal is defined in the appropriate AS specification.

If successful registration is achieved, the MS indicates the selected PLMN.

If registration cannot be achieved because no PLMNs are available and allowable, the MS indicates "no service" to the user, waits until a new PLMN is available and allowable and then repeats the procedure.

If there were one or more PLMNs which were available and allowable, but an LR failure made registration on those PLMNs unsuccessful or an entry in any of the lists "forbidden LAs for roaming", "forbidden TAs for roaming", ~~or~~ "forbidden LAs for regional provision of service" or "forbidden TAs for regional provision of service" prevented a registration attempt, the MS selects the first such PLMN again and enters a limited service state.

4.4.3.1.2 Manual Network Selection Mode Procedure

The MS indicates whether there are any PLMNs, which are available using all supported access technologies. This includes PLMNs in the "forbidden PLMNs" list and PLMNs which only offer services not supported by the MS. An MS which supports GSM COMPACT shall also indicate GSM COMPACT PLMNs (which use PBCCH).

If displayed, PLMNs meeting the criteria above are presented in the following order:

i)- either the HPLMN (if the EHPLMN list is not present or is empty) or, if one or more of the EHPLMNs are available then based on an optional data field on the SIM either only the highest priority available EHPLMN is to be presented to the user or all available EHPLMNs are presented to the user in priority order. If the data field is not present on the SIM, then only the highest priority available EHPLMN is presented;

ii)- PLMN/access technology combinations contained in the " User Controlled PLMN Selector with Access Technology " data file in the SIM (in priority order);

iii)- PLMN/access technology combinations contained in the "Operator Controlled PLMN Selector with Access Technology" data file in the SIM (in priority order);

iv)- other PLMN/access technology combinations with received high quality signal in random order;

v)- other PLMN/access technology combinations in order of decreasing signal quality.

In ii and iii, an MS using a SIM without access technology information storage (i.e. the "User Controlled PLMN Selector with Access Technology" and the "Operator Controlled PLMN Selector with Access Technology" data files are not present) shall instead present the PLMNs contained in the "PLMN Selector" data file in the SIM (in priority order).

In v, requirement h) in clause 4.4.3.1.1 applies.

In GSM COMPACT, the non support of voice services shall be indicated to the user.

The HPLMN may provide on the SIM additional information on the available PLMNs. If this information is provided then the MS shall indicate it to the user. This information, provided as free text may include:

- preferred partner,
- roaming agreement status,
- supported services

Furthermore, the MS may indicate whether the available PLMNs are present on the EHPLMN list, the Forbidden list, the User Controlled PLMN List or the Operator Controlled PLMN List. The MS may also indicate that the PLMN is not present on any of these lists.

The user may select his desired PLMN and the MS then initiates registration on this PLMN using the access technology chosen by the user for that PLMN or using the highest priority available access technology for that PLMN, if the associated access technologies have a priority order. (This may take place at any time during the presentation of PLMNs). For such a registration, the MS shall ignore the contents of the "forbidden LAs for roaming", "forbidden TAs for roaming", "forbidden LAs for regional provision of service", "forbidden TAs for regional provision of service", "forbidden PLMNs for GPRS service" and "forbidden PLMNs" lists.

Once the UE has registered on a PLMN selected by the user, the UE shall not automatically register on a different PLMN unless:

i) the new PLMN is declared as an equivalent PLMN by the registered PLMN; or

ii) the user selects automatic mode.

NOTE 1: It is an MS implementation option whether to indicate access technologies to the user. If the MS does display access technologies, then the access technology used should be the access technology chosen by the user for that PLMN. If the MS does not display access technologies, then the access technology chosen for a particular PLMN should be the highest priority available access technology for that PLMN, if the associated access technologies have a priority order.

If the user does not select a PLMN, the selected PLMN shall be the one that was selected before the PLMN selection procedure started. If no such PLMN was selected or that PLMN is no longer available, then the MS shall attempt to camp on any acceptable cell and enter the limited service state.

NOTE 2: High quality signal is defined in the appropriate AS specification.

A.7 Next change

4.5 Location registration process

4.5.1 General

When the MS is switched on and capable of services requiring registration, the action taken by the location registration process is as follows:

a) SIM present and no LR needed (because of the status of the stored registration area identity and "attach" flag): The MS is in the update state UPDATED;

b) SIM present and LR needed: A LR request is made;

c) No SIM present: The MS enters the update state Idle, NO IMSI.

In case b) above, and subsequently whenever a LR request is made, the MS enters a state depending on the outcome of the LR request, as listed in clause 4.3.2 above. In case c) the GPRS and the non-GPRS update state enters "IDLE, NO IMSI".

Whenever the MS goes to connected mode and then returns to idle mode again, the MS selects the appropriate state.

A multi mode MS that also supports 3GPP2 access technology may fall back to 3GPP2 mode if no SIM is inserted.

4.5.2 Initiation of Location Registration

An LR request indicating Normal Updating is made when, in idle mode,

- the MS changes cell while being in the update state NOT UPDATED; (for MS capable of GPRS and non-GPRS services when at least one of both update states is NOT UPDATED)
- the MS detects that it has entered a new registration area, i.e., when the received registration area identity differs from the one stored in the MS, and the LAI or the PLMN identity is not contained in any of the lists of "forbidden LAs for roaming", "forbidden TAs for roaming", "forbidden LAs for regional provision of service", "forbidden TAs for regional provision of service", "forbidden PLMNs for GPRS service" or "forbidden PLMNs" respectively, while being in one of the following update states:
  - UPDATED;
  - NOT UPDATED;
  - ROAMING NOT ALLOWED.
- the Periodic Location Updating Timer expires while being in the non-GPRS update state NOT UPDATED (triggers Location Updating);
- the Periodic Routing Area Update timer expires while being in the GPRS update state NOT UPDATED (triggers Routing Area Update);
- the Periodic Tracking Area Update timer expires while being in the EPS update state NOT UPDATED (triggers Tracking Area Update);
- a manual network reselection has been performed, an acceptable cell of the selected PLMN is present, and the MS is not in the UPDATED state on the selected PLMN.

If a new PLMN is entered, a MS which is attached for PS services shall perform a routeing area update if the LAI or the PLMN identity is not contained in any of the lists "forbidden LAs for roaming", "forbidden TAs for roaming", "forbidden LAs for regional provision of service", "forbidden TAs for regional provision of service", "forbidden PLMNs for GPRS service" or "forbidden PLMNs" and if the current update status is different from "IDLE, NO IMSI".

An LR request indicating Periodic Location Updating is made when, in idle mode, the Periodic Location Updating timer expires while being in the non-GPRS update state UPDATED.

An LR request indicating Periodic Routing Area Update is made when the Periodic Routing Area Update timer expires while being in the GPRS update state UPDATED.

An LR request indicating IMSI attach is made when the MS is activated in the same location area in which it was deactivated while being in the non-GPRS update state UPDATED, and the system information indicates that IMSI attach/detach shall be used.

A GPRS attach is made by a GPRS MS when activated and capable of services which require registration. A GPRS attach may only performed if the selected PLMN is not contained in the list of "forbidden PLMNs for GPRS service".

Depending on system information about GPRS network operation mode MSs operating in MS operation mode A or B perform combined or non-combined location registration procedures. When the combined routing area update or GPRS attach is accepted with indication "MSC not reachable" or is not answered the MS performs also the corresponding location updating procedure or falls back to a GPRS only MS. When the combined routing area update or GPRS attach is rejected with cause "GPRS not allowed" the GPRS update state is "IDLE, NO IMSI" and the MS performs the corresponding location updating procedure.

Furthermore, an LR request indicating Normal Location Updating is also made when the response to an outgoing request shows that the MS is unknown in the VLR or SGSN, respectively.

Table 2 in clause 5 summarizes the events in each state that trigger a new LR request. The actions that may be taken while being in the various states are also outlined in table 2.

A GPRS MS which is both IMSI attached for GPRS and non-GPRS services and which is capable of simultaneous operation of GPRS and non-GPRS services shall perform Routing Area Update in connected mode when it has entered a new routing area which is not part of a LA contained in the list of "forbidden LAs for roaming", "forbidden TAs for roaming", ~~or~~ "forbidden LAs for regional provision of service" or "forbidden TAs for regional provision of service".

A.8 Next change

4.5.5 No Suitable Cells In Location Area or Tracking Area

If during location registration the LR response "No Suitable Cells In Location Area" or "No Suitable Cells In Tracking Area" is received:

> The MS shall attempt to find another LA or TA of the same PLMN on which it received the LR response. If the MS is able to find another LA or TA it shall attempt registration. If the MS is unable to find an LA or TA the PLMN Automatic or Manual Mode Selection Procedure of clause 4.4.3.1 shall be followed, depending on whether the MS is in automatic or manual mode.

A.9 Next change

5 Tables and Figures

Table 1: Effect of LR Outcomes on PLMN Registration

Location Registration Task State	Registration Status	Registered PLMN is
Updated	Successful	Indicated in the stored registration area identity
Idle, No IMSI	Unsuccessful	No registered PLMN (3) (4)
Roaming not allowed:		
a) PLMN not allowed	Unsuccessful	No registered PLMN (4)
b) LA not allowed or TA not allowed	Indeterminate(1)	No registered PLMN
c) Roaming not allowed in this LA or Roaming not allowed in this TA	Indeterminate (2)	No registered PLMN (4)
d) No Suitable Cells In Location Area or No Suitable Cells In Tracking Area	Indeterminate (5)	No registered PLMN
Not updated	Unsuccessful	No registered PLMN (4)

1) The MS will perform a cell selection and will eventually either enter a different state when the registration status will be determined, or fail to be able to camp on a new cell, when registration status will be unsuccessful.
2) The MS will select the HPLMN (if the EHPLMN list is not present or is empty) or an EHPLMN (if the EHPLMN list is present) if in automatic mode and will enter Automatic Network Selection Mode Procedure of clause 4.4.3.1. If in manual mode, the MS will display the list of available PLMNs and follow the Manual Network Selection Mode Procedure of clause 4.4.3.1.2 If the appropriate process does not result in registration, the MS will eventually enter the limited service state.
3) An MS may have different update states for GPRS and non-GPRS. A PLMN is registered when at least one of both update states is updated.
4) The stored list of equivalent PLMNs is invalid and can be deleted.
5) The MS will attempt registration on another LA or TA of the same PLMN, or equivalent PLMN if available.Otherwise it will enter either the Automatic Network Selection Mode procedure of clause 4.4.3.1 or follow the Manual Network Selection Mode procedure of clause 4.4.3.1.2. If the appropriate process does not result in registration, the MS will eventually enter the limited service state.

NOTE 1: MSs capable of GPRS and non-GPRS services may have different registration status for GPRS and for non-GPRS.
NOTE 2: The registered PLMN is determined by looking at the stored registration area identity and stored location registration status.

Table 2: LR Process States and Allowed Actions

Location registration task state	New LR request when				Normal Calls Supported (1)	Paging responded to
	Changing Cell	Changing registration area	Changing PLMN	Other		
Null (4)	No	Yes	Yes	No	No	No
Updated, (5)	No	Yes	Yes	(2)	Yes	Yes
Idle, No IMSI (7)	No	No	No	No	No	No
Roaming not allowed:						
a) Idle, PLMN not allowed	No	No	Yes	No	No	Optional if with IMSI
b) Idle, LA not allowed; or TA not allowed	No	Yes(6)	Yes	No	No	Optional if with IMSI
c) Idle, Roaming not allowed in this LA; or Roaming not allowed in this TA	No	Yes(6)	Yes	No	No	Optional if with IMSI
d) No Suitable Cells In Location Area; or No Suitable Cells In Tracking Area	No	Yes(6)	Yes	No	No	Optional if with IMSI
Not updated	Yes	Yes	Yes	(2)&(3)	(3)	Yes if with IMSI

1): Emergency calls may always be made, subject to access control permitting it.
2): A new LR is made when the periodic registration timer expires.
3): If a normal call request is made, an LR request is made. If successful the updated state is entered and the call may be made.
4): The MS is in the null state from switch on until it has camped on a cell and either made an LR attempt or decided that no LR attempt is needed.
5): In this state, IMSI detach is performed if the MS is deactivated and the BCCH indicates that IMSI attach/detach shall be used. An LR request indicating IMSI attach is performed if the MS is activated in the same registration area in which it was deactivated while being in this state.
6): An MS shall not perform a new LR when the new routing area is part of an LA or TA contained in any of the lists "forbidden LAs for roaming", "forbidden TAs for roaming", ~~or~~ "forbidden LAs for regional provision of service", or "forbidden TAs for regional provision of service".
7): The GPRS registration status "Idle, no IMSI" is entered when LR is rejected with cause "GPRS not allowed". The non-GPRS registration status "Idle, no IMSI" is entered when the cause "IMSI unknown in HLR" is received.

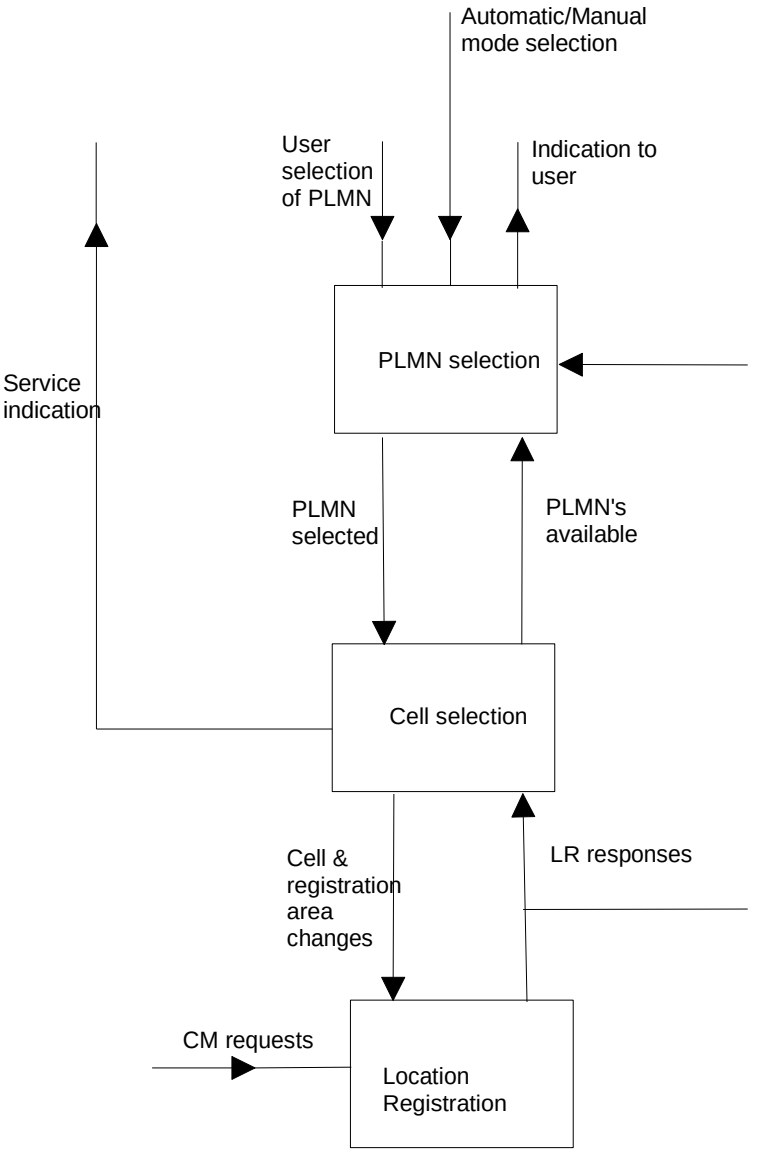
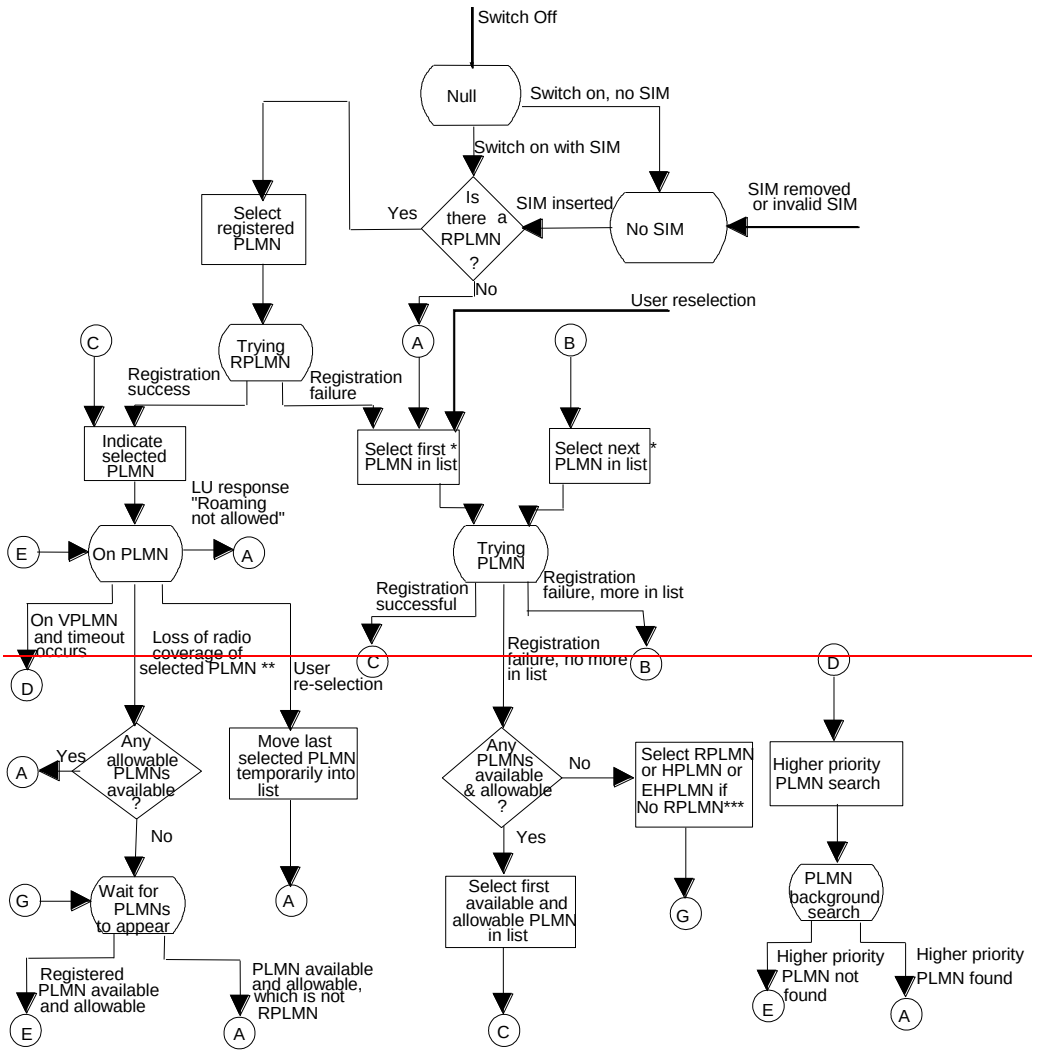


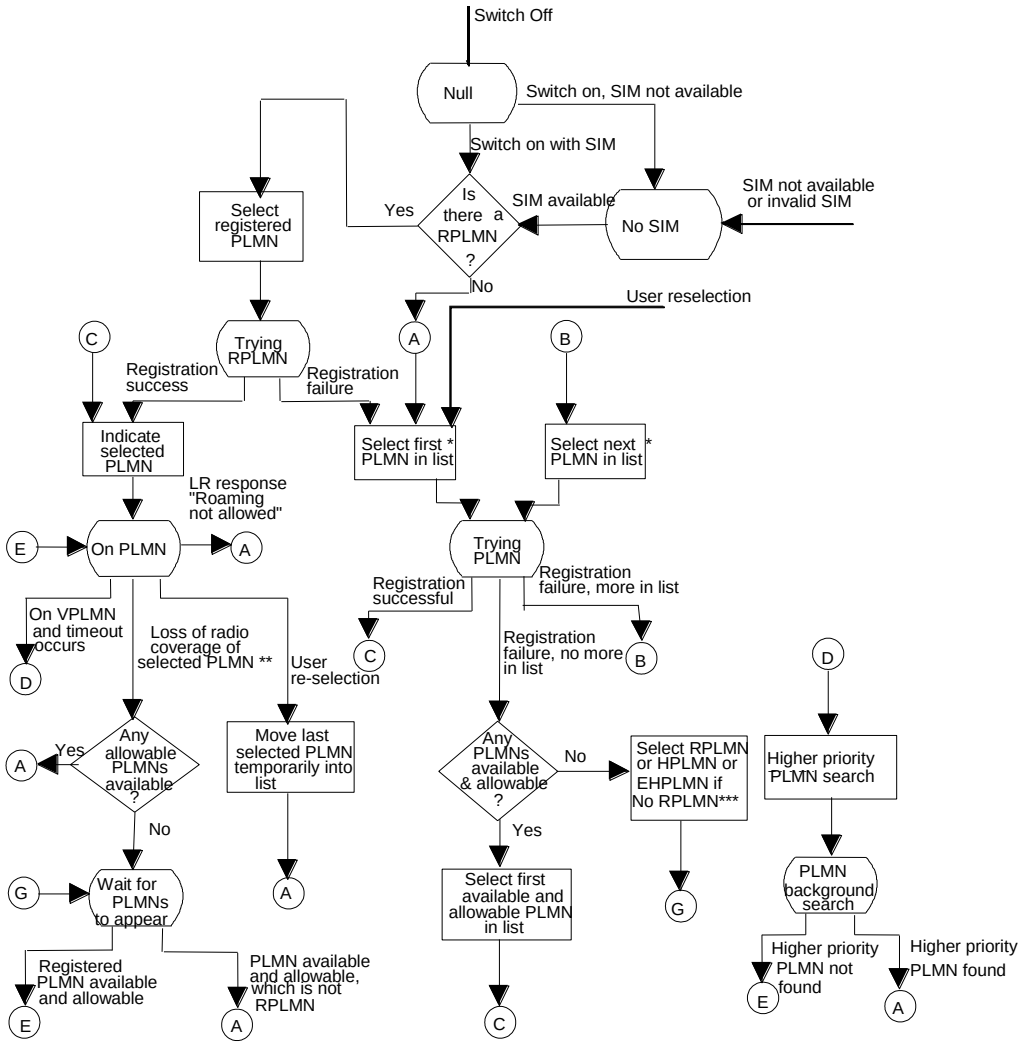
Figure 1: Overall Idle Mode process



* "List" consists of points i) to v) as defined in section 4.4.3.1.1 except in case of a user re-selection in which case "list" consists of points i) to vi) as defined in section 4.4.3.2.1

** Includes effective loss of coverage due to LAs being forbidden in all potentially suitable cells

*** HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the list is present)

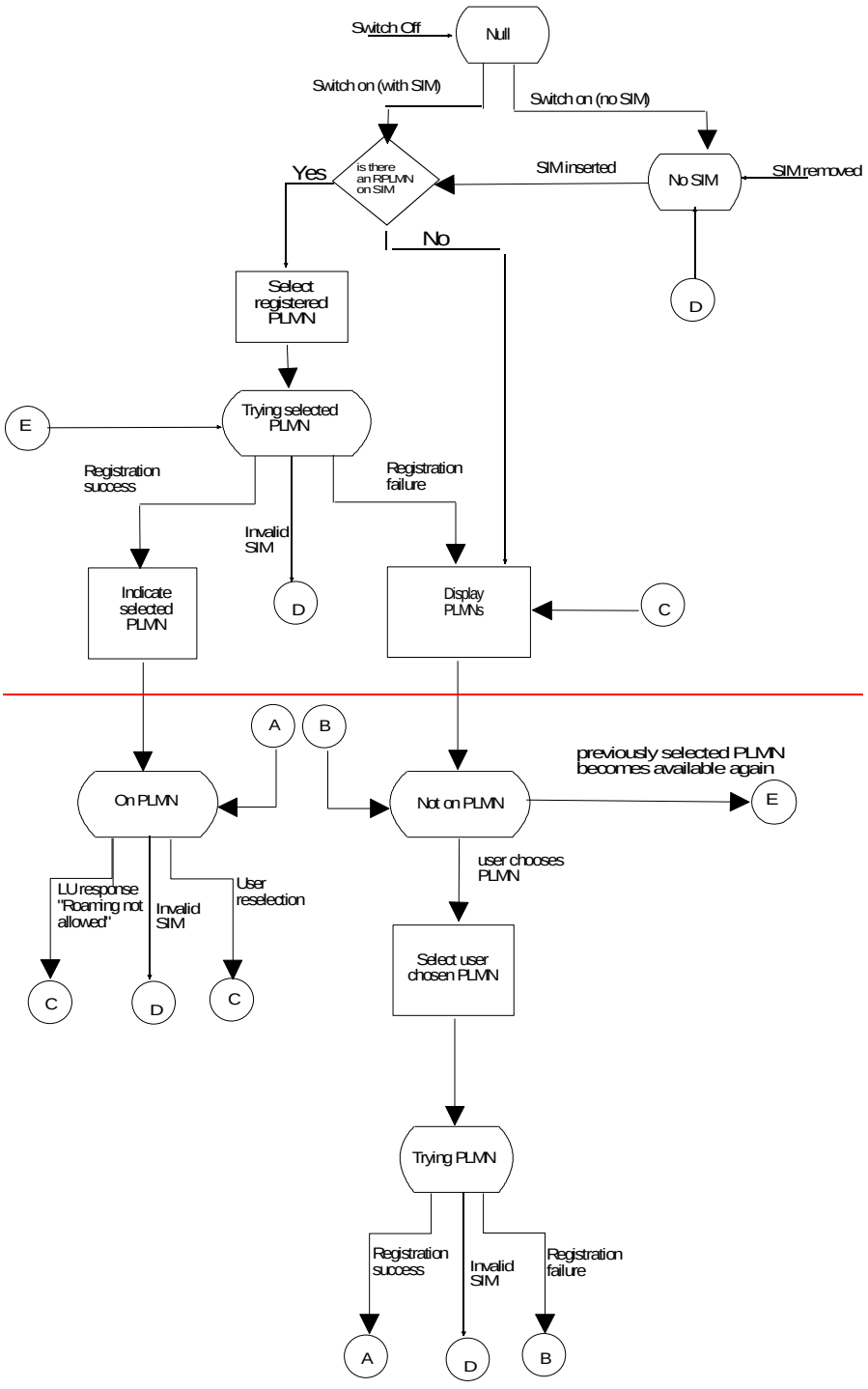


* "List" consists of points i) to v) as defined in section 4.4.3.1.1 except in case of a user re-selection in which case "list" consists of points i) to vi) as defined in section 4.4.3.2.1

** Includes effective loss of coverage due to LAs/TAs being forbidden in all potentially suitable cells

*** HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the list is present)

Figure 2a: PLMN Selection State diagram (automatic mode)


Switch Off
Null
Switch on (with SIM)
Switch on (no SIM)
Yes
is there an RPLMN on SIM
SIM inserted
No SIM
SIM removed
No
D
Select registered PLMN
E
Trying selected PLMN
Registration success
Registration failure
Invalid SIM
Indicate selected PLMN
D
Display PLMNs
C
A
B
previously selected PLMN becomes available again
On PLMN
Not on PLMN
E
user chooses PLMN
LU response "Roaming not allowed"
Invalid SIM
User reselection
C
D
C
Select user chosen PLMN
Trying PLMN
Registration success
Invalid SIM
Registration failure
A
D
B

