ETSI TS 124 301 V8.0.0 (2009-01)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
Non-Access-Stratum (NAS)
protocol for Evolved Packet System (EPS);
Stage 3
(3GPP TS 24.301 version 8.0.0 Release 8)

Reference
DTS/TSGC-0124301v800

Keywords
LTE, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

This Technical Specification 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 specifies the procedures used by the protocols for mobility management and session management between User Equipment (UE) and Mobility Management Entity (MME) in the Evolved Packet System (EPS). These protocols belong to the non-access stratum (NAS).

The EPS Mobility Management (EMM) protocol defined in the present document provides procedures for the control of mobility when the User Equipment (UE) is using the Evolved UMTS Terrestrial Radio Access Network (E-UTRAN). The EMM protocol also provides control of security for the NAS protocols.

The EPS Session Management (ESM) protocol defined in the present document provides procedures for the handling of EPS bearer contexts. Together with the bearer control provided by the access stratum, this protocol is used for the control of user plane bearers.

For both NAS protocols the present document specifies procedures for the support of inter-system mobility between E-UTRAN and other 3GPP or non-3GPP access networks:

- For inter-system mobility between E-UTRAN and GERAN or UTRAN, this includes rules for a mapping between parameters and procedures used by the NAS protocols defined in the present document and the NAS protocols specified in 3GPP TS 24.008 [13].

- For inter-system mobility between E-UTRAN and generic non-3GPP access networks, this includes specific NAS procedures to maintain IP connectivity to the PDN Gateway and to provide parameters needed by the UE when using mobility management based on Dual-Stack Mobile IPv6 (see 3GPP TS 24.303 [14]) or MIPv4 (see 3GPP TS 24.304 [15]).

Editor's note: Currently the home agent address is the only parameter provided by the network for use with DSMIPv6 or MIPv4. The need for other parameters is FFS.

Editor's note: For optimized handover from cdma2000® HRPD to E-UTRAN, EMM and ESM signalling messages will be tunnelled between UE and MME via the cdma2000® HRPD access network and the S101 interface. Currently no impact on the NAS protocols has been identified.

The present document is applicable to the UE and to the Mobility Management Entity (MME) in the EPS.

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

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

[2] 3GPP TS 23.003: "Numbering, addressing and identification".

[3] 3GPP TS 23.038: "Alphabets and language-specific information".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[5] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[6] 3GPP TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".

[7] 3GPP TS 23.203: "Policy and charging control architecture".

[8] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[9] 3GPP TS 23.272: "Circuit Switched Fallback in Evolved Packet System; Stage 2".

[10] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".

[11] 3GPP TS 23.402: "GPRS architecture enhancements for non-3GPP accesses".

[12] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[13] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[14] 3GPP TS 24.303: "Mobility Management based on DSMIPv6; User Equipment (UE) to network protocols; Stage 3".

[15] 3GPP TS 24.304: "Mobility management based on Mobile IPv4; User Equipment (UE) - foreign agent interface; Stage 3".

[16] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[17] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[18] 3GPP TS 33.102: "3G security; Security architecture".

[19] 3GPP TS 33.401: "3GPP System Architecture Evolution; Security architecture".

[20] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description".

[21] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[22] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC) protocol specification".

[23] 3GPP TS 36.413: "Evolved Universal Terrestrial Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

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

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

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

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

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

[29] ISO/IEC 10646: "Information technology – Universal Multiple-Octet Coded Character Set (UCS)".

[30] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP 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 3GPP 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 [10].

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.

Cached EPS security context: a cached security context to be used in EPS. Definition derived from 3GPP TS 33.401 [19].

CSG ID: A CSG ID is an identifier defined in 3GPP TS 23.003 [2] and associated to a cell or group of cells to which access is restricted to a defined group of users.

Current EPS security context: the EPS security context which has been taken into use by the network most recently. Definition derived from 3GPP TS 33.401 [19].

The label **(E-UTRAN only)** indicates that 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 [10].

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 [10].

Evolved packet core network: the successor to the 3GPP Release 7 packet-switched core network, developed 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 [10].

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 [10].

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 [10].

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 [10].

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.

IPv4v6 capability: capability of the IP stack associated with a UE to support a dual stack configuration with both an IPv4 address and an IPv6 address allocated.

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.

Mapped EPS security context: a mapped security context to be used in EPS. Definition derived from 3GPP TS 33.401 [19].

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

NAS signalling connection recovery: is a mechanism initiated by the NAS to restore the NAS signalling connection on indication of "RRC connection failure" by the lower layers.

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. Additionally, for the purpose of optimized handover or idle mode mobility from cdma2000® HRPD access to E-UTRAN (see 3GPP TS 23.402 [11]), the NAS signalling connection can consist of a concatenation of an S101-AP connection and a signalling tunnel over a cdma2000® HRPD access network.

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 [10].

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

Plain NAS message: a NAS message with a header including neither a message authentication code nor a sequence number.

Procedure Transaction Identity: An identity which is dynamically allocated by the UE for the UE requested ESM procedures. The procedure transaction identity is released when the procedure is completed.

RAT-related TMSI: When the UE is camping on an E-UTRAN cell, the RAT-related TMSI is the GUTI; when it is camping on a GERAN or UTRAN cell, the RAT-related TMSI is the P-TMSI.

The label **(S1 mode only)** indicates that 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.

S101 mode: applies to a system that operates with a functional division that is in accordance with the use of an S101 interface. For the definition of the S101 reference point, see 3GPP TS 23.402 [11].

TAI list: A list of TAIs that identify the tracking areas that the UE can enter without performing a tracking area updating procedure. The TAIs in a TAI list assigned by an MME to a UE pertain to the same MME area. Additionally, the TAIs in a TAI list assigned by an MME to a CS fallback capable UE pertain to the same location area (see 3GPP TS 23.272 [9]). In this case, the defining of the relationship between the tracking area(s) and the location area(s) is operator specific.

Editor's note: It is FFS whether updates of the above descriptions are needed.

Traffic flow aggregate: A temporary aggregate of packet filters that are included in a UE requested bearer resource modification procedure and that is inserted into a traffic flow template (TFT) for an EPS bearer context by the network once the UE requested bearer resource modification procedure is completed.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.401 [10] apply:

MME pool area

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.272 [9] apply:

CS fallback capable UE

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.008 [13] apply:

A/Gb mode
Iu mode

TFT

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.102 [18] apply:

UMTS security context

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.401 [19] apply:

Cached security context
Current security context
EPS security context
Mapped security context

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

AKA	Authentication and Key Agreement
AMBR	Aggregate Maximum Bit Rate
APN	Access Point Name
APN-AMBR	APN Aggregate Maximum Bit Rate
ARP	Allocation Retention Priority
CGI	Cell Global Identifier
CSG	Closed Subscriber Group
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
ECM	EPS Connection Management
eKSI	Key Set Identifier for E-UTRAN
EMM	EPS Mobility Management
EPC	Evolved Packet Core Network
EPS	Evolved Packet System
ESM	EPS Session Management
GBR	Guaranteed Bit Rate
GUMMEI	Globally Unique MME Identifier
GUTI	Globally Unique Temporary Identifier
HRPD	High Rate Packet Data
ISR	Idle mode Signalling Reduction
KSI	Key Set Identifier
M-TMSI	M-Temporary Mobile Subscriber Identity
MBR	Maximum Bit Rate
MME	Mobility Management Entity
MMEC	MME Code
PCO	Protocol Configuration Options
PD	Protocol Discriminator
PDN GW	Packet Data Network Gateway
PTI	Procedure Transaction Identity
QCI	QoS Class Identifier
QoS	Quality of Service
S-TMSI	S-Temporary Mobile Subscriber Identity
S101-AP	S101 Application Protocol
S1AP	S1 Application Protocol
SAE	System Architecture Evolution
TAC	Tracking Area Code
TAI	Tracking Area Identity
TFT	Traffic Flow Template
TI	Transaction Identifier
TIN	Temporary Identity used in Next update

4 General

4.1 Overview

4.2 Linkage between the protocols for EPS mobility management and EPS session management

During the EPS attach procedure, the network activates a default EPS bearer context. Additionally, the network can activate one or several dedicated EPS bearer contexts in parallel. To this purpose the EPS session management messages for the default EPS bearer context activation are transmitted in an information element in the EPS mobility management messages. The UE and the network execute the attach procedure and the default EPS bearer context activation procedure in parallel. The success of the attach procedure is dependent on the success of the default EPS bearer context activation procedure. If the attach procedure fails, then the ESM session management procedures also fail.

Except for the attach procedure, during EMM procedures the transmission of ESM messages shall be suspended.

4.3 UE mode of operation

A UE attached for EPS services may operate in one of the following operation modes:

- PS mode of operation: the UE registers only to EPS services;
- CS/PS mode 1 of operation: the UE is CS fallback capable and configured to use CS fallback, and non-EPS services are preferred. The UE registers to both EPS and non-EPS services; and
- CS/PS mode 2 of operation: the UE is CS fallback capable and configured to use CS fallback, and EPS services are preferred. The UE registers to both EPS and non-EPS services.

4.4 NAS security

4.4.1 General

This clause describes the principles for the handling of EPS security contexts in the UE and in the MME and the procedures used for the security protection of EPS NAS messages between UE and MME. Security protection involves integrity protection and ciphering of the EMM and ESM NAS messages.

The signalling procedures for the control of NAS security are part of the EMM protocol and are described in detail in clause 5.

NOTE: The use of ciphering in a network is an operator option. In this subclause, for the ease of description, it is assumed that ciphering is used, unless explicitly indicated otherwise. Operation of a network without ciphering is achieved by configuring the MME so that it always selects the "null ciphering algorithm", 128-EEA0.

4.4.2 Handling of EPS security contexts

4.4.2.1 General

Before security can be activated, the MME and the UE need to establish an EPS security context (see 3GPP TS 33.401 [19]). Usually, the EPS security context is created as the result of an authentication procedure between MME and UE. Alternatively, during inter-system handover from A/Gb mode to S1 mode or Iu mode to S1 mode, the MME and the UE derive a mapped EPS security context from a UMTS security context that has been established while the UE was in A/Gb mode or Iu mode.

The EPS security context is identified by a key set identifier for E-UTRAN (eKSI) which is assigned by the MME either during the authentication procedure or, for the mapped security context, during the handover procedure.

The EPS security context is taken into use, when the MME initiates a security mode control procedure or, if it is a mapped EPS security context, during the inter-system handover procedure. The security context which has been taken into use by the network most recently is called current security context.

The UE and the MME need to be able to maintain two EPS security contexts simultaneously, since:

- after a re-authentication, the UE and the MME can have both a current EPS security context and a new EPS security context which has not yet been taken into use; and
- after an inter-system handover from A/Gb mode to S1 mode or Iu mode to S1 mode, the UE and the MME can have both a mapped EPS security context and an EPS security context that was created during a previous access in S1 mode or S101 mode ("cached EPS security context").

The number of EPS security contexts that need to be maintained simultaneously by the UE and the MME is limited by the following requirements:

- After a successful (re-)authentication, the MME and the UE shall delete any old EPS security context different from the current EPS security context.
- When a new EPS security context is taken into use, the MME and the UE shall delete the current EPS security context.
- When the MME and the UE derive a new mapped EPS security context during inter-system handover from A/Gb mode to S1 mode or Iu mode to S1 mode, the MME and the UE shall delete any existing mapped EPS security context.
- When a cached EPS security context is taken into use, the MME and the UE shall delete any mapped EPS security context.

4.4.2.2 Establishment of secure exchange of NAS messages

Secure exchange of NAS messages via a NAS signalling connection is usually established by the MME during the attach procedure by initiating a security mode control procedure. After successful completion of the security mode control procedure, except for the messages specified in subclauses 4.4.4 and 4.4.5, all NAS messages exchanged between the UE and the MME are sent integrity protected and ciphered using the current EPS security algorithm.

During inter-system handover from A/Gb mode to S1 mode or Iu mode to S1 mode, secure exchange of NAS messages is established between the MME and the UE by:

- the transmission of NAS security related parameters encapsulated in the AS signalling from the MME to the UE triggering the inter-system handover (see 3GPP TS 33.401 [19]). The UE uses these parameters to generate the mapped EPS security context; and,
- after the handover, the transmission of a TRACKING AREA UPDATE REQUEST message from the UE to the MME. The UE shall send this message integrity protected using the mapped EPS security context, but unciphered. From this time onward, except for the messages specified in subclauses 4.4.4 and 4.4.5, all NAS messages exchanged between the UE and the MME are sent integrity protected and ciphered using the mapped EPS security context.

The secure exchange of NAS messages shall be continued after S1 mode to S1 mode handover. It is terminated after inter-system handover from S1 mode to A/Gb mode or Iu mode or when the NAS signalling connection is released.