Formatted: TH

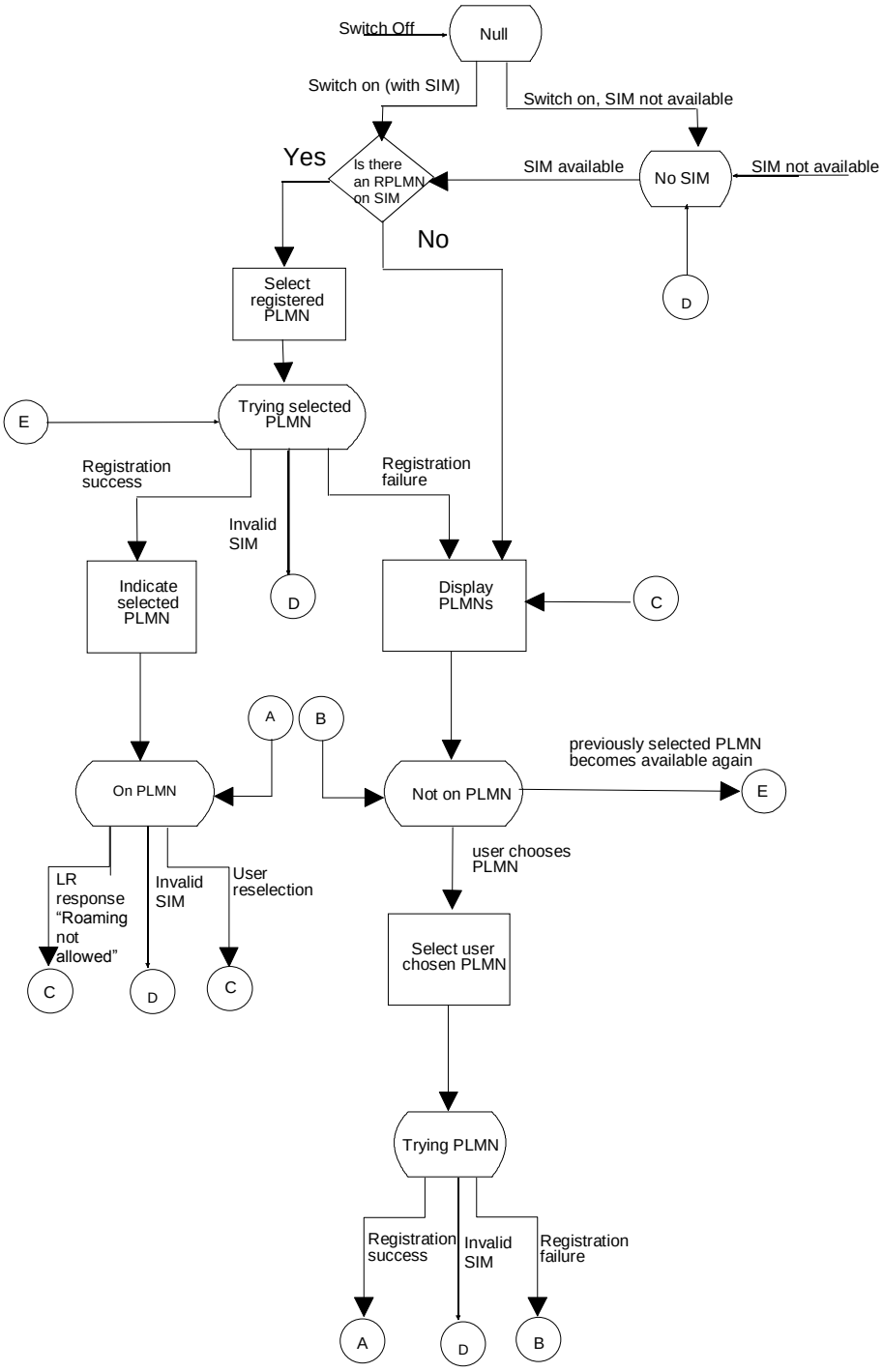
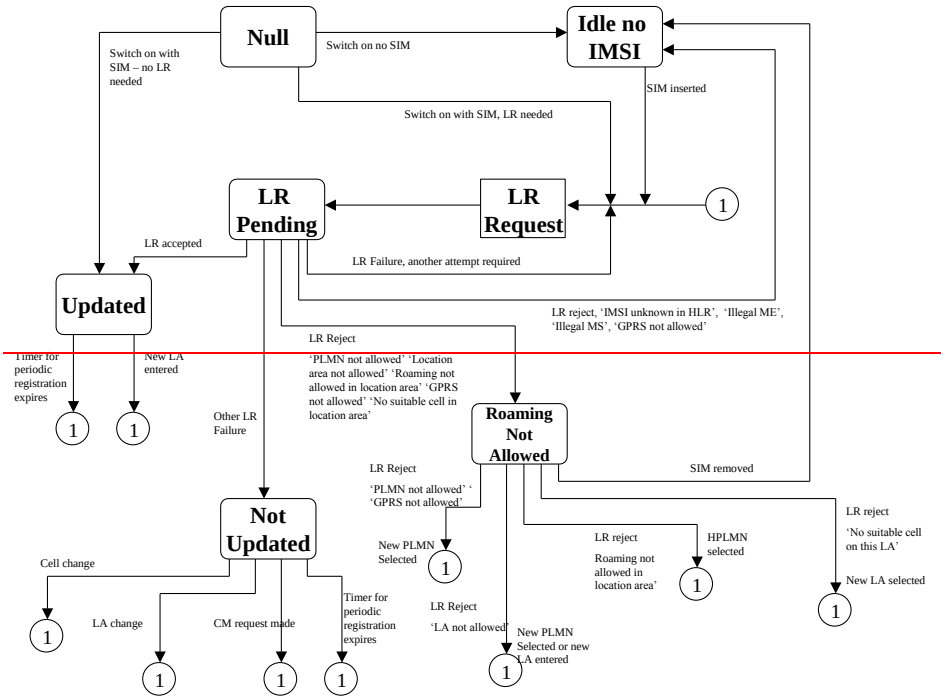
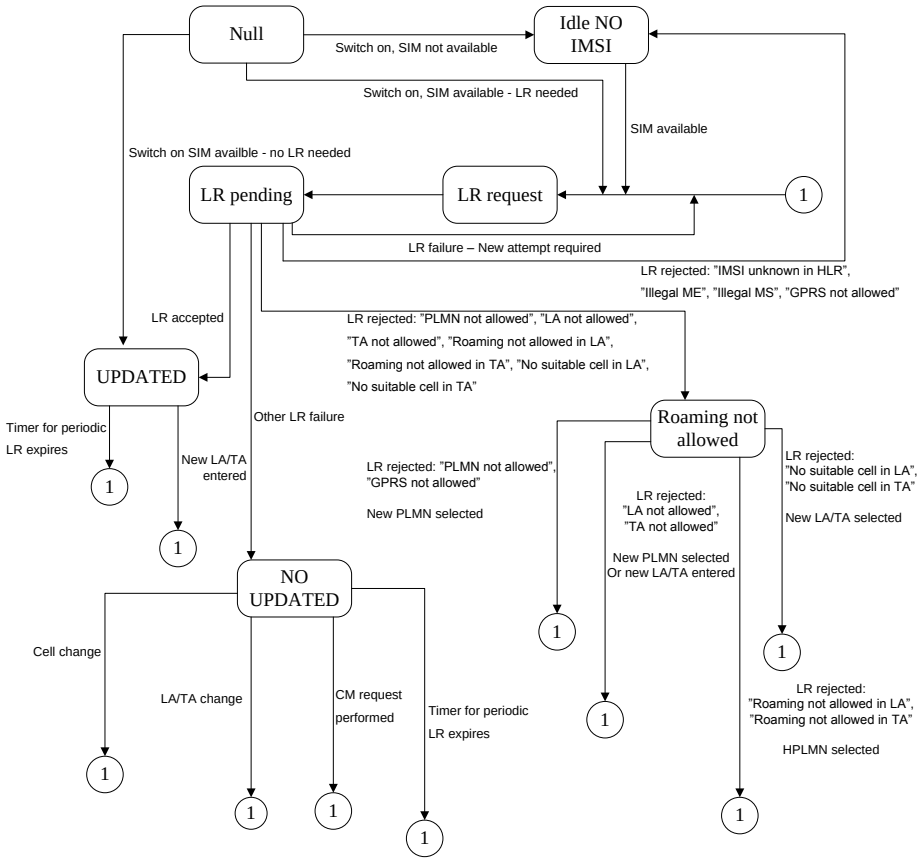


Figure 2b: PLMN Selection State diagram (manual mode)


Null
Idle no IMSI
Switch on no SIM
Switch on with SIM – no LR needed
SIM inserted
Switch on with SIM, LR needed
LR Pending
LR Request
1
LR accepted
LR Failure, another attempt required
Updated
LR reject, 'IMSI unknown in HLR', 'Illegal ME', 'Illegal MS', 'GPRS not allowed'
LR Reject
'PLMN not allowed' 'Location area not allowed' 'Roaming not allowed in location area' 'GPRS not allowed' 'No suitable cell in location area'
Timer for periodic registration expires
New LA entered
Other LR Failure
Roaming Not Allowed
SIM removed
LR Reject
'PLMN not allowed' ' 'GPRS not allowed'
LR reject
'No suitable cell on this LA'
Not Updated
New PLMN Selected
LR reject
Roaming not allowed in location area'
HPLMN selected
New LA selected
Cell change
LA change
CM request made
Timer for periodic registration expires
LR Reject
'LA not allowed'
New PLMN Selected or new LA entered

Formatted: TH



NOTE 1: Whenever the MS goes to connected mode and then returns to idle mode again the MS selects appropriate state.
NOTE 2: A MS capable of GPRS and non-GPRS services has two Task State machines one for GPRS and one for non-GPRS operation.

Figure 3: Location Registration Task State diagram

A.10 Next change

6 MS supporting access technologies defined both by 3GPP and 3GPP2

6.1 General

An MS that supports access technologies defined both by 3GPP and 3GPP2 shall consider all supported access technologies in all supported bands when performing PLMN selection.

The goal of the PLMN selection process for such a multi mode mobile is to find the highest priority PLMN and to attempt to register to it.

A multi mode MS shall follow the requirements in the present document for the PLMN selection procedures across both 3GPP and 3GPP2 access technologies. Additionally the MS shall follow the requirements of the present document in its signalling procedures towards any 3GPP network. If the common PLMN selection procedure leads to selection of a 3GPP2 network, then the MS shall follow 3GPP2 specifications in all signalling procedures towards the 3GPP2 network.

Annex B (informative): Proposed changes to 3GPP TS 24.008

B.1 Summary of changes

Editor's note: The following subclauses are a place holder for a draft CR to 3GPP TS 24.008 [4] until CT1 decides to send it to TSG CT plenary for approval. This annex includes only subclauses of 3GPP TS 24.008 [4] which need to be updated or added as new subclauses.

- Update of references to include 3GPP TS 23.401 and 3GPP TS 24.301.
- Addition of references to the definitions of EPS specific terms and abbreviations like Globally Unique MME Identifier (GUMMEI), Tracking Area Identity (TAI), etc.
- When normal or combined attach procedure is rejected with cause #3, #6, #7, #8, #11, #12, #13, #14 and #15, interaction with EMM is required for parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI, if S1 mode is supported.
- When network initiated GPRS detach procedure is triggered with re-attach not required and cause code is #3, #6, #7, #8, #11, #12, #13, #14 and #15, interaction with EMM is required on parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI, if S1 mode is supported.
- When normal/periodic routing area update procedure is rejected with cause #3, #6, #7, #11, #12 and #14, interaction with EMM is required for parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI, if S1 mode is supported. Also, when combined routing area update procedure is rejected with cause #3, #6, #7, #8, #11, #12 and #14, interaction with EMM is required.
- When normal/periodic routing area update procedure is rejected with cause #13 and #15, interaction with EMM is required for parameters EMM state and EPS update status, if S1 mode is supported. Also, when combined routing area update procedure is rejected with cause #13 and #15, interaction with EMM is required for parameters EMM state and EPS update status, if S1 mode is supported.
- When service request procedure is rejected with cause #3, #6, #7, #11 and #12, interaction with EMM is required for parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI, if S1 mode is supported.
- When service request procedure is rejected with cause #13 and #15, interaction with EMM is required for parameters EMM state and EPS update status, if S1 mode is supported.- Handling of control parameter "Temporary Identity for Next update (TIN)" during attach procedure and routing area update procedure.
- Handling of temporary identities at intersystem change from S1 mode to Iu mode or A/Gb mode.
- "Additional mobile identity" and "Additonal old routing area identity" are added to ROUTING AREA UPDATE REQUEST message.
- "ISR indication" is added to ROUTING AREA UPDATE ACCEPT message.
- Enhancement of Mobile identity IE: type of identity "TMSI/P-TMSI" is extended to "TMSI/P-TMSI/M-TMSI".
- Addition of EPS and UMTS security algorithms to the MS network capability IE.

B.2 First change

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] Void.

[2] Void.

[2a] 3GPP TR 21.905 "Vocabulary for 3GPP Specifications"

[3] 3GPP TS 22.002: "Circuit Bearer Services (BS) supported by a Public Land Mobile Network (PLMN)".

[4] 3GPP TS 22.003: "Teleservices supported by a Public Land Mobile Network (PLMN)".

[5] 3GPP TS 42.009: "Security aspects".

[5a] 3GPP TS 33.102: "3G security; Security architecture".

[6] 3GPP TS 22.011: "Service accessibility".

[7] 3GPP TS 42.017: "Subscriber Identity Modules (SIM); Functional characteristics".

[8] 3GPP TS 22.101: "Service aspects; Service principles".

[8a] 3GPP TS 22.001: "Principles of circuit telecommunication services supported by a Public Land Mobile Network (PLMN)".

[8b] 3GPP TS 23.038: "Alphabets and language-specific information".

[9] 3GPP TS 23.101: "General UMTS Architecture".

[9a] 3GPP TS 23.108: "Mobile radio interface layer 3 specification core network protocols; Stage 2 (structured procedures)".

[10] 3GPP TS 23.003: "Numbering, addressing and identification".

[11] 3GPP TS 43.013: "Discontinuous Reception (DRX) in the GSM system".

[12] 3GPP TS 23.014: "Support of Dual Tone Multi-Frequency (DTMF) signalling".

[12a] ETSI ES 201 235-2, v1.2.1: "Specification of Dual Tone Multi-Frequency (DTMF); Transmitters and Receivers; Part 2: Transmitters".

[13] 3GPP TS 43.020: "Security-related network functions".

[14] 3GPP TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".

[15] 3GPP TS 24.002: "GSM-UMTS Public Land Mobile Network (PLMN) access reference configuration".

[16] 3GPP TS 44.003: "Mobile Station - Base Station System (MS - BSS) interface; Channel structures and access capabilities".

[17] 3GPP TS 44.004: "Layer 1; General requirements".

[18] 3GPP TS 44.005: "Data Link (DL) layer; General aspects".

[19] 3GPP TS 44.006: "Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification".

[19a] 3GPP TS 25.321: "Medium Access Control (MAC) protocol specification".

[19b] 3GPP TS 25.322: "Radio Link Control (RLC) protocol specification".

[19c] 3GPP TS 25.413: "UTRAN Iu interface RANAP signalling".

[20] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[21] 3GPP TS 24.010: "Mobile radio interface layer 3; Supplementary services specification; General aspects".

[22] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[23] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[23a] 3GPP TS 44.071: "Location Services (LCS); Mobile radio interface layer 3 specification."

[23b] 3GPP TS 44.031 "Location Services LCS); Mobile Station (MS) - Serving Mobile Location Centre (SMLC); Radio Resource LCS Protocol (RRLP)".

[23c] 3GPP TS 25.331: "Radio Resource Control (RRC) protocol specification"

[24] 3GPP TS 24.080: "Mobile radio Layer 3 supplementary service specification; Formats and coding".

[25] 3GPP TS 24.081: "Line identification supplementary services; Stage 3".

[26] 3GPP TS 24.082: "Call Forwarding (CF) supplementary services; Stage 3".

[27] 3GPP TS 24.083: "Call Waiting (CW) and Call Hold (HOLD) supplementary services; Stage 3".

[28] 3GPP TS 24.084: "MultiParty (MPTY) supplementary services; Stage 3".

[29] 3GPP TS 24.085: "Closed User Group (CUG) supplementary services; Stage 3".

[30] 3GPP TS 24.086: "Advice of Charge (AoC) supplementary services; Stage 3".

[31] 3GPP TS 24.088: "Call Barring (CB) supplementary services; Stage 3".

[32] 3GPP TS 45.002: "Multiplexing and multiple access on the radio path".

[33] 3GPP TS 45.005: "Radio transmission and reception".

[34] 3GPP TS 45.008: "Radio subsystem link control".

[35] 3GPP TS 45.010: "Radio subsystem synchronization".

[36] 3GPP TS 27.001: "General on Terminal Adaptation Functions (TAF) for Mobile Stations (MS)".

[36a] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services ".

[37] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[38] 3GPP TS 29.007: "General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)".

[39] 3GPP TS 51.010: "Mobile Station (MS) conformance specification".

[40] 3GPP TS 51.021: "GSM radio aspects base station system equipment specification".

[41] ISO/IEC 646 (1991): "Information technology - ISO 7-bit coded character set for information interchange".

[42] ISO/IEC 6429: "Information technology - Control functions for coded character sets".

[43] ISO 8348 (1987): "Information technology -- Open Systems Interconnection -- Network Service Definition".

[44] ITU-T Recommendation E.163: "Numbering plan for the international telephone service".

[45] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[46] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users".

[47] ITU-T Recommendation F.69 (1993): "The international telex service - Service and operational provisions of telex destination codes and telex network identification codes".

[48] ITU-T Recommendation I.330: "ISDN numbering and addressing principles".

[49] ITU-T Recommendation I.440 (1989): "ISDN user-network interface data link layer - General aspects".

[50] ITU-T Recommendation I.450 (1989): "ISDN user-network interface layer 3 General aspects".

[51] ITU-T Recommendation I.500 (1993): "General structure of the ISDN interworking recommendations".

[52] ITU-T Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) - Information technology - 7-bit coded character set for information interchange".

[53] ITU Recommendation Q.931: ISDN user-network interface layer 3 specification for basic control".

[54] ITU-T Recommendation V.21: "300 bits per second duplex modem standardized for use in the general switched telephone network".

[55] ITU-T Recommendation V.22: "1200 bits per second duplex modem standardized for use in the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits".

[56] ITU-T Recommendation V.22bis: "2400 bits per second duplex modem using the frequency division technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits".

[57] Void.

[58] ITU-T Recommendation V.26ter: "2400 bits per second duplex modem using the echo cancellation technique standardized for use on the general switched telephone network and on point-to-point 2-wire leased telephone-type circuits".

[59] ITU-T Recommendation V.32: "A family of 2-wire, duplex modems operating at data signalling rates of up to 9600 bit/s for use on the general switched telephone network and on leased telephone-type circuits".

[60] ITU-T Recommendation V.110: "Support by an ISDN of data terminal equipments with V-Series type interfaces".

[61] ITU-T Recommendation V.120: "Support by an ISDN of data terminal equipment with V-Series type interfaces with provision for statistical multiplexing".

[62] ITU-T Recommendation X.21: "Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for synchronous operation on public data networks".

[63] Void.

[64] Void.

[65] ITU-T Recommendation X.30: "Support of X.21, X.21 bis and X.20 bis based Data Terminal Equipments (DTEs) by an Integrated Services Digital Network (ISDN)".

[66] ITU-T Recommendation X.31: "Support of packet mode terminal equipment by an ISDN".

[67] Void.

[68] Void.

[69] ITU-T Recommendation X.121: "International numbering plan for public data networks".

[70] ETSI ETS 300 102-1: "Integrated Services Digital Network (ISDN); User-network interface layer 3; Specifications for basic call control".

[71] ETSI ETS 300 102-2: "Integrated Services Digital Network (ISDN); User-network interface layer 3; Specifications for basic call control; Specification Description Language (SDL) diagrams".

[72] ISO/IEC 10646: "Information technology -- Universal Multiple-Octet Coded Character Set (UCS)".

[73] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service Description; Stage 1".

[74] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[75] 3GPP TS 43.064: "General Packet Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2".

[75a] 3GPP TS 43.318: "Generic Access Network (GAN); Stage 2".

[76] 3GPP TS 44.060: "General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/Medium Access Control (RLC/MAC) protocol".

[76b] 3GPP TS 44.318: "Generic Access Network (GAN); Mobile GAN interface layer 3 specification; Stage 3".

[77] IETF RFC 1034: "Domain names - concepts and facilities".

[78] 3GPP TS 44.065: "Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[78a] 3GPP TS 44.064: "Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) Layer Specification".

[79] ITU Recommendation I.460: "Multiplexing, rate adaption and support of existing interfaces".

[80] 3GPP TS 26.111: "Codec for Circuit Switched Multimedia Telephony Service; Modifications to H.324".

[81] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[82] 3GPP TS 43.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[83] 3GPP TS 26.103: "Speech Codec List for GSM and UMTS".

[84] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[85] 3GPP TS 48.008: "Mobile-services Switching Centre – Base Station System (MSC – BSS) interface; layer 3 specification".

[86] 3GPP TS 48.018: "General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP)".

[87] 3GPP TS 43.055: "Dual Transfer Mode (DTM); Stage 2".

[88] 3GPP TS 23.067: "enhanced Multi-Level Precedence and Pre-emption service (eMLPP); Stage 2".

[88a] 3GPP TS 23.093: "Technical realization of Completion of Calls to Busy Subscriber (CCBS); Stage 2".

[89] 3GPP TS 22.042: "Network Identity and Time Zone (NITZ), Stage 1".

[90] 3GPP TS 23.040: "Technical realization of Short Message Service (SMS)".

[91] 3GPP TS 44.056: "GSM Cordless Telephony System (CTS), (Phase 1) CTS Radio Interface Layer 3 Specification".

[92] 3GPP TS 23.226: "Global Text Telephony; Stage 2 "

[93] 3GPP TS 26.226: "Cellular Text Telephone Modem (CTM), General Description "

[94] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes"

[95] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP"

[96] 3GPP TS 23.205: "Bearer-independent circuit-switched core network; Stage 2".

[97] 3GPP TS 23.172: "UDI/RDI Fallback and Service Modification; Stage 2".

[98] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode"

[99] RFC 3513 (April 2003): "Internet Protocol Version 6 (IPv6) Addressing Architecture".

[100] 3GPP TS 29.207: "Policy control over Go interface".

[101] 3GPP TS 21.111: "USIM and IC card requirements".

[102] RFC 1661 (July 1994): "The Point-to-Point Protocol (PPP)".

[103] RFC 3232 (January 2002): "Assigned Numbers: RFC 1700 is Replaced by an On-line Database".

[104] 3GPP TS 23.034: "High Speed Circuit Switched Data (HSCSD) – Stage 2".

[105] 3GPP TS 23.271: "Functional stage 2 description of LCS".

[106] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[107] RFC 3376 (October 2002): "Internet Group Management Protocol, Version 3".

[108] RFC 2710 (October 1999): "Multicast Listener Discovery (MLD) for IPv6".

[109] 3GPP TS 23.251: "Network Sharing; Architecture and Functional Description".

[110] 3GPP TS 25.346: "Introduction of the Multimedia Broadcast Multicast Service (MBMS) in the Radio Access Network"

[111] 3GPP TS 44.118: "Radio Resource Control (RRC) protocol; Iu mode".

[112] 3GPP TS 31.102: "Characteristics of the USIM Application".

[113] 3GPP TS 43.129: "Packet-switched handover for GERAN A/Gb mode; Stage 2".

[114] 3GPP TS 23.009: "Handover procedures".

[115] 3GPP TR 23.903: " Redial solution for voice-video switching".

[116] 3GPP TS 24.279: "Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services, stage 3".

[117] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[118] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".

B.3 Next change

2.2.2 Vocabulary

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

- A **GSM security context** is established and stored in the MS and the network as a result of a successful execution of a GSM authentication challenge. The GSM security context consists of the GSM ciphering key and the ciphering key sequence number.
- A **UMTS security context** is established and stored in the MS and the network as a result of a successful execution of a UMTS authentication challenge. The UMTS security context consists of the UMTS ciphering key, the UMTS integrity key, the GSM ciphering key and the cipher key sequence number.
- **idle mode:** In this mode, the mobile station is not allocated any dedicated channel; it listens to the CCCH and the BCCH;
- **group receive mode:** (only applicable for mobile stations supporting VGCS listening or VBS listening) In this mode, the mobile station is not allocated a dedicated channel with the network; it listens to the downlink of a voice broadcast channel or voice group call channel allocated to the cell. Occasionally, the mobile station has to listen to the BCCH of the serving cell as defined in 3GPP TS 43.022 [82] and 3GPP TS 45.008 [34];
- **dedicated mode:** In this mode, the mobile station is allocated at least two dedicated channels, only one of them being a SACCH;
- **group transmit mode:** (only applicable for mobile stations supporting VGCS talking) In this mode, one mobile station of a voice group call is allocated two dedicated channels, one of them being a SACCH. These channels can be allocated to one mobile station at a time but to different mobile stations during the voice group call;
- **packet idle mode**: (only applicable for mobile stations supporting GPRS) In this mode, mobile station is not allocated any radio resource on a packet data physical channel; it listens to the PBCCH and PCCCH or, if those are not provided by the network, to the BCCH and the CCCH, see 3GPP TS 44.060 [76].
- **packet transfer mode**: (only applicable for mobile stations supporting GPRS) In this mode, the mobile station is allocated radio resource on one or more packet data physical channels for the transfer of LLC PDUs.
- **main DCCH:** In Dedicated mode and group transmit mode, only two channels are used as DCCH, one being a SACCH, the other being a SDCCH or a FACCH; the SDCCH or FACCH is called here "the main DCCH";
- A channel is **activated** if it can be used for transmission, in particular for signalling, at least with UI frames. On the SACCH, whenever activated, it must be ensured that a contiguous stream of layer 2 frames is sent;
- A TCH is **connected** if circuit mode user data can be transferred. A TCH cannot be connected if it is not activated. A TCH which is activated but not connected is used only for signalling, i.e. as a DCCH;
- The data link of SAPI 0 on the main DCCH is called the **main signalling link**. Any message specified to be sent on the main signalling link is sent in acknowledged mode except when otherwise specified;

- The term **"to establish"** a link is a short form for **"to establish the multiframe mode"** on that data link. It is possible to send UI frames on a data link even if it is not established as soon as the corresponding channel is activated. Except when otherwise indicated, a data link layer establishment is done without an information field.
- **"channel set"** is used to identify TCHs that carry related user information flows, e.g., in a multislot configuration used to support circuit switched connection(s), which therefore need to be handled together.
- A **temporary block flow** (TBF) is a physical connection used by the two RR peer entities to support the uni-directional transfer of LLC PDUs on packet data physical channels, see 3GPP TS 44.060 [76].
- **RLC/MAC block:** A RLC/MAC block is the protocol data unit exchanged between RLC/MAC entities, see 3GPP TS 44.060 [76].
- A **GMM context** is established when a GPRS attach procedure is successfully completed.
- **Network operation mode**

  The three different network operation modes I, II, and III are defined in 3GPP TS 23.060 [74].

  The network operation mode shall be indicated as system information. For proper operation, the network operation mode should be the same in each cell of one routing area.
- **GAN mode:** See 3GPP TS 43.318 [75a].
- GPRS MS operation mode

  The three different GPRS MS operation modes A, B, and C are defined in 3GPP TS 23.060 [74].
- **RR connection:** A RR connection is a dedicated physical circuit switched domain connection used by the two RR or RRC peer entities to support the upper layers' exchange of information flows.
- **PS signalling connection** is a peer to peer Iu mode connection between MS and CN packet domain node.
- **Inter-System change** is a change of an MS from A/Gb mode to Iu mode of operation or vice versa.
- **GPRS:** Packet Services for systems which operate the Gb or Iu-PS interfaces.
- The label **(A/Gb mode only)** indicates this section or paragraph applies only to a system which operates in A/Gb mode, i.e. with a functional division that is in accordance with the use of an A or a Gb interface between the radio access network and the core network. For multi system case this is determined by the current serving radio access network.
- The label **(Iu mode only)** indicates this section or paragraph applies only to a system which operates in Iu mode. The Iu mode includes UTRAN and GERAN Iu modes, i.e. with a functional division that is in accordance with the use of an Iu-CS or Iu-PS interface between the radio access network and the core network. For multi system case this is determined by the current serving radio access network.
- **In A/Gb mode,...** Indicates this paragraph applies only to a system which operates in A/Gb mode. For multi system case this is determined by the current serving radio access network.
- **In Iu mode,...** Indicates this paragraph applies only to a system which operates in Iu mode. The Iu mode includes both UTRAN Iu mode and GERAN Iu mode. For multi system case this is determined by the current serving radio access network.
- **In A/Gb mode and GERAN Iu mode,...** Indicates this paragraph applies only to a system which operates in A/Gb mode or GERAN Iu mode. For multi system case this is determined by the current serving radio access network.
- **In UTRAN Iu mode,...** Indicates this paragraph applies only to a system which operates in UTRAN Iu mode. For multi system case this is determined by the current serving radio access network.
- **In a shared network,...** Indicates this paragraph applies only to a shared network. For the definition of shared network see 3GPP TS 23.122 [14].

- **SIM,** Subscriber Identity Module (see 3GPP TS 42.017 [7]).
- **USIM,** Universal Subscriber Identity Module (see 3GPP TS 21.111 [101]).
- **MS,** Mobile Station. The present document makes no distinction between MS and UE.
- **Cell Notification** is an (optimised) variant of the Cell Update Procedure which uses the LLC NULL frame for cell change notification which does not trigger the restart of the READY timer
- **DTM:** dual transfer mode, see 3GPP TS 44.018 [84] and 3GPP TS 43.055 [87]

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.401 [118], subclause 3.2, apply:

Globally Unique MME Identifier (GUMMEI)
Globally Unique Temporary Identity (GUTI)
GUTI update status
Idle Mode Signalling Reduction (ISR)
M-Temporary Mobile Subscriber Identity (M-TMSI)
P-TMSI update status
Tracking Area Identity (TAI)
Temporary Identity used in Next update (TIN)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.301 [117] apply:

S1 mode

B.4 Next change

4.7.1.4.1 Radio resource sublayer address handling (A/Gb mode only)

This subclause describes how the RR addressing is managed by GMM. For the detailed coding of the different TLLI types and how a TLLI can be derived from a P-TMSI, see 3GPP TS 23.003 [10].

~~Two~~Three cases can be distinguished:

- a valid P-TMSI is available in the MS; ~~or~~
- no valid P-TMSI is available in the MS; or
- no valid P-TMSI is available, but valid M-TMSI is available.

i) valid P-TMSI available

If the MS has stored a valid P-TMSI, the MS shall derive a foreign TLLI from that P-TMSI and shall use it for transmission of the:

- ATTACH REQUEST message of any GPRS combined/non-combined attach procedure; other GMM messages sent during this procedure shall be transmitted using the same foreign TLLI until the ATTACH ACCEPT message or the ATTACH REJECT message is received; and
- ROUTING AREA UPDATE REQUEST message of a combined/non-combined RAU procedure if the MS has entered a new routing area, or if the GPRS update status is not equal to GU1 UPDATED. Other GMM messages sent during this procedure shall be transmitted using the same foreign TLLI, until the ROUTING AREA UPDATE ACCEPT message or the ROUTING AREA UPDATE REJECT message is received.

After a successful GPRS attach or routing area update procedure, independent whether a new P-TMSI is assigned, if the MS has stored a valid P-TMSI then the MS shall derive a local TLLI from the stored P-TMSI and shall use it for addressing at lower layers.

NOTE: Although the MS derives a local TLLI for addressing at lower layers, the network should not assume that it will receive only LLC frames using a local TLLI. Immediately after the successful GPRS attach or routing area update procedure, the network must be prepared to continue accepting LLC frames from the MS still using the foreign TLLI.

ii) no valid P-TMSI available

When the MS has not stored a valid P-TMSI, i.e. the MS is not attached to GPRS, the MS shall use a randomly selected random TLLI for transmission of the:

- ATTACH REQUEST message of any combined/non-combined GPRS attach procedure.

The same randomly selected random TLLI value shall be used for all message retransmission attempts and for the cell updates within one attach attempt.

Upon receipt of an ATTACH REQUEST message, the network shall assign a P-TMSI to the MS. The network derives a local TLLI from the assigned P-TMSI, and transmits the assigned P-TMSI to the MS.

Upon receipt of the assigned P-TMSI, the MS shall derive the local TLLI from this P-TMSI and shall use it for addressing at lower layers.

NOTE: Although the MS derives a local TLLI for addressing at lower layers, the network should not assume that it will receive only LLC frames using a local TLLI. Immediately after the successful GPRS attach, the network must be prepared to continue accepting LLC frames from the MS still using the random TLLI.

In ~~both~~ cases i) and ii), the MS shall acknowledge the reception of the assigned P-TMSI to the network. After receipt of the acknowledgement, the network shall use the local TLLI for addressing at lower layers.

iii) no valid P-TMSI available, but valid M-TMSI available

In this case, the radio resource sublayer address handling is described in subclause 4.7.1.5.4 of the present document.

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

B.5 Next change

4.7.1.5 P-TMSI handling

4.7.1.5.1 P-TMSI handling in A/Gb mode

If a new P-TMSI is assigned by the network the MS and the network shall handle the old and the new P-TMSI as follows:

Upon receipt of a GMM message containing a new P-TMSI the MS shall consider the new P-TMSI and new RAI and also the old P-TMSI and old RAI as valid in order to react to paging requests and downlink transmission of LLC frames. For uplink transmission of LLC frames the new P-TMSI shall be used.

The MS shall consider the old P-TMSI and old RAI as invalid as soon as an LLC frame is received with the local TLLI derived from the new P-TMSI.

Upon the transmission of a GMM message containing a new P-TMSI the network shall consider the new P-TMSI and new RAI and also the old P-TMSI and old RAI as valid in order to be able to receive LLC frames from the MS.

The network shall consider the old P-TMSI and old RAI as invalid as soon as an LLC frame is received with the local TLLI derived from the new P-TMSI.

4.7.1.5.2 P-TMSI handling in Iu mode

If a new P-TMSI is assigned by the network the MS and the network shall handle the old and the new P-TMSI as follows:

Upon receipt of a GMM message containing a new P-TMSI the MS shall consider the new P-TMSI and new RAI as valid. Old P-TMSI and old RAI are regarded as invalid.

The network shall consider the old P-TMSI and old RAI as invalid as soon as an acknowledge message (e.g. ATTACH COMPLETE, ROUTING AREA UPDATE COMPLETE and P-TMSI REALLOCATION COMPLETE) is received.

4.7.1.5.3 P-TMSI handling in S1 mode to Iu mode intersystem change

When initiating a routing area updating procedure as a result of an S1 mode to Iu mode intersystem change, the MS shall handle the P-TMSI as follows:

- If the TIN indicates "GUTI" and the MS holds a valid GUTI, the MS shall indicate the M-TMSI in the P-TMSI IE and the GUMMEI in the Old routing area identification IE. Additionally, if the MS holds a valid P-TMSI and RAI, the MS shall indicate the valid P-TMSI in the Additional mobile identity IE and the RAI in the Additional old routing area identification IE.

- If the TIN indicates "P-TMSI" or "RAT-related TMSI" and the MS holds a valid P-TMSI and a RAI, the MS shall indicate the P-TMSI in the P-TMSI IE and the RAI in the Old routing area identification IE.

Formatted: B1

4.7.1.5.4 P-TMSI handling in S1 mode to A/Gb mode intersystem change

When initiating a routing area updating procedure as a result of an S1 mode to A/Gb mode intersystem change, the MS shall handle the P-TMSI as follows:

- If the TIN indicates "GUTI" and the MS holds a valid GUTI, the MS shall derive a foreign TLLI from the M-TMSI and indicate the GUMMEI in the Old routing area identification IE. Additionally, if the MS holds a valid P-TMSI and a RAI, the MS shall indicate the valid P-TMSI in the Additional mobile identity IE and the RAI in the Additional old routing area identification IE.

- If the TIN indicates "P-TMSI" or "RAT-related TMSI" and the MS holds a valid P-TMSI and a RAI, the MS shall derive a foreign TLLI from the P-TMSI and indicate the RAI in the Old routing area identification IE.

Editor's note: Whether the P-TMSI handling rules in subclauses 4.7.1.5.3 and 4.7.1.5.4 apply to the Attach procedure, and whether these two subclauses will be reorganized into subclause 4.7.5 is FFS.

B.6 Next change

4.7.3.1.3 GPRS attach accepted by the network

If the GPRS attach request is accepted by the network, an ATTACH ACCEPT message is sent to the MS.

The P-TMSI reallocation may be part of the GPRS attach procedure. When the ATTACH REQUEST includes the IMSI, the SGSN shall allocate the P-TMSI. The P-TMSI that shall be allocated is then included in the ATTACH ACCEPT message together with the routing area identifier. The network shall, in this case, change to state GMM-COMMON-PROCEDURE-INITIATED and shall start timer T3350 as described in subclause 4.7.6. Furthermore, the network may assign a P-TMSI signature for the GMM context which is then also included in the ATTACH ACCEPT message. If the LAI or PLMN identity that has been transmitted in the ATTACH ACCEPT message is a member of any of the "forbidden" lists, any such entry shall be deleted. Additionally, the network shall include the radio priority level to be used by the MS for mobile originated SMS transfer in the ATTACH ACCEPT message. In a shared network, the network shall indicate the PLMN identity of the CN operator that has accepted the GPRS attach request in the RAI contained in the ATTACH ACCEPT message (see 3GPP TS 23.251 [109]).

If the MS has indicated in the ATTACH REQUEST message that it supports PS inter-RAT handover to UTRAN Iu mode, the network may include in the ATTACH ACCEPT message a request to provide the Inter RAT information container.

In A/Gb mode, the Cell Notification information element shall be included in the ATTACH ACCEPT message by the network which indicates that the Cell Notification is supported by the network.

In Iu mode, the network should prolong the PS signalling connection if the mobile station has indicated a follow-on request pending in ATTACH REQUEST. The network may also prolong the PS signalling connection without any indication from the mobile terminal.

The MS, receiving an ATTACH ACCEPT message, stores the received routing area identification, stops timer T3310, reset the GPRS attach attempt counter, reset the routing area updating attempt counter, enters state GMM-REGISTERED and sets the GPRS update status to GU1 UPDATED.

If the message contains a P-TMSI, the MS shall use this P-TMSI as the new temporary identity for GPRS services. In this case, an ATTACH COMPLETE message is returned to the network. The MS shall delete its old P-TMSI and shall store the new one. If no P-TMSI has been included by the network in the ATTACH ACCEPT message, the old P-TMSI, if any available, shall be kept.

If the message contains a P-TMSI signature, the MS shall use this P-TMSI signature as the new temporary signature for the GMM context. The MS shall delete its old P-TMSI signature, if any is available, and shall store the new one. If the message contains no P-TMSI signature, the old P-TMSI signature, if available, shall be deleted.

If the network has requested the provision of the Inter RAT information container the MS shall return an ATTACH COMPLETE message including the Inter RAT information container IE to the network.

The network may also send a list of "equivalent PLMNs" in the ATTACH ACCEPT message. Each entry of the list contains a PLMN code (MCC+MNC). The mobile station shall store the list, as provided by the network, except that any PLMN code that is already in the "forbidden PLMN" list shall be removed from the "equivalent PLMNs" list before it is stored by the mobile station. In addition the mobile station shall add to the stored list the PLMN code of the registered PLMN that sent the list. All PLMNs in the stored list shall be regarded as equivalent to each other for PLMN selection, cell selection/re-selection and handover. The stored list in the mobile station shall be replaced on each occurrence of the ATTACH ACCEPT message. If no list is contained in the message, then the stored list in the mobile station shall be deleted. The list shall be stored in the mobile station while switched off so that it can be used for PLMN selection after switch on.

In Iu mode, if the network wishes to prolong the PS signalling connection (for example, if the mobile station has indicated "follow-on request pending" in ATTACH REQUEST message) the network shall indicate the "follow-on proceed" in the ATTACH ACCEPT message. If the network wishes to release the PS signalling connection, the network shall indicate "no follow-on proceed" in the ATTACH ACCEPT message.

After that in Iu mode, the mobile station shall act according to the follow-on proceed flag included in the Attach result information element in the ATTACH ACCEPT message (see subclause 4.7.13).

In A/Gb mode, if the ATTACH ACCEPT message contains the Cell Notification information element, then the MS shall start to use the LLC NULL frame to perform cell updates. The network receiving an ATTACH COMPLETE message stops timer T3350, changes to GMM-REGISTERED state and considers the P-TMSI sent in the ATTACH ACCEPT message as valid.

The network may also send a list of local emergency numbers in the ATTACH ACCEPT, by including the Emergency Number List IE. The mobile equipment shall store the list, as provided by the network, except that any emergency number that is already stored in the SIM/USIM shall be removed from the list before it is stored by the mobile equipment. If there are no emergency numbers stored on the SIM/USIM, then before storing the received list the mobile equipment shall remove from it any emergency number stored permanently in the ME for use in this case (see 3GPP TS 22.101 [8]). The list stored in the mobile equipment shall be replaced on each receipt of a new Emergency Number List IE.

The emergency number(s) received in the Emergency Number List IE are valid only in networks with the same MCC as in the cell on which this IE is received. If no list is contained in the ATTACH ACCEPT message, then the stored list in the mobile equipment shall be kept, except if the mobile equipment has successfully registered to a PLMN with an MCC different from that of the last registered PLMN.

The mobile equipment shall use the stored list of emergency numbers received from the network in addition to the emergency numbers stored on the SIM/USIM or ME to detect that the number dialled is an emergency number.

NOTE: The mobile equipment may use the emergency numbers list to assist the end user in determining whether the dialled number is intended for an emergency service or for another destination, e.g. a local directory service. The possible interactions with the end user are implementation specific.

The list of emergency numbers shall be deleted at switch off and removal of the SIM/USIM. The mobile equipment shall be able to store up to ten local emergency numbers received from the network.

If the ATTACH ACCEPT message contains no ISR indication, the MS shall set the TIN to "P-TMSI".

4.7.3.1.4 GPRS attach not accepted by the network

If the attach request cannot be accepted by the network, an ATTACH REJECT message is transferred to the MS. The MS receiving the ATTACH REJECT message, stops timer T3310 and for all causes except #12, #14 and #15 deletes the list of "equivalent PLMNs".

The MS shall then take one of the following actions depending upon the reject cause:

3 (Illegal MS);

6 (Illegal ME);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The new GMM state is GMM-DEREGISTERED. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed.

If the MS is IMSI attached, the MS shall in addition set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall abort the RR connection, unless an emergency call is ongoing. The SIM/USIM shall be considered as invalid also for non-GPRS services until switching off or the SIM/USIM is removed.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

7 (GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed. The new state is GMM-DEREGISTERED.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

Formatted: Not Highlight

8 (GPRS services and non-GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The new GMM state is GMM-DEREGISTERED.

The MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall abort the RR connection, unless an emergency call is ongoing. The SIM/USIM shall be considered as invalid for GPRS and non-GPRS services until switching off or the SIM/USIM is removed.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

Formatted: Not Highlight

11 (PLMN not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature, and GPRS ciphering key sequence number stored, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to

subclause 4.1.3.2), shall reset the GPRS attach attempt counter and shall change to state GMM-DEREGISTERED.

The MS shall store the PLMN identity in the "forbidden PLMN list".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.
- The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

  An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when attach procedure is rejected with this cause value.

Formatted: Not Highlight

Formatted: Not Highlight

12 (Location area not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2) and shall reset the attach attempt counter. The state is changed to GMM-DEREGISTERED.LIMITED-SERVICE.

The mobile station shall store the LAI in the list of "forbidden location areas for regional provision of service".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.
- The MS shall perform a cell selection according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 1: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

Formatted: Not Highlight

Formatted: Not Highlight

13 (Roaming not allowed in this location area);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2) and shall reset the attach attempt counter. The state is changed to GMM-DEREGISTERED.LIMITED-SERVICE or optionally to GMM-DEREGISTERED.PLMN-SEARCH.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.
- The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

  An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

Formatted: Not Highlight

14 (GPRS services not allowed in this PLMN);

The MS shall delete any RAI, P-TMSI, P-TMSI signature, and GPRS ciphering key sequence number stored, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-DEREGISTERED.

The MS shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list. A GPRS MS operating in MS operation mode C shall perform a PLMN selection instead of a cell selection.

A GPRS MS operating in MS operation mode A or B in network operation mode II or III, is still IMSI attached for CS services in the network.

As an implementation option, a GPRS MS operating in operation mode A or B may perform the following additional action. If no RR connection exists the MS may perform the action immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS may only perform the action when the RR connection is subsequently released:

- The MS may perform a PLMN selection according to 3GPP TS 23.122 [14].

If an MS in GAN mode performs a PLMN selection, it shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

The MS shall not perform the optional PLMN selection in the case where the PLMN providing this reject cause is:

- On the "User Controlled PLMN Selector with Access Technology " list or,
- On the "Operator Controlled PLMN Selector with Access Technology " list or,
- A PLMN identified as equivalent to any PLMN, with the same MCC, contained in the lists above.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

Formatted: Not Highlight

15 (No Suitable Cells In Location Area);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED(and shall store it according to clause 4.1.3.2) and shall reset the attach attempt counter. The state is changed to GMM-DEREGISTERED.LIMITED-SERVICE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.
- The MS shall search for a suitable cell in another location area in the same PLMN according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 2: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

Formatted: Not Highlight

Other values are considered as abnormal cases. The specification of the MS behaviour in those cases is specified in subclause 4.7.3.1.5.

B.7 Next change

4.7.3.2.4 Combined GPRS attach not accepted by the network

If the attach request can neither be accepted by the network for GPRS nor for non-GPRS services, an ATTACH REJECT message is transferred to the MS. The MS receiving the ATTACH REJECT message stops timer T3310, and for all causes except #12, #14 and #15 deletes the list of "equivalent PLMNs".

The MS shall then take one of the following actions depending upon the reject cause:

3 (Illegal MS);

6 (Illegal ME), or

8 (GPRS services and non-GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The new GMM state is GMM-DEREGISTERED. The new MM state is MM IDLE.

The MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number. The SIM/USIM shall be considered as invalid for GPRS and non-GPRS services until switching off or the SIM/USIM is removed.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

7 (GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed. The new GMM state is GMM-DEREGISTERED; the MM state is MM IDLE.

A GPRS MS operating in MS operation mode A or B which is not yet IMSI attached for CS services in the network shall then perform an IMSI attach for non-GPRS services according to the conditions for the MM IMSI attach procedure (see 4.4.3).

A GPRS MS operating in MS operation mode A or B which is already IMSI attached for CS services in the network is still IMSI attached for CS services in the network and shall then proceed with the appropriate MM specific procedure according to the MM service state.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

11 (PLMN not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number stored, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2), shall reset the routing area updating attempt counter and reset the GPRS attach attempt counter and changes to state GMM-DEREGISTERED.

The MS shall set the update status to U3 ROAMING NOT ALLOWED, reset the location update attempt counter and shall delete any TMSI, LAI and ciphering key sequence number. The new MM state is MM IDLE.

The MS shall store the PLMN identity in the "forbidden PLMN list".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

12 (Location area not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED(and shall store it according to clause 4.1.3.2) and shall reset the attach attempt counter. The state is changed to GMM-DEREGISTERED.LIMITED-SERVICE.

The MS shall set the update status to U3 ROAMING NOT ALLOWED, reset the location update attempt counter and shall delete any TMSI, LAI and ciphering key sequence number. The new MM state is MM IDLE.

The MS shall store the LAI in the list of "forbidden location areas for regional provision of service".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

The MS shall perform a cell selection according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 1: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

13 (Roaming not allowed in this location area);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED(and shall store it according to clause 4.1.3.2) and shall reset the attach attempt counter. The state is changed to GMM-DEREGISTERED.LIMITED-SERVICE or optionally to GMM-DEREGISTERED.PLMN-SEARCH.

The MS shall set the update status to U3 ROAMING NOT ALLOWED, reset the location update attempt counter and shall delete any TMSI, LAI and ciphering key sequence number. The new MM state is MM IDLE.

The mobile station shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

14 (GPRS services not allowed in this PLMN);

The MS shall delete any RAI, P-TMSI, P-TMSI signature, and GPRS ciphering key sequence number stored, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-DEREGISTERED.

The MS shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list.

As an implementation option, a GPRS MS operating in operation mode A or B may perform a PLMN selection according to 3GPP TS 23.122 [14].

If an MS in GAN mode performs a PLMN selection, it shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

The MS shall not perform the optional PLMN selection in the case where the PLMN providing this reject cause is:

- On the "User Controlled PLMN Selector with Access Technology " or,
- On the "Operator Controlled PLMN Selector with Access Technology " list or,
- A PLMN identified as equivalent to any PLMN, with the same MCC, contained in the lists above.

If the MS does not perform a PLMN selection then a GPRS MS operating in MS operation mode A or B which is not yet IMSI attached for CS services in the network shall then perform an IMSI attach for non-GPRS services according to the conditions for the MM IMSI attach procedure (see 4.4.3).

A GPRS MS operating in MS operation mode A or B which is already IMSI attached for CS services in the network is still IMSI attached for CS services in the network and shall then proceed with the appropriate MM specific procedure according to the MM service state.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

15 (No Suitable Cells In Location Area);

Formatted: B1

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED(and shall store it according to clause 4.1.3.2) and shall reset the attach attempt counter. The state is changed to GMM-DEREGISTERED.LIMITED-SERVICE.

The MS shall set the update status to U3 ROAMING NOT ALLOWED, reset the location update attempt counter and shall delete any TMSI, LAI and ciphering key sequence number. The new MM state is MM IDLE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

The MS shall search for a suitable cell in another location area in the same PLMN according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 2: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the attach procedure is rejected with this cause value.

Other values are considered as abnormal cases. The specification of the MS behaviour in those cases is specified in subclause 4.7.3.2.5.

B.8 Next change

4.7.4.2 Network initiated GPRS detach procedure

4.7.4.2.1 Network initiated GPRS detach procedure initiation

The network initiates the GPRS detach procedure by sending a DETACH REQUEST message to the MS. The DETACH REQUEST message shall include a detach type IE. In addition, the network may include a cause IE to specify the reason for the detach request. The network shall start timer T3322. If the detach type IE indicates "re-attach not required" or "re-attach required", the network shall deactivate the PDP contexts, the MBMS contexts and deactivate the logical link(s), if any, and shall change to state GMM-DEREGISTERED-INITIATED.

4.7.4.2.2 Network initiated GPRS detach procedure completion by the MS

When receiving the DETACH REQUEST message and the detach type IE indicates "re-attach required", the MS shall deactivate the PDP contexts, the MBMS contexts and deactivate the logical link(s), if any. The MS shall then send a DETACH ACCEPT message to the network and shall change state to GMM-DEREGISTERED. The MS shall, after the completion of the GPRS detach procedure, initiate a GPRS attach procedure. The MS should also activate PDP context(s) to replace any previously active PDP context(s). The MS should also perform the procedures needed in order to activate any previously active multicast service(s).

NOTE 1: In some cases, user interaction may be required and then the MS cannot activate the PDP/MBMS context(s) automatically.

A GPRS MS operating in MS operation mode A or B in network operation mode I, which receives an DETACH REQUEST message with detach type indicating "re-attach required" or "re-attach not required" and no cause code, is only detached for GPRS services in the network.

When receiving the DETACH REQUEST message and the detach type IE indicates "IMSI detach", the MS shall not deactivate the PDP/MBMS contexts. The MS shall set the MM update status to U2 NOT UPDATED. A MS in operation mode A or B in network operation mode I may send a DETACH ACCEPT message to the network, and shall re-attach to non-GPRS service by performing the combined routing area updating procedure according to subclause 4.7.5.2, sending a ROUTING AREA UPDATE REQUEST message with Update type IE indicating "combined RA/LA updating with IMSI attach". A MS in operation mode A that is in an ongoing circuit-switched transaction shall initiate the combined routing area updating after the circuit-switched transaction has been released. A MS in operation mode C, or in MS operation mode A or B in network operation mode II or III, shall send a DETACH ACCEPT message to the network.

If the detach type IE indicates "IMSI detach", or "re-attach required" then the MS shall ignore the cause code if received.

If the detach type information element value indicates "re-attach required" or "re-attach not required" and the MS is attached for GPRS and non-GPRS services and the network operates in network operation mode I, then if in the MS the timer T3212 is not already running, the timer T3212 shall be set to its initial value and restarted.

When receiving the DETACH REQUEST message and the detach type IE indicates "re-attach not required" and the cause code is not "#2 (IMSI unknown in HLR)", the MS shall deactivate the PDP contexts, the MBMS contexts and deactivate the logical link(s), if any. The MS shall then send a DETACH ACCEPT message to the network and shall change state to GMM-DEREGISTERED.

If the detach type IE indicates "re-attach not required", then, depending on the received cause code, the MS shall act as follows:

2 (IMSI unknown in HLR);

The MS shall set the update status to U3 ROAMING NOT ALLOWED and shall delete any TMSI, LAI and ciphering key sequence number. The new MM state is MM IDLE. The SIM/USIM shall be considered as invalid for non-GPRS services until switching off or the SIM/USIM is removed.

A GPRS MS operating in MS operation mode A or B in network operation mode I, is still IMSI attached for GPRS services in the network.

3 (Illegal MS);

6 (Illegal ME);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The new GMM state is GMM-DEREGISTERED. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed.

A GPRS MS operating in MS operation mode A or B shall in addition set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall abort the RR connection, unless an emergency call is ongoing. The SIM/USIM shall be considered as invalid also for non-GPRS services until switching off or the SIM/USIM is removed.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

NOTE: The possibility to configure a UE so that the radio transceiver for a specific radio access technology is not active, although it is implemented in the UE, is out of scope of the present specification.

7 (GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed. The new state is GMM-DEREGISTERED.

A GPRS MS operating in MS operation mode A or B in network operation mode I shall set the timer T3212 to its initial value and restart it, if it is not already running.

A GPRS MS operating in MS operation mode A or B in network operation mode I, is still IMSI attached for CS services in the network.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

8 (GPRS services and non-GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The new GMM state is GMM-DEREGISTERED.

The MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall abort the RR connection, unless an emergency call is ongoing. The SIM/USIM shall be considered as invalid for GPRS and non-GPRS services until switching off or the SIM/USIM is removed.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

11 (PLMN not allowed);

The MS shall delete any RAI or LAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2). The new GMM state is GMM-DEREGISTERED.

The MS shall store the PLMN identity in the "forbidden PLMN list".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- A GPRS MS operating in MS operation mode A or B shall set the update status to U3 ROAMING NOT ALLOWED and shall delete any TMSI, LAI and ciphering key sequence number. The new MM state is MM IDLE.

- The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

12 (Location area not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED(and shall store it according to clause 4.1.3.2) and shall reset the attach attempt counter. The state is changed to GMM-DEREGISTERED.LIMITED-SERVICE.

The MS shall store the LAI in the list of "forbidden location areas for regional provision of service".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.

- The MS shall perform a cell selection according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 2: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

13 (Roaming not allowed in this location area);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2) and shall reset the attach attempt counter. The state is changed to GMM-DEREGISTERED.LIMITED-SERVICE or optionally to GMM-DEREGISTERED.PLMN-SEARCH.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.

- The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

Formatted: Not Highlight

Formatted: Not Highlight

14 (GPRS services not allowed in this PLMN);

The MS shall delete any RAI, P-TMSI, P-TMSI signature, and GPRS ciphering key sequence number stored, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-DEREGISTERED.

The MS shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list.

A GPRS MS operating in MS operation mode A or B in network operation mode I shall set the timer T3212 to its initial value and restart it, if it is not already running.

A GPRS MS operating in MS operation mode A or B, is still IMSI attached for CS services in the network.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

15 (No Suitable Cells In Location Area);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED(and shall store it according to clause 4.1.3.2) and shall reset the attach attempt counter. The state is changed to GMM-DEREGISTERED.LIMITED-SERVICE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.

- The MS shall search for a suitable cell in another location area in the same PLMN according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 3: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state and EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

Formatted: Not Highlight

Formatted: Not Highlight

Other cause values shall not impact the update status. Further actions of the MS are implementation dependent.

B.9 Next change

4.7.5 Routing area updating procedure

This procedure is used for:

- normal routing area updating to update the registration of the actual routing area of an MS in the network. This procedure is used by GPRS MSs in MS operation mode C and by GPRS MSs in MS operation modes A or B that are IMSI attached for GPRS and non-GPRS services if the network operates in network operation mode II or III;

- combined routing area updating to update the registration of the actual routing and location area of an MS in the network. This procedure is used by GPRS MSs in MS operation modes A or B that are IMSI attached for GPRS and non-GPRS services provided that the network operates in network operation mode I;

- periodic routing area updating. This procedure is used by GPRS MSs in MS operation mode C and by GPRS MSs in MS operation modes A or B that are IMSI attached for GPRS or for GPRS and non-GPRS services independent of the network operation mode;

- IMSI attach for non-GPRS services when the MS is IMSI attached for GPRS services. This procedure is used by GPRS MSs in MS operation modes A or B, if the network operates in network operation mode I;

- in A/Gb mode, resuming GPRS services when the RR sublayer indicated a resumption failure after dedicated mode was left, see 3GPP TS 44.018 [84]

- in A/Gb mode, updating the network with the new MS Radio Access Capability IE when the content of the IE has changed;

- updating the network with the new DRX parameter IE when the content of the IE has changed

NOTE 1: Such changes can be used e.g. when the MS activates a PDP context with service requirements that cannot be met with the current DRX parameter. As PDP context(s) are activated and deactivated, the GMM context will be updated with an appropriate DRX parameter;

- re-negotiation of the READY timer value;

- Iu mode to A/Gb mode and for A/Gb mode to Iu mode intersystem change, see subclause 4.7.1.7; ~~or~~

- in Iu mode, to re-synchronize the PMM mode of MS and network after RRC connection release with cause "Directed signalling connection re-establishment", see subclause 4.7.2.5;~~.~~

- S1 mode to Iu mode or S1 mode to A/Gb mode intersystem change and ISR is not activated; or

- S1 mode to Iu mode or S1 mode to A/Gb mode intersystem change and ISR is activated, but the MS changes to a routeing area it has not previously registered with the network.

The routing area updating procedure shall also be used by a MS which is attached for GPRS services if a new PLMN is entered (see 3GPP TS 23.122 [14]).

Subclause 4.7.5.1 describes the routing area updating procedures for updating the routing area only. The combined routing area updating procedure used to update both the routing and location area is described in subclause 4.7.5.2.

The routing area updating procedure is always initiated by the MS. It is only invoked in state GMM-REGISTERED.

To limit the number of subsequently rejected routing area update attempts, a routing area updating attempt counter is introduced. The routing area updating attempt counter shall be incremented as specified in subclause 4.7.5.1.5. Depending on the value of the routing area updating attempt counter, specific actions shall be performed. The routing area updating attempt counter shall be reset when:

- a GPRS attach procedure is successfully completed; or

- a routing area updating procedure is successfully completed;

and additionally when the MS is in substate ATTEMPTING-TO-UPDATE:

- a new routing area is entered;
- expiry of timer T3302; or
- at request from registration function.

The mobile equipment shall contain a list of "forbidden location areas for roaming", as well as a list of "forbidden location areas for regional provision of service". The handling of these lists is described in subclause 4.4.1.

The Mobile Equipment shall contain a list of "equivalent PLMNs". The handling of this list is described in subclause 4.4.1.