When a UE in EMM-IDLE mode establishes a new NAS signalling connection and has a valid current EPS security context, secure exchange of NAS messages can be re-established in the following ways:

1) Except for the case described in item 2 below, the UE shall transmit the initial NAS message integrity protected with the current EPS security context, but unciphered. The MME shall check whether the eKSI included in the initial NAS message belongs to an EPS security context available in the MME, and shall verify the MAC of the NAS message. If the verification is successful, the MME may re-establish the secure exchange of NAS messages:

- by replying with a NAS message that is integrity protected and ciphered using the current EPS security context. From this time onward, except for the messages specified in subclauses 4.4.4 and 4.4.5, all NAS messages exchanged between the UE and the MME are sent integrity protected and ciphered; or

NOTE: This option is also applicable during the attach procedure, unless the UE indicates in the initial PDN CONNECTIVITY REQUEST sent with the ATTACH REQUEST message that it has ESM information that needs to be sent security protected.

- by initiating a security mode control procedure. This can be used by the MME to take a cached or a new EPS security context into use or to modify the current EPS security context by selecting new NAS security algorithms; or

- if the initial NAS message was a SERVICE REQUEST message or EXTENDED SERVICE REQUEST message, by executing an AS security mode control procedure. After successful completion of the procedure, except for the messages specified in subclauses 4.4.4 and 4.4.5, all NAS messages exchanged between the UE and the MME are sent integrity protected and ciphered.2) If the UE establishes the new NAS signalling connection for a tracking area updating procedure after an inter-system change in idle mode from A/Gb mode to S1 mode or Iu mode to S1 mode, and the UE has no cached EPS security context, the UE shall send the TRACKING AREA UPDATE REQUEST message without integrity protection and unciphered. The MME creates a fresh mapped EPS security context and takes this context into use by initiating a security mode control procedure. This re-establishes the secure exchange of NAS messages.

4.4.2.3 Change of security keys

When the MME initiates a re-authentication to create a new EPS security context, the messages exchanged during the authentication procedure are integrity protected and ciphered using the current EPS security context, if any.

Both UE and MME shall continue to use the current EPS security context, until the MME initiates a security mode control procedure. The SECURITY MODE COMMAND message sent by the MME includes the eKSI of the new EPS security context to be used. The MME shall send the message integrity protected with the new EPS security context, but unciphered. When the UE responds with a SECURITY MODE COMPLETE, it shall send the message integrity protected and ciphered with the new EPS security context.

The MME can also modify an existing EPS security context, e.g. the current security context or a cached security context, by sending a SECURITY MODE COMMAND message including the eKSI of the EPS security context to be modified and including a new set of selected NAS security algorithms. In this case the MME shall send the SECURITY MODE COMMAND message integrity protected with the modified EPS security context, but unciphered. When the UE replies with a SECURITY MODE COMPLETE message, it shall send the message integrity protected and ciphered with the modified EPS security context.

4.4.3 Handling of NAS COUNT and NAS sequence number

4.4.3.1 General

There are two separate counters NAS COUNT: one related to uplink NAS messages and one related to downlink NAS messages. The NAS COUNT counters use 24 bit internal representation and are independently maintained by UE and MME. The NAS COUNT is constructed as a NAS sequence number (least significant bits) concatenated with a NAS overflow counter (most significant bits).

When NAS COUNT is input to NAS ciphering or NAS integrity algorithms it is considered to be a 32-bit entity where the most significant bits are padded with zeros.

The network NAS COUNT shall be initialized to zero in the first SECURITY MODE COMMAND when a new security context is activated following a successful authentication and key agreement (AKA) procedure. The UE NAS COUNT shall be initialized to zero when the UE receives the first SECURITY MODE COMMAND message after a successful AKA procedure and uses it in the following SECURITY MODE COMPLETE message.

Editor's note: How the NAS COUNT shall be handled after handover from UTRAN/GERAN to E-UTRAN is FFS.

The NAS sequence number part of the NAS COUNT is exchanged between the UE and the MME as part of the NAS signalling. After each new or retransmitted outbound NAS message, the sender shall always increase the NAS COUNT number by one. Specifically, the NAS sequence number is increased by one, and if the result is zero (due to wrap

around), the NAS overflow counter is also incremented by one (see subclause 4.4.3.5). The receiving side estimates the NAS COUNT used by the sending side. Specifically, if the NAS sequence number wraps around, the NAS overflow counter is incremented by one.

Editor's note: Other general details are FFS.

4.4.3.2 Replay protection

Replay protection shall be supported for received NAS messages both in the MME and the UE. However, since the realization of replay protection does not affect the interoperability between nodes, no specific mechanism is required for implementation.

Replay protection must assure that one and the same NAS message is not accepted twice by the receiver. Specifically, for a given NAS security context, a given NAS COUNT value shall be accepted at most one time and only if message integrity verifies correctly.

4.4.3.3 Integrity protection and verification

The sender shall use its locally stored NAS COUNT as input to the integrity protection algorithm.

The receiver shall use the NAS sequence number included in the received message and an estimate for the NAS overflow counter to form the NAS COUNT input to the integrity verification algorithm.

4.4.3.4 Ciphering and deciphering

The sender shall use its locally stored NAS COUNT as input to the ciphering algorithm.

The receiver shall use the NAS sequence number included in the received message and an estimate for the NAS overflow counter to form the NAS COUNT input to the deciphering algorithm.

4.4.3.5 NAS COUNT wrap around

If, when increasing the NAS COUNT as specified above, the MME detects that its NAS COUNT is "close" to wrap around, (close to 2^{24}), the MME shall initiate a new AKA procedure with the UE, leading to a new established NAS security context and the NAS COUNT being reset to 0 in both the UE and the MME when the new NAS security context is activated as discussed above.

Similarly, the MME shall initiate an AKA procedure if it detects that the UE's uplink NAS COUNT is close to wrap around. If for some reason a new K_{ASME} has not been established using AKA before the NAS COUNT wraps around, the node (MME or UE) in need of sending a NAS message shall instead release the NAS signalling connection. Prior to sending the next uplink NAS message, the UE shall delete the KSI.

4.4.4 Integrity protection of NAS signalling messages

4.4.4.1 General

For the UE, integrity protected signalling is mandatory for the NAS messages once a valid EPS security context exists and has been taken into use. For the network, integrity protected signalling is mandatory for the NAS messages once a secure exchange of NAS messages has been established for the NAS signalling connection. Integrity protection of all NAS signalling messages is the responsibility of the NAS. It is the network which activates integrity protection.

Details of the integrity protection and verification of NAS signalling messages are specified in 3GPP TS 33.401 [19].

When both ciphering and integrity protection are activated, the NAS message is first encrypted and then the encrypted NAS message and the NAS sequence number are integrity protected by calculating the MAC.

When only integrity protection is activated, and ciphering is not activated, the unciphered NAS message and the NAS sequence number are integrity protected by calculating the MAC.

When during the EPS attach procedure an ESM message is piggybacked in an EMM message, there is only one sequence number IE and one message authentication code IE, if any, for the combined NAS message.

4.4.4.2 Integrity checking of NAS signalling messages in the UE

Except the messages listed below, no NAS signalling messages shall be processed by the receiving EMM entity in the UE or forwarded to the ESM entity, unless the secure exchange of NAS messages has been established for the NAS signalling connection:

- EMM messages:
  - IDENTITY REQUEST (if requested identification parameter is IMSI);
  - AUTHENTICATION REQUEST;
  - AUTHENTICATION REJECT;
  - ATTACH REJECT;
  - DETACH REQUEST;
  - DETACH ACCEPT (for non switch off);
  - TRACKING AREA UPDATE REJECT;
  - SERVICE REJECT.

NOTE: These messages are accepted by the UE without integrity protection, as in certain situations they are sent by the network before security can be activated.

Editor's note: The messages in this list need to fulfil one or several SA3 requirement(s) as follows: the message may be sent before the security mode control procedure is performed, or when too much complexity would be involved if the message were received with integrity protection.

Once the secure exchange of NAS messages has been established, 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. If NAS signalling messages, having not successfully passed the integrity check, are received, then the NAS in the UE shall discard that message. If any NAS signalling message is received as not integrity protected even though the secure exchange of NAS messages has been established by the network, then the NAS shall discard this message.

4.4.4.3 Integrity checking of NAS signalling messages in the MME

Except the messages listed below, no NAS signalling messages shall be processed by the receiving EMM entity in the MME or forwarded to the ESM entity, unless the secure exchange of NAS messages has been established for the NAS signalling connection:

- EMM messages:
  - ATTACH REQUEST;
  - IDENTITY RESPONSE (if requested identification parameter is IMSI);
  - AUTHENTICATION RESPONSE;
  - AUTHENTICATION FAILURE;
  - SECURITY MODE REJECT;
  - DETACH REQUEST;
  - DETACH ACCEPT;
  - TRACKING AREA UPDATE REQUEST.

NOTE 1: The TRACKING AREA UPDATE REQUEST message is sent by the UE without integrity protection, if the tracking area updating procedure is initiated due to an inter-system change in idle mode and no cached EPS security context is available in the UE. The other messages are accepted by the MME without integrity protection, as in certain situations they are sent by the UE before security can be activated.

Editor's note: The messages in this list need to fulfil one or several SA3 requirement(s) as follows: the message may be sent before the security mode control procedure is performed, or when too much complexity would be involved if the message were received with integrity protection.

Once a current EPS security context exists, until the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving EMM entity in the MME shall process the following NAS signalling messages, even if the MAC included in the message fails the integrity check or cannot be verified, as the EPS security context is not available in the network:

- ATTACH REQUEST;
- IDENTITY RESPONSE (if requested identification parameter is IMSI);
- AUTHENTICATION RESPONSE;
- AUTHENTICATION FAILURE;
- SECURITY MODE REJECT;
- DETACH REQUEST (if sent before security has been activated);
- DETACH ACCEPT;
- TRACKING AREA UPDATE REQUEST;
- SERVICE REQUEST;
- EXTENDED SERVICE REQUEST.

NOTE 2: These messages are accepted by the MME even when the MAC that fails the integrity check or cannot be verified, as in certain situations they can be sent by the UE protected with an EPS security context that is no longer available in the network.

If an ATTACH REQUEST message fails the integrity check, the MME shall authenticate the subscriber before processing the attach request any further.

If a TRACKING AREA UPDATE REQUEST message fails the integrity check, the MME shall initiate a security mode control procedure to take a new mapped EPS security context into use, if the UE provided a KSI_{SGSN}, P-TMSI and RAI in the TRACKING AREA UPDATE REQUEST message; otherwise the MME shall reject the request with EMM cause value #9, "UE identity cannot be derived by the network".

If a SERVICE REQUEST or EXTENDED SERVICE REQUEST message fails the integrity check, the MME shall reject the request with EMM cause value #9, "UE identity cannot be derived by the network".

Once the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving EMM or ESM entity in the MME shall not process any NAS signalling messages unless they have been successfully integrity checked by the NAS. If any NAS signalling message, having not successfully passed the integrity check, is received, then the NAS in the MME shall discard that message. If any NAS signalling message is received, as not integrity protected even though the secure exchange of NAS messages has been established, then the NAS shall discard this message.

4.4.5 Ciphering of NAS signalling messages

The use of ciphering in a network is an operator option.

When the UE establishes a new NAS signalling connection, it shall send the initial NAS message unciphered.

The UE shall start the ciphering and deciphering of NAS messages when the secure exchange of NAS messages has been established for a NAS signalling connection. From this time onward, except for the ATTACH REQUEST message and TRACKING AREA UPDATE REQUEST message, the UE shall send all NAS messages ciphered until the NAS signalling connection is released, or the UE performs intersystem handover to A/Gb mode or Iu mode.

The MME shall start ciphering and deciphering of NAS messages as described in subclause 4.4.2.2. From this time onward, except for the SECURITY MODE COMMAND message, the MME shall send all NAS messages ciphered until the NAS signalling connection is released, or the UE performs intersystem handover to A/Gb mode or Iu mode.

Details of ciphering and deciphering of NAS signalling messages are specified in 3GPP TS 33.401 [19].

5 Elementary procedures for EPS mobility management

5.1 Overview

5.1.1 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 and the short message services (SMS) entity of the connection management (CM) 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 [22]).

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

5.1.2 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;
   - security mode control;
   - 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 (S1 mode only);
- periodic tracking area updating (S1 mode only).

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

3) EMM connection management procedures (S1 mode only):

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.

Initiated by the UE or the network and used to transport NAS messages:

- transport of NAS messages.

The transport of NAS messages procedure cannot be initiated while an EMM specific procedure is ongoing.

5.1.3 EMM sublayer states

5.1.3.1 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 5.1.3.2, 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 5.1.3.3. The states for the MME side are described in subclause 5.1.3.4.

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 [20]). E.g. the state LTE_DETACHED in 3GPP TS 36.300 [20] 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.

5.1.3.2 EMM sublayer states in the UE

5.1.3.2.1 General

In the following subclauses, the possible EMM states of an EMM entity in the UE are described. Subclause 5.1.3.2.2 summarizes the main states of an EMM entity. The substates that have been defined are described in subclause 5.1.3.2.3 and subclause 5.1.3.2.4.

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 5.2. For the behaviour of the UE in abnormal cases refer to the description of the elementary EMM procedures in subclauses 5.4, 5.5, 5.6 and 5.7.

5.1.3.2.2 Main states

5.1.3.2.2.1 EMM-NULL

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

5.1.3.2.2.2 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 5.5.1).

5.1.3.2.2.3 EMM-REGISTERED-INITIATED

A UE enters the state EMM-REGISTERED-INITIATED after it has started the attach or the combined attach procedure and is waiting for a response from the MME (see subclause 5.5.1).

5.1.3.2.2.4 EMM-REGISTERED

In the state EMM-REGISTERED an EMM context has been established and a default EPS bearer context has been activated 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 serving eNodeB. 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 5.5.3).

5.1.3.2.2.5 EMM-DEREGISTERED-INITIATED

A UE enters the state EMM-DEREGISTERED-INITIATED after it has requested release of the EMM context by starting the detach or combined detach procedure and is waiting for a response from the MME (see subclause 5.5.2).

5.1.3.2.2.6 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 5.5.3).

5.1.3.2.2.7 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 5.6.1).

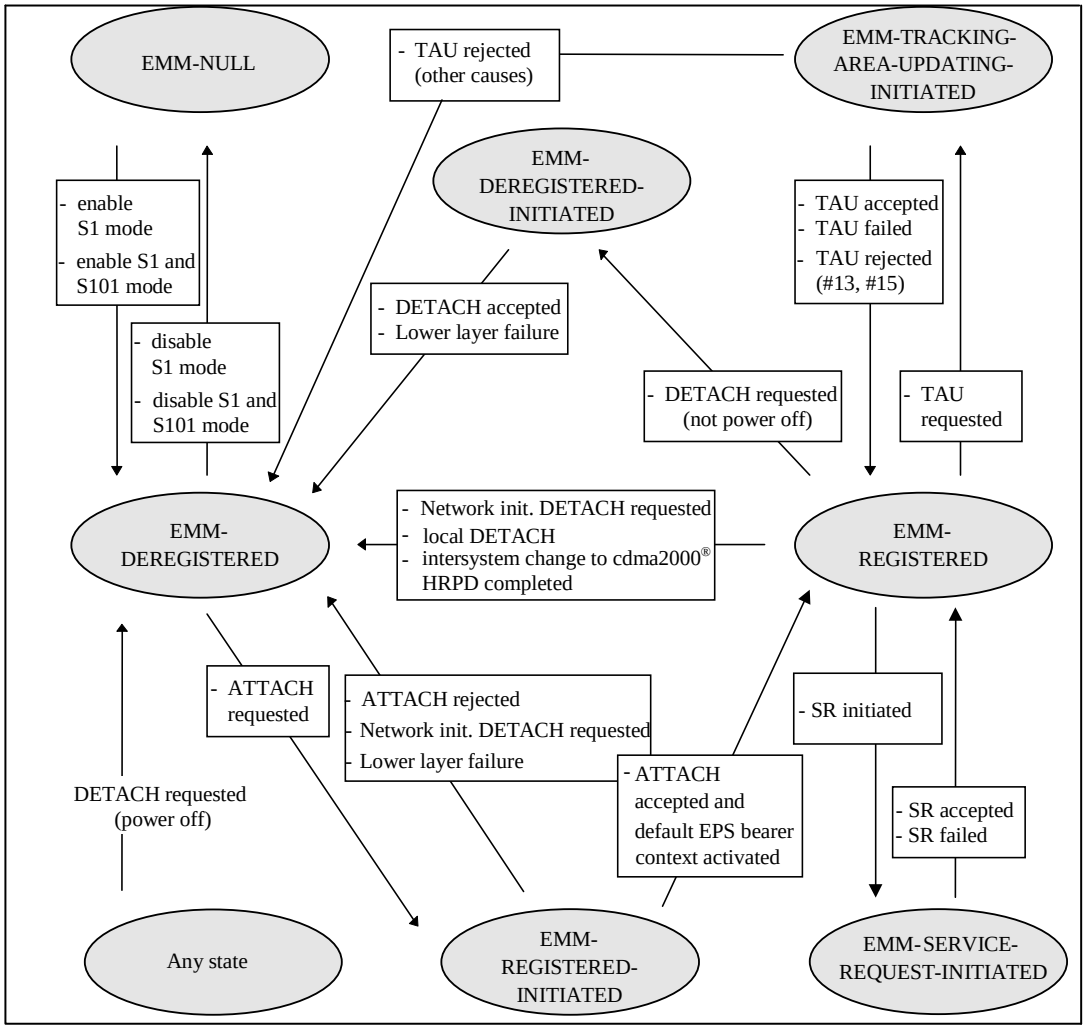

Figure 5.1.3.2.2.7.1: EMM main states in the UE

5.1.3.2.3 Substates of state EMM-DEREGISTERED

5.1.3.2.3.1 General

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 substate EMM-DEREGISTERED.NO-IMSI.

5.1.3.2.3.2 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.

5.1.3.2.3.3 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 known not to be able to provide normal service (e.g. the selected cell is in a forbidden PLMN, is in a forbidden tracking area or has a CSG ID not included in the UE's Allowed CSG list).

5.1.3.2.3.4 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.

5.1.3.2.3.5 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.

5.1.3.2.3.6 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.

5.1.3.2.3.7 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 substate can be entered if the access class is blocked due to access class control, or if the network rejects the NAS signalling connection establishment.

5.1.3.2.3.8 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.

5.1.3.2.4 Substates of state EMM-REGISTERED

5.1.3.2.4.1 General

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

5.1.3.2.4.2 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.

5.1.3.2.4.3 EMM-REGISTERED.ATTEMPTING-TO-UPDATE

The substate EMM-REGISTERED.ATTEMPTING-TO-UPDATE 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.

5.1.3.2.4.4 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.

5.1.3.2.4.5 EMM-REGISTERED.PLMN-SEARCH

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

5.1.3.2.4.6 EMM-REGISTERED.UPDATE-NEEDED

The UE has to perform a tracking area updating procedure, but access to the current cell is barred. This state can be entered if the access class is blocked due to access class control, or if the network rejects the NAS signalling connection establishment. No EMM procedure except tracking area updating shall be initiated by the UE in this substate.

5.1.3.2.4.7 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.

5.1.3.2.4.8 EMM-REGISTERED.ATTEMPTING-TO-UPDATE-MM

A combined attach procedure or a combined tracking area updating procedure was successful for EPS services only. User data and signalling information may be sent and received.

5.1.3.2.4.9 EMM-REGISTERED.IMSI-DETACH-INITIATED

The UE performs a combined detach procedure for non-EPS services only (detach type "IMSI Detach"). This substate is entered if the UE is attached for EPS and non-EPS services and wants to detach for non-EPS services only. User data and signalling information may be sent and received.

5.1.3.3 EPS update status

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

The EPS update status is stored in a non-volatile memory in the USIM if the corresponding file is present in the USIM, else in the non-volatile memory in the ME, as described in Annex C.

The EPS update status value is changed only after the execution of an attach, network initiated detach, authentication, tracking area update or service request procedure.

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).

5.1.3.4 EMM sublayer states in the MME

5.1.3.4.1 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 or a combined attach procedure initiated by the UE (see subclause 5.5.1).

5.1.3.4.2 EMM-COMMON-PROCEDURE-INITIATED

The MME enters the state EMM-COMMON-PROCEDURE-INITIATED, after it has started a common EMM procedure (see subclause 5.4) and is waiting for a response from the UE.

5.1.3.4.3 EMM-REGISTERED

In the state EMM-REGISTERED, an EMM context has been established and a default EPS bearer context has been activated in the MME.

5.1.3.4.4 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 5.5.2).

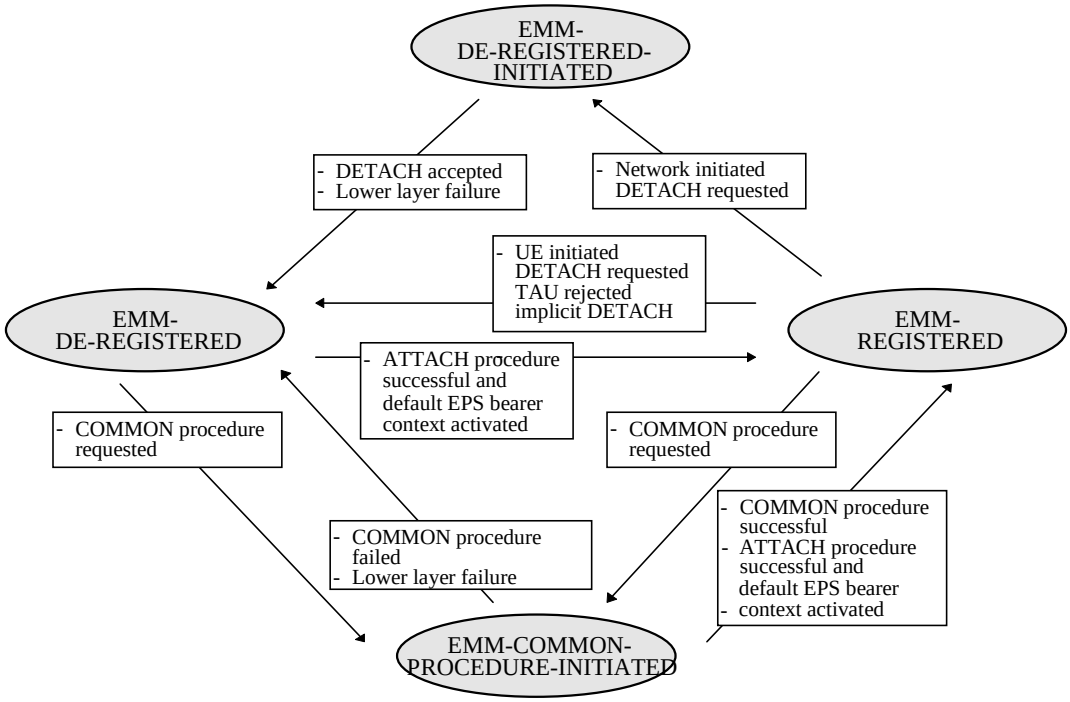

Figure 5.1.3.4.4.1: EMM main states in the MME

5.1.4 Coordination between EMM and GMM

If GMM and EMM are both enabled, a UE capable of S1 mode and A/Gb mode or Iu mode or both shall maintain one common registration for GMM and EMM indicating whether the UE is registered for packet services or not.

A UE that is not registered shall be in state GMM-DEREGISTERED and in state EMM-DEREGISTERED.

If the UE performs a successful attach procedure in S1 mode, it shall enter substates GMM-REGISTERED.NO-CELL-AVAILABLE and EMM-REGISTERED.NORMAL-SERVICE.

If the UE performs a successful GPRS attach procedure in A/Gb or Iu mode, it shall enter substates GMM-REGISTERED.NORMAL-SERVICE and EMM-REGISTERED.NO-CELL-AVAILABLE.

After successful completion of routing area updating and tracking area updating procedures in both S1 mode and A/Gb or Iu mode, if the network has indicated that ISR is activated, the UE shall maintain registration and related periodic update timers in both GMM and EMM.

5.1.5 Coordination between EMM and MM

UEs that operate in CS/PS mode 1 or CS/PS mode 2 of operation and wish to be simultaneously attached to EPS and non-EPS services, shall use the combined EPS/IMSI attach procedure.

UEs that operate in CS/PS mode 1 or CS/PS mode 2 of operation and are already attached to both EPS and non-EPS services shall use the combined tracking area updating and periodic tracking area updating procedures.

UEs that operate in CS/PS mode 1 or CS/PS mode 2 of operation and are already attached to both EPS and non-EPS services shall perform a combined detach procedure in order to detach for non-EPS services.

UEs that operate in CS/PS mode 1 or CS/PS mode 2 of operation should not use any MM timers related to MM specific procedures (e.g. T3210, T3211, T3212, T3213) while camped on E-UTRAN, unless the re-activation of these timers is explicitly described. If the MM timers are already running, the UE should not react on the expiration of the timers.