In a shared network, the MS shall choose one of the PLMN identities as specified in 3GPP TS 23.122 [14]. The MS shall construct the Routing Area Identification of the cell from this chosen PLMN identity, and the LAC and the RAC received on the BCCH. If the constructed RAI is different from the stored RAI, the MS shall initiate the routing area updating procedure. The chosen PLMN identity shall be indicated to the RAN in the RRC INITIAL DIRECT TRANSFER message (see 3GPP TS 25.331 [23c]). Whenever a ROUTING AREA UPDATING REJECT message with the cause "PLMN not allowed" is received by the MS, the chosen PLMN identity shall be stored in the "forbidden PLMN list". Whenever a ROUTING AREA UPDATING REJECT message is received by the MS with the cause "Roaming not allowed in this location area", "Location Area not allowed", or "No suitable cells in Location Area", the LAI that is part of the constructed RAI which triggered the routing area updating procedure shall be stored in the suitable list.

In A/Gb mode, user data transmission in the MS shall be suspended during the routing area updating procedure, except if the routing area updating procedure is triggered by a PS handover procedure as described in 3GPP TS 43.129 [113]; user data reception shall be possible. User data transmission in the network may be suspended during the routing area updating procedure.

In Iu mode, user data transmission and reception in the MS shall not be suspended during the routing area updating procedure. User data transmission in the network shall not be suspended during the routing area updating procedure.

In Iu mode, when a ROUTING AREA UPDATE REQUEST is received by the SGSN over a new PS signalling connection while there is an ongoing PS signalling connection (network is already in mode PMM-CONNECTED) for this UE, the network shall progress the routing area update procedure as normal and release the previous PS signalling connection when the routing area update procedure has been accepted by the network.

NOTE 2: The re-establishment of the radio bearers of active PDP contexts is done as described in subclause "Service Request procedure".

The network informs the MS about the support of specific features, such as LCS-MOLR or MBMS, in the "Network feature support" Information Element. The information is either explicitly given by sending the "Network feature support" IE or implicitly by not sending it. The handling in the network is described in subclause 9.4.15.11. The MS may use the indication to inform the user about the availability of the appropriate services and it shall not request services that have not been indicated as available. The indication for MBMS is defined in subclause "MBMS feature support indication" in 3GPP TS 23.246 [106].

B.10 Next change

4.7.5.1.1 Normal and periodic routing area updating procedure initiation

To initiate the normal routing area updating procedure, the MS sends the message ROUTING AREA UPDATE REQUEST to the network, starts timer T3330 and changes to state GMM-ROUTING-AREA-UPDATING-INITIATED. The message ROUTING AREA UPDATE REQUEST shall contain the P-TMSI signature when received within a previous ATTACH ACCEPT or ROUTING AREA UPDATE ACCEPT message.

In Iu mode, if the MS wishes to prolong the established PS signalling connection after the normal routing area updating procedure (for example, the MS has any CM application request pending), it may set a follow-on request pending indicator on (see subclause 4.7.13).

4.7.5.1.2 GMM Common procedure initiation

Upon receiving the ROUTING AREA UPDATE REQUEST message containing the P-TMSI IE and the Additional mobile identity IE with same encoded mobile identity type, but indicating different mobile identities, the network shall regard the first mobile identity type as an M-TMSI and the second Mobile identity IE as a P-TMSI.

The network may initiate GMM common procedures, e.g. the GMM authentication and ciphering procedure.

4.7.5.1.3 Normal and periodic routing area updating procedure accepted by the network

If the routing area updating request has been accepted by the network, a ROUTING AREA UPDATE ACCEPT message shall be sent to the MS. The network may assign a new P-TMSI and/or a new P-TMSI signature for the MS. If a new P-TMSI and/or P-TMSI signature have been assigned to the MS, it/they shall be included in the ROUTING AREA UPDATE ACCEPT message together with the routing area identification. In a shared network the network shall indicate the PLMN identity of the CN operator that has accepted the routing area updating request in the RAI contained in the ROUTING AREA UPDATE ACCEPT message (see 3GPP TS 23.251 [109]).

If a new DRX parameter was included in the ROUTING AREA UPDATE REQUEST message, the network shall store the new DRX parameter and use it for the downlink transfer of signalling and user data.

If the MS has indicated in the ROUTING AREA UPDATE REQUEST message that it supports PS inter-RAT handover to UTRAN Iu mode, the network may include in the ROUTING AREA UPDATE ACCEPT message a request to provide the Inter RAT information container.

In A/Gb mode the Cell Notification information element shall be included in the ROUTING AREA UPDATE ACCEPT message in order to indicate the ability of the network to support the Cell Notification.

The network shall change to state GMM-COMMON-PROCEDURE-INITIATED and shall start the supervision timer T3350 as described in subclause 4.7.6.

If the LAI or PLMN identity contained in the ROUTING AREA UPDATE ACCEPT message is a member of any of the "forbidden" lists then any such entry shall be deleted.

In Iu mode, the network should prolong the PS signalling connection if the mobile station has indicated a follow-on request pending in ROUTING AREA UPDATE REQUEST. The network may also prolong the PS signalling connection without any indication from the mobile terminal.

If the PDP context status information element is included in ROUTING AREA UPDATE REQUEST message, then the network shall deactivate all those PDP contexts locally (without peer to peer signalling between the MS and the network), which are not in SM state PDP-INACTIVE on network side but are indicated by the MS as being in state PDP-INACTIVE.

If the MBMS context status information element is included in the ROUTING AREA UPDATE REQUEST message, then the network shall deactivate all those MBMS contexts locally (without peer to peer signalling between the MS and network) which are not in SM state PDP-INACTIVE on the network side, but are indicated by the MS as being in state PDP-INACTIVE. If no MBMS context status information element is included, then the network shall deactivate all MBMS contexts locally which are not in SM state PDP-INACTIVE on the network side.

Upon receipt of a ROUTING AREA UPDATE ACCEPT message, the MS stores the received routing area identification, stops timer T3330, shall reset the routing area updating attempt counter and sets the GPRS update status to GU1 UPDATED. If the message contains a P-TMSI, the MS shall use this P-TMSI as new temporary identity for GPRS services and shall store the new P-TMSI. If no P-TMSI was included by the network in the ROUTING AREA UPDATING ACCEPT message, the old P-TMSI shall be kept. Furthermore, the MS shall store the P-TMSI signature if received in the ROUTING AREA UPDATING ACCEPT message. If no P-TMSI signature was included in the message, the old P-TMSI signature, if available, shall be deleted.

If the ROUTING AREA UPDATE REQUEST message was used to update the network with a new DRX parameter IE, the MS shall start using the new DRX parameter upon receipt of the ROUTING AREA UPDATE ACCEPT message.

If the PDP context status information element is included in ROUTING AREA UPDATE ACCEPT message, then the MS shall deactivate all those PDP contexts locally (without peer to peer signalling between the MS and network), which are not in SM state PDP-INACTIVE in the MS but are indicated by the network as being in state PDP-INACTIVE.

If the MBMS context status information element is included in the ROUTING AREA UPDATE ACCEPT message, then the MS shall deactivate all those MBMS contexts locally (without peer to peer signalling between the MS and network) which are not in SM state PDP-INACTIVE in the MS, but are indicated by the network as being in state PDP-INACTIVE. If no MBMS context status information element is included, then the MS shall deactivate all those MBMS contexts locally which are not in SM state PDP-INACTIVE in the MS.

In A/Gb mode, if the ROUTING AREA UPDATE ACCEPT message contains the Cell Notification information element, then the MS shall start to use the LLC NULL frame to perform cell updates.

The network may also send a list of "equivalent PLMNs" in the ROUTING AREA UPDATE ACCEPT message. Each entry of the list contains a PLMN code (MCC+MNC). The mobile station shall store the list, as provided by the network, except that any PLMN code that is already in the "forbidden PLMN" list shall be removed from the "equivalent PLMNs" list before it is stored by the mobile station. In addition the mobile station shall add to the stored list the PLMN code of the registered PLMN that sent the list. All PLMNs in the stored list shall be regarded as equivalent to each other for PLMN selection, cell selection/re-selection and handover. The stored list in the mobile station shall be replaced on each occurrence of the ROUTING AREA UPDATE ACCEPT message. If no list is contained in the message, then the stored list in the mobile station shall be deleted. The list shall be stored in the mobile station while switched off so that it can be used for PLMN selection after switch on.

A ROUTING AREA UPDATE COMPLETE message shall be returned to the network if the ROUTING AREA UPDATE ACCEPT message contained any of:

- a P-TMSI;
- Receive N-PDU Numbers (see 3GPP TS 44.065 [78] and 3GPP TS 25.322); or
- a request for the provision of the Inter RAT information container.

If Receive N-PDU Numbers were included, the Receive N-PDU Numbers values valid in the MS, shall be included in the ROUTING AREA UPDATE COMPLETE message.

If the network has requested the provision of the Inter RAT information container the MS shall return a ROUTING AREA UPDATE COMPLETE message including the Inter RAT information container IE to the network.

NOTE 1: In Iu mode, after a routing area updating procedure, the mobile station can initiate Service Request procedure to request the resource reservation for the active PDP contexts if the resources have been released by the network or send upper layer message (e.g. ACTIVATE PDP CONTEXT REQUEST) to the network via the existing PS signaling connection.

In Iu mode, if the network wishes to prolong the PS signalling connection (for example, if the mobile station has indicated "follow-on request pending" in ROUTING AREA UPDATE REQUEST message) the network shall indicate the "follow-on proceed" in the ROUTING AREA UPDATE ACCEPT message. If the network wishes to release the PS signalling connection, the network shall indicate "no follow-on proceed" in the ROUTING AREA UPDATE ACCEPT message.

After that in Iu mode, the mobile station shall act according to the follow-on proceed flag included in the Update result information element in the ROUTING AREA UPDATE ACCEPT message (see subclause 4.7.13).

The network may also send a list of local emergency numbers in the ROUTING AREA UPDATE ACCEPT, by including the Emergency Number List IE. The mobile equipment shall store the list, as provided by the network, except that any emergency number that is already stored in the SIM/USIM shall be removed from the list before it is stored by the mobile equipment. If there are no emergency numbers stored on the SIM/USIM, then before storing the received list the mobile equipment shall remove from it any emergency number stored permanently in the ME for use in this case (see 3GPP TS 22.101 [8]). The list stored in the mobile equipment shall be replaced on each receipt of a new Emergency Number List IE.

The emergency number(s) received in the Emergency Number List IE are valid only in networks with the same MCC as in the cell on which this IE is received. If no list is contained in the ROUTING AREA UPDATE ACCEPT message, then the stored list in the mobile equipment shall be kept, except if the mobile equipment has successfully registered to a PLMN with an MCC different from that of the last registered PLMN.

The mobile equipment shall use the stored list of emergency numbers received from the network in addition to the emergency numbers stored on the SIM/USIM or ME to detect that the number dialled is an emergency number.

NOTE 2: The mobile equipment may use the emergency numbers list to assist the end user in determining whether the dialled number is intended for an emergency service or for another destination, e.g. a local directory service. The possible interactions with the end user are implementation specific.

The list of emergency numbers shall be deleted at switch off and removal of the SIM/USIM. The mobile equipment shall be able to store up to ten local emergency numbers received from the network.

In order to indicate to the MS that the GUTI and TAI list assigned to the MS remain registered with the network and are valid in the MS, the network shall include the ISR indication IE in the ROUTING AREA UPDATE ACCEPT message.

If the ROUTING AREA UPDATE ACCEPT message contains

i) no ISR indication, the MS shall set the TIN to "P-TMSI"; or

ii) an ISR indication, the MS shall regard the available GUTI and TAI list as valid and registered with the network and clear the GUTI update status, and

- if the TIN currently indicates "P-TMSI", the MS shall set the TIN to "P-TMSI"; or

- if the TIN currently indicates "GUTI" or "RAT-related TMSI", the MS shall set the TIN to "RAT-related TMSI".

Formatted: B2

4.7.5.1.4 Normal and periodic routing area updating procedure not accepted by the network

If the routing area updating cannot be accepted, the network sends a ROUTING AREA UPDATE REJECT message to the MS. An MS that receives a ROUTING AREA UPDATE REJECT message, stops timer T3330, and for all causes except #12, #14 and #15 deletes the list of "equivalent PLMNs". If a ROUTING AREA UPDATE REJECT message is received, the MS shall stop any ongoing transmission of user data.

The MS shall then take different actions depending on the received reject cause value:

3 (Illegal MS);

6 (Illegal ME);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED. Furthermore, it shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number and shall consider the SIM/USIM as invalid for GPRS services until switching off or the SIM/USIM is removed.

If the MS is IMSI attached, the MS shall in addition set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall abort the RR connection, unless an emergency call is ongoing. The SIM/USIM shall be considered as invalid also for non-GPRS services until switching off or the SIM/USIM is removed.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

NOTE: The possibility to configure a UE so that the radio transceiver for a specific radio access technology is not active, although it is implemented in the UE, is out of scope of the present specification.

7 (GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2.9) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed. The new state is GMM-DEREGISTERED.

If the update type is "periodic updating" a GPRS MS operating in MS operation mode A or B in networkoperation mode I shall set the timer T3212 to its initial value and restart it, if it is not already running.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

9 (MS identity cannot be derived by the network);

The MS shall set the GPRS update status to GU2 NOT UPDATED (and shall store it according to subclause 4.1.3.2), enter the state GMM-DEREGISTERED, and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. Subsequently, the MS may automatically initiate the GPRS attach procedure.

10 (Implicitly detached);

The MS shall change to state GMM-DEREGISTERED.NORMAL-SERVICE. The MS shall then perform a new attach procedure. The MS should also activate PDP context(s) to replace any previously active PDP contexts. The MS should also perform the procedures needed in order to activate any previously active multicast service(s).

NOTE 1: In some cases, user interaction may be required and then the MS cannot activate the PDP and MBMS context(s) automatically.

11 (PLMN not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED.

The MS shall store the PLMN identity in the "forbidden PLMN list".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED and shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.

- The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

  An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

12 (Location area not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2), shall reset the routing area updating attempt counter and shall change to state GMM-DEREGISTERED.LIMITED-SERVICE.

Editor's note: The equivalent behaviour for cause #12 for EMM as described in 3GPP TS 24.301 [117] may be changed if RAN2 is going to abandon the additional cell re-selection hysteresis at tracking area boundaries. In that case, the behaviour described above for GMM may need to be aligned, i.e. the MS could remain in REGISTERED state and P-TMSI could be kept.

The mobile station shall store the LAI in the list of "forbidden location areas for regional provision of service".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.

- The MS shall perform a cell selection according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 2: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

Formatted: Not Highlight

Formatted: Not Highlight

13 (Roaming not allowed in this location area);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2) shall reset the routing area updating attempt counter and shall change to state GMM-REGISTERED.LIMITED-SERVICE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.

- The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

  An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state and EPS update status as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

Formatted: Not Highlight

14 (GPRS services not allowed in this PLMN);

The MS shall delete any RAI, P-TMSI, P-TMSI signature, and GPRS ciphering key sequence number stored, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-DEREGISTERED.

The MS shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list. A GPRS MS operating in MS operation mode C shall perform a PLMN selection instead of a cell selection.

If the update type is "periodic updating" a GPRS MS operating in MS operation mode A or B in network operation mode I shall set the timer T3212 to its initial value and restart it, if it is not already running.

A GPRS MS operating in MS operation mode A or B in network operation mode II or III, is still IMSI attached for CS services in the network.

As an implementation option, a GPRS MS operating in operation mode A or B may perform the following additional action. If no RR connection exists the MS may perform the action immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS may only perform the action when the RR connection is subsequently released:

- The MS may perform a PLMN selection according to 3GPP TS 23.122 [14].

If an MS in GAN mode performs a PLMN selection, it shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

The MS shall not perform the optional PLMN selection in the case where the PLMN providing this reject cause is:

- On the "User Controlled PLMN Selector with Access Technology " or,
- On the "Operator Controlled PLMN Selector with Access Technology " list or,
- A PLMN identified as equivalent to any PLMN, with the same MCC, contained in the lists above.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

15 (No Suitable Cells In Location Area);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2) shall reset the routing area updating attempt counter and shall change to state GMM-REGISTERED.LIMITED-SERVICE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

- If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.
- The MS shall search for a suitable cell in another location area in the same PLMN according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 3: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state and EPS update status as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

Formatted: Not Highlight

Formatted: Not Highlight

Other values are considered as abnormal cases. The specification of the MS behaviour in those cases is described in subclause 4.7.5.1.5.

B.11 Next change

4.7.5.2.4 Combined routing area updating not accepted by the network

If the combined routing area updating cannot be accepted, the network sends a ROUTING AREA UPDATE REJECT message to the MS. An MS that receives a ROUTING AREA UPDATE REJECT message stops timer T3330, enters state MM IDLE, and for all causes except #12, #14 and #15 deletes the list of "equivalent PLMNs". If a ROUTING AREA UPDATE REJECT message is received, the MS shall stop any ongoing transmission of user data.

The MS shall then take different actions depending on the received reject cause:

3 (Illegal MS);

6 (Illegal ME), or

8 (GPRS services and non GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED and the update status to U3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED. Furthermore, it shall delete any P-TMSI, P-TMSI signature, TMSI, RAI, LAI, ciphering key sequence number and GPRS ciphering key sequence number and shall consider the SIM/USIM as invalid for GPRS and non GPRS services until switching off or the SIM/USIM is removed.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

7 (GPRS services not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed. The new state is GMM-DEREGISTERED. If in the MS the timer T3212 is not already running, the timer shall be set to its initial value and restarted.

A GPRS MS operating in MS operation mode A or B in network operation mode I, is still IMSI attached for CS services in the network. and shall then proceed with the appropriate MM specific procedure according to the MM service state.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

9 (MS identity cannot be derived by the network);

The MS shall set the GPRS update status to GU2 NOT UPDATED (and shall store it according to subclause 4.1.3.2), enter the state GMM-DEREGISTERED, and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. Subsequently, the MS may automatically initiate the GPRS attach procedure.

A GPRS MS operating in MS operation mode A or B in network operation mode I, is still IMSI attached for CS services in the network.

10 (Implicitly detached);

A GPRS MS operating in MS operation mode A or B in network operation mode I, is IMSI detached for both GPRS and CS services in the network.

The MS shall change to state GMM-DEREGISTERED.NORMAL-SERVICE. The MS shall then perform a new attach procedure. The MS should also activate PDP context(s) to replace any previously active PDP context(s). The MS should also perform the procedures needed in order to activate any previously active multicast service(s).

NOTE 1: In some cases, user interaction may be required and then the MS cannot activate the PDP/MBMS context(s) automatically.

11 (PLMN not allowed);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED and the update status to U3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED. Furthermore, it shall delete any P-TMSI, P-TMSI signature, TMSI, RAI, LAI, ciphering key sequence number GPRS ciphering key sequence number, and reset the location update attempt counter.

The MS shall store the PLMN identity in the "forbidden PLMN list".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

The MS shall then perform a PLMN selection according to 3GPP TS 23.122 [14].

An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

12 (Location area not allowed);

The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2), shall reset the routing area updating attempt counter and shall change to state GMM-DEREGISTERED.LIMITED-SERVICE.

Editor's note: The equivalent behaviour for cause #12 for EMM as described in 3GPP TS 24.301 [117] may be changed if RAN2 is going to abandon the additional cell re-selection hysteresis at tracking area boundaries. In that case, the behaviour described above for GMM may need to be aligned, i.e. the MS could remain in REGISTERED state and P-TMSI could be kept.

The MS shall in addition set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.

The mobile station shall store the LAI in the list of "forbidden location areas for regional provision of service".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

The MS shall perform a cell selection according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 2: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

13 (Roaming not allowed in this location area);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2), shall reset the routing area updating attempt counter and shall change to state GMM-REGISTERED.LIMITED-SERVICE.

The MS shall in addition set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

The MS shall indicate the Update type IE "combined RA/LA updating with IMSI attach" when performing the routing area updating procedure following the PLMN selection.

An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state and EPS update status as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

Formatted: Not Highlight

14 (GPRS services not allowed in this PLMN);

The MS shall delete any RAI, P-TMSI, P-TMSI signature, and GPRS ciphering key sequence number stored, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-DEREGISTERED. If in the MS the timer T3212 is not already running, the timer shall be set to its initial value and restarted.

The MS shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list.

A GPRS MS operating in MS operation mode A or B in network operation mode I, is still IMSI attached for CS services in the network and shall then proceed with the appropriate MM specific procedure according to the MM service state.

As an implementation option, a GPRS MS operating in operation mode A or B may perform a PLMN selection according to 3GPP TS 23.122 [14].

If an MS in GAN mode performs a PLMN selection, it shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

The MS shall not perform the optional PLMN selection in the case where the PLMN providing this reject cause is:

- On the "User Controlled PLMN Selector with Access Technology " or,
- On the "Operator Controlled PLMN Selector with Access Technology " list or,
- A PLMN identified as equivalent to any PLMN, with the same MCC, contained in the lists above.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

15 (No Suitable Cells In Location Area);

The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to clause 4.1.3.2), shall reset the routing area updating attempt counter and shall change to state GMM-REGISTERED.LIMITED-SERVICE.

The MS shall in addition set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.

The MS shall store the LAI in the list of "forbidden location areas for roaming".

The MS shall start timer T3340 as described in subclause 4.7.1.9.

The MS shall search for a suitable cell in another location area in the same PLMN according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 3: The cell selection procedure is not applicable for an MS in GAN mode.

The MS shall indicate the Update type IE "combined RA/LA updating with IMSI attach" when performing the routing area updating procedure.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state and EPS update status as specified in 3GPP TS 24.301 [117] for the case when the tracking area update procedure is rejected with this cause value.

Formatted: Not Highlight

Formatted: Not Highlight

Other values are considered as abnormal cases. The specification of the MS behaviour in those cases is described in subclause 4.7.5.2.5.

B.12 Next change

4.7.13.4 Service request procedure not accepted by the network

Formatted: Indent: Left: 0 cm, Hanging: 2,5 cm

If the Service request cannot be accepted, the network returns a SERVICE REJECT message to the mobile station. An MS that receives a SERVICE REJECT message stops timer T3317. The MS shall then take different actions depending on the received reject cause value:

3 (Illegal MS); or

6 (Illegal ME);

- The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED. Furthermore, it shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number and shall consider the SIM/USIM as invalid for GPRS services until switching off or the SIM/USIM is removed.

- A GPRS MS operating in MS operation mode A shall in addition set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall abort the RR connection, unless an emergency call is ongoing. The SIM/USIM shall be considered as invalid also for non-GPRS services until switching off or the SIM/USIM is removed.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the service request procedure is rejected with this cause value.

7 (GPRS services not allowed);

- The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2.9) and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. The SIM/USIM shall be considered as invalid for GPRS services until switching off or the SIM/USIM is removed. The new state is GMM-DEREGISTERED.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the service request procedure is rejected with this cause value.

9 (MS identity cannot be derived by the network);

- The MS shall set the GPRS update status to GU2 NOT UPDATED (and shall store it according to subclause 4.1.3.2), enter the state GMM-DEREGISTERED, and shall delete any P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number. Subsequently, the MS may automatically initiate the GPRS attach procedure.

10 (Implicitly detached);

- The MS shall change to state GMM-DEREGISTERED.NORMAL-SERVICE. The MS shall then perform a new attach procedure. The MS should also activate PDP context(s) to replace any previously active PDP contexts. The MS should also perform the procedures needed in order to activate any previously active multicast service(s).

NOTE 1: In some cases, user interaction may be required and then the MS cannot activate the PDP and MBMS context(s) automatically.

11 (PLMN not allowed);

- The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and enter the state GMM-DEREGISTERED.

- The MS shall store the PLMN identity in the "forbidden PLMN list".

  The MS shall start timer T3340 as described in subclause 4.7.1.9.

- If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

  - A GPRS MS operating in MS operation mode A shall set the update status to U3 ROAMING NOT ALLOWED and shall delete any TMSI, LAI and ciphering key sequence number. The new MM state is MM IDLE.

- The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

  An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the service request procedure is rejected with this cause value.

12 (Location area not allowed);

- The MS shall delete any RAI, P-TMSI, P-TMSI signature and GPRS ciphering key sequence number, shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-DEREGISTERED.LIMITED-SERVICE.
- The mobile station shall store the LAI in the list of "forbidden location areas for regional provision of service".

  The MS shall start timer T3340 as described in subclause 4.7.1.9.
- If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:
  - If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED, shall delete any TMSI, LAI and ciphering key sequence number and shall reset the location update attempt counter. The new MM state is MM IDLE.
  - The MS shall perform a cell selection according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 2: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state, EPS update status, GUTI, last visited registered TAI, TAI list and KSI as specified in 3GPP TS 24.301 [117] for the case when the service request procedure is rejected with this cause value.

13 (Roaming not allowed in this location area);

- The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-REGISTERED.LIMITED-SERVICE.
- The MS shall store the LAI in the list of "forbidden location areas for roaming".

  The MS shall start timer T3340 as described in subclause 4.7.1.9.
- If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:
  - If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.
  - The MS shall perform a PLMN selection according to 3GPP TS 23.122 [14].

    An MS in GAN mode shall request a PLMN list in GAN (see 3GPP TS 44.318 [76b]) prior to perform a PLMN selection from this list according to 3GPP TS 23.122 [14].

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state and EPS update status as specified in 3GPP TS 24.301 [117] for the case when the service request procedure is rejected with this cause value.

15 (No Suitable Cells In Location Area);

- The MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED (and shall store it according to subclause 4.1.3.2) and shall change to state GMM-REGISTERED.LIMITED-SERVICE.

- The MS shall store the LAI in the list of "forbidden location areas for roaming".

  The MS shall start timer T3340 as described in subclause 4.7.1.9.

- If no RR connection exists, the MS shall perform the following additional actions immediately. If the MS is operating in MS operation mode A and an RR connection exists, the MS shall perform these actions when the RR connection is subsequently released:

  - If the MS is IMSI attached, the MS shall set the update status to U3 ROAMING NOT ALLOWED and shall reset the location update attempt counter. The new MM state is MM IDLE.

  - The MS shall search for a suitable cell in another location area in the same PLMN according to 3GPP TS 43.022 [82] and 3GPP TS 25.304 [98].

NOTE 3: The cell selection procedure is not applicable for an MS in GAN mode.

If S1 mode is supported in the UE, the UE shall handle the EMM parameters EMM state and EPS update status as specified in 3GPP TS 24.301 [117] for the case when the service request procedure is rejected with this cause value.

40 (No PDP context activated)

- The MS shall deactivate locally all active PDP and MBMS contexts and the MS shall enter the state GMM-REGISTERED.NORMAL-SERVICE. The MS may also activate PDP context(s) to replace any previously active PDP contexts. The MS may also perform the procedures needed in order to activate any previously active multicast service(s).

NOTE 4: In some cases, user interaction may be required and then the MS cannot activate the PDP and MBMS context(s) automatically.

Other values are considered as abnormal cases. The specification of the MS behaviour in those cases is described in subclause 4.7.13.5.

B.13 Next change

9.4.14 Routing area update request

This message is sent by the MS to the network either to request an update of its location file or to request an IMSI attach for non-GPRS services. See table 9.4.14/3GPP TS 24.008.

Message type: ROUTING AREA UPDATE REQUEST

Significance: dual

Direction: MS to network

Table 9.4.14/3GPP TS 24.008: ROUTING AREA UPDATE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Routing area update request message identity	Message type 10.4	M	V	1
	Update type	Update type 10.5.5.18	M	V	1/2
	GPRS ciphering key sequence number	Ciphering key sequence number 10.5.1.2	M	V	1/2
	Old routing area identification	Routing area identification 10.5.5.15	M	V	6
	MS Radio Access capability	MS Radio Access capability 10.5.5.12a	M	LV	6 - 52
19	Old P-TMSI signature	P-TMSI signature 10.5.5.8	O	TV	4
17	Requested READY timer value	GPRS Timer 10.5.7.3	O	TV	2
27	DRX parameter	DRX parameter 10.5.5.6	O	TV	3
9-	TMSI status	TMSI status 10.5.5.4	O	TV	1
18	P-TMSI	Mobile identity 10.5.1.4	O	TLV	7
31	MS network capability	MS network capability 10.5.5.12	O	TLV	4-10
32	PDP context status	PDP context status 10.5.7.1	O	TLV	4
33	PS LCS Capability	PS LCS Capability 10.5.5.22	O	TLV	3
35	MBMS context status	MBMS context status 10.5.7.6	O	TLV	2 - 18
xx	Additional Mobile identity	Mobile identity 10.5.1.4	O	TLV	7
yy	Additional old routing area identification	Routing area identification 10.5.5.15	O	TV	7

9.4.14.1 Old P-TMSI signature

This IE is included by the MS if it was received from the network in an ATTACH ACCEPT or ROUTING AREA UPDATE ACCEPT message.

9.4.14.2 Requested READY timer value

This IE may be included if the MS wants to indicate a preferred value for the READY timer.

9.4.14.3 DRX parameter

This IE shall be included if the MS changes the access network from GSM to UMTS, or the MS wants to indicate new DRX parameters to the network.