5.2 Behaviour of the UE in state EMM-DEREGISTERED and state EMM-REGISTERED

5.2.1 General

In this subclause, the detailed behaviour of the UE in the states EMM-DEREGISTERED and EMM-REGISTERED is described.

5.2.2 UE behaviour in state EMM-DEREGISTERED

5.2.2.1 General

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

- the detach or combined detach is performed either by the UE or by the MME (see subclause 5.5.2);
- the attach request is rejected by the MME (see subclause 5.5.1);
- the tracking area update request is rejected by the MME (see subclause 5.5.3);
- the UE is switched on; or
- when an inter-system change from S1 mode to S101 mode is completed.

Editor's note: Other conditions are FFS.

In state EMM-DEREGISTERED, the UE shall behave according to the substate as explained in subclause 5.2.2.3.

5.2.2.2 Primary substate selection

5.2.2.2.1 Selection of the substate after power on

When the UE is switched on, the substate shall be PLMN-SEARCH if the USIM is available and valid. See 3GPP TS 23.122 [6] for further details.

The substate chosen after PLMN-SEARCH, following power on is:

- if no cell can be selected, the substate shall be NO-CELL-AVAILABLE;
- if no USIM is present, the substate shall be NO-IMSI;
- if a suitable cell has been found and the PLMN or tracking area is not in the forbidden list, then the substate shall be NORMAL-SERVICE;
- if the selected cell is in a forbidden PLMN or a forbidden tracking area, then the UE shall enter the substate LIMITED-SERVICE;
- if the UE is in manual network selection mode and no cell of the selected PLMN has been found, the UE shall enter the substate NO-CELL-AVAILABLE; and
- if the selected cell is a non-3GPP cell, the substate shall be NO-CELL-AVAILABLE.

5.2.2.3 Detailed description of UE behaviour in state EMM-DEREGISTERED

5.2.2.3.1 NORMAL-SERVICE

The UE shall perform an attach procedure.

5.2.2.3.2 LIMITED-SERVICE

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

5.2.2.3.3 ATTEMPTING-TO-ATTACH

The UE shall:

- perform an attach procedure on the expiry of timers T3411 or T3402; and
- perform an attach procedure when the serving cell has changed and the tracking area this cell is belonging to is not in the list of forbidden tracking areas.

Editor's note: Other conditions are FFS.

5.2.2.3.4 PLMN-SEARCH

No specific action is required.

5.2.2.3.5 NO-IMSI

The UE shall only perform cell selection according to 3GPP TS 36.304 [21].

5.2.2.3.6 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.

5.2.2.3.7 NO-CELL-AVAILABLE

The UE shall perform cell selection according to 3GPP TS 36.304 [21] and choose an appropriate substate when a cell is found. When the lower layers indicate to prepare for an S101 mode to S1 mode handover, the UE shall enter substate NORMAL-SERVICE.

5.2.2.4 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 [21].

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 [6]) 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; and
- if the selected cell is a non-3GPP cell, the substate shall be NO-CELL-AVAILABLE.

5.2.3 UE behaviour in state EMM-REGISTERED

5.2.3.1 General

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

- the attach procedure is performed by the UE (see subclause 5.5.1).

In state EMM-REGISTERED, the UE shall behave according to the substate as explained in subclause 5.2.3.2.

5.2.3.2 Detailed description of UE behaviour in state EMM-REGISTERED

5.2.3.2.1 NORMAL-SERVICE

The UE:

- shall perform normal and periodic tracking area updating (see subclause 5.5.3); and
- shall respond to paging.

5.2.3.2.2 ATTEMPTING-TO-UPDATE

The UE:

- shall not send any user data;
- shall perform tracking area updating on the expiry of timers T3411 or T3402; and
- shall perform tracking area updating when the tracking area of the serving cell has changed and this tracking area is not in the list of forbidden tracking areas.

Editor's note: Other conditions are FFS.

5.2.3.2.3 LIMITED-SERVICE

The UE:

- shall perform cell selection/reselection according to 3GPP TS 36.304 [21]; and
- may respond to paging (with IMSI).

5.2.3.2.4 PLMN-SEARCH

The UE may enter this substate when it is in automatic network selection mode and the maximum allowed number of subsequently unsuccessful tracking area updating have been performed. The UE may also enter this substate as a result of a tracking area update rejected by the network (see subclause 5.5.3) or as a result of a service request rejected by the network (see subclause 5.6.1). If a new PLMN is selected, the UE shall perform the tracking area updating procedure (see subclause 5.5.3).

5.2.3.2.5 UPDATE-NEEDED

The UE:

- shall not send any user data nor signalling information;
- may respond to paging;
- shall perform cell selection/reselection according to 3GPP TS 36.304 [21]; and
- shall 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.

5.2.3.2.6 NO-CELL-AVAILABLE

The UE shall perform cell selection/reselection according to 3GPP TS 36.304 [21].

5.2.3.2.7 ATTEMPTING-TO-UPDATE-MM

The UE:

- shall perform cell selection/reselection according to 3GPP TS 36.304 [21];
- shall be able to receive and transmit user data and signalling information; and
- shall perform tracking area updating procedure indicating "combined TA/LA updating with IMSI attach" on the expiry of timers T3411 or T3402 or when the UE enters a tracking area not in the list of registered tracking areas.

5.3 General on elementary EMM procedures

5.3.1 EMM modes and NAS signalling connection

5.3.1.1 Establishment of the NAS signalling connection

When the UE is in EMM-IDLE mode and needs to transmit an initial NAS message, the UE shall request the lower layer to establish a NAS signalling connection.

Initial NAS messages are:

- ATTACH REQUEST;
- DETACH REQUEST;
- TRACKING AREA UPDATE REQUEST;
- SERVICE REQUEST; and
- EXTENDED SERVICE REQUEST.

For the routing of the initial NAS message to the appropriate MME, the UE NAS provides the lower layers with either the S-TMSI or the registered globally unique MME identifier (GUMMEI) that consists of the PLMN ID, the MME group ID, and the MME code (see 3GPP TS 23.003 [2]).

- When the UE is registered in the tracking area of the current cell during the NAS signalling connection establishment, the UE NAS shall provide the lower layers with the S-TMSI, but shall not provide the registered MME identifier to the lower layers. Exceptionally, when the UE in EMM-IDLE mode initiates a tracking area updating procedure for load balancing purposes, the UE NAS shall provide the lower layers with neither S-TMSI nor registered MME identifier.
- When the UE is not registered in the tracking area of the current cell during the NAS signalling connection establishment, the UE NAS does not provide the lower layers with the S-TMSI. If the UE has a valid registered MME identifier from a previous registration, the UE NAS shall provide the lower layers with the registered MME identifier.

In S1 mode, when the RRC connection has been established successfully, the UE shall enter EMM-CONNECTED mode and consider the NAS signalling connection established.

In S101 mode, when the cdma2000® HRPD access network resources are available for tunnelled NAS signalling, the UE shall enter EMM-CONNECTED mode and consider the S101 mode NAS signalling connection established.

5.3.1.2 Release of the NAS signalling connection

The signalling procedure for the release of the NAS signalling connection is initiated by the network.

In S1 mode, when the RRC connection has been released, the UE shall enter EMM-IDLE mode and consider the NAS signalling connection released.

To allow the network to release the NAS signalling connection, the UE shall start the timer T3440 in the following cases:

a) the UE receives any of the EMM cause values #11, #12, #13, #14 (not applicable to the service request procedure) or #15; or

b) the UE receives a TRACKING AREA UPDATE ACCEPT message and the UE has not set the "active" flag in the TRACKING AREA UPDATE REQUEST message.

Upon expiry of T3440, the UE shall locally release the established NAS signalling connection.

In case b,

- upon an indication from the lower layers that the user plane radio bearers are set up, the UE shall stop timer T3440 and may send uplink signalling via the existing NAS signalling connection or user data via the user plane bearers; or

- upon receipt of a DETACH REQUEST message, the UE shall stop timer T3440 and respond to the network initiated detach as specified in subclause 5.5.2.3.

In S101 mode, when the cdma2000® HRPD radio access connection has been released, the UE shall enter EMM-IDLE mode and consider the S101 mode NAS signalling connection released.

5.3.2 Lists of forbidden tracking areas

The UE shall store a list of "forbidden tracking areas for roaming", as well as a list of "forbidden tracking areas for regional provision of service". These lists shall be erased when the UE is switched off or when the USIM is removed, and periodically (with a period in the range 12 to 24 hours).

In S1 mode, the UE shall update the suitable list whenever an ATTACH REJECT, TRACKING AREA UPDATE REJECT, SERVICE REJECT or DETACH REQUEST message is received with the EMM cause "roaming not allowed in this tracking area", "tracking area not allowed", or "no suitable cells in tracking area".

Each list shall accommodate 40 or more TAIs. When the list is full and a new entry has to be inserted, the oldest entry shall be deleted.

5.3.3 Equivalent PLMNs list

The UE shall store a list of equivalent PLMNs. These PLMNs shall be regarded by the UE as equivalent to each other for PLMN selection and cell selection/re-selection. The same list is used by EMM, GMM and MM.

The UE shall update or delete this list at the end of each attach or tracking area updating procedure. The stored list consists of a list of equivalent PLMNs as downloaded by the network plus the PLMN code of the registered PLMN that downloaded the list. When the UE is switched off, it shall keep the stored list so that it can be used for PLMN selection after switch on. The UE shall delete the stored list if the USIM is removed. The maximum number of possible entries in the stored list is 16.

5.3.4 Handling of the periodic tracking area update timer and mobile reachable timer (S1 mode only)

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 (timer T3412). The value of timer T3412 is sent by the network to the UE in the ATTACH ACCEPT message and can be sent in 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 or EMM-DEREGISTERED state.

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.

If ISR is activated, the UE shall keep both the periodic tracking area update timer (timer T3412) and the periodic routeing area update timer (timer T3312). The two separate timers run in the UE for updating MME and SGSN independently. If the periodic tracking area update timer expires and the UE cannot initiate the tracking area updating procedure, as it is in state EMM-REGISTERED.NO-CELL-AVAILABLE, the UE shall start the E-UTRAN deactivate ISR timer T3423. The UE shall initiate the tracking area updating procedure and stop the timer T3423 when it enters state EMM-REGISTERED.NORMAL-SERVICE before timer T3423 expires. After expiry of timer T3423 the UE shall deactivate ISR by setting its TIN to "P-TMSI" and initiate the tracking area updating procedure when it returns to state EMM-REGISTERED.NORMAL-SERVICE.

The network supervises the periodic tracking area updating procedure of the UE by means of the mobile reachable timer. The mobile reachable timer shall be longer than T3412. By default, the mobile reachable timer is 4 minutes greater than T3412. If ISR is not activated, the network behaviour upon expiry of the mobile reachable timer is network dependent, but typically the network stops sending paging messages to the UE on the first expiry, and may take other appropriate actions.

The mobile reachable timer shall be reset and started with its initial value, when the MME releases the NAS signalling connection for the UE. The mobile reachable timer shall be stopped when a NAS signalling connection is established for the UE.

If ISR is activated, upon expiry of the mobile reachable timer the network shall start the implicit detach timer. By default, the implicit detach timer is 4 minutes greater than T3423. If the implicit detach timer expires before the UE contacts the network, the network shall implicitly detach the UE.

The implicit detach timer shall be stopped when a NAS signalling connection is established for the UE.

5.3.5 Handling of timer T3402

The value of timer T3402 can be sent by the network to the UE in the ATTACH ACCEPT message and 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, or until one of the above messages is received without a value specified, in which case the default value applies.

5.4 EMM common procedures

5.4.1 GUTI reallocation procedure

5.4.1.1 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 5.5.1 and 5.5.3).

The PLMN identity in the GUTI indicates the current registered PLMN.

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.

5.4.1.2 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 (see example in figure 5.4.1.2.1).

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

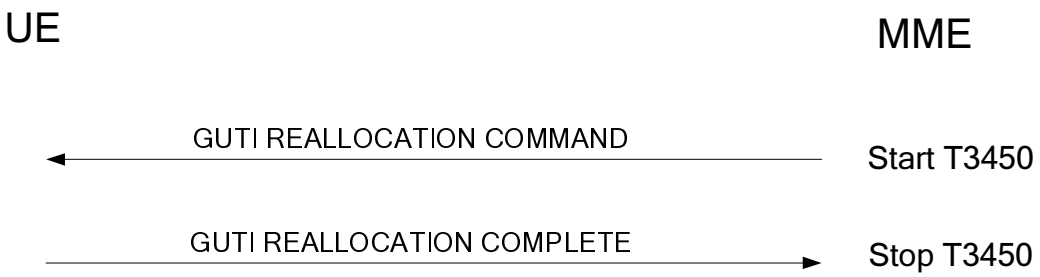

Figure 5.4.1.2.1: GUTI reallocation procedure

5.4.1.3 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. 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

5.4.1.4 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. If a new TAI list is provided in the GUTI REALLOCATION COMMAND message, the MME shall consider the new TAI list as valid and the old TAI list as invalid.

5.4.1.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of GUTI REALLOCATION COMPLETE message indication with TAI change from lower layers

   If the current TAI is not in the TAI list, the GUTI reallocation procedure shall be aborted and a tracking area updating procedure shall be initiated.

   If the current TAI is still part of the TAI list, it is up to the UE implementation how to re-run the ongoing procedure that triggered the GUTI reallocation procedure.

b) Transmission failure of GUTI REALLOCATION COMPLETE message indication without TAI change from lower layers

   It is up to the UE implementation how to re-run the ongoing procedure that triggered the GUTI reallocation procedure.

5.4.1.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure

   If a lower layer failure is detected before the GUTI REALLOCATION COMPLETE message is received, the old and the new GUTI shall be considered as valid until the old GUTI can be considered as invalid by the network.

If a new TAI list was provided in the GUTI REALLOCATION COMMAND message, the old and new TAI list shall also be considered as valid until the old TAI list can be considered as invalid by the network.

During this period the network:

- may first use the old S-TMSI from the old GUTI for paging within the area defined by the old TAI list for an implementation dependent number of paging attempts for network originated transactions. If a new TAI list was provided with old GUTI in the GUTI REALLOCATION COMMAND message, the new TAI list should also be used for paging. Upon response from the UE, the network may re-initiate the GUTI reallocation. If the response is received from a tracking area within the old and new TAI list, the network shall re-initiate the GUTI reallocation. If no response is received to the paging attempts, the network may use the new S-TMSI from the new GUTI for paging for an implementation dependent number of paging attempts. In this case, if a new TAI list was provided with new GUTI in the GUTI REALLOCAITON COMMAND message, the new TAI list shall be used instead of the old TAI list. Upon response from the UE the network shall consider the new GUTI as valid and the old GUTI as invalid.

  The network may use the IMSI for paging if it needs to establish a NAS signalling connection as described in subclause 5.6.2.2.2. Upon response from the UE the GUTI reallocation is restarted;

- shall consider the new GUTI as valid if it is used by the UE and, additionally, the new TAI list as valid if it was provided with this GUTI in the GUTI REALLOCATION COMMAND message; and

- may use the identification procedure followed by a new GUTI reallocation if the UE uses the old GUTI.

b) Expiry of timer T3450

   The GUTI reallocation procedure is supervised by the timer T3450. The network shall, on the first expiry of timer T3450, reset and restart timer T3450 and shall retransmit the GUTI REALLOCATION COMMAND. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3450, the network shall abort the reallocation procedure and shall follow the rules described for case a above.

c) GUTI reallocation and EPS attach procedure collision

   If the network receives an ATTACH REQUEST message before the ongoing GUTI reallocation procedure has been completed the network shall proceed with the attach procedure after deletion of the EMM context.

d) GUTI reallocation and UE initiated detach procedure collision

   If the network receives a DETACH REQUEST message before the ongoing GUTI reallocation procedure has been completed, the network shall abort the GUTI reallocation procedure and shall progress the detach procedure.

e) GUTI reallocation and tracking area updating procedure collision

   If the network receives a TRACKING AREA UPDATE REQUEST message before the ongoing GUTI reallocation procedure has been completed, the network shall abort the GUTI reallocation procedure and shall progress the tracking area updating procedure. The network may then perform a new GUTI reallocation.

f) GUTI reallocation and service request procedure collision

   If the network receives a SERVICE REQUEST message before the ongoing GUTI reallocation procedure has been completed, the network shall progress both procedures.

If there is a different new GUTI and optionally a new TAI list included in a subsequent GUTI REALLOCATION COMMAND message, the UE always regards the newest GUTI and the newest TAI list as valid for the recovery time.

5.4.2 Authentication procedure

5.4.2.1 General

The purpose of the EPS authentication and key agreement (AKA) procedure is to provide mutual authentication between the user and the network and to agree on a key K_{ASME} (see 3GPP TS 33.401 [19]). The cases when the EPS AKA procedure should be used are defined in 3GPP TS 33.401 [19].

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

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

An EPS security context is established in the UE and the network when an EPS authentication is successfully performed. During a successful EPS authentication, the CK and IK keys are computed. CK and IK are then used as key material to compute a new key, $K_{ASME.}$ K_{ASME} is stored in the EPS security contexts (see 3GPP TS 33.401 [19]) of both the network and the UE, and is the root for the EPS integrity protection and ciphering key hierarchy.

5.4.2.2 Authentication initiation by the network

When a NAS signalling connection exists, the network can initiate an authentication procedure at any time. The network initiates the authentication procedure by sending an AUTHENTICATION REQUEST message to the UE and starting the timer T3460 (see example in figure 5.4.2.2.1). The AUTHENTICATION REQUEST message contains the parameters necessary to calculate the authentication response (see 3GPP TS 33.401 [19]).

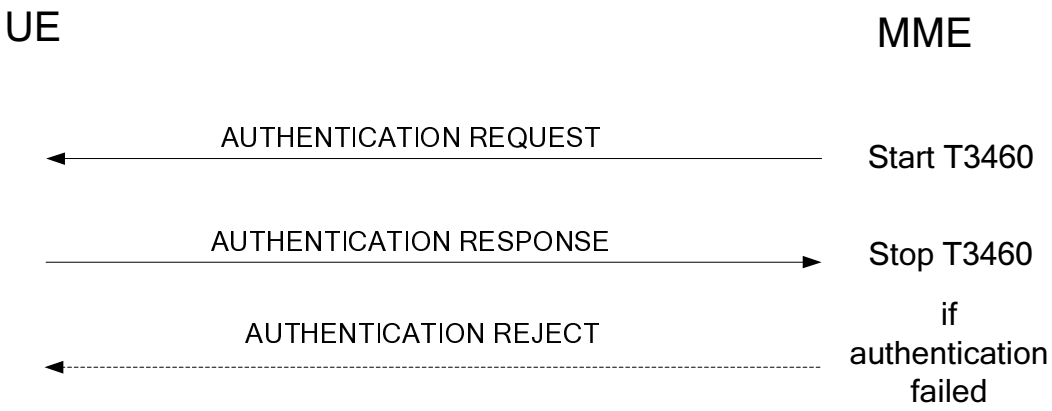

Figure 5.4.2.2.1: Authentication procedure

5.4.2.3 Authentication response by the UE

The UE shall respond to an AUTHENTICATION REQUEST message. With the exception of the cases described in subclause 5.4.2.6, the UE shall process the authentication challenge data and respond with an AUTHENTICATION RESPONSE message to the network.

Upon a successful EPS authentication challenge, the new K_{ASME} calculated from the authentication challenge data shall be stored in a new EPS security context.

The USIM will compute the authentication response (RES) using the authentication challenge data received from the ME, and pass RES to the ME.

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

In order to avoid a synchronisation failure, when the UE receives an AUTHENTICATION REQUEST message, the UE shall store the received RAND together with the RES returned from the USIM in the volatile memory. When the UE receives a subsequent AUTHENTICATION REQUEST message, if the stored RAND value is equal to the new received value in the AUTHENTICATION REQUEST message, then the UE shall not pass the RAND to the USIM, but shall send the AUTHENTICATION RESPONSE message with the stored RES. If there is no valid stored RAND in the UE or the stored RAND is different from the new received value in the AUTHENTICATION REQUEST message, the UE shall pass the RAND to the USIM, shall override any previously stored RAND and RES with the new ones and start, or reset and restart timer T3416.

The RAND and RES values stored in the UE shall be deleted and timer T3416, if running, shall be stopped:

- upon receipt of a
  - SECURITY MODE COMMAND,

- SERVICE REJECT,
- TRACKING AREA UPDATE ACCEPT, or
- AUTHENTICATION REJECT message;

- upon expiry of timer T3416; or
- if the UE enters the EMM state EMM-DEREGISTERED or EMM-NULL.

5.4.2.4 Authentication completion by the network

5.4.2.4.1 Authentication response received by the network

Upon receipt of an AUTHENTICATION RESPONSE message, the network stops the timer T3460 and checks the correctness of RES (see 3GPP TS 33.401 [19]).

Upon receipt of an 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.

5.4.2.4.2 EPS key identification

The security parameters for authentication, integrity protection and ciphering are tied together in sets and identified by the Key Set Identifier (KSI_{ASME}). The relationship between the security parameters is defined in 3GPP TS 33.401 [19].

The KSI_{ASME} is assigned by the network and passed with the AUTHENTICATION REQUEST message to the UE to enable the start of ciphering and integrity protection of NAS signalling at the next establishment of a NAS signalling connection without executing a new authentication procedure.

If an authentication procedure has been completed successfully and the related KSI_{ASME} is stored in the EPS security context of the network, the network shall include a different KSI_{ASME} value in the AUTHENTICATION REQUEST message when it initiates a new authentication procedure.

The UE stores the KSI_{ASME} along with the K_{ASME}, the EPS NAS ciphering key and the EPS NAS integrity key in its EPS security context. In the initial NAS message the UE sends the effective KSI_{ASME} value back to the network. The network may start ciphering and integrity protection with the stored EPS NAS ciphering key and EPS NAS integrity key (under the restrictions given in 3GPP TS 33.401 [19]) if the KSI_{ASME} stored in the network and the one sent by the UE are equal.

In the present document, when the UE is required to delete a KSI_{ASME}, the UE shall set the KSI_{ASME} to the value "no key is available" and consider also the associated K_{ASME}, EPS NAS ciphering key and EPS NAS integrity key invalid (i.e. the EPS NAS security context associated with the KSI_{ASME} as no longer valid).

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

5.4.2.5 Authentication not accepted by the network

If the authentication response returned by the UE is not valid, the network response depends upon the type of identity used by the UE in the initial NAS message, that is:

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

If the GUTI was used, the network should initiate an identification procedure. If the IMSI given by the UE during the identification procedure differs from the IMSI the network had associated with the GUTI, the authentication should be restarted with the correct parameters. Otherwise, if the IMSI provided by the UE is the same as the IMSI stored in the network (i.e. authentication has really failed), the network should proceed as described below.

If the IMSI was used for identification in the initial NAS message, or the network decides not to initiate the identification procedure after an unsuccessful authentication procedure, the network should send an AUTHENTICATION REJECT message to the UE.

Upon receipt of an AUTHENTICATION REJECT message, the UE shall set the update status to EU3 ROAMING NOT ALLOWED, delete the stored GUTI, TAI list, last visited registered TAI and KSI_{ASME}. The USIM shall be considered invalid until switching off the UE or the UICC containing the USIM is removed.

If the AUTHENTICATION REJECT message is received by the UE, the UE shall abort any EMM signalling procedure, stop any of the timers T3410, T3417 or T3430 (if running) and enter state EMM-DEREGISTERED.

5.4.2.6 Authentication not accepted by the UE

In an EPS authentication challenge, the UE shall check the authenticity of the core network by means of the AUTN parameter received in the AUTHENTICATION REQUEST message. This enables the UE to detect a false network.

During an EPS authentication procedure, the UE may reject the core network due to an incorrect AUTN parameter (see 3GPP TS 33.401 [19]). This parameter contains two possible causes for authentication failure:

a) MAC code failure:

   If the UE finds the MAC code (supplied by the core network in the AUTN parameter) to be invalid, the UE shall send an AUTHENTICATION FAILURE message to the network, with the EMM cause "MAC failure". The UE shall then follow the procedure described in subclause 5.4.2.7, item c.

b) SQN failure:

   If the UE finds the SQN (supplied by the core network in the AUTN parameter) to be out of range, the UE shall send an AUTHENTICATION FAILURE message to the network, with the EMM cause "synch failure" and a re-synchronization token AUTS provided by the USIM (see 3GPP TS 33.102 [18]). The UE shall then follow the procedure described in subclause 5.4.2.7, item d.

Editor's note: It is FFS under which conditions, if any, the UE will accept a UMTS authentication challenge via E-UTRAN.

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 T3416, if running.

5.4.2.7 Abnormal cases

a) Lower layer failure:

   Upon detection of lower layer failure before the AUTHENTICATION RESPONSE is received, the network shall abort the procedure.

b) Expiry of timer T3460:

   The network shall, on the first expiry of the timer T3460, retransmit the AUTHENTICATION REQUEST and shall reset and start timer T3460. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3460, the network shall abort the authentication procedure and any ongoing EMM specific procedure and release the NAS signalling connection.

c) Authentication failure (EMM cause "MAC failure"):

   The UE shall send an AUTHENTICATION FAILURE message, with EMM cause "MAC failure" according to subclause 5.4.2.6, to the network and start timer T3418 (see example in figure 5.4.2.7.1). Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3410, T3417, T3421 or T3430). Upon the first receipt of an AUTHENTICATION FAILURE message from the UE with EMM cause "MAC failure", the network may initiate the identification procedure described in subclause 5.4.4. This is to allow the network to obtain the IMSI from the UE. The network may then check that the GUTI originally used in the authentication challenge corresponded to the correct IMSI. Upon receipt of the IDENTITY REQUEST message from the network, the UE shall send the IDENTITY RESPONSE message.