9.4.14.4 TMSI status

This IE shall be included if the MS performs a combined routing area update and no valid TMSI is available.

9.4.14.5 P-TMSI (UMTS only)

This IE shall be included by the MS.

9.4.14.6 MS network capability

This IE shall be included by the MS to indicate it's capabilities to the network.

9.4.14.7 PDP context status

This IE shall be included by the MS.

9.4.14.8 PS LCS Capability

This IE shall be included if the MS supports at least one positioning method for the provision of location services (LCS) via the PS domain in Gb-mode.

9.4.14.9 MBMS context status

This IE shall be included by the MS, if it has MBMS contexts with an SM state different from PDP-INACTIVE.

9.4.14.10 Additional mobile identity and additional old routing area identification

These two IEs shall be included by the MS, if the TIN indicates "GUTI" and the MS holds a valid GUTI, P-TMSI and RAI.

9.4.15 Routing area update accept

This message is sent by the network to the MS to provide the MS with GPRS mobility management related data in response to a *routing area update request* message. See table 9.4.15/3GPP TS 24.008.

Message type: ROUTING AREA UPDATE ACCEPT

Significance: dual

Direction: network to MS

Table 9.4.15/3GPP TS 24.008: ROUTING AREA UPDATE ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Routing area update accept message identity	Message type 10.4	M	V	1
	Force to standby	Force to standby 10.5.5.7	M	V	1/2
	Update result	Update result 10.5.5.17	M	V	1/2
	Periodic RA update timer	GPRS Timer 10.5.7.3	M	V	1
	Routing area identification	Routing area identification 10.5.5.15	M	V	6
19	P-TMSI signature	P-TMSI signature 10.5.5.8	O	TV	4
18	Allocated P-TMSI	Mobile identity 10.5.1.4	O	TLV	7
23	MS identity	Mobile identity 10.5.1.4	O	TLV	7-10
26	List of Receive N-PDU Numbers	Receive N-PDU Number list 10.5.5.11	O	TLV	4 - 19
17	Negotiated READY timer value	GPRS Timer 10.5.7.3	O	TV	2
25	GMM cause	GMM cause 10.5.5.14	O	TV	2
2A	T3302 value	GPRS Timer 2 10.5.7.4	O	TLV	3
8C	Cell Notification	Cell Notification 10.5.5.21	O	T	1
4A	Equivalent PLMNs	PLMN List 10.5.1.13	O	TLV	5-47
32	PDP context status	PDP context status 10.5.7.1	O	TLV	4
B-	Network feature support	Network feature support 10.5.5.23	O	TV	1
34	Emergency Number List	Emergency Number List 10.5.3.13	O	TLV	5-50
35	MBMS context status	MBMS context status 10.5.7.6	O	TLV	2 - 18
A-	Requested MS Information	Requested MS Information 10.5.5.25	O	TV	1
37	T3319 value	GPRS Timer 2 10.5.7.4	O	TLV	3
zz	ISR indication	FFS	O	FFS	FFS

9.4.15.1 P-TMSI signature

This IE may be included to assign an identity to the MS's GMM context.

9.4.15.2 Allocated P-TMSI

This IE may be included to assign a P-TMSI to an MS in case of a GPRS or combined routing area updating procedure.

9.4.15.3 MS identity

This IE may be included to assign or unassign a TMSI to a MS in case of a combined routing area updating procedure.

9.4.15.4 List of Receive N-PDU Numbers

This IE shall be included in case of an inter SGSN routing area updating from A/Gb mode to A/Gb mode, or inter SGSN routing area updating from Iu mode to A/Gb mode, or intra SGSN routing area updating from Iu mode to A/Gb mode, if there are PDP contexts that have been activated in LLC acknowledged transfer mode.

9.4.15.5 Negotiated READY timer value

This IE may be included to indicate a value for the READY timer.

9.4.15.6 GMM cause

This IE shall be included if the combined GPRS routing area updating procedure was successful for GPRS services only.

9.4.15.7 T3302 value

This IE may be included to indicate a value for the T3302 timer.

In Iu mode, the network shall not include this IE if this message is to be sent non-integrity protected.

In Iu mode, if this message is received without integrity protection the MS shall ignore the contents of this IE and use the last received value if available. If there is no last received value, the MS shall use the default value.

If this IE is not included in the message in A/Gb mode or if in Iu mode this IE is not included in an integrity protected message, the MS shall use the default value.

9.4.15.8 Cell Notification (A/Gb mode only)

In A/Gb mode, this IE shall be included if by the SGSN in order to indicate the ability to support the Cell Notification.

9.4.15.9 Equivalent PLMNs

The *Equivalent PLMNs* information element is included if the network wants to inform the mobile station of equivalent PLMNs.

9.4.15.10 PDP context status

This IE shall be included by the NW.

9.4.15.11 Network feature support

This IE may be included to inform the MS of the support of certain features. If this IE is not included then the respective features are not supported.

9.4.15.12 Emergency Number List

This IE may be sent by the network. If this IE is sent, the contents of this IE indicates a list of emergency numbers valid within the same MCC as in the cell on which this IE is received.

9.4.15.13 MBMS context status

This IE shall be included by the network, if it has MBMS contexts for the MS with an SM state different from PDP-INACTIVE.

9.4.15.14 Requested MS Information

This IE may be sent by the network to request the MS to provide feature-related information.

9.4.15.15 T3319 value

This IE may be included to indicate a value for the T3319 timer.

9.4.15.16 ISR indication

This IE may be included to indicate to the MS that the GUTI and TAI list assigned to the MS remain registered with the network and are valid in the MS.

Editor's note: The coding of the ISR indication needs to be specified.

Formatted: Editor'sNote;EN

B.14 Next change

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/M-TMSI, the international mobile equipment identity, IMEI, the international mobile equipment identity together with the software version number, IMEISV, or the temporary mobile group identity (TMGI), associated with the optional MBMS Session Identity.

The IMSI shall not exceed 15 digits, the TMSI/P-TMSI/M-TMSI is 4 octets long, and the IMEI is composed of 15 digits, the IMEISV is 16 digits (see 3GPP TS 23.003 [10]). The TMGI is at maximum 6 octets long and is defined in subclause 10.5.6.13. The MBMS Session Identity, if included, is 1 octet long (see 3GPP TS 48.018 [86]).

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 shall be used in cases where no P-TMSI is available.

For MBMS (pre-)notification (see 3GPP TS 44.018 [84] and 3GPP TS 44.060 [76]) the network shall select the mobile identity type "TMGI and optional MBMS Session Identity".

NOTE 1: The type of identity "TMGI and optional MBMS Session Identity" is only used by the MBMS (pre-)notification procedure in of A/Gb mode.

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 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. In case of enhanced DTM CS establishment (see 3GPP TS 44.018 [84]) the mobile station shall select the mobile identity type with the following priority in the PAGING RESPONSE message:

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

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

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 and if the location update status is UPDATED, and the stored LAI is equal to the one received on the BCCH from the current serving cell.

2- IMSI: The IMSI shall be used in cases where no TMSI is available or TMSI is available but either the update status is different from UPDATED, or the stored LAI is different from the one received on the BCCH from the current serving cell.

3- IMEI: The IMEI shall be used in cases where no SIM/USIM is available or the SIM/USIM 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 available. If the requested identity is not available, then the mobile station shall indicate the identity type "No Identity".

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 10.5.4/3GPP TS 24.008 and table 10.5.4/3GPP TS 24.008.

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

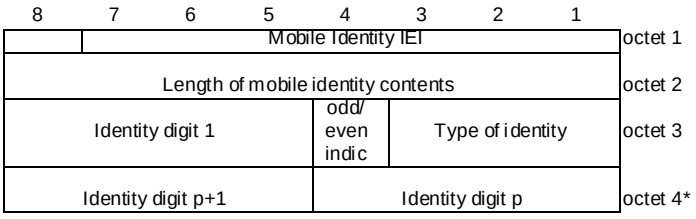


Figure 10.5.4/3GPP TS 24.008 *Mobile Identity* information element

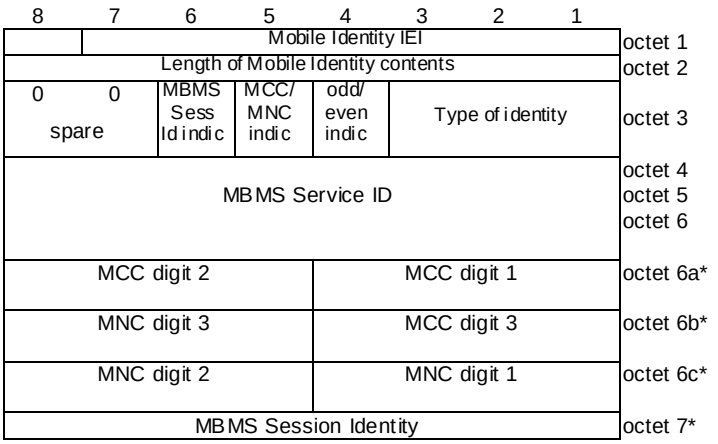


Figure 10.5.4a/3GPP TS 24.008: *Mobile Identity* information element for type of identity "TMGI and optional MBMS Session Identity"

Table 10.5.4/3GPP 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/M-TMSI
1	0	1	TMGI and optional MBMS Session Identity
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 or TMGI and optional MBMS Session Identity is used
1	odd number of identity digits

Identity digits (octet 3 etc)

For the IMSI, IMEI 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".

For Type of identity "No Identity", the Identity digit bits shall be encoded with all 0s and the Length of mobile identity contents parameter shall be set to one of the following values:
- "1" if the identification procedure is used (see subclause 9.2.11);
- "3" if the GMM identification procedure is used (see subclause 9.4.13)

If the mobile identity is the TMSI/P-TMSI/M-TMSI then bits 5 to 8 of octet 3 are coded as "1111" and bit 8 of octet4 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.

For type of identity "TMGI and optional MBMS Session Identity" the coding of octet 3 etc is as follows:

MCC/MNC indication (octet 3)
Bit

5	
0	MCC/MNC is not present
1	MCC/MNC is present

MBMS Session Identity indication (octet 3)
Bit

6	
0	MBMS Session Identity is not present
1	MBMS Session Identity is present

MBMS Service ID (octet 4, 5 and 6)

The contents of the MBMS Service ID field are coded as octets 3 to 5 of the *Temporary Mobile Group Identity* IE in Figure 10.5.154/3GPP TS 24.008. Therefore, bit 8 of octet 4 is the most significant bit and bit 1 of octet 6 the least significant bit. The coding of the MBMS Service ID is the responsibility of each administration. Coding using full hexadecimal representation may be used. The MBMS Service ID consists of 3 octets.

MCC, Mobile country code (octet 6a, octet 6b bits 1 to 4)

The MCC field is coded as in ITU-T Rec. E.212, Annex A.

MNC, Mobile network code (octet 6b bits 5 to 8, octet 6c) The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 6b shall be coded as "1111". The contents of the MCC and MNC digits are coded as octets 6 to 8 of the *Temporary Mobile Group Identity* IE in Figure 10.5.154/3GPP TS 24.008. **MBMS Session Identity** (octet 7) The MBMS Session Identity field is encoded as the value part of the MBMS Session Identity IE as specified in 3GPP TS 48.018 [86].
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 and when the requested identity is not available at the mobile station during the identity request procedure.

B.15 Next change

10.5.5.12 MS network capability

The purpose of the *MS network capability* information element is to provide the network with information concerning aspects of the mobile station related to GPRS and EPS. The contents might affect the manner in which the network handles the operation of the mobile station. The *MS network capability* information indicates general mobile station characteristics and it shall therefore, except for fields explicitly indicated, be independent of the frequency band of the channel it is sent on.

The *MS network capability* is a type 4 information element with a maximum of 10 octets length.

The value part of a *MS network capability* information element is coded as shown in figure 10.5.128/3GPP TS 24.008 and table 10.5.145/3GPP TS 24.008.

NOTE: The requirements for the support of the GEA algorithms in the MS are specified in 3GPP TS 43.020 [13].

8	7	6	5	4	3	2	1	
MS network capability IEI								octet 1
Length of MS network capability contents								octet 2
MS network capability value								octet 3-10

Figure 10.5.128/3GPP TS 24.008 MS network capability information element

Table 10.5.145/3GPP TS 24.008 *MS network capability* information element

<MS network capability value part> ::=

<**GEA1 bits**>
<**SM capabilities via dedicated channels**: bit>
<**SM capabilities via GPRS channels**: bit>
<**UCS2 support**: bit>
<**SS Screening Indicator**: bit string(2)>
<SoLSA Capability : bit>
<Revision level indicator: bit>
<PFC feature mode: bit>
<Extended GEA bits>
<-LCS VA capability: bit->
<-PS inter-RAT HO to UTRAN Iu mode capability: bit->
<Alignment bits>
<EEA bits>
<EIA bits>
<UEA bits>
<UIA bits>
<Spare bits>;

<**GEA1 bits**> ::= < **GEA/1** :bit>;

<Extended GEA bits> ::= <GEA/2:bit><GEA/3:bit>< GEA/4:bit >< GEA/5:bit >< GEA/6:bit ><GEA/7:bit>;

<Alignment bits> ::= <spare bit (7)>;

<EEA bits> ::= <EEA0:bit><EEA1:bit><EEA2:bit><EEA3:bit><EEA4:bit><EEA5:bit><EEA6:bit><EEA7:bit>;
<EIA bits> ::= <spare bit><EIA1:bit><EIA2:bit><EIA3:bit><EIA4:bit><EIA5:bit><EIA6:bit><EIA7:bit>;

<UEA bits> ::= <UEA0:bit><UEA1:bit><UEA2:bit><UEA3:bit><UEA4:bit><UEA5:bit><UEA6:bit><UEA7:bit>;
<UIA bits> ::= <spare bit><UIA1:bit><UIA2:bit><UIA3:bit><UIA4:bit><UIA5:bit><UIA6:bit><UIA7:bit>;

<**Spare bits**> ::= null | {<spare bit> < **Spare bits** >};

SS Screening Indicator
0 0 defined in 3GPP TS 24.080

0 1 defined in 3GPP TS 24.080
1 0 defined in 3GPP TS 24.080
1 1 defined in 3GPP TS 24.080

SM capabilities via dedicated channels
0 Mobile station does not support mobile terminated point to point SMS via CS domain
1 Mobile station supports mobile terminated point to point SMS via CS domain

SM capabilities via GPRS channels
0 Mobile station does not support mobile terminated point to point SMS via PS domain
1 Mobile station supports mobile terminated point to point SMS via PS domain

UCS2 support
This information field indicates the likely treatment by the mobile station of UCS2 encoded character strings.
0 the ME has a preference for the default alphabet (defined in 3GPP TS 23.038 [8b]) over UCS2.
1 the ME has no preference between the use of the default alphabet and the use of UCS2.

GPRS Encryption Algorithm GEA/1
0 encryption algorithm **GEA/1** not available

1 encryption algorithm **GEA/1** available

SoLSA Capability
0 The ME does not support SoLSA.
1 The ME supports SoLSA.

Revision level indicator
0 used by a mobile station not supporting R99 or later versions of the protocol
1 used by a mobile station supporting R99 or later versions of the protocol

PFC feature mode
0 Mobile station does not support BSS packet flow procedures
1 Mobile station does support BSS packet flow procedures

GEA/2
0 encryption algorithm GEA/2 not available
1 encryption algorithm GEA/2 available

GEA/3
0 encryption algorithm GEA/3 not available
1 encryption algorithm GEA/3 available

GEA/4
0 encryption algorithm GEA/4 not available
1 encryption algorithm GEA/4 available

GEA/5
0 encryption algorithm GEA/5 not available
1 encryption algorithm GEA/5 available

GEA/6
0 encryption algorithm GEA/6 not available
1 encryption algorithm GEA/6 available

GEA/7
0 encryption algorithm GEA/7 not available
1 encryption algorithm GEA/7 available

LCS VA capability (LCS value added location request notification capability)
This information field indicates the support of the LCS value added location request notification via PS domain as defined in 3GPP TS 23.271 [105].
0 location request notification via PS domain not supported
1 location request notification via PS domain supported

PS inter-RAT HO to UTRAN Iu mode capability
This information field indicates the support of the PS inter-RAT HO to UTRAN Iu mode.
0 PS inter-RAT HO to UTRAN Iu mode not supported
1 PS inter-RAT HO to UTRAN Iu mode supported

EEA0
0 EPS encryption algorithm 128-EEA0 not supported
1 EPS encryption algorithm 128-EEA0 supported

EEA1
0 EPS encryption algorithm 128-EEA1 not supported
1 EPS encryption algorithm 128-EEA1 supported

EEA2
0 EPS encryption algorithm 128-EEA2 not supported
1 EPS encryption algorithm 128-EEA2 supported

EEA3
0 EPS encryption algorithm EEA3 not supported
1 EPS encryption algorithm EEA3 supported

EEA4
0 EPS encryption algorithm EEA4 not supported
1 EPS encryption algorithm EEA4 supported

EEA5
0 EPS encryption algorithm EEA5 not supported
1 EPS encryption algorithm EEA5 supported

EEA6
0 EPS encryption algorithm EEA6 not supported
1 EPS encryption algorithm EEA6 supported

EEA7
0 EPS encryption algorithm EEA7 not supported
1 EPS encryption algorithm EEA7 supported

EIA1
0 EPS integrity algorithm 128-EIA1 not supported
1 EPS integrity algorithm 128-EIA1 supported

EIA2
0 EPS integrity algorithm 128-EIA2 not supported
1 EPS integrity algorithm 128-EIA2 supported

EIA3
0 EPS integrity algorithm EIA3 not supported
1 EPS integrity algorithm EIA3 supported

EIA4
0 EPS integrity algorithm EIA4 not supported
1 EPS integrity algorithm EIA4 supported

EIA5
0 EPS integrity algorithm EIA5 not supported
1 EPS integrity algorithm EIA5 supported

EIA6
0 EPS integrity algorithm EIA6 not supported
1 EPS integrity algorithm EIA6 supported

EIA7
0 EPS integrity algorithm EIA7 not supported
1 EPS integrity algorithm EIA7 supported

UEA0
0 UMTS encryption algorithm UEA0 not supported
1 UMTS encryption algorithm UEA0 supported

UEA1
0 UMTS encryption algorithm UEA1 not supported
1 UMTS encryption algorithm UEA1 supported

UEA2
0 UMTS encryption algorithm UEA2 not supported
1 UMTS encryption algorithm UEA2 supported

UEA3

0 UMTS encryption algorithm UEA3 not supported
1 UMTS encryption algorithm UEA3 supported

UEA4
0 UMTS encryption algorithm UEA4 not supported
1 UMTS encryption algorithm UEA4 supported

UEA5
0 UMTS encryption algorithm UEA5 not supported
1 UMTS encryption algorithm UEA5 supported

UEA6
0 UMTS encryption algorithm UEA6 not supported
1 UMTS encryption algorithm UEA6 supported

UEA7
0 UMTS encryption algorithm UEA7 not supported
1 UMTS encryption algorithm UEA7 supported

UIA1
0 UMTS integrity algorithm UIA1 not supported
1 UMTS integrity algorithm UIA1 supported

UIA2
0 UMTS integrity algorithm UIA2 not supported
1 UMTS integrity algorithm UIA2 supported

UIA3
0 UMTS integrity algorithm UIA3 not supported
1 UMTS integrity algorithm UIA3 supported

UIA4
0 UMTS integrity algorithm UIA4 not supported
1 UMTS integrity algorithm UIA4 supported

UIA5
0 UMTS integrity algorithm UIA5 not supported
1 UMTS integrity algorithm UIA5 supported

UIA6
0 UMTS integrity algorithm UIA6 not supported
1 UMTS integrity algorithm UIA6 supported

UIA7
0 UMTS integrity algorithm UIA7 not supported
1 UMTS integrity algorithm UIA7 supported

Formatted: Body Text Indent, Indent: First line: 0 cm

Formatted: Indent: First line: 0,16 cm

Annex C (informative): Proposed changes to 3GPP TS 24.007

C.1 Summary of changes

Editor's note: The following subclauses are a place holder for a draft CR to 3GPP TS 24.007 [36] until CT1 decides to send it to TSG CT plenary for approval. This annex includes only subclauses of 3GPP TS 24.007 [36] which need to be updated or added as new subclauses.

- The principal protocol architecture is updated to include a description of the EPS NAS and its sublayers. The scope and the references are updated accordingly.

Formatted: B1

- Definition of a new type of standard information element for NAS L3 messages ("type 6 IE"). The new type TLV-E (enhanced TLV) contains a length indicator of 2 octets, allowing to include up to 65535 octets in the value part of the information element. This can be used for information elements which are intended to include complete EPS NAS messages. Rules are specified how the receiving entity can recognize new type 6 IEs from the coding of their IEI, and the 'comprehension required' scheme is extended to type 6 IEs.

- Definition of new PD values for EPS NAS protocols for mobility management and session management, and of new information elements for the header of these protocols.

C.2 First change

1 Scope

The present document defines the principal architecture of layer 3 and its sublayers on the GSM Um interface, i.e. the interface between Mobile Station (MS) and network; for the CM sublayer, the description is restricted to paradigmatic examples, call control, supplementary services, and short message services for non-GPRS services. It also defines the basic message format and error handling applied by the layer 3 protocols.

For CTS services, the present document defines the principal architecture of layer 3 on the GSM Um* interface, i.e. the interface between a CTS capable Mobile Station (CTS-MS) and a Fixed Part (FP).

The corresponding protocols are defined in other Technical Specifications, see subclause 4.3.4.

For non-GPRS services the communication between sublayers and adjacent layers and the services provided by the sublayers are distributed by use of abstract service primitives. But only externally observable behaviour resulting from the description is normatively prescribed by the present document.

For GPRS services in addition the local information transfer and stimuli sent between sublayers is informatively included within Annex C of in the present document

This document also defines the principal architecture of the EPS NAS layer 3 protocol and its sublayers, including the message format applied by layer 3.

In the present document MS is also used as a synonym for UE.

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] GSM 01.02(R97): "Digital cellular telecommunications system (Phase 2+); General description of a GSM Public Land Mobile Network (PLMN)".

[1a] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.101: "General UMTS Architecture".

[3] 3GPP TS 44.001: "Mobile Station - Base Station System (MS - BSS) interface; General aspects and principles".

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

[3b] GSM 03.56(R98): "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephony System (CTS), Phase 1; CTS Architecture Description; Stage 2".

[3c] 3GPP TS 23.271: "Functional stage 2 description of location services".

[4] 3GPP TS 44.005: "Data Link (DL) layer; General aspects".

[5] 3GPP TS 44.006: "Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification".

[5a] 3GPP TS 44.014: "Individual equipment type requirements and interworking; Special conformance testing functions".

[6] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification Core Network Protocols-Stage 3".

[6a] 3GPP TS 23.108: "Mobile radio interface Layer 3 specification Core Network Protocols Stage 2 (structured procedures)".

[6b] 3GPP TS 44.018: "Mobile radio interface layer 3 specification; Radio Resource Control Protocol".

[7] 3GPP TS 24.010: "Mobile radio interface Layer 3; Supplementary services specification; General aspects".

[8] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[8a] 3GPP TS 44.071: "Location Services (LCS); Mobile radio interface layer 3 LCS specification".

[9] 3GPP TS 24.080: "Mobile radio Layer 3 supplementary services specification; Formats and coding".

[10] 3GPP TS 24.081: "Line identification supplementary services; Stage 3".

[10a] 3GPP TS 44.060: "General Packet Radio Services (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/Medium Access Control (RLC/MAC) protocol".

[10b] 3GPP TS 44.056: "GSM Cordless Telephony System (CTS), phase 1; CTS radio interface Layer 3 specification".

[11] 3GPP TS 24.082: "Call Forwarding (CF) supplementary services - Stage 3".

[11a] 3GPP TS 44.064: "General Packet Radio Service (GPRS); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) layer specification".

[12] 3GPP TS 24.083: "Call Waiting (CW) and Call Hold (HOLD) supplementary services; Stage 3".

[12a] 3GPP TS 44.065: "General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[13] 3GPP TS 24.084: "MultiParty (MPTY) supplementary services; Stage 3".

[14] 3GPP TS 24.085: "Closed User Group (CUG) supplementary services; Stage 3".

[15] 3GPP TS 24.086: "Advice of Charge (AoC) supplementary services; Stage 3".

[16] 3GPP TS 24.088: "Call Barring (CB) supplementary services; Stage 3".

[17] 3GPP TS 24.090: "Unstructured Supplementary Service Data (USSD) - Stage 3".

[17a] 3GPP TS 34.109: "Terminal logical test interface; Special conformance testing functions".

[18] ITU-T Recommendation X.200: "Information technology - Open Systems Interconnection - Basic Reference Model: The basic model".

[19] 3GPP TS 44.068: "Group Call Control (GCC) Protocol".

[20] 3GPP TS 23.110: "UMTS Access Stratum Services and Functions".

[21] 3GPP TS 24.030: "Location Services (LCS); Supplementary service operations – Stage 3".

[22] 3GPP TS 23.251: "Network Sharing; Architecture and functional description".

[23] 3GPP TS 25.413: "UTRAN Iu interface RANAP signalling".

[24] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC) protocol specification".

[25] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

C.3 Next change

4 Introduction

4.1 General

Four~~Three~~ models are defined for Layer 3, one model for non-GPRS services, one for GPRS services supporting Class C MSs only, ~~and~~ one model for GPRS-services supporting Class A and Class B MSs and one model for EPS services. (The third model is a combination of the first two models listed). In the present document GPRS services and EPS services will be used as synonyms.

The layer 3 for non-GPRS services provides the functions necessary:

- for Radio Resource (RR) management;
- for Mobility Management (MM); and
- for the Connection Management (CM) functions, i.e. functions for the control, provision, and support of services offered by the network; among which there are, e.g.:
  - the functions to establish, maintain and terminate circuit-switched connections across a GSM PLMN and other networks to which the GSM PLMN is connected;
  - supporting functions for supplementary services control;
  - supporting functions for short messages service control;
  - supporting functions for location services control (only for a type A LMU).

The layer 3 for non-GPRS services is composed of three sublayers comprising:

- the Radio Resource Management (RR) functions;
- the Mobility Management (MM) functions; and
- the Connection Management (CM) functions.

When CTS services are added to non-GPRS services, the following functions are added:

- CTS Radio Resource Management (CTS-RR) functions to RR; and
- CTS Mobility Management (CTS-MM) functions to MM.

The layer 3 for GPRS services is composed of four sublayers comprising:

- the Radio Resource Management (RR) functions;
- the Mobility Management (GMM);
- for the Logical Link Control (LLC);
- the Connection Management (CM) functions.

The Connection Management (CM) sublayer is composed of functional blocks for:

- Call Control (CC) for non-GPRS services;
- Short Message Service Support (SMS) for non-GPRS services;
- GPRS Short Message Service Support (GSMS) (for GPRS services supporting Class A, B and C MSs);
- Session Management (SM) (for GPRS services supporting Class A, B and C MSs);
- Supplementary Services Support (SS) for non-GPRS services;
- Group Call Control for non-GPRS services;
- Broadcast Call Control (BCC) for non-GPRS services;
- Connection Management of Packet Data on Signalling channels for non-GPRS services;
- Location Services support (LCS) for non-GPRS services (only for a type A LMU).

Within the context of LCS, for GSM LCS, the services defined for an MS are equally applicable to a type A LMU, unless otherwise stated. However, services defined specifically for a type A LMU are not applicable to an MS. The following is a list of services essential for a type A LMU.

The layer 3 for non-GPRS services provides the functions necessary:

- for Radio Resource (RR) management;
- for Mobility Management (MM); and
- supporting functions for location service control.

The layer 3 for non-GPRS services is composed of three sublayers comprising:

- the Radio Resource Management (RR) functions;
- the Mobility Management (MM) functions; and
- the Connection Management (CM) functions.

The Connection Management (CM) sublayer is composed of a functional block for:

- location services support (LCS) for non-GPRS services.

The present document does not consider the distribution of signalling functions among the different network equipments. The signalling functions are described between two systems which represent the MS side and the network side of the radio interface of layer 3. Only the functions in the network for signalling communication with one MS is considered.

For GPRS services, in addition to the signalling functions also the user data transfer is included in the present document.

The layer 3 for EPS services is composed of four sublayers comprising:

- the EPS Radio Resource Management (RR) functions;
- the EPS Mobility Management (EMM) functions; and
- the Connection Management (CM) functions.

The Connection Management (CM) sublayer is composed of a functional block for:

- the EPS Session Management (ESM) functions.

Formatted: B1, No bullets or numbering

Formatted: B1, No bullets or numbering

C.4 Next change

4.3.3 Protocols and peer-to-peer communication

By use of the services provided by lower (sub-)layers, peer entities in a (sub-)layer in the MS and the network exchange information. Exchange of information between two peer entities is performed according to the corresponding (sub-)layer protocols. A protocol is a set of rules and formats by which the information (control information and user data) is exchanged between the two peers. The information is exchanged by use of messages which are defined in the protocol. (Therefore, the messages are also called Protocol Data Units, PDUs).

There are several protocols of the RR sublayer, one protocol of the LLC sublayer, three protocols of the MM sublayer, and several protocols of the CM sublayer. For each functional block of the CM sublayer as defined in subclause 4.1 there is one protocol. The CM protocols are specified in the Technical Specifications identified in subclause 4.3.4.

In the model used in the present document, there are:

1) for non-GPRS services:

- one RR sub-layer entity in the MS and one RR sub-layer entity in the network;
- one MM sub-layer entity in the MS and one MM sub-layer entity in the network;
- for each functional block of the CM sublayer as defined in subclause 4.1 which is supported in the MS (in the network), there are, depending on the protocol, one or more entities in the MS (in the network). Two different entities of the same functional block in the MS (in the network) are called parallel entities. The entities of the same functional block in the MS correspond in a one-to-one relation to the entities of the functional block in the network. The corresponding entities are called peer entities;

2) for CTS services (in addition to non-GPRS services):

- one RR sub-layer entity in the MS and one in the CTS fixed part. These RR sub-layers include one CTS-RR sub-entity on each side;
- one MM sub-layer entity in the MS and one in the CTS fixed part These MM sub-layers include one CTS-MM sub-entity on each side;
- for each functional block of the CM sublayer as defined in subclause 4.1 which is supported in the MS (in the fixed part), there are, depending on the protocol, one or more entities in the MS (in the fixed part). Two different entities of the same functional block in the MS (in the fixed part) are called parallel entities. The entities of the same functional block in the MS correspond in a one-to-one relation to the entities of the functional block in the fixed part. The corresponding entities are called peer entities;

3) for GPRS services supporting Class C MSs:

- one RR sublayer entity (RR) in the MS and one RR sublayer entity in the network;
- six LLC sublayer entities (QoS1-QoS4, signalling, SMS) in the MS and six LLC sublayer entities in the network;

- one MM sublayer entity (GMM) in the MS and one MM sublayer entity in the network (GMM);
- one SM entity in the MS's CM sublayer and one SM sublayer entity in the network's CM sublayer;
- one or more GSMS functional blocks in the CM sublayer if supported;

4) for non-GPRS and GPRS services supporting Class A and Class B MSs:

- two RR sublayer entities (RR) in the MS and two RR sublayer entities in the network;
- six LLC sublayer entities (QoS1-QoS4, signalling, SMS) in the MS and six LLC sublayer entities in the network;
- two MM sublayer entities (GMM + MM) in the MS and one or two MM sublayer entities in the network (GMM or MM);
- one SM entity in the MS's CM sublayer and one SM entity in the network's CM sublayer;
- for each functional block of the CM sublayer as defined in subclause 4.1 which is supported in the MS (in the network), there are, depending on the protocol, one or more entities in the MS (in the network). Two different entities of the same functional block in the MS (in the network) are called parallel entities. The entities of the same functional block in the MS correspond in a one-to-one relation to the entities of the functional block in the network. The corresponding entities are called peer entities;

5) for EPS services:

- one RR entity in the MS and one RR entity in the network;
- one EMM entity in the MS and one EMM entity in the network;
- for each functional block of the CM sublayer as defined in subclause 4.1 which is supported in the MS (in the network), there are, depending on the protocol, one or more entities in the MS (in the network). Two different entities of the same functional block in the MS (in the network) are called parallel entities. The entities of the same functional block in the MS correspond in a one-to-one relation to the entities of the functional block in the network. The corresponding entities are called peer entities.

As each sub-layer entity is specified by one and only one protocol, it is also called a protocol entity or protocol control entity.

For GPRS-services supporting Class A and Class B MSs, the MM entities of the MM-sublayer are able to exchange information by means of GMM PDUs as well as MM PDU's. This means if a mobile is GPRS attached, non-GPRS mobility management procedures may make use of GRPS mobility management messages.

When two peer protocol entities exchange PDUs, a transaction is said to be established (or: to be active; or: to exist). It depends from the protocol when exactly a protocol entity considers the transaction to be active, normally this is the case:

- from the moment when it has passed the first suitable message to lower (sub-) layers or received the first suitable message from its peer entity;
- up to the moment when it has released the transaction.

4.3.4 Contents of layer 3 related Technical Specifications

- The Radio Resource (RR) management protocol is defined in 3GPP TS 44.018 [6b];
- the Mobility Management (MM) protocol is defined in 3GPP TS 24.008 [6];
- the Session Management (SM) protocol is defined in 3GPP TS 24.008 [6];
- the Call Control (CC) protocol is defined in 3GPP TS 24.008 [6];
- the Supplementary Services (SS) protocol is defined in 3GPP TS 24.010 [7], 3GPP TS 24.08x, 3GPP TS 24.09x, and 3GPP TS 24.030 [21];
- the Short Message Service (SMS) protocol is defined in 3GPP TS 24.011 [8];
- the Group Call Control (GCC) protocol is defined in 3GPP TS 44.068 [19];
- the Logical Link Control (LLC) protocol is defined in 3GPP TS 44.064 [11a];
- the GPRS Radio Resource (GRR) protocol is defined in 3GPP TS 44.060 [10a] and 3GPP TS 24.008 [6];
- the CTS Radio Resource (CTS-RR) sub-protocol is defined in 3GPP TS 44.056 [10b];
- the CTS Mobility Management (CTS-MM) sub-protocol is defined in 3GPP TS 44.056 [10b];
- the CTS additions to the Call Control (CC) protocol are defined in 3GPP TS 44.056 [10b];
- the Location Services (LCS) protocol for a type A LMU is defined in 3GPP TS 23.271 [3c] and 3GPP TS 44.071 [8a];
- the EPS Radio Resource (RR) management protocol is defined in 3GPP TS 36.331 [24];
- the EPS Mobility Management (EMM) protocol is defined in 3GPP TS 24.301 [25];
- the EPS Session Management (ESM) protocol is defined in 3GPP TS 24.301 [25].

5 Structure of layer 3 functions

5.1 Basic groups of functions

Most functions of layer 3 and its sub-layers are described by the service specifications and protocol specifications of the (sub-)layers.

These functions are in the model realized by protocol control entities, see subclause 4.3.3.

In addition, routing functions are contained in layer 3 which are related to the transport of messages, e.g. multiplexing and splitting. These routing functions are defined in the Radio Resource Management and Mobility Management sub-layers.

1) They have the task to pass the messages from upper (sub-)layers to lower (sub-)layers.
2) They also have the task to pass messages provided by lower (sub-layers) to the appropriate sub-layer and, if applicable, entity.

The routing functions with task 2 make use of the protocol discriminator (PD) which is part of the message header.

A CM sublayer protocol may also define a transaction identifier (TI), procedure transaction identity (PTI) or EPS bearer identity as a part of the message header. This is at least the case if there are parallel entities of the same functional block, see subclause 4.3.3. If they are~~it is~~ a part of a message, the TI, PTI, EPS bearer identity, or both PTI and EPS bearer identity are ~~is~~ also used by the routing functions.

- The MM-sublayer routing function passes the messages of the CM entities as well as of the MM, GMM and CTS-MM entities of its own sublayer to the service access point of RR, GRR, LLC or CTS-RR. Furthermore it multiplexes them in case of parallel transactions.
- The routing function of Radio Resource Management distributes the messages to be sent according to their message type and protocol discriminator (PD), to the actual channel configuration, and, if applicable, to further information received from upper sub-layers to the appropriate service access point of layer 2 (identified by SAPI and logical channel). Paging messages received from the PPCH are always routed to GMM, while paging messages received from the PCH are distributed to GMM or MM based on the temporary identifier (TMSI or TLL). For EPS services, the Paging messages received from the PCH are always routed to EMM.
- The messages provided at the different service access points of layer 2 are distributed by the RR sublayer routing function according to their protocol discriminator (PD). Messages with a PD equal to RR are passed to the RR entity of the own sublayer, all other messages are passed to the MM sublayer at the service access point RR-SAP.
- The routing function of MM-sublayer passes Standard L3 messages according to the protocol discriminator (PD) and, if applicable, the transaction identifier (TI) or the PDP address towards the MM entity or towards the CM entities via the various MM-SAP's. GPRS L3 messages are routed to mobility management or session management according to the protocol discriminator.
- For EPS services, the routing function of EPS NAS passes standard L3 messages according to the protocol discriminator (PD) and, if applicable, the procedure transaction identity (PTI) and/or EPS bearer identity towards the EMM entity or towards the CM (ESM) entities of the various EPS NAS SAP's.
- The routing function of LLC passes the messages according to the SAPIs to the MM sublayer or to the SNDCP entities.

The message (message header or other parts of the message) are neither changed nor removed by the RR routing function or MM routing function before passing it to the appropriate service access point.

5.2 Protocol architecture

The protocol architecture is visualized for each of the three models:

- Figure 5.1/3GPP TS 24.007 shows the protocol architecture for a MS not supporting the GPRS service, restricting the representation of CM sublayer protocols to three paradigmatic examples, CC, SS, and SMS. The LCS protocol entity of a type A LMU would be included in the same manner. Note that the protocol stack for a class C GPRS service may be present in the MS, but it is not active simultaneously.
- Figure 5.2 shows the protocol architecture for a MS supporting the Class C GPRS service. (Note that the protocol stack for a circuit switched services may be present in the MS, but it is not active simultaneously).
- Figure 5.3 shows the protocol architecture for non-GPRS and GPRS-services supporting Class A and Class B MSs.
- Figure 5.4 shows the protocol architecture for a MS supporting CTS services in addition to non-GPRS services.
- Figure 5.5 shows the protocol architecture for a MS supporting the PS mode of operation UMTS service.
- Figure 5.6 shows the protocol architecture for UMTS services supporting CS/PS mode of operation MSs.
- Figure 5.7 shows the protocol architecture for a MS supporting EPS services.

Editor's note: Figure 5.7 is FFS.

C.5 Next change

11 L3 Messages

This clause specifies the generic methods used in the layer 3 protocol specifications to describe messages. It define in particular a generic message structure, that of the "standard L3 messages". Not all messages in layer 3 protocols follow this structure, but many do, and this clause specifies how to interpret the standard description.

This clause also addresses basic aspects of the handling of messages received but not compliant with the allowed structure. In most cases, only the conditions that lead to the diagnosis of an error are described. The reaction of an entity receiving a message leading to such a diagnosis is in general specified for each protocol in the relevant protocol specification.

11.1 General

11.1.1 Messages

For all concerned protocols, concrete messages are bit strings of variable length, formally a succession of a finite, possibly null, number of bits (i.e., elements of the set {"0", "1"}), with a beginning and an end.

The services provided by lower layers includes the transmission of such bit strings.

Considered as messages, these bit strings follow some structure (the syntax), enabling to organize bits in information pieces of a different meaning level.

The term *message* is used as well for a concrete message (i.e., a bit-string, as defined by the giving of all its bits, in practice appearing at one point of time in a concrete dialog), as for a class of concrete messages sharing a common structure. A concrete message is an instance of the corresponding class of messages. Message classes can be described as sets of potential bit strings, and of a common structure, enabling in particular to identify parts meaningful for the co-operation functions the protocol supports.

In general, in the rest of the clause as in the protocol specifications, the term *message* will be used to refer to the class. It may be used, when the context prevents ambiguity, to refer to a message instance (e.g., a received is usually a message instance). In the rest of this clause, the term *message instance* will be used when needed to refer unambiguously to specific concrete message, i.e. to a specific bit string.

A message (message class) can be described directly as a set of bit strings, using the formal notation described in Annex B.

A message can also be described as a standard L3 message, in which case the interpretation of the message description in term of a set of bit strings is specified in the next sub-clauses.

In all cases, structuring messages is based on the underlying bit string. Thus, the following terms are used:

- a *part* of a message instance is a sub-string of the corresponding string; a part of a message (as a class) is described by a definition applicable to all instances; a part of a message then is both a structural attribute of the message as a class, and a set of sub-strings, composed of the sub-strings obtained by applying the definition to each possible instance; for instance, « the first octet » of a message instance is defined from the moment its length is greater than 8, and is the sub-string composed of the first 8 bits of the message instance; the « first octet » of a message as a class is the structural definition given above, and the set of all 8-bit octet strings that can be obtained as the first octet of one instance of the class;
- "part A *follows* part B" means that in the message the sub-string corresponding to part B is concatenated with the sub-string of part B;
- the *length* of a message instance, or of part of message instance, is the number of bits of the corresponding sub string; rigorously speaking, a message as a class (or a part seen as a class) has a length only if all the

corresponding instances have the same length; by extension, sentences such as « a message as a length in the range so and so » means that the length of an instances of the class always fall in the range.

11.1.2 Octets

In many places, a message is described as a succession of octets. An octet is generally a succession of 8 bits. Unless otherwise indicated, the term octet is used more restrictively to refer to a part of message, defined when considering a message as a succession of octets, e.g., the first 8 bits of a message, or the 17th to the 23rd, form an octet, but not the second bit to the 9th.

Unless specified otherwise, the numbering conventions are the following:

- Octets in a message or in a part are numbered from 1 onward, starting at the beginning of the bit string. This numbering can be strictly applied only for message instances, and for the first part of a message structurally identical for all instances.
- Bits in octets are numbered from 8 down to 1, starting at the beginning of the octet.
- When represented as tables showing the different bit positions, octets are presented in the natural occidental order, i.e., from the top of a page downward. Bits in octets are presented with the first bit on the left of the page.

11.1.3 Integer

In many places, message parts are described as encoding integers. Two generic encoding are defined in this subclause.

11.1.3.1 Binary

A message part is said to encode in binary an integer to indicate that concrete strings are mapped, for some usage, on the set of non signed integers with the following rule:

- Let k denote the length of the bit string, and let b(i) denote an integer of value 0 if the i th bit in the string is "0", and 1 otherwise. The encoded integer n respects the equation:

$$n = \sum_{i=1 to k} b(i) 2^{k-i-1}$$

11.1.3.2 2-complement binary

A message part is said to encode in 2-complement binary an integer to indicate that concrete strings are mapped, for some usage, on the set of signed integers with the following rule:

- Let k denote the length of the bit string, and let b(i) denote an integer of value 0 if the i th bit in the string is "0", and 1 otherwise. The encoded integer n respects the equation:

$$\text{if } b(1) = 0 \text{ then } n = \sum_{i=1 to k} b(i) 2^{k-i-1}$$

$$\text{else } n = \sum_{i=1 to k} b(i) 2^{k-i-1} - 2^k$$

11.1.4 Spare parts

In some cases the specification is that which message instances can be accepted by a receiver comprise more that the legal message instances that can be sent. One example of this is the notion of spare bit. A spare bit has to send as the

value indicated in the specification (typically 0), but can be accepted as a 0 or a 1 by the receiver without error diagnosis. A spare field is a field composed entirely of spare bits.

11.2 Standard L3 messages

11.2.1 Components of a standard L3 message

A standard L3 message consists of an imperative part, itself composed of a header and the rest of imperative part, followed by a non-imperative part. Both the non-header part of the imperative part and the non-imperative part are composed of successive parts referred as standard information elements.

11.2.1.1 Format of standard information elements

A standard IE may have the following parts, in that order:

- an information element identifier (IEI);
- a length indicator (LI);
- a value part.

A standard IE has one of the formats shown in table 11.1:

Table 11.1: Formats of information elements

Format	Meaning	IEI present	LI present	Value part present
T	Type only	yes	no	no
V	Value only	no	no	yes
TV	Type and Value	yes	no	yes
LV	Length and Value	no	yes	yes
TLV	Type, Length and Value	yes	yes	~~Y~~yes
TLV-E	Type, Length and Value	yes	yes	yes

Some IEs may appear in the structure, but not in all instances of messages. An IE is then said to be present or not present in the message instance. If an IE is not present in a message instance, none of the three parts is present. Otherwise, parts must be present according to the IE format.

In the message structure, an IE that is allowed not to be present in all message instances is said not to be mandatory. Other IEs are said to be mandatory.

TLV-E is used for EPS Mobility Management (EMM) and EPS Session Management (ESM) only.

11.2.1.1.1 Information element type and value part

Every standard IE has an information element type which determines the values possible for the value part of the IE, and the basic meaning of the information. The information element type describes only the value part. Standard IEs of the same information element type may appear with different formats. The format used for a given standard IE in a given message is specified within the description of the message.

The value part of a standard IE either consists of a half octet or one or more octets; the value part of a standard IE with format LV or TLV consists of an integral number of octets, between 0 and 255 inclusive; it then may be empty, i.e., consist of zero octets; if it consists of a half octet and has format TV, its IEI consists of a half octet, too. For TLV-E, the value part of a standard IE consists of an integral number of octets, between 0 and 65535 inclusive. The value part of a standard IE may be further structured into parts, called fields.

11.2.1.1.2 Length indicator

For LV or TLV, ~~When present,~~ the LI of a standard IE consists of one octet. For TLV-E, the LI of a standard IE consists of two octets. It contains the binary encoding of the number of octets of the IE value part. The length indicator of a standard IE with empty value part indicates 0 octets. Standard IE of an information element type such that the possible values may have different values must be formatted with a length field, i.e., LV, ~~or~~ TLV, or TLV-E.

11.2.1.1.3 Information element identifier

When present, the IEI of a standard IE consists of a half octet or one octet. A standard IE with IEI consisting of a half octet has format TV, and its value part consists of a half octet. The value of the IEI depends on the standard IE, not on its information element type. The IEI, if any, of a given standard IE in a given message is specified within the description of the message. In some protocol specifications, default IEI values can be indicated. They are to be used if not indicated in the message specification. Non mandatory standard IE in a given message, i.e., IE which may be not be present (formally, for which the null string is acceptable in the message), must be formatted with an IEI, i.e., with format T, TV, TLV or TLV-E.

11.2.1.1.4 Categories of IEs; order of occurrence of IEI, LI, and value part

Totally four categories of standard information elements are defined:

- information elements of format V or TV with value part consisting of 1/2 octet (type 1);
- information elements of format T with value part consisting of 0 octets (type 2);
- information elements of format V or TV with value part that has fixed length of at least one octet (type 3);
- information elements of format TLV or LV with value part consisting of zero, one or more octets (type 4)
- information elements of format TLV-E with value part consisting of zero, one or more octets and a maximum of 65535 octets (type 6). This category is used in EPS only.

Type 1 standard information elements of format V provide the value in bit positions 8, 7, 6, 5 of an octet (see figure 11.1) or bits 4, 3, 2, 1 of an octet (see figure 11.2).

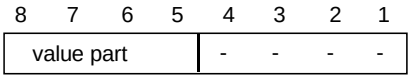


Figure 11.1: Type 1 IE of format V

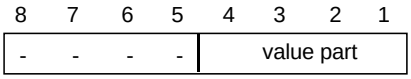


Figure 11.2: Type 1 IE of format V

Type 1 standard information elements of format TV have an IEI of a half octet length; they provide the IEI in bit positions 8, 7, 6, 5 of an octet and the value part in bit positions 4, 3, 2, 1 of the same octet, see figure 11.3.

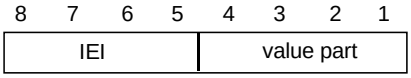


Figure 11.3: Type 1 IE of format TV

A type 2 standard IE has format T; its IEI consists of one octet, its value part is empty, see figure 11.4.

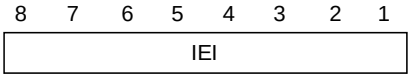


Figure 11.4: Type 2 IE

A type 3 standard information element has format V or TV; if it has format TV, its IEI consists of one octet and proceeds the value part in the IE. The value part consists of at least one octet. See figure 11.5 and figure 11.6.

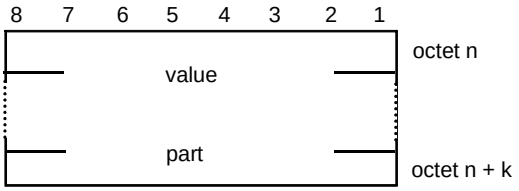


Figure 11.5: Type 3 IE of format V (k = 0, 1, 2, ...)

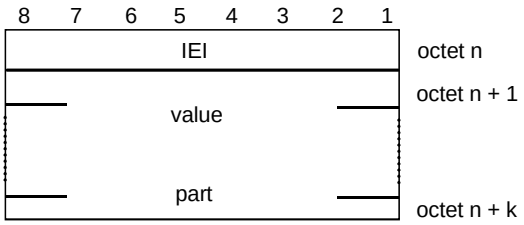


Figure 11.6: Type 3 IE of format TV (k = 1, 2, ...)

A type 4 standard information element has format LV or TLV. Its LI precedes the value part, which consists of zero, one, or more octets; if present, its IEI has one octet length and precedes the LI. See figure 11.7 and figure 11.8.

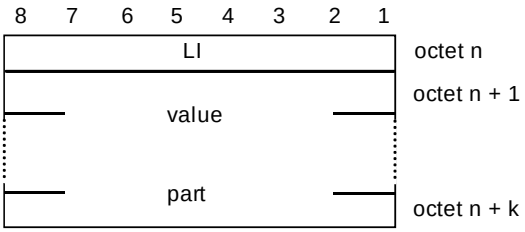


Figure 11.7: Type 4 IE of format LV (k = 0, 1, 2, ...)

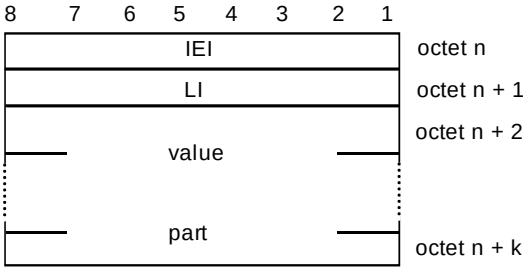


Figure 11.8: Type 4 IE of format TLV (k = 1, 2, ...)

A type 6 standard information element has format TLV-E. The IEI has one octet length and precedes the LI of 2 octets and the value part which consists of zero, one or up to 65535 octets. See figure 11.9.

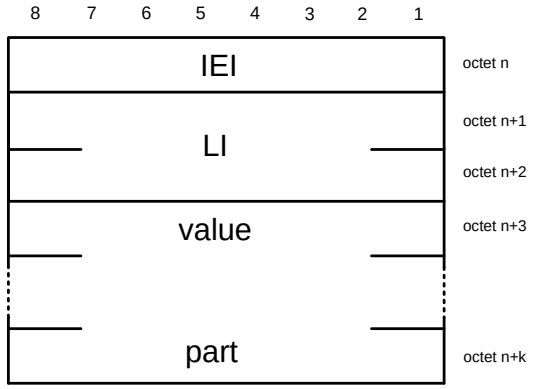


Figure 11.9: Type 6 IE of format TLV-E (k = 1, 2, ...)

11.2.2 Description methods for IE structure

Standard IEs can be further structured in parts called fields. Two description methods are recommended and described hereafter.

11.2.2.1 Tables

According to this description method, the IE is presented in its maximum format, i.e., T, TV ~~or,~~ TLV or TLV-E, in a picture representing the bits in a table, each line representing an octet. Bits appear in the occidental order, i.e., from left of the page to right of the page, and from top of the page to bottom of the page.

Boxes so delimited contains typically the field name, possibly an indication of which bits in the field are in the box, and possibly a value (e.g., for spare bits).

A specific method can be used in the IE description to describe a branching structure, i.e., a structure variable according to the value of particular fields in the IE. This design is unusual outside type 4 IEs, and as, a design rule, should be used only in type 4 IEs.

a) The octet number of an octet within the IE is defined typically in the table. It consists of a positive integer, possibly of an additional letter, and possibly of an additional asterisk, see clause f). The positive integer identifies one octet or a group of octets.

b) Each octet group is a self contained entity. The internal structure of an octet group may be defined in alternative ways.

c) An octet group is formed by using some extension mechanism. The preferred extension mechanism is to extend an octet (N) through the next octet(s) (Na, Nb, etc.) by using bit 8 in each octet as an extension bit.

- The bit value "0" indicates that the octet group continues through to the next octet. The bit value "1" indicates that this octet is the last octet of the group. If one octet (Nb) is present, the preceding octets (N and Na) shall also be present.

- In the format descriptions of the individual information elements, bit 8 is marked "0/1 ext" if another octet follows. Bit 8 is marked "1 ext" if this is the last octet in the extension domain.

- Additional octets may be defined in later versions of the protocols ("1 ext" changed to "0/1 ext") and equipments shall be prepared to receive such additional octets; the contents of these octets shall be ignored. However the length indicated in the formal description of the messages and of the individual information elements only takes into account this version of the protocols.

d) In addition to the extension mechanism defined above, an octet (N) may be extended through the next octet(s) (N+1, N+2 etc.) by indications in bits 7-1 (of octet N).

e) The mechanisms in c) and d) may be combined.

f) Optional octets are marked with asterisks (*). As a design rule, the presence of absence of an optional octet should be determinable from information in the IE and preceding the optional octet. Care should be taken not to introduce ambiguities with optional octets.

g) At the end of the IE, additional octets may be added in later versions of the protocols also without using the mechanisms defined in c) and d). Equipments shall be prepared to receive such additional octets; the contents of these octets shall be ignored. However the length indicated in the formal description of the messages and of the individual information elements only takes into account this version of the protocols.

11.2.2.1.1 Compact notation

The compact notation described in Annex B can be used to describe the value part of a standard IE. This method is recommended for complex structures, or for a branching structure not respecting octet boundaries.

11.2.3 Imperative part of a standard L3 message

The imperative part of a standard L3 message is composed a header possibly followed by mandatory standard IEs having the format V or LV.

11.2.3.1 Standard L3 message ~~H~~header

The header of a standard L3 message is composed of two octets, and structured in three main parts, the protocol discriminator (1/2 octet), a message type octet, and a half octet used in some cases as a Transaction Identifier, in some other cases as a sub-protocol discriminator, and called skip indicator otherwise.

For the EPS protocols EMM and ESM, the header of a standard L3 message without security protection is composed of two or three octets, and structured in four main parts, the protocol discriminator (1/2 octet), a half octet used in some cases as security header type and in other cases as an EPS bearer identity (1/2 octet), a message type octet, and one octet included in some cases and used as a protocol transaction identity (PTI). If the protocol transaction identity is present, it is preceding the message type octet.

In EPS, the header of a security protected standard L3 message is composed of six octets, and structured in four main parts, the protocol discriminator (1/2 octet), a half octet used as security header type, a message authentication code of four octets, and a sequence number of one octet. This header is followed by a complete non-security protected standard L3 message (i.e. including the header of this standard L3 message).

11.2.3.1.1 Protocol discriminator

Bits 1 to 4 of the first octet of a standard L3 message contain the protocol discriminator (PD) information element. The PD identifies the L3 protocol to which the standard layer 3 message belongs. The correspondence between L3 protocols and PDs is one-to-one.

For future evolution an extension mechanism is foreseen which allows the use of protocol discriminators with one octet length, where bits 4 to one are coded as 1 1 1 0. Messages of such protocols may not be standard L3 messages. In particular, the rest of the header may not respect the structure described in this sub-clause.

The PD can take the following values:

Table 11.2: Protocol discriminator values

bits 4 3 2 1	
0 0 0 0	group call control
0 0 0 1	broadcast call control
0 0 1 0	EPS session management messages~~Reserved: was allocated in earlier phases of the protocol~~
0 0 1 1	call control; call related SS messages
0 1 0 0	GPRS Transparent Transport Protocol (GTTP)
0 1 0 1	mobility management messages
0 1 1 0	radio resources management messages
0 1 1 1	EPS mobility management messages
1 0 0 0	GPRS mobility management messages
1 0 0 1	SMS messages
1 0 1 0	GPRS session management messages
1 0 1 1	non call related SS messages
1 1 0 0	Location services specified in 3GPP TS 44.071 [8a]
1 1 1 0	reserved for extension of the PD to one octet length
1 1 1 1	reserved for tests procedures described in 3GPP TS 44.014 [5a] and 3GPP TS 34.109 [17a].

If the network receives, on a SAP where it expects standard L3 messages, a message with a protocol discriminator different from those specified in table 11.2, the network may ignore the message or initiate the channel release procedure defined in 3GPP TS 44.018 [6b].

If the Mobile Station receives, on a SAP where it expects standard L3 messages, a standard L3 message with a protocol discriminator different from those specified in table 11.2, or for a protocol that it does not support, the Mobile Station shall ignore the message.

11.2.3.1.2 Skip indicator

Bits 5 to 8 of octet 1 of a standard L3 message may be used differently, depending on the protocol and the SAP. The use of this half-octet is consistent for a given PD and SAP. One possibility is that this half-octet contains the skip indicator. Unless otherwise specified in the protocol, the skip indicator IE is a spare field.

11.2.3.1.3 Transaction identifier

A L3 protocol may define that bits 5 to 8 of octet 1 of a standard L3 message of the protocol contains the transaction identifier (TI). The TI allows to distinguish up to 16 different bi-directional messages flows for a given PD and a given SAP. Such a message flow is called a transaction.

An extension mechanism for TI is also defined. This mechanism allows to distinguish up to 256 different bi-directional messages flows for a given PD and a given SAP. The extension mechanism shall not be used unless explicitly stated in the core specification(s) for the protocol. The TI IE is coded as shown in figure 11.9 and table 11.3. It is composed of the TI value and the TI flag.