NOTE 1: Upon receipt of an AUTHENTICATION FAILURE message from the UE with EMM cause "MAC failure", the network may also terminate the authentication procedure (see subclause 5.4.2.5).

If the GUTI/IMSI mapping in the network was incorrect, the network should respond by sending a new AUTHENTICATION REQUEST message to the UE. Upon receiving the new AUTHENTICATION REQUEST

message from the network, the UE shall stop the timer T3418, if running, and then process the challenge information as normal.

If the network is validated successfully (an AUTHENTICATION REQUEST that contains a valid SQN and MAC is received), the UE shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3410, T3417, T3421 or T3430) if they were running and stopped when the UE received the first failed AUTHENTICATION REQUEST message.

If the UE receives the second AUTHENTICATION REQUEST while T3418 is running, and the MAC value cannot be resolved or the message contains an EPS authentication challenge, the UE shall follow the procedure specified in this subclause, item c, starting again from the beginning. If the SQN is invalid, the UE shall proceed as specified in item d.

It can be assumed that the source of the authentication challenge is not genuine (authentication not accepted by the UE) if any of the following occur:

- after sending the AUTHENTICATION FAILURE message with the EMM cause "MAC failure" the timer T3418 expires;
- the UE detects any combination of the authentication failures: "MAC failure" and "invalid SQN", during three consecutive authentication challenges. The authentication challenges shall be considered as consecutive only, if the authentication challenges causing the second and third authentication failure are received by the UE, while the timer T3418 or T3420 started after the previous authentication failure is running.

When it has been deemed by the UE that the source of the authentication challenge is not genuine (i.e. authentication not accepted by the UE), the UE shall proceed as described in item e.

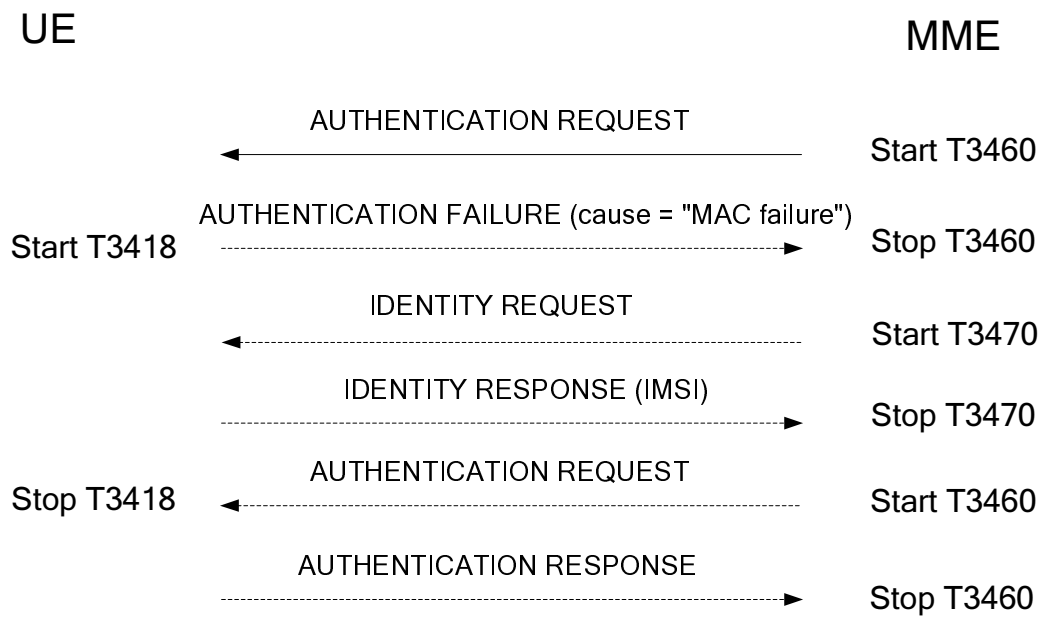

Figure 5.4.2.7.1: Authentication failure procedure (EMM cause "MAC failure")

d) Authentication failure (EMM cause "synch failure"):

The UE shall send an AUTHENTICATION FAILURE message, with EMM cause "synch failure", to the network and start the timer T3420 (see example in figure 5.4.2.7.2). Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3410, T3417, T3421 or T3430). Upon the first receipt of an AUTHENTICATION FAILURE message from the UE with the EMM cause "synch failure", the network shall use the returned AUTS parameter from the authentication failure parameter IE in the AUTHENTICATION FAILURE message, to re-synchronise. The re-synchronisation procedure requires the MME to delete all unused authentication vectors for that IMSI and obtain new vectors from the HSS. When re-synchronisation is complete, the network shall initiate the authentication procedure. Upon receipt of the AUTHENTICATION REQUEST message, the UE shall stop the timer T3420, if running.

NOTE 2: Upon receipt of two consecutive AUTHENTICATION FAILURE messages from the UE with EMM cause "synch failure", the network may terminate the authentication procedure by sending an AUTHENTICATION REJECT message.

If the network is validated successfully (a new AUTHENTICATION REQUEST is received which contains a valid SQN and MAC) while T3420 is running, the UE shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3410, T3417, T3421 or T3430), if they were running and stopped when the UE received the first failed AUTHENTICATION REQUEST message.

If the UE receives the second AUTHENTICATION REQUEST while T3420 is running, and the MAC value cannot be resolved or the message contains a EPS authentication challenge, the UE shall proceed as specified in item c; if the SQN is invalid, the UE shall follow the procedure specified in this subclause, item d, starting again from the beginning.

The UE shall deem that the network has failed the authentication check and proceed as described in item e if any of the following occurs:

- the timer T3420 expires;
- the UE detects any combination of the authentication failures: "MAC failure" or "invalid SQN", during three consecutive authentication challenges. The authentication challenges shall be considered as consecutive only if the authentication challenges causing the second and third authentication failure are received by the UE while the timer T3418 or T3420 started after the previous authentication failure is running.

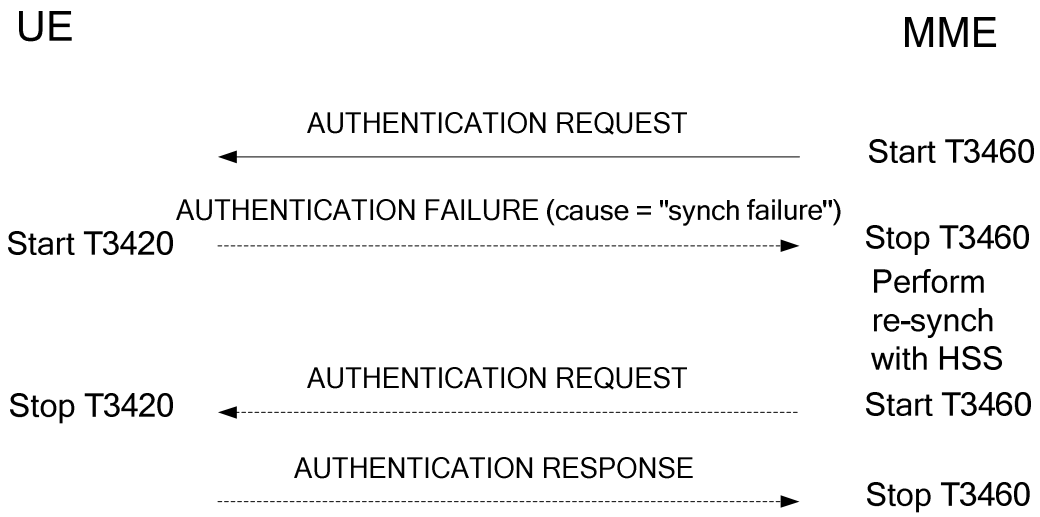

Figure 5.4.2.7.2: Authentication failure procedure (EMM cause "synch failure")

e) Network failing the authentication check:

If the UE deems that the network has failed the authentication check, then it shall request RRC to locally release the RRC connection and the NAS signalling connection, and treat the active cell as barred (see 3GPP TS 36.331 [22]). The UE shall start any retransmission timers (e.g. T3410, T3417, T3421 or T3430), if they were running and stopped when the UE received the first AUTHENTICATION REQUEST message containing an invalid MAC or SQN.

f) Transmission failure of AUTHENTICATION RESPONSE message or AUTHENTICATION FAILURE message indication from lower layers (if the authentication procedure is triggered by a tracking area updating procedure)

The UE shall re-initiate the tracking area updating procedure.

g) Transmission failure of AUTHENTICATION RESPONSE message or AUTHENTICATION FAILURE message indication with TAI change from lower layers (if the authentication procedure is triggered by a service request procedure)

If the current TAI is not in the TAI list, the authentication procedure shall be aborted and a tracking area updating procedure shall be initiated.

If the current TAI is still part of the TAI list, it is up to the UE implementation how to re-run the ongoing procedure that triggered the authentication procedure.

h) Transmission failure of AUTHENTICATION RESPONSE message or AUTHENTICATION FAILURE message indication without TAI change from lower layers (if the authentication procedure is triggered by a service request procedure)

It is up to the UE implementation how to re-run the ongoing procedure that triggered the authentication procedure.

5.4.3 Security mode control procedure

5.4.3.1 General

The purpose of the NAS security mode control procedure is to take an EPS security context into use, and initialise and start NAS signalling security between the UE and the MME with the corresponding NAS keys and security algorithms.

5.4.3.2 NAS security mode control initiation by the network

The MME initiates the NAS security mode control procedure by sending a SECURITY MODE COMMAND message to the UE and starting timer T3460 (see example in figure 5.4.3.2.1).

The MME shall send the SECURITY MODE COMMAND message unciphered, but shall integrity protect the message with the NAS integrity key based on K_{ASME} indicated by the KSI_{ASME} included in the message. The MME shall set the security header type of the message to "integrity protected with new EPS security context".

If the security mode control procedure is not initiated due to inter-system handover from A/Gb mode to S1 mode or Iu mode to S1 mode, the MME shall set the KSI_{SGSN} to the value "no key is available".

For inter-system handover from A/Gb mode to S1 mode or Iu mode to S1 mode, if the MME has a cached EPS security context, the MME shall include the KSI_{ASME} IE in the SECURITY MODE COMMAND message, and shall integrity protect the SECURITY MODE COMMAND message with the NAS integrity key based on K_{ASME} indicated by the KSI_{ASME} indicated in the message.

For idle mode mobility from A/Gb mode or Iu mode to S1 mode, if the MME uses the mapped EPS security context, the MME shall include the KSI_{SGSN} IE in the SECURITY MODE COMMAND message and integrity protect the SECURITY MODE COMMAND message with the NAS integrity key based on K'_{ASME} indicated by the KSI_{SGSN} indicated in the message.

The MME shall include the replayed security capabilities of the UE (including the security capabilities with regard to NAS, RRC and UP (user plane) ciphering as well as NAS, RRC integrity, and other possible target network security capabilities, i.e. UTRAN/GERAN if UE included them in the message to network), the replayed $nonce_{UE}$ if the UE included it in the message to the network, the selected NAS ciphering and integrity algorithms and the Key Set Identifier (KSI_{ASME} or KSI_{SGSN}). A SECURITY MODE COMMAND that follows a successful execution of the authentication procedure shall use a NAS COUNT reset to zero.

Additionally, the MME may request the UE to include its IMEISV in the SECURITY MODE COMPLETE message.

NOTE: The AS and NAS security capabilities will be the same, i.e. if the UE supports one algorithm for NAS it is also be supported for AS.