The TI value and the TI flag occupy bits 5 - 7 and bit 8 of the first octet respectively.

The extended TI shall not be used unless TI values of 7 or greater are needed.

Where the extended TI is used, the TI IE includes a second octet. The TI value in the first octet is ignored, and the TI value is encoded in bits 7-1 of the second octet.

NOTE: In other specifications, in respect to error handling, there are references to TI value "111". This refers to the binary encoding of bits 5 –7 in octet 1. For protocols which do not use the extended TI this '111' encoding is still handled as an error case.Transactions are dynamically created, and their TI value is assigned at creation time. TI values are assigned by the side of the interface initiating a transaction. At the beginning of a transaction a free TI value (i.e., a value not yet used for the given PD, the given SAP, and with the given initiator) is chosen and assigned to this transaction. It then remains fixed for the lifetime of the transaction. After a transaction ends, the associated TI value is free and may be reassigned to a later transaction.

Two identical TI values may be used when each value pertains to a transaction initiated by the different sides of the interface. In this case the TI flag shall avoid ambiguity. The transaction identifier flag can take the values "0" or "1". The TI flag is used to identify which side of the interface initiated the transaction. A message has a TI flag set to "0" when it belongs to transaction initiated by its sender, and to "1" otherwise.

Hence the TI flag identifies who allocated the TI value for this transaction and the only purpose of the TI flag is to resolve simultaneous attempts to allocate the same TI value.

The TI extension mechanism may in future evolution of the L3 protocols be further extended by setting the EXT flag in octet 2 to "0" (see figure 11.9).

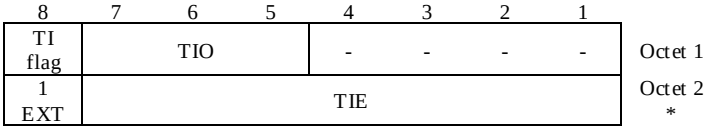


Figure 11.9: Transaction identifier

Table 11.3: Transaction identifier

TI flag (octet 1)	
Bit	
8	
0	The message is sent from the side that originates the TI
1	The message is sent to the side that originates the TI
TIO (octet 1)	
Bits	
7 6 5	
0 0 0	TI value 0
0 0 1	- - 1
0 1 0	- - 2
0 1 1	- - 3
1 0 0	- - 4
1 0 1	- - 5
1 1 0	- - 6
1 1 1	The TI value is given by the TIE in octet 2
TIE (octet 2)	
Bits 7-1	
0000000	Reserved.
0000001	
0000010	
0000011	
0000100	
0000101	
0000110	
All other values	The TI value is the binary representation of TIE Where bit 7 is the most significant bit And bit 1 is the least significant bit

11.2.3.1.4 Sub-protocol discriminator

A L3 protocol may define that bits 5 to 8 of octet 1 of a standard L3 message of the protocol contains the sub-protocol discriminator (SPD). The SPD allows to distinguish between different protocols inside one sublayer.

Table 11.4: Sub-Protocol discriminator values

bits 8 7 6 5	
0 0 0 0	Value used by the Skip Indicator (see 11.2.3.1.2)
0 0 0 1	CTS sub-protocol
0 0 1 0	\
To	} all other values are reserved
1 1 1 1	/

11.2.3.1.5 EPS bearer identity

A L3 protocol may define that bits 5 to 8 of octet 1 of a standard L3 message of the protocol contain the EPS bearer identity. The EPS bearer identity is used to identify a message flow.

Editor's note: It is proposed to define that value '0000' is to be used, if no EPS bearer identity is assigned to a procedure, values '0001 to '0100' are reserved, and values '0101' to '1111' are allocated for EPS bearer identity values 5 to 15, respectively.

11.2.3.1.6 Security header type

A L3 protocol may define that bits 5 to 8 of octet 1 of a standard L3 message of the protocol contain the security header type.

11.2.3.1a Procedure transaction identity

A L3 protocol may define that octet 2 of a standard L3 message of the protocol contains the procedure transaction identity (PTI). The PTI allows distinguishing up to 256 different bi-directional messages flows for a given PD and a given SAP. Such a message flow is called a transaction. The procedure transaction identity is released when the procedure is completed.

11.2.3.2 Message type octet

11.2.3.2.1 Message type octet (when accessing Release 98 and older networks only)

The message type octet is the second octet in a standard L3 message.

When a standard L3 message is expected, and a message is received that is less than 16 bit long, that message shall be ignored.

When the radio connection started with a core network node of a Release 98 or older network, the message type IE is coded as shown in figure 11.10a and 11.10x.

Bit 8 is encoded as "0"; value "1" is reserved for possible future use as an extension bit. A protocol entity expecting a standard L3 message, and receiving a message containing bit 8 of octet 2 encoded as "1" shall diagnose a " message not defined for the PD" error and treat the message accordingly.

In messages of MM, CC, SS (via CS domain), GCC and BCC protocol sent using the transmission functionality provided by the RR layer to upper layers, and sent from the mobile station or the LMU to the network, bit 7 of octet 2 is used for send sequence number, see subclause 11.2.3.2.3.

In messages of the LCS protocol sent using the transmission functionality provided by the RR layer to upper layers, and sent from the type A LMU to the network, bit 7 of octet 2 is used for send sequence number, see subclause 11.2.3.2.3.

In all other standard layer 3 messages, except for RR messages, bit 7 is set to a default value. A protocol entity expecting a standard L3 message, and not using the transmission functionality provided by the RR layer, and receiving a message containing bit 7 of octet 2 encoded different to the default value shall diagnose a "message not defined for the PD" error and treat the message accordingly.

The default value for bit 7 is 0 except for the SM protocol where the default value is 1. No default value for bit 7 is specified for RR protocol. For RR message types see 3GPP TS 44.018.

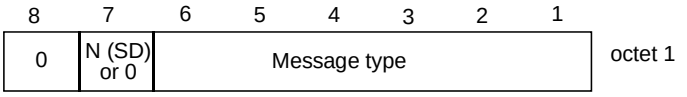


Figure 11.10a: Message type IE (MM, CC, SS, GCC, BCC and LCS)

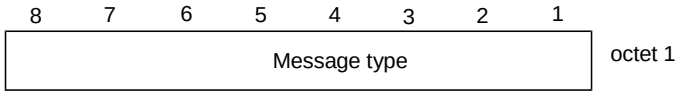


Figure 11.10x: Message type IE (protocol other than MM, CC, SS, GCC, BCC and LCS)

For MM, CC, SS, GCC, BCC and LCS protocols bits 1 to 6 of octet 2 of standard L3 messages contain the message type. For all other L3 protocols bits 1 to 8 of octet 2 of standard L3 message contain the message type.

The message type determines the function of a message within a protocol in a given direction. The meaning of the message type is therefore dependent on the protocol (the same value may have different meanings in different protocols), and the direction (the same value may have different meanings in the same protocol, when sent from the Mobile Station to the network and when sent from the network to the Mobile Station).

Each protocol defines a list of allowed message types for each relevant SAP. A message received analysed as a standard L3 message, and with a message type not in the corresponding list leads to the diagnosis "message not defined for the PD". Some message types may correspond to a function not implemented by the receiver. They are then said to be not implemented by the receiver.

The reaction of a protocol entity expecting a standard L3 message and receiving a message with message type not defined for the PD or not implemented by the receiver and the reception conditions is defined in the relevant protocol specification. As a general rule, a protocol specification should not force the receiver to analyse the message further.

11.2.3.2.2 Message type octet (when accessing Release 99 and newer networks)

The message type octet is the second octet in a standard L3 message.

When a standard L3 message is expected, and a message is received that is less than 16 bit long, that message shall be ignored.

When the radio connection started with a core network node of a Release 99 or later network, the message type IE is coded dependent on the PD as shown in figures 11.10b, c and d.

In messages of MM, CC and SS (via CS domain) protocol sent using the transmission functionality provided by the RR and/or access stratum layer to upper layers, and sent from the mobile station or the LMU to the network, bits 7 and 8 of octet 2 are used for send sequence number, see clause 11.2.3.2.3.

In messages of GCC and BCC protocol sent using the transmission functionality provided by the RR layer to upper layers, and sent from the mobile station or the LMU to the network, only bit 7 of octet 2 is used for send sequence number. Bit 8 is set to the default value.

In messages of the LCS protocol sent using the transmission functionality provided by the RR layer to upper layers, and sent from the type A LMU to the network, only bit 7 of octet 2 is used for send sequence number. Bit 8 is set to the default value.

In all other standard layer 3 messages, except for RR messages, bits 7 and 8 are set to the default value. A protocol entity expecting a standard L3 message, and not using the transmission functionality provided by the RR and/or access stratum layer, and receiving a message containing bit 7 or bit 8 of octet 2 encoded different to the default value shall diagnose a "message not defined for the PD" error and treat the message accordingly.

In messages of the RR protocol entity, bit 8 of octet 2 is set to the default value. The other value is reserved for possible future use as an extension bit .If an RR protocol entity expecting a standard L3 message receives message containing bit 8 of octet 2 encoded different from the default value it shall diagnose a "message not defined for the PD" error and treat the message accordingly.

The default value for bit 8 is 0. The default value for bit 7 is 0 except for the SM protocol which has a default value of 1. No default value for bit 7 is specified for RR protocol. For RR message types see 3GPP TS 44.018.

For EPS; the default value for bit 7 is 1. The value for bit 8 is 0 for the EMM protocol and 1 for the ESM protocol.

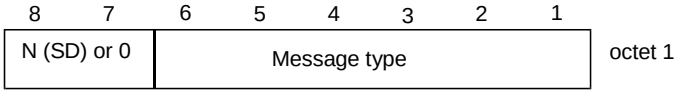


Figure 11.10b: Message type IE (MM, CC and SS)

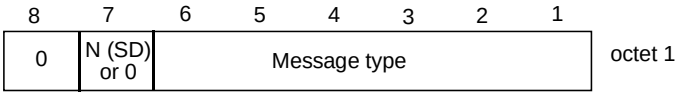


Figure 11.10c: Message type IE (GCC, BCC and LCS)

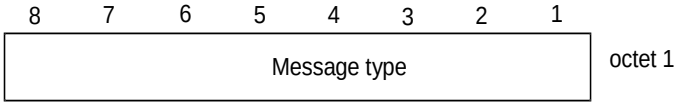


Figure 11.10d: Message type IE (protocol other than MM, CC, SS, GCC, BCC and LCS)

For MM, CC, SS, GCC, BCC and LCS protocols bits 1 to 6 of octet 2 of standard L3 messages contain the message type. For all other L3 protocols bits 1 to 8 of octet 2 of standard L3 message contain the message type.

The message type determines the function of a message within a protocol in a given direction. The meaning of the message type is therefore dependent on the protocol (the same value may have different meanings in different protocols), and the direction (the same value may have different meanings in the same protocol, when sent from the Mobile Station to the network and when sent from the network to the Mobile Station).

Each protocol defines a list of allowed message types for each relevant SAP. A message received analysed as a standard L3 message, and with a message type not in the corresponding list leads to the diagnosis "message not defined for the PD". Some message types may correspond to a function not implemented by the receiver. They are then said to be not implemented by the receiver.

The reaction of a protocol entity expecting a standard L3 message and receiving a message with message type not defined for the PD or not implemented by the receiver and the reception conditions is defined in the relevant protocol specification. As a general rule, a protocol specification should not force the receiver to analyse the message further.

11.2.3.2.3 Sequenced message transfer operation

Upper layer messages sent using the RR sub-layer transport service from the mobile station to the network can be duplicated by the data link layer in at least the following cases:

- in A/Gb mode, when a channel change of dedicated channels is required (assignment or handover procedure) and the last layer 2 frame has not been acknowledged by the peer data link layer before the mobile station leaves the old channel;
- in Iu mode, when an RLC re-establishment occurs (e.g. due to relocation) and the RLC layer has not acknowledged the last one or more RLC PDUs before RLC re-establishment;

- an inter-system change from Iu mode to A/Gb mode is performed and the RLC layer has not acknowledged the last one or more RLC PDUs;

- an inter-system change from A/Gb mode to Iu mode is performed and the ~~the~~ last layer 2 frame in A/Gb mode has not been acknowledged by the peer data link layer before the mobile station leaves the old channel.

Editor's note: the corresponding scenario for message duplication in S1 mode is FFS.

In these cases, the mobile station does not know whether the network has received the messages correctly. Therefore, the mobile station has to send the messages again when the channel change is completed.

The network must be able to detect the duplicated received messages. Therefore, each concerned upper layer messages must be marked with a send sequence number.

To allow for different termination points in the infrastructure of the messages of different PDs, the sequence numbering is specific to each PD. For historical reasons, an exception is that messages sent with the CC, SS (via CS domain) and MM PDs share the same sequence numbering. In the following, the phrase **upper layer message flow** refers to a flow of messages sharing the same sequence numbering. The different upper layer flows are MM+CC+SS (via CS domain), GCC, BCC and LCS. The GMM, EMM, SM, ESM, SMS, SS (via PS domain) and TC (Test Control, see 3GPP TS 44.014 [5a] and 3GPP TS 34.109 [17a]) protocols do not use layer 3 sequence numbering.

Editor's note: a test specification for EPS needs to be added.

Formatted: Editor'sNote;EN

In a shared network with a MOCN configuration, Network Sharing non-supporting UEs can be redirected between CN operators (see 3GPP TS 23.251 [22]). When the redirection takes place, the CN node of the redirecting CN operator shall forward via the RAN the value of N(SD) of the last message received on the MM+CC+SS (via CS domain) message flow to the CN node of the next CN operator (3GPP TS 25.413 [23]).

11.2.3.2.3.1 Variables and sequence numbers

11.2.3.2.3.1.1 Send state variable V(SD)

The mobile station shall have one associated send state variable V(SD) ("Send Duplicated") for each upper layer message flow. The send state variable denotes the sequence number of the next in sequence numbered message in the flow to be transmitted. The value of the corresponding send state variable shall be incremented by one with each numbered message transmission.

For the MM+CC+SS (via CS domain) upper layer message flow, when the RR connection starts with a core network of release 98 or earlier, arithmetic operations on V(SD) are performed modulo 2. When the RR connection starts with a core network of Release 99 or later, arithmetic operations on V(SD) are performed modulo 4. The mobile station shall keep using the same modulo (2 or 4) for the duration of the RR connection.

For the GCC, BCC, and LCS upper layer message flows, arithmetic operations on V(SD) are performed modulo 2.

NOTE: In GSM, the release supported by the core network is indicated in the MSCR bit and in the SGSNR bit in the system information broadcast (see 3GPP TS 44.018 [6b] and 3GPP TS 44.060 [10a]).

11.2.3.2.3.1.2 Send sequence number N(SD)

At the time when such a message to be numbered is designated for transmission, the value of N(SD) for the message to be transferred is set equal to the value of the send state variable V(SD).

11.2.3.2.3.2 Procedures for the initiation, transfer execution and termination of the sequenced message transfer operation

11.2.3.2.3.2.1 Initiation

The sequenced message transfer operation is initiated by establishing a RR connection. The send state variables V(SD) are set to 0.

11.2.3.2.3.2.2 Transfer Execution

The core network shall compare the send sequence numbers of pairs of subsequent messages in the same upper layer messages flow.

For the GCC, BCC, and LCS upper layer message flows, in case the send sequence numbers of two subsequent messages in a flow are not identical, no duplication has occurred. In case the send sequence numbers are identical, the network must ignore the second one of the received messages.

For the MM+CC+SS (via CS domain) upper layer message flow:

- when accessed by a release 98 or earlier mobile station, in case the send sequence numbers of two subsequent messages in the flow are identical, the core network shall discard the second one of the received messages;
- when accessed by a release 99 or later mobile station, the core network shall discard any message whose N(SD) is not the increment by one (modulo 4) of the N(SD) of the last accepted message.

NOTE: The release supported by the mobile station is indicated by the revision level in *the Mobile Station Classmark 1* or *Mobile Station Classmark 2* information element, or by the revision level indicator in the *MS network capability* information element (see 3GPP TS 24.008, subclause 10.5).

In a shared network with a MOCN configuration, the core network node to which the mobile station was redirected shall compare the send sequence number of the first message received after the redirection in the MM+CC+SS (via CS domain) message flow with the value of N(SD) received during the redirection procedure (see 3GPP TS 23.251 [22]):

- when accessed by a release 98 or earlier mobile station, if the two send sequence numbers are identical, the core network shall discard the received message from the mobile station;
- when accessed by a release 99 or later mobile station, the core network shall discard any message whose N(SD) is not the increment by one (modulo 4) of the N(SD) received during the redirection procedure.

11.2.3.2.3.2.3 Termination

The sequenced message transfer operation is terminated by the RR connection release procedure.

Inter system change from A/Gb mode to Iu mode or from Iu mode to A/Gb mode shall not terminate the sequenced message transfer. UMTS SRNC relocation shall not terminate the sequenced message transfer.

11.2.3.3 Standard information elements of the imperative part

The message type octet of a standard L3 message may be followed by mandatory standard IEs having the format V or LV as specified in the message description in the relevant protocol specification.

As a design rule, octet boundaries must be respected. This implies that half-octet standard IEs (i.e., V formatted type 1 standard IEs) must appear by pair.

If message is received as a standard L3 message, and that is too short to contain the complete imperative part as specified in the relevant protocol specification, an imperative message part error is diagnosed. (The same error may be diagnosed at detection of certain contents of the imperative part of a message; this is defined in the relevant protocol specification.) The treatment of an imperative message part error is defined in the relevant protocol specification.

11.2.4 Non-imperative part of a standard L3 message

Editor's note: This text needs to be revised and open issues need to be identified to cover for TLV-E format type 6 - FFS.

The imperative part of a standard L3 message is followed by the (possibly empty) non-imperative part. The relevant protocol specification defines where the imperative part of a standard L3 message ends. The non-imperative part of a standard L3 message is composed of (zero, one, or several) standard IEs having the format T, TV, ~~or~~ TLV or TLV-E. The receiver of a standard L3 message shall analyse the non imperative part as a succession of standard IEs each containing an IEI, and shall be prepared for the non-imperative part of the message to contain standard IEs that are not specified in the relevant protocol specification.

An IEI may be known in a message or unknown in a message. Each protocol specification lists, for each message (i.e., according to the message type, the direction and the lower layer SAP), the known standard IEs in the non-imperative part.

An IEI that is known in a message designates the IE type of the IE the first part of which the IEI is, as well as the use of the information. Which IE type it designates is specified in the relevant protocol specification. Within a message, different IEIs may designate the same IE type if that is defined in the relevant protocol specification.

Whether the second part of an IE with IEI known in a message is the length or not (in other words, whether the IEI is the first part of an IE formatted as TLV, TLV-E or not) is specified in the relevant protocol specification.

Unless otherwise specified in the protocol specification, the receiver shall assume that IE with unknown IEI are TV formatted type 1, T formatted type 2, ~~or~~ TLV formatted type 4 or TLV-E formatted type 6 standard IEs. The IEI of unknown IEs together with, when applicable, the length indicator, enable the receiver to determine the total length of the IE, and then to skip unknown IEs. The receiver shall assume the following rule for IEs with unknown IEI:

> Bit 8 of the IEI octet is set to "1" indicates a TV formatted type 1 standard IE or a T formatted type 2 IEs.; Hence, a 1 valued bit 8 indicates that the whole IE is one octet long.

Furthermore, for the EPS protocols EMM and ESM:

> Bit 8 of the IEI octet set to "0" and bits 7 to 4 set to "1" indicates a TLV-E formatted type 6 IE, i.e. the following two octets are length octets. Bit 8 of the IEI octet set to "0" and bit 7 to 4 set to any other bit combination indicates a TLV formatted type 4 IE, i.e. the following octet is a length octet.

For all other protocols:

> Bit 8 of the IEI octet set ~~and~~ to "0" indicates a TLV formatted type 4 IE. Hence, ~~a 1 valued bit 8 indicates that the whole IE is one octet long, and a 0 valued bit 8 indicates that~~ the following octet is a length octet.

As a design rule, it is recommended that IEIs of any TV formatted type 1, T formatted type 2, ~~or~~ TLV formatted type 4 or TLV-E formatted type 6 IE follow the rule, even if assumed to be known by all potential receivers.

A message may contain two or more IEs with equal IEI. Two IEs with the same IEI in a same message must have the same format, and, when of type 3, the same length. More generally, care should be taken not to introduce ambiguities by using an IEI for two purposes. Ambiguities appear in particular when two IEs potentially immediately successive have the same IEI but different meanings and when both are non-mandatory. As a recommended design rule, messages should contain a single IE of a given IEI.

Each protocol specification may put specific rules for the order of IEs in the non-imperative part. An IE known in the message, but at a position non compliant with these rules is said to be out of sequence. An out of sequence IE is decoded according to the format, and, when of type 3 the length, as defined in the message for its IEI.

11.2.5 Presence requirements of information elements

The relevant protocol specification may define three different presence requirements (M, C, or O) for a standard IE within a given standard L3 message:

- M ("Mandatory") means that the IE shall be included by the sending side, and that the receiver diagnoses a "missing mandatory IE" error when detecting that the IE is not present. An IE belonging to the imperative part of a message has presence requirement M. An IE belonging to the non-imperative part of a message may have presence requirement M;
- C ("Conditional") means:
  - * that inclusion of the IE by the sender depends on conditions specified in the relevant protocol specification;
  - * that there are conditions for the receiver to expect that the IE is present and/or conditions for the receiver to expect that the IE is not present in a received message of a given PD, SAP and message type; these conditions depend only on the content of the message itself, and not for instance on the state in which the message was received, or on the receiver characteristics; they are known as static conditions;

* that the receiver detecting that the IE is not present when sufficient static conditions are fulfilled for its presence, shall diagnose a "missing conditional IE" error;

* that the receiver detecting that the IE is present when sufficient static conditions are fulfilled for its non-presence, shall diagnose an "unexpected conditional IE" error.

- Only IEs belonging to the non-imperative part of a message may have presence requirement C;

- O ("Optional") means that the receiver shall never diagnose a "missing mandatory IE" error, a "missing conditional IE" error, or an "unexpected conditional IE" error because it detects that the IE is present or that the IE is not present. (There may however be conditions depending on the states, resources, etc. of the receiver to diagnose other errors.) Only IEs belonging to the non-imperative part of a message may have presence requirement O.

Unless otherwise specified the presence of a IE of unknown IEI or of an out of sequence IE shall not lead by itself to an error. An alternative specification is the 'comprehension required' scheme. A ~~n~~ type 4 IE is encoded as 'comprehension required' if bits 5, 6, 7 and 8 of its IEI are set to zero. A type 6 IE is encoded as 'comprehension required' if bit 8 is set to zero and bits 3, 4, 5, 6, and 7 of its IEI are set to one. The 'comprehension required' scheme is to be applied if explicitly indicated in the protocol specification. The reaction on the reception of an unknown or out of sequence IE coded as 'comprehension required' is specified in the relevant protocol specification.

11.2.6 Description of standard L3 messages

This subclause describes a generic description method for standard L3 messages, the tabular description. Protocol specification may follow other methods.

A standard L3 message is described by a table listing the header elements and the standard IEs in the message. For each element is given:

- if applicable the IEI, in hexadecimal representation (one digit followed by and hyphen for TV formatted type 1, and two digits for the other cases);

- the name of the IE (this is used in particular for the description of conditional presence rules);

- the type of the information element, with a reference of where the internal structure of the value part is specified;

- the format of the standard IE (T, V, TV, LV ~~or~~, TLV or TLV-E); and

- the length, or the range of lengths, of the whole standard IE, including when applicable the T and L parts.

The list of elements is given in the table in the order they appear in the resulting bit string, with the exception of half-octet elements in the imperative part: half octets in a pair are inverted. This applies in particular for the two first header elements: the protocol discriminator appears first in a table describing a standard L3 message.

11.3 Non standard L3 messages

In some protocols, the structure of part or all of the messages might not always follow the standard L3 message structure. As a design rule, this should be consistent for a given protocol, direction and lower layer SAP.

A possibility is to describe the message with the compact notation described in Annex B.

A few consistent structures are found in the present protocol specifications, and are described hereafter.

Other structures can be described directly in the protocol specifications.

11.3.1 Case A: BCCH and AGCH/PCH messages

In these cases, the SAP capability is for fixed length messages. The messages are structured as standard L3 messages plus one octet in front, the L2 pseudo length octet, and a rest octet part at the end.

11.3.1.1 L2 Pseudo Length octet

This octet, the L2 pseudo length indicator octet, indicates the length in octets of the subsequent octet string that can be analysed as a standard L3 message.

The octet is structured as follows:

Bits 3 to 8 encodes in binary the L2 pseudo length, i.e., the length of the part to be analysed as a standard L3 message;

Bit 2 is set to "0";

Bit 1 is set to "1".

A receiver expecting a message so structured and receiving a message with bit 1 of octet 1 (i.e., the 8th bit of the message) set to "1" and bit 2 of octet 1 (i.e., the 7th bit of the message) different from "0", shall abandon the analysis of the message.

A receiver expecting a message so structured and receiving a message on AGCH/PCH:

- with an L2 pseudo length indicator encoding 0 or 1 shall skip the indicated number of octets and not try to analyse the standard L3 message part;

- with a L2 pseudo length indicator bigger than what is compatible with the SAP capability shall abandon the analysis of the message.

11.3.1.2 Rest Octets

The part after the part structured as a standard L3 message, and up to the end of the message as constrained by lower layers, is presented as a non standard IE of variable length (sometime indicated as of type 5), the "rest octets" IE.

The rest octets element may be described by table description, or, preferably, using the compact notation described in Annex B of the present document.

11.3.1.3 Description of a modified standard L3 message

The description can be provided in the same way as a standard L3 message, with in the case of a tabular description one non standard IE at the beginning (of type L2 pseudo length), and one non standard IE at the end.

11.3.2 Case B: SACCH / SDCCH / FACCH messages sent in unacknowledged mode

The messages are structured either as standard L3 messages, or in the so-called short header format. The value of the 8th bit (bit 1 of octet 1) of the link layer PDU distinguishes the two cases. In the case of the short header, the L3 message is the same bit string as the link layer PDU, and has a fixed length. The following description includes the 2-bit link layer header.

11.3.2.1 The first octet

Bits 1 and 2 are the link layer header. Bit 2 of octet 1 is set to "0", and bit 1 is reserved for the link layer.

A protocol discriminator is the first part of the message (starting bit 8 of octet 1). The protocol discriminator field may have different lengths. The following protocol discriminator is defined:

- 0 RR.

All additional PD defined for this structure shall start by 1. The reception of a message with bit 8 of octet 1 set to 1 when expecting a message structured as defined by this clause shall be diagnosed as an unknown PD, and the message ignored.

As a design rule, a message type field should follow the PD, and of a length such that the PD and the message type fit in the 6 first bits of the message.

11.3.2.2 The rest of the message

The rest of the structure is not more constrained.

The preferred description method is the one described in Annex B.

11.3.3 Design guidelines for non standard parts

The guidelines in this subclause apply to non standard parts, such as rest octets, short header broadcast message or fully non standard L3 messages.

11.3.3.1 General

The structure should be as far as possible be such that the analysis can be conducted from beginning to end. In other terms, the conditions determining the syntactic analysis of a part (e.g., tags, lengths) should appear before that part.

The part should be structured as a succession of information elements, each carrying an elementary semantic information. An information element should be composed of (possibly) a tag, than (possibly) a length indicator, then a value part.

Tags can be of fixed or variable length, their extent being analysable from beginning to end. A typical tagging is the one bit tagging, which should preferably used as follows: value "0" indicates that the IE is no more than the tag bit, and "1" indicates that the IE continues at least with the next bit.

Variable length tagging should be used to distinguish between several possible formats of the element. Tag lengths are then chosen according to packing efficiency criteria.

The T field of standard IEs can be presented as a variable tagging with only two lengths: 4 and 8 bits.

The length indicator can be of fixed or variable length, their extent being analysable from beginning to end. It should preferably be presented as encoding the length in bits of the value part.

The L field of standard IEs can be presented as a fixed length (one octet) length indicator which can encode only lengths multiple of 8 bits.

The value part can be described as further structured, in a similar way. This can be used to help the reading, and to cover some presence dependence.

11.4 Handling of superfluous information

All equipment should be able to ignore any extra information present in an L3 message, which is not required for the proper operation of that equipment. For example, a mobile station may ignore the calling party BCD number if that number is of no interest to the Mobile Station when a SETUP message is received.

11.4.1 Information elements that are unnecessary in a message

The relevant protocol specification may define certain IEs to be under some conditions unnecessary in a L3 message. A protocol entity detecting an unnecessary IE in a received L3 message shall ignore the contents of that IE for treating the message; it is not obliged to check whether the contents of the IE are syntactically correct.

11.4.2 Other syntactic errors

This clause applies to the analysis of the value part of an information element. It defines the following terminology:

- An IE is defined to be syntactically incorrect in a message if it contains at least one value defined as "reserved", or if its value part violates syntactic rules given in the specification of the value part.

- It is not a syntactical error that a type 4 and type 6 standard IE specifies in its length indicator a greater length than possible according to the value part specification: extra bits shall be ignored.

- It should not be considered a syntactical error if a type 4 and type 6 IE is received with a shorter length than defined in this version of the specification if the IE is correctly encoded according to an earlier version of the specification.

- A message is defined to have semantically incorrect contents if it contains information which, possibly dependant on the state of the receiver, is in contradiction to the resources of the receiver and/or to the procedural part.

Annex D (informative): Selection of the protocol to be used between the UE and Access Network Discovery and Selection Function (ANDSF)

D.1 Introduction

This Annex documents the candidate protocols that CT1 is studying for use as the protocol to be used between UE and ANDSF.

D.2 Candidate protocols

D.2.1 General

The following protocols have been identified as workable candidate protocols to be used for signalling between UE and ANDSF to fulfil the requirement set down in 3GPP TS 23.402 [12]. The order in which these candidate protocols are presented in the following subclauses is the order in which the candidate protocols were first identified to CT1 and does not represent

- any order of preference of the candidate protocols;
- the workability of one candidate protocol over another;
- the pros and cons weighted against each candidate protocol;
- that any other candidate protocol not yet identified by CT1 is excluded for consideration.

D.2.2 Candidate 1 – IEEE 802.21 Media Independent Handover (MIH) Protocol

D.2.2.1 General

The IEEE 802.21 standard is defining the MIH protocol for facilitating handovers between different access technologies. The latest version of the IEEE 802.21 draft standard [60] describes the different MIH services supported by this protocol. The MIH protocol satisfies the requirements for ANDSF as specified in 3GPP TS 23.402 [12].

D.2.2.2 IEEE 802.21 Information Service

The concept of ANDSF for Network Discovery and Selection was introduced in 3GPP SA2 based on the Media Independent Information Service (MIIS) as described in IEEE 802.21 [60]. The MIIS defines information elements (IEs) for different access networks that can assist with access network discovery and selection. The MIIS also defines data types which can be used to define inter-system mobility policies. The description of operator specific policies is however outside the scope of the current specification. The IEs can be described in RDF (Resource Description Framework)/XML (eXtended Mark up Language) format as part of a schema or in a binary format based on a TLV (Type Length Value) format. Certain core IEs are part of the base schema. Additional IEs can be defined as part of the extended schema (e.g., vendor specific or other SDO specific). These IEs are suitable for specifying both network policies and access network and discovery information that are required by ANDSF.

The support for RDF/ XML based schema allows the UE to make flexible queries. In particular, RDF query (SPARCL) can query structures in any graph topologies while XML query can query only hierarchically structured data. For example, when data type values contained in two IEs are semantically related, XML DTD (Document Type Definition)

cannot express such relationships while RDF schema can. The flexible query mechanism also allows the ANDSF to limit the amount of information that may be sent to the UE. For example, the UE can inquire about a specific type of access network supported within its vicinity (say within a radius of 100 metres) by a specific operator. Using RDF/XML based schema, the UE shall be able to make flexible queries to the ANDSF and can obtain necessary information for Network Discovery and Selection more efficiently.

The information supported by the ANDSF can be easily extended by defining additional IEs using the Extended Schema without impacting the base specification. RDF schema is highly extensible and new data types or structures can be added as separate schema file(s) that extends originally defined schema file(s). This is possible because each piece of information in RDF schema is identified by a global unique URI. The IEEE 802.21 standard places no restriction as to how the information is stored at the server (e.g., as part of ANDSF) or at the UE and thereby allows complete flexibility and extensibility of design. Information can be stored in the UE as part of a schema or in any other form depending on the choice of operating system or system specific implementation.

The base MIH Protocol is independent of the underlying transport. The transport options for MIH Protocol are being defined in IETF as per draft-ietf-mipshop-mstp-solution [61]. For information service, TCP is recommended. The MIH payload can be easily carried by any of the higher layer transport protocols as well. Draft-ietf-mipshop-mstp-solution [61] also defines how the MIH Protocol messages may be transferred across firewalls and NAT traversal.

D.2.2.3 Support of Pull

The IEEE 802.21 MIH Protocol supports a ***request-response*** framework for UEs to obtain information from the information server. This request-response framework can be used to support a pull mechanism between UE and ANDSF. The pull mechanism can be used to obtain both inter-system mobility policies and access network discovery information by the UE.

MIH protocol uses two identifiers: i) Media Independent Handover Function (MIHF) ID and ii) Transaction ID. The MIHF ID is an identifier that is required to uniquely identify an MIHF entity for delivering the information. MIHF ID is used in all MIH protocol messages. MIHF ID is assigned to the MIHF during its configuration process. MIHF_ID is an NAI. NAI shall be unique as per IETF RFC 4282 [64]. If MIHF entity resides in the network node then MIHF_ID is the FQDN or IP address of the entity that hosts the MIH Services. Transaction Identifier (Transaction ID) is an identifier that is used to match a request message with its corresponding response message. The UE can specify query specific parameters as part of the request message. Multiple UEs can issue multiple queries at any time and these can be satisfied asynchronously by the ANDSF using the Transaction Identifier.

D.2.2.4 Support of Push

The IEEE 802.21 MIH Protocol supports an ***indication*** framework to send information from the information server to the UE. Using this framework ANDSF can push information to the UE asynchronously. The indication message that is built into the protocol can push both inter-system mobility policies and access network discovery information to the UEs. The location of the UE can be made known to the ANDSF through the MIH registration performed by the UE.

D.2.2.5 Security

Security for MIH Protocol is being defined by IETF draft-ietf-mipshop-mstp-solution [61]. Security options include using either transport layer or IP layer security. For Information Service TCP is used for transport connection between two MIH peers, Therefore TLS as specified in IETF RFC 4346 [62] should be used for authentication, message confidentiality and data integrity. The peer's identity can be authenticated using asymmetric or public key cryptography. In addition, it is recommended to follow the IETF RFC 4366 [63] that provides generic extension mechanisms for the TLS protocol suitable for wireless environments. The advantage of TLS is that it is application protocol independent. Alternatively, generic IP layer security, such as IPSec (IETF RFC 4301 [27]) may be used where transport layer security is not available.

D.2.2.6 Location

The IEEE 802.21 defines a location IE to represent the UE's point of attachment location. Multiple location types are supported including coordinate-based location information, civic address and cell ID. If UE has its own location information (e.g. GPS location) available, it can add its location as a parameter while sending a query to the information

server (ANDSF). For pull mechanism, UE can then add location information in its query request message and ANDSF can search for access networks in vicinity of UE and return the necessary information via response message. Alternatively, during MIH registration UE can add its own location or point of attachment location (e.g., Cell ID, LAC). In response the information server (ANDSF) can push the necessary information to the UE. Therefore IEEE 802.21 information service and MIH protocol have necessary capabilities to inform UE location to ANDSF.

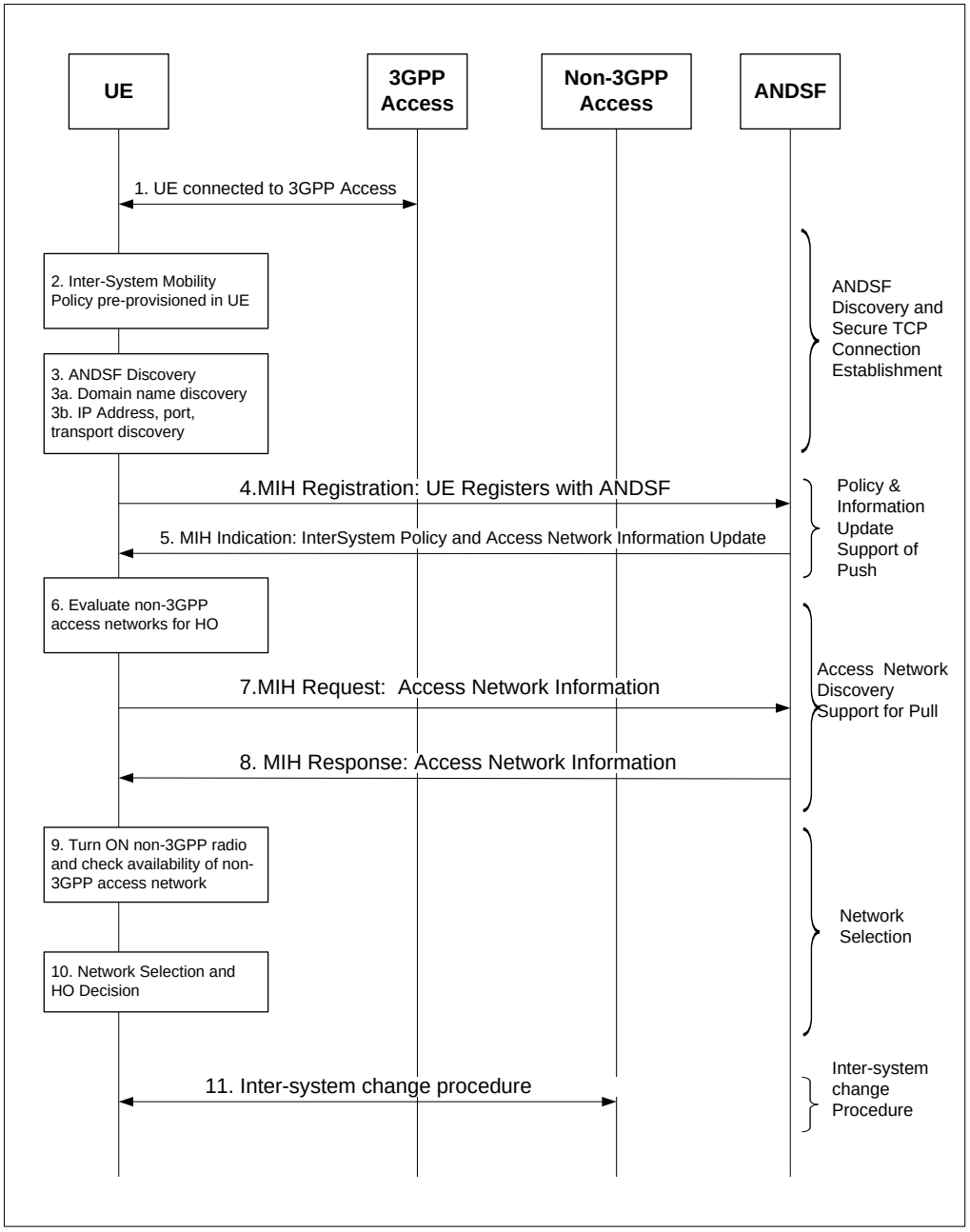


Figure D.2.2.6.1: Procedure for inter-system change between 3GPP access and non-3GPP access using MIH protocol

D.2.2.7 Timeline

The IEEE 802.21 specification is expected to be completed in 2008 timeframe. The IETF draft for transport options is also expected to be completed in 2008 timeframe. The work for defining additional IEs for either policies or access network specific information can be completed within 3GPP CT1 without any dependencies. Appropriate liaisons can be very easily set up between IEEE and 3GPP, if required. Since IEEE 802.21 information service and MIH protocol have the basic framework done and rest of the work can be completed within CT1, it would be very easy to meet the 3GPP Release 8 time frame.

D.2.2.8 Example query

An example query request and response when RDF_DATA is specified as InfoQueryType to obtain a list of IEEE 802.11 point of attachments (poa) (i.e., basic service set identifiers (BSSIDs)) around a specific location is shown below.

EXAMPLE:

MIH_Get_Information.request (RDF_DATA, "PREFIX mihbasic: <URL_TO_BE_ASSIGNED>

SELECT ?poa_address

WHERE {?x1 mihbasic:neighboring-poa ?x2 .

?x2 mihbasic:link-type 19 .

?x2 mihbasic:poa_address ?x3 .

?x3 mihbasic:address ?poa_address .

?x1 mihbasic:poa_address ?x4 .

?x4 mihbasic:address "001122334455" }")

MIH_Information.response(RDF_DATA, "<?xml version="1.0"?>

<sparql xmlns="http://www.w3.org/2005/sparql-results#">

<head>

<variable name="poa_address"/>

</head>

<results>

<result>

<binding name="poa-address"><literal
datatype="http://www.w3.org/2001/XMLSchema#hexBinary">aabbccddeeff</

literal></binding>

<binding name="poa-address"><literal datatype="http://www.w3.org/2001/XMLSchema#hexBinary">

0123456789ab</literal></binding>

</result>

</results>

</sparql>", Success)

D.2.3 Candidate 2 – OMA DM

D.2.3.1 Introduction

The OMA Device Management (OMA DM) protocol is specified by the Open Mobile Alliance (OMA) with latest version 1.2 in OMA-ERELD-DM-V1_2 [52]. OMA DM enables distribution of any kind of information such as applications, data and configuration settings to any single handset or groups of handsets.

The protocol allows two-way communication and is used for data exchange between a server (which is managing the device) called OMA DM Server and the OMA DM client. The communication protocol is a request-response protocol and supports a push- as well as a pull model. It is assumed here that the UE contains an OMA DM client, and that the ANDSF contains an OMA DM server.

Information is stored in the client in an OMA DM management tree. The nodes of the management tree are the entities that can be manipulated by management actions carried over the OMA DM protocol. A management object is a sub-tree of the management tree that is intended to be a collection of nodes that are related in some way. It is assumed here that the information sets provided by the ANDSF (inter-system mobility policy and access network discovery) will be organized in one or more OMA DM Managed Objects (MOs) defined by 3GPP CT1.

The OMA DM protocol uses SyncML *packages* that contain one or more DM *message(s)*. Each message consists of a header (SyncHdr) and a message body (SyncBody), where the header specifies sender, receiver, version, and session information. The message body contains one or more DM *commands*.

The DM server in the ANDSF sends DM commands like Add, Copy, Delete, and Replace to manipulate the management tree, and uses the Get command to retrieve the contents of a particular node. The client in the UE returns the contents through a Result command. The status command conveys another command's execution results.

OMA Device Management consists of two stages:

- Bootstrap; the process of provisioning the DM client to a state where it is able to initiate a management session to a new DM server.
- DM Provisioning; the process by which the device is provisioned, through an OMA DM server, with further information after the device is bootstrapped.

The SyncML Representation and DM protocols are transport-independent. The initial bindings specified by OMA DM are HTTP, WSP and OBEX. It is assumed here that the provisioning from the ANDSF is carried in one HTTPS session, except for the server initiated alert (Package 0 used in D.2.3.3.3, ANDSF-initiated provision of information from ANDSF to UE) that is sent in using HTTP Push (WAP Push in a HTTP post). It is further assumed that this HTTP Push operation is handled by the ANDSF.

Bootstrapping a DM device can be conducted through all the transport mechanisms defined for DM.

D.2.3.2 OMA DM bootstrap

In the bootstrap process a trust relationship is set between the DM client and the DM server. There is only one bootstrap per DM server and DM client pair needed.

The bootstrap process can be carried out in different ways:

- Manual
- Factory configured (Phone or SIM)
- Point of sale bootstrap using local connectivity (e.g. InfraRed, Bluetooth, Cable)
- Point of sale bootstrap triggering over the air bootstrap
- Over the air, a Bootstrap server can be used to send out bootstrap messages via a push mechanism, e.g. WAP Push or OBEX.

In order to bootstrap initial OMA DM settings, bootstrap profiles define the security, transport and data format. Currently two profiles are defined: OMA CP Profile and OMA DM Profile.

D.2.3.3 Dynamic provisioning with OMA DM

D.2.3.3.1 General

Once the bootstrap process has been carried out, the UE and ANDSF may start to communicate using the OMA DM Provisioning process.

D.2.3.3.2 UE initiated provision of information from ANDSF to UE ('Pull')

The UE may initiate the provision of information from the ANDSF using a client initiated session alert message of code "Generic Alert". A typical message flow is shown in figure D.2.3.3.2.1.

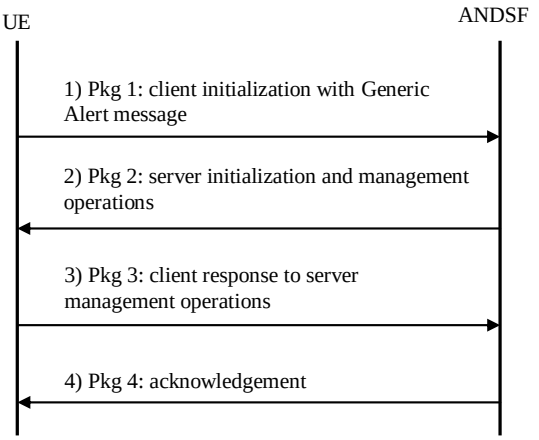


Figure D.2.3.3.2.1: UE initiated provision of information

1) The UE sends OMA DM package 1 containing: device information (like manufacturer, model etc), client identification, indication of client initiated session, and Generic Alert message.
2) The ANDSF sends OMA DM package 2 containing: server identification, and management data and commands to update the inter-system mobility policy and access network discovery information in the UE.
3) The UE sends OMA DM package 3 containing results of the management actions sent from server to client.
4) The ANDSF sends OMA DM package 4 to close the management session.

The detailed contents and coding of the different packages are described in OMA-TS-DM_Protocol-V1_2 [53].

D.2.3.3.3 ANDSF initiated provision of information from ANDSF to UE ('Push')

The ANDSF may initiate the provision of information from the ANDSF using a server initiated session alert message. A typical message flow is shown in figure D.2.3.3.3.1.

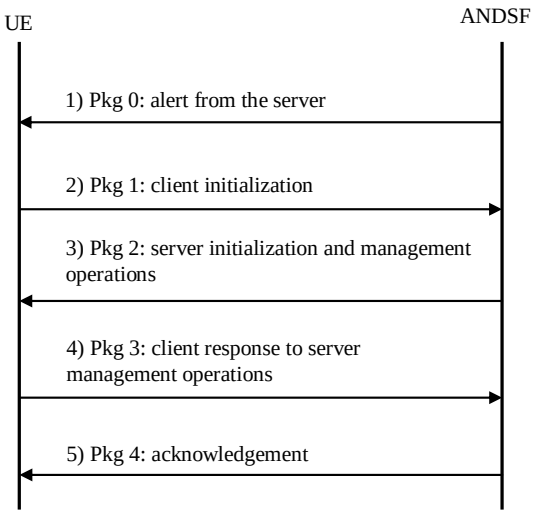


Figure D.2.3.3.3.1: ANDSF initiated provision of information

1) The ANDSF sends OMA DM package 0 notification to cause the UE to initiate a connection back to the ANDSF.
2) The UE sends OMA DM package 1 containing; device information (like manufacturer, model etc), client identification, and indication of server initiated session.
3) The ANDSF sends OMA DM package 2 containing; server identification, and management data and commands to update the inter-system mobility policy and access network discovery information in the UE.
4) The UE sends OMA DM package 3 containing results of the management actions sent from server to client.
5) The ANDSF sends OMA DM package 4 to close the management session.

The detailed contents and coding of the different packages are described in OMA-TS-DM_Protocol-V1_2 [53] and OMA-TS-DM_Notification-V1_2 [54].

D.2.3.4 Security aspects

The information exchanged between the UE and the ANDSF will in many cases be sensitive. Such information may include UE location (cell identity or GPS coordinates), available SSIDs, and carrier frequencies. Hence security aspects are important, including mutual authentication of server and client, confidentiality of data, and data integrity protection.

OMA DM provides an extensive security framework in OMA-TS-DM_Security-V1_2 [55]; authentication and challenge of authentication are built-in to ensure the server and client are communicating only after proper validation. Integrity of OMA DM messages is achieved using a HMAC-MD5. The server and client are both stateful, meaning that a specific sequence of messages is to be exchanged and only after authentication is completed. OMA DM management sessions are encrypted (confidentiality is provided over SSL).

In addition OMA DM fully supports the use of encrypted Management Objects (MO). An MO can remain encrypted in storage space within either the device or the OMA DM server. All in all, OMA DM provides a secure way of storing information in devices and also for exchanging this information.

Security for bootstrapping is very important and the receiver of a bootstrap message needs to know that the information originates from the correct source and that it has not been tampered with en-route. It is important that the DM client in the UE accepts bootstrapping commands only from authorized servers.

OMA DM offers the ability for a Device Management Server to make private any data that is stored under Device Management control from another Device Management Server. This is facilitated by the use of an ACL (Access Control List) that allows the protection of any group, or any individual Device Management object. The ACL property defines which server that can manage the node and in what fashion (ADD, GET, REPLACE and DELETE).

D.2.3.5 Location

It shall be possible for the ANDSF to retrieve the UE location in order to provide relevant access network information. This can be achieved in a number of different ways:

- Represent the location information as a leaf node in a part of the OMA DM tree. This allows the OMA DM server to issue a separate command to retrieve the location.
- Provide the location in the first OMA DM package from the client to the server, e.g. as a vendor extension part of the mandatory device information.
- Provide the location in a proprietary/3GPP defined HTTP header in conjunction with the first OMA DM package from the client to the server.

In all of these cases, the actual location information is transported in HTTP over TLS, which means they are equivalent from a security perspective. Possibly the last alternative (HTTP header) gives the least amount of flexibility and extensibility for different ways of expressing locations, and the first alternative (leaf node representation) requires an extra command round trip to retrieve the location, which leaves the second alternative as the apparent best choice.

D.2.3.6 Deployment aspects

OMA DM is an already released standard, and 3GPP (and CT1 in particular) already specifies OMA DM management objects (e.g. 3GPP TS 24.167 [57], 3GPP TS 24.305 [37], 3GPP TS 24.216 [58], and 3GPP TS 26.114 [59]). The pull model using Generic Alert is used in e.g. OMA Firmware Update in OMA-TS-DM-FUMO-V1_0 [56] and Selective Disabling of 3GPP User Equipment Capabilities (SDoUE) (3GPP TS 24.305 [37]). Using OMA DM for ANDSF would mean creating new Management Object(s) (MO) defined by CT1 for inter-system mobility policy and access network discovery information. The design of the MOs as well as possible future updates of these would be fully under 3GPP control.

Beyond 3GPP, OMA DM is also already used for providing connectivity settings for multiple bearer technologies: 3GPP2, WiFi, WiMAX, and also PacketCable. For example, PacketCable specifications make use of OMA DM which includes defining MOs in order to support cable devices, and similarly WiMAX Forum has adopted OMA DM by the definition of MOs.

All major device manufacturers support the OMA standards, and are already shipping handsets and devices with built-in support for OMA DM. Millions of handsets are on the market and many operators do also support OMA DM in their networks.

The OMA provides OMA Enabler Test Specification (ETS) for OMA DM which is used by the world standard certification bodies, i.e. Global Certification Forum (GCF) and PCS Type Certification Review Board (PTCRB). This enables the possibility for testing products supporting OMA DM according to the latest certification requirements of GCF and PTCRB for OMA DM. Note that all handsets supporting OMA Device Management 1.2 are required to pass these tests for the GCF and PTCRB certification before the product reaches the market.

D.3 Discussion and conclusion on selection of protocol between UE and ANDSF

CT1 has discussed two alternatives for the protocol between the ANDSF and the UE. The alternatives are:

- IEEE 802.21 Media Independent Handover Protocol (MIH)
- a new Managed Object using OMA DM framework.

Both alternatives are reasonably similar with regards to being request-response protocols that can support push and pull mechanisms for communication between the UE and the ANDSF. Location information can also be provided by both alternatives. Using OMA DM as framework and specifying the content of the Managed Object within CT1 will ensure timely completion of the work within the Rel-8 timeframe.

On security, the OMA DM framework has already been discussed within SA3 and the mechanisms provided by the OMA DM framework have been found acceptable. It is not known whether the security provided by MIH in particular has been discussed by SA3, but it is assumed that this will not be an obstacle even though it would have been useful to get some opinion from SA3 on the topic.

MIH has been in development in IEEE over the last few years and has recently been approved, and the latest specification can be found in IEEE P802.21/D123.0 [60] and draft-ietf-mipshop-mstp-solution [61].

OMA DM is a released standard from OMA. The most recent version 1.2 is documented in OMA-ERELD-DM-V1_2 [52]. All major device manufacturers support the OMA standards and are already shipping handsets and devices with built-in support for OMA DM. Millions of handset are on the market and many operators support OMA DM in their networks.

The major differences found between MIH and using a Managed Object using OMA DM as framework for message transport are:

- flexibility on content
- maturity and more widespread use of OMA DM by operators.

To ensure that the ANDSF work can be completed within the Rel-8 timeframe, it is proposed to progress the work and select OMA DM as the framework for communication between the UE and the ANDSF. This will also require a new TS with Management Object(s) for parameters related to the functionality of the ANDSF.

Annex E (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2007-03					Draft skeleton provided by the rapporteur		0.0.0
2007-04	CT1#46				Includes the following contributions agreed by CT1: C1-070911, C1-070913, C1-070915, C1-070978, C1-070990, C1-070991, C1-070999	0.0.0	0.1.0
2007-05	CT1#47				Includes the following contributions agreed by CT1: C1-071154, C1-071316, C1-071365, C1-071366, C1-071369, C1-071370, C1-071371, C1-071469	0.1.0	0.2.0
2007-09	CT1#48				Includes the following contributions agreed by CT1: C1-071662, C1-071764, C1-071765, C1-071979, C1-071984, C1-071985, C1-071986, C1-071994, C1-072102, C1-072103, C1-072105, C1-072109, C1-072110, C1-072112, C1-072115, C1-072116, C1-072118, C1-072119, C1-072120, C1-072168	0.2.0	0.3.0
2007-10	CT1#49				Includes the following contributions agreed by CT1: C1-072303, C1-072352, C1-072357, C1-072405, C1-072520, C1-072521, C1-072522, C1-072525, C1-072527, C1-072536, C1-072538, C1-072539, C1-072630, C1-072631, C1-072632, C1-072633, C1-072635, C1-072636, C1-072637, C1-072641, C1-072642, C1-072643, C1-072644, C1-072645, C1-072710, C1-072711, C1-072712	0.3.0	0.4.0
2007-11	CT1#50				Includes the following contributions agreed by CT1: C1-072743, C1-072827, C1-072828, C1-073000, C1-073002, C1-073003, C1-073004, C1-073005, C1-073007, C1-073008, C1-073009, C1-073011, C1-073012, C1-073017, C1-073019, C1-073020, C1-073021, C1-073022, C1-073028, C1-073032, C1-073034, C1-073035, C1-073120, C1-073121, C1-073123, C1-073124, C1-073127, C1-073128, C1-073129, C1-073131, C1-073133, C1-073134, C1-073135, C1-073136, C1-073139, C1-073220, C1-073222, C1-073223	0.4.0	0.5.0
2007-12	E-mail review				Correction of implementation of C1-073121 and addition of reference to RFC 4861.	0.5.0	0.5.1
2008-02	CT1#51				Includes the following contributions agreed by CT1: C1-080064, C1-080155, C1-080157, C1-080293, C1-080294, C1-080296, C1-080418, C1-080419, C1-080420, C1-080434, C1-080439, C1-080443, C1-080450, C1-080454, C1-080455, C1-080456, C1-080539, C1-080540, C1-080547, C1-080548, C1-080550, C1-080551, C1-080552, C1-080554, C1-080557, C1-080559, C1-080562, C1-080563, C1-080565, C1-080566, C1-080570, C1-080650, C1-080651, C1-080652, C1-080653, C1-080654, C1-080655	0.5.1	0.6.0
2008-02	CT1#51 bis				Includes the following contributions agreed by CT1: C1-080698, C1-080705, C1-080745, C1-080748, C1-080749, C1-080750, C1-080754, C1-080756, C1-080757, C1-080761, C1-080771, C1-080774, C1-080785, C1-080788, C1-080789, C1-080790, C1-080792	0.6.0	0.7.0
2008-04	CT1#52				Includes the following contributions agreed by CT1: C1-080816, C1-081258, C1-081260, C1-081260, C1-081263, C1-081295, C1-081300, C1-081416	0.7.0	0.8.0
2008-05	CT1#53				Includes the following contributions agreed by CT1: C1-081579, C1-081877, C1-081880, C1-081881, C1-081882, C1-082094, C1-082096	0.8.0	0.9.0
2008-05	-	-	-	-	Version 1.0.0 created for presentation to TSG CT#40 for information	0.9.0	1.0.0
2008-07	CT1#54				Includes the following contributions agreed by CT1: C1-082555, C1-082556, C1-082557, C1-082560, C1-082565, C1-082704, C1-082707, C1-082715, C1-082716, C1-082717, C1-082792, C1-082793	1.0.0	1.1.0
2008-07	Review				Contents like version 1.1.0, but change marks in annexes A, B and C are kept.	1.1.0	1.1.1
2008-08	CT1#55				Includes the following contributions agreed by CT1: C1-082980, C1-083197, C1-083238, C1-083427, C1-083428, C1-083431, C1-083435, C1-083436, C1-083437, C1-083438, C1-083611, C1-083613, C1-083614	1.1.1	1.2.0
2008-09	-	-	-	-	Version 2.0.0 created for presentation to TSG CT#41 for approval	1.0.0	2.0.0

2008-09	CT#41				Version 8.0.0 created after approval in TSG CT#41	2.0.0	8.0.0
2008-10					Revision marks in annexes A, B and C were restored.	8.0.0	8.0.1
2008-12	CT#42	CP-080838	0010	1	Clarification of the CSG mobility list	8.0.1	8.1.0