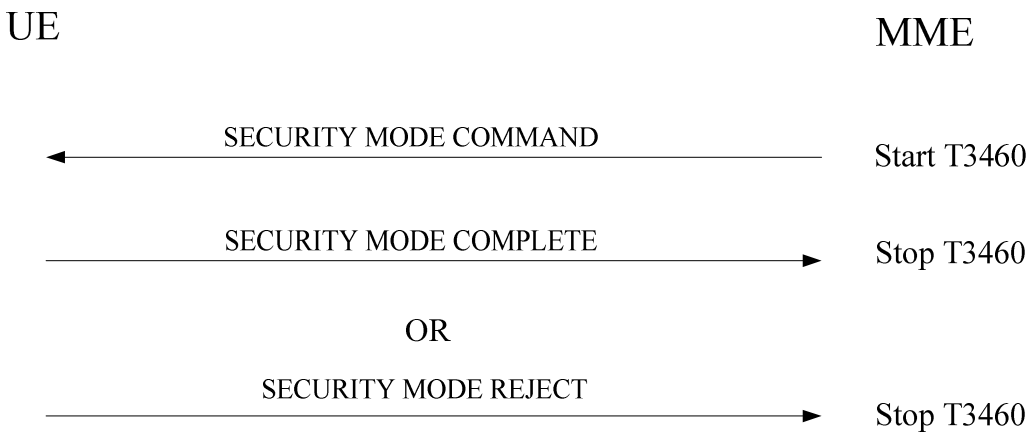

Figure 5.4.3.2.1: Security mode control procedure

5.4.3.3 NAS security mode command accepted by the UE

Upon receipt of the SECURITY MODE COMMAND message, the UE shall check whether the security mode command can be accepted or not. This is done by performing the integrity check of the message and by checking that the received UE security capabilities and the received $nonce_{UE}$ have not been altered compared to what the UE provided in the initial layer 3 message that triggered this procedure.

If the security mode command can be accepted and the KSI_{ASME} was included in the SECURITY MODE COMMAND message, the UE shall send a SECURITY MODE COMPLETE message integrity protected with the selected NAS integrity algorithm and the NAS integrity key based on the K_{ASME} indicated by the KSI_{ASME}. If the SECURITY MODE COMMAND message includes KSI_{SGSN}, $nonce_{MME}$ and $nonce_{UE}$, the UE shall generate K'_{ASME} from both nonces as indicated in 3GPP TS 33.401 [19] to check whether the SECURITY MODE COMMAND can be accepted or not. The UE shall cipher the SECURITY MODE COMPLETE message with the selected NAS ciphering algorithm and the NAS ciphering key based on the K_{ASME} indicated by the KSI_{ASME} or fresh K'_{ASME}. The UE shall set the security header type of the message to "integrity protected and ciphered with new EPS security context". A SECURITY MODE COMPLETE that follows a successful execution of the authentication procedure shall use a NAS COUNT reset to zero.

From this time onward the UE shall cipher and integrity protect all NAS signalling messages with the selected NAS ciphering and NAS integrity algorithms.

If the MME indicated in the SECURITY MODE COMMAND message that the IMEISV is requested, the UE shall include its IMEISV in the SECURITY MODE COMPLETE message.

5.4.3.4 NAS security mode control completion by the network

The MME shall, upon receipt of the SECURITY MODE COMPLETE message, stop timer T3460. From this time onward the MME shall integrity protect and encipher all signalling messages with the selected NAS integrity and ciphering algorithms.

5.4.3.5 NAS security mode command not accepted by the UE

If the security mode command cannot be accepted, the UE shall send a SECURITY MODE REJECT message, which shall not be integrity protected. The SECURITY MODE REJECT message contains an EMM cause that typically indicates one of the following cause values:

#23: UE security capabilities mismatch;

#24: security mode rejected, unspecified.

Editor's note: The actions to be taken by the network are FFS.

Upon receipt of the SECURITY MODE REJECT message, the MME shall stop timer T3460. The MME shall also abort the ongoing procedure that triggered the initiation of the NAS security mode control procedure.

5.4.3.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication from lower layers (if the security mode control procedure is triggered by a tracking area updating procedure)

The UE shall re-initiate the tracking area updating procedure.

b) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication with TAI change from lower layers (if the security mode control procedure is triggered by a service request procedure)

If the current TAI is not in the TAI list, the security mode control procedure shall be aborted and a tracking area updating procedure shall be initiated.

If the current TAI is still part of the TAI list, it is up to the UE implementation how to re-run the ongoing procedure that triggered the security mode control procedure.

c) Transmission failure of SECURITY MODE COMPLETE message or SECURITY MODE REJECT message indication without TAI change from lower layers (if the security mode control procedure is triggered by a service request procedure)

It is up to the UE implementation how to re-run the ongoing procedure that triggered the security mode control procedure.

5.4.3.7 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure before the SECURITY MODE COMPLETE or SECURITY MODE REJECT message is received

The network shall abort the procedure.

b) Expiry of timer T3460

The network shall, on the first expiry of the timer T3460, retransmit the SECURITY MODE COMMAND and shall reset and start timer T3460. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3460, the procedure shall be aborted.

c) Collision between security mode control procedure and attach, service request, tracking area updating procedure or detach procedure not indicating power off

The network shall abort the security mode control procedure and proceed with the UE initiated procedure.

d) Collision between security mode control procedure and other EMM procedures than in item c

The network shall progress both procedures.

5.4.4 Identification procedure

5.4.4.1 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). IMEI and IMSI definition and structure are specified in 3GPP TS 23.003 [2].

5.4.4.2 Identification initiation by the network

The network initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and starting the timer T3470 (see example in figure 5.4.4.2.1). The IDENTITY REQUEST message specifies the requested identification parameters in the Identity type information element.

Editor's note: The use of this procedure to request other types of mobile equipment identifiers is FFS.

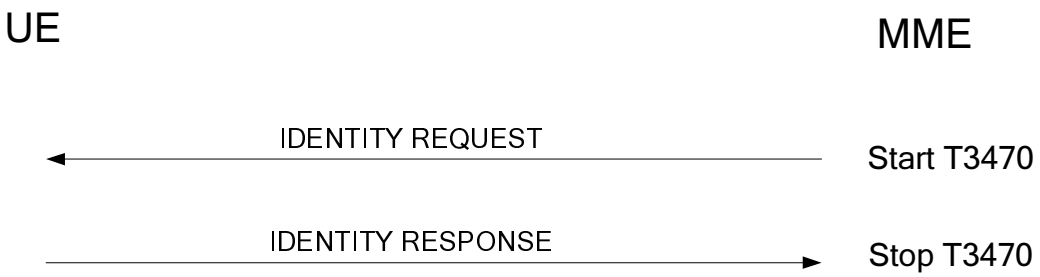

Figure 5.4.4.2.1: Identification procedure

5.4.4.3 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.

5.4.4.4 Identification completion by the network

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

5.4.4.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Requested identity is not available

If the UE cannot encode the requested identity in the IDENTITY RESPONSE message, e.g. because no valid USIM is available, then it shall encode the identity type as "No identity".

b) Transmission failure of IDENTITY RESPONSE message indication from lower layers (if the identification procedure is triggered by a tracking area updating procedure)

The UE shall re-initiate the tracking area updating procedure.

Editor's note: Other abnormal cases in the UE need to be defined.

5.4.4.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure

Upon detection of a lower layer failure before the IDENTITY RESPONSE is received, the network shall abort any ongoing EMM procedure.

b) Expiry of timer T3470

The identification procedure is supervised by the network by the timer T3470. The network shall, on the first expiry of the timer T3470, retransmit the IDENTITY REQUEST message and reset and restart the timer T3470.

This retransmission is repeated four times, i.e. on the fifth expiry of timer T3470, the network shall abort the identification procedure and any ongoing EMM procedure.

c) Collision of an identification procedure with an EPS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing identification procedure has been completed and no EPS attach procedure is pending on the network (i.e. no ATTACH ACCEPT/REJECT message has still to be sent as an answer to an ATTACH REQUEST message), the network shall proceed with the EPS attach procedure.

d) Collision of an identification procedure with an EPS attach procedure when the identification procedure has been caused by an EPS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing identification procedure has been completed and an EPS attach procedure is pending (i.e. an ATTACH ACCEPT/REJECT message has to be sent as an answer to an earlier ATTACH REQUEST message), then:

- If one or more of the information elements in the ATTACH REQUEST message differ from the ones received within the previous ATTACH REQUEST message, the network shall proceed with the new EPS attach procedure; or
- If the information elements do not differ, then the network shall not treat any further this new ATTACH REQUEST.

e) Collision of an identification procedure with a UE initiated EPS detach procedure

EPS detach containing cause "power off":

If the network receives a DETACH REQUEST message before the ongoing identification procedure has been completed, the network shall abort the identification procedure and shall progress the EPS detach procedure.

EPS detach containing other causes than "power off":

If the network receives a DETACH REQUEST message before the ongoing identification procedure has been completed, the network shall complete the identification procedure and shall respond to the EPS detach procedure as described in subclause 5.5.2.

f) Collision of an identification procedure with a tracking area updating procedure

If the network receives a TRACKING AREA UPDATE REQUEST message before the ongoing identification procedure has been completed, the network shall progress both procedures.

g) Collision of an identification procedure with a service request procedure

If the network receives a SERVICE REQUEST message or EXTENDED SERVICE REQUEST message before the ongoing identification procedure has been completed, the network shall progress both procedures.

5.4.5 EMM information procedure

5.4.5.1 General

The purpose of sending the EMM INFORMATION message is to allow the network to provide information to the UE. The message implementation is optional in the network. The UE may use the received information if the UE supports implementing this message.

The EMM information procedure may be invoked by the network at any time during an established EMM context.

5.4.5.2 EMM information procedure initiation by the network

The EMM information procedure consists only of the EMM INFORMATION message sent from the network to the UE (see example in figure 5.4.5.2.1). During an established EMM context, the network may send none, one, or more EMM INFORMATION messages to the UE. If more than one EMM INFORMATION message is sent, the messages need not have the same content.

Figure 5.4.5.2.1: EMM information procedure

5.4.5.3 EMM information procedure in the UE

When the UE (supporting the EMM information message) receives an EMM INFORMATION message, it shall accept the message and optionally use the contents to update appropriate information stored within the UE.

If the UE does not support the EMM information message the UE shall ignore the contents of the message and return an EMM STATUS message with cause value #97, "message type non-existent or not implemented".

5.5 EMM specific procedures

5.5.1 Attach procedure

5.5.1.1 General

The attach procedure is used to attach to an EPC for packet services in EPS.

The attach procedure is used for two purposes:

- by a UE in PS mode of operation to attach for EPS services only; or
- by a UE in CS/PS mode 1 or CS/PS mode 2 of operation to attach for both EPS and non-EPS services.

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.

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

In a shared network, the UE shall choose one of the PLMN identities as specified in 3GPP TS 23.122 [6]. The UE shall construct the TAI of the cell from this chosen PLMN identity and the TAC received as part of the broadcast system information. The chosen PLMN identity shall be indicated to the E-UTRAN (see 3GPP TS 36.331 [22]). Whenever an ATTACH REJECT message with the cause "PLMN not allowed" is received by the UE, the chosen PLMN identity shall be stored in the "forbidden PLMN list". Whenever an ATTACH REJECT message is received by the UE with the cause "Roaming not allowed in this tracking area", "Tracking area not allowed", or "No suitable cells in tracking area", the constructed TAI shall be stored in the suitable list.

An attach attempt counter is used to limit the number of subsequently rejected attach attempts. The attach attempt counter shall be incremented as specified in subclause 5.5.1.2.6. Depending on the value of the attach attempt counter, specific actions shall be performed. The attach attempt counter shall be reset when:

- the UE is powered on;
- a USIM is inserted;
- an attach or combined attach procedure is successfully completed;
- a combined EPS attach procedure is completed for EPS services only with cause value #2, #16, #17, #18 or #22;
- an attach or combined attach procedure is rejected with cause value #11, #12, #13, #14, #15 or #25; or
- a network initiated detach procedure is completed with cause value #11, #12, #13, #14, #15 or #25.

Additionally the attach attempt counter shall be reset when the UE is in substate EMM-DEREGISTERED.ATTEMPTING-TO-ATTACH and:

- a new tracking area is entered; or
- T3402 expires.

5.5.1.2 Attach procedure for EPS services

5.5.1.2.1 General

This procedure is used by a UE to attach for EPS services only. When the UE initiates the EPS attach procedure, the UE shall indicate "EPS attach" in the EPS attach type IE.

5.5.1.2.2 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 (see example in figure 5.5.1.2.2.1). If timer T3402 is currently running, the UE shall stop timer T3402. If timer T3411 is currently running, the UE shall stop timer T3411. 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 send the ATTACH REQUEST message together with a PDN CONNECTIVITY REQUEST message contained in the ESM message container information element to request PDN connectivity.

The UE may also include the DRX parameter.

If a valid NAS security context exists, the UE shall integrity protect the ATTACH REQUEST message combined with the PDN CONNECTIVITY REQUEST message. When the UE does not have a valid NAS security context, the ATTACH REQUEST message combined with the PDN CONNECTIVITY REQUEST message is not integrity protected.

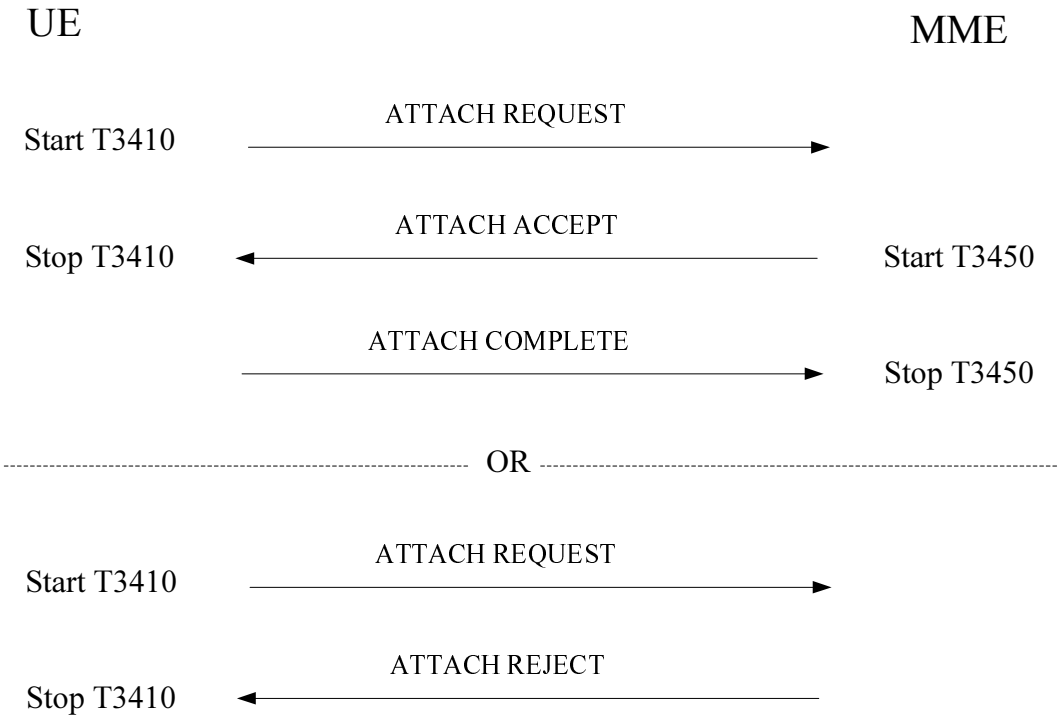

Figure 5.5.1.2.2.1: Attach procedure and combined attach procedure

5.5.1.2.3 EMM common procedure initiation

The network may initiate EMM common procedures, e.g. the identification, authentication and security mode control procedures during the attach procedure, depending on the information received in the ATTACH REQUEST message (e.g. IMSI, GUTI and KSI).

5.5.1.2.4 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 and start timer T3450. The MME shall send the ATTACH ACCEPT message together with an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message contained in the ESM message container information element to activate the default bearer (see subclause 6.4.1). The network may also initiate the activation of dedicated bearers towards the UE by invoking the dedicated EPS bearer context activation procedure (see subclause 6.4.2).

If the attach request is accepted by the network, the MME shall delete the stored UE radio capability information, if any.

If the UE has included the UE network capability IE or the MS network capability IE or both in the ATTACH REQUEST message, the MME shall store all octets received from the UE, up to the maximum length defined for the respective information element.

NOTE: This information is forwarded to the new MME during inter-MME handover or to the new SGSN during inter-system handover to A/Gb mode or Iu mode.

The MME shall assign and include the TAI list the UE is registered to in the ATTACH ACCEPT message. The UE, upon 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.

The GUTI reallocation may be part of the attach procedure. When the ATTACH REQUEST message includes the IMSI, or the MME considers the GUTI provided by the UE is invalid, or the GUTI provided by the UE was assigned by another MME, 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 enter state EMM-COMMON-PROCEDURE-INITIATED as described in subclause 5.4.1.

For a shared network, the TAIs included in the TAI list can contain different PLMN identities.

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.

If A/Gb mode or Iu mode is supported in the UE, the UE shall set its TIN to "GUTI" when receiving the ATTACH ACCEPT message.

The MME may also include a list of equivalent PLMNs in the ATTACH ACCEPT message. Each entry in the list contains a PLMN code (MCC+MNC). The UE shall store the list as provided by the network, after having removed from the list any PLMN code that is already in the list of forbidden PLMNs. In addition, the UE shall add to the stored list the PLMN code of the registered PLMN that sent the list. The UE shall replace the stored list on each receipt of the ATTACH ACCEPT message. If the ATTACH ACCEPT message does not contain a list, then the UE shall delete the stored list.

For manual update of the Allowed CSG list, the UE, when receiving the ATTACH ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the ATTACH REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSD ID to the Allowed CSG list.

When the UE receives the ATTACH ACCEPT message combined with the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, it shall forward the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message to the ESM sublayer. Upon receipt of an indication from the ESM sublayer that the default EPS bearer context has been activated, the UE shall send an ATTACH COMPLETE message together with an ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message contained in the ESM message container information element to the network.

Additionally, the UE shall reset the attach attempt counter and tracking area updating attempt counter, enter state EMM-REGISTERED and set the EPS update status to EU1 UPDATED.

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

5.5.1.2.5 Attach not accepted by the network

If the attach request cannot be accepted by the network, the MME shall send an ATTACH REJECT message to the UE including an appropriate EMM cause value. If the attach procedure fails due to a default EPS bearer setup failure or an ESM procedure failure, the MME shall combine the ATTACH REJECT message with a PDN CONNECTIVITY REJECT message contained in the ESM message container information element. In this case the EMM cause value in the ATTACH REJECT message shall be set to #19, "ESM failure".

Upon receiving the ATTACH REJECT message, the UE shall stop timer T3410 and take the following actions depending on the EMM cause value received.

#3 (Illegal UE); or

#6 (Illegal ME);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. The UE shall consider the USIM as invalid for EPS services and non-EPS services until switching off or the UICC containing the USIM is removed. Additionally, the UE shall delete the list of equivalent PLMNs and enter state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the MM parameters update status, TMSI, LAI and ciphering key sequence number, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the normal attach procedure is rejected with this cause value.

NOTE: The possibility to configure a UE so that the radio transceiver for a specific RAT is not active, although it is implemented in the UE, is out of scope of the present specification.

#7 (EPS services not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. Additionally, the UE shall delete the list of equivalent PLMNs and enter state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the normal attach procedure is rejected with this cause value.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. The UE shall consider the USIM as invalid for EPS services and non-EPS services until switching off or the UICC containing the USIM is removed. Additionally, the UE shall delete the list of equivalent PLMNs and enter state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the MM parameters update status, TMSI, LAI and ciphering key sequence number, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the normal attach procedure is rejected with this cause value.

#11 (PLMN not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. Additionally, the UE shall delete the list of equivalent PLMNs, reset the attach attempt counter, and enter state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMN list".

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the MM parameters update status, TMSI, LAI, ciphering key sequence number and location update attempt counter, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal attach procedure is rejected with this cause value and no RR connection exists.

#12 (Tracking area not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. Additionally, the UE shall reset the attach attempt counter and enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for regional provision of service".

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal attach procedure is rejected with this cause value.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. The UE shall delete the list of equivalent PLMNs and reset the attach attempt counter. Additionally, the UE shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE or optionally EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming".

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal attach procedure is rejected with this cause value.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. Additionally, the UE shall reset the attach attempt counter and enter state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list.

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal attach procedure is rejected with this cause value.

#15 (No suitable cells in tracking area);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. Additionally, the UE shall reset the attach attempt counter and enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming".

The UE shall search for a suitable cell in another tracking area or in another location area in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS

attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal attach procedure is rejected with this cause value.

#25 (Not authorized for this CSG);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). Additionally, the UE shall reset the attach attempt counter and shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall remove the CSG ID of the cell where the UE has sent the ATTACH REQUEST message from the Allowed CSG list.

The UE shall search for a suitable cell in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal attach procedure is rejected with this cause value.

Other values are considered as abnormal cases.

5.5.1.2.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Access barred because of access class barring or NAS signalling connection establishment rejected by the network

If access is barred for "signalling" (see 3GPP TS 36.331 [22]), the attach procedure shall not be started. The UE stays in the current serving cell and applies the normal cell reselection process. The attach procedure is started as soon as possible, i.e. when access for "signalling" is granted on the current cell or when the UE moves to a cell where access for "signalling" is granted.

b) Lower layer failure or release of the NAS signalling connection before the ATTACH ACCEPT or ATTACH REJECT message is received

The attach procedure shall be aborted, and the UE shall proceed as described below.

c) T3410 timeout

The UE shall abort the attach procedure and proceed as described below. The NAS signalling connection shall be released locally.

d) ATTACH REJECT, other cause values than those treated in subclause 5.5.1.2.5

Upon reception of the cause value #19, "ESM failure", the UE may set the attach attempt counter to 5. Upon reception of the cause values #95, #96, #97, #99 and #111 the UE should set the attach attempt counter to 5.

The UE shall proceed as described below.

e) Change of cell into a new tracking area

If a cell change into a new tracking area occurs before the attach procedure is completed, the attach procedure shall be aborted and re-initiated immediately. If a tracking area border is crossed when the ATTACH ACCEPT message has been received but before an ATTACH COMPLETE message is sent, the attach procedure shall be re-initiated. If a GUTI was allocated during the attach procedure, this GUTI shall be used in the attach procedure.

f) Mobile originated detach required

The attach procedure shall be aborted, and the UE initiated detach procedure shall be performed.

g) Detach procedure collision

If the UE receives a DETACH REQUEST message from the network in state EMM-REGISTERED-INITIATED and the detach type indicates "re-attach not required", the detach procedure shall be progressed and the attach

procedure shall be aborted. Otherwise the attach procedure shall be progressed and the DETACH REQUEST message shall be ignored.

h) Transmission failure of ATTACH REQUEST message or ATTACH COMPLETE message indication from lower layers

The UE shall restart the attach procedure.

i) Access barred because the CSG ID is not in the UE's Allowed CSG list

If access is barred because the CSG ID is not in the UE's Allowed CSG list, the attach procedure shall not be started. The UE stays in the current serving cell and applies the normal cell reselection process. The attach procedure is started as soon as possible, e.g. when the UE moves to a cell where access is granted.

j) If the ACTIVATE DEFAULT BEARER CONTEXT REQUEST message combined with the ATTACH ACCEPT is not accepted by the UE due to failure in the UE ESM sublayer, then the UE shall initiate the detach procedure by sending a DETACH REQUEST message to the network. The UE shall include the identity previously used for the attach procedure in the DETACH REQUEST message.

For the cases b, c, d and j the UE shall proceed as follows. Timer T3410 shall be stopped if still running. The attach attempt counter shall be incremented, unless it was already set to 5.

If the attach attempt counter is less than 5:

- timer T3411 is started and the state is changed to EMM-DEREGISTERED.ATTEMPTING-TO-ATTACH. When timer T3411 expires the attach procedure shall be restarted.

If the attach attempt counter is equal to 5:

- the UE shall delete any GUTI, TAI list, last visited registered TAI, list of equivalent PLMNs and KSI, shall set the update status to EU2 NOT UPDATED, and shall start timer T3402. The state is changed to EMM-DEREGISTERED.ATTEMPTING-TO-ATTACH or optionally to EMM-DEREGISTERED.PLMN-SEARCH in order to perform a PLMN selection according to 3GPP TS 23.122 [6].

  If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the abnormal case when a normal attach procedure fails and the attach attempt counter is equal to 5.

5.5.1.2.7 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure

If a lower layer failure occurs before the message ATTACH COMPLETE has been received from the UE and a new GUTI has been assigned, the network shall consider both the old and new GUTI as valid until the old GUTI can be considered as invalid by the network (see subclause 5.4.1.6) and shall not resend the message ATTACH ACCEPT. During this period the network may:

- use the identification procedure followed by a GUTI reallocation procedure if the old GUTI is used by the UE in a subsequent message.

b) Protocol error

If the ATTACH REQUEST message is received with a protocol error, the network shall return an ATTACH REJECT message with one of the following EMM cause values:

#96: invalid mandatory information;

#99: information element non-existent or not implemented;

#100: conditional IE error; or

#111: protocol error, unspecified.

c) T3450 time-out

On the first expiry of the timer, the network shall retransmit the ATTACH ACCEPT message and shall reset and restart timer T3450.

This retransmission is repeated four times, i.e. on the fifth expiry of timer T3450, the attach procedure shall be aborted. If a new GUTI was allocated in the ATTACH ACCEPT message, the network shall consider both the old and new GUTI as valid until the old GUTI can be considered as invalid by the network (see subclause 5.4.1.6). During this period the network acts as specified for case a above.

d) ATTACH REQUEST received after the ATTACH ACCEPT message has been sent and before the ATTACH COMPLETE message is received

- If one or more of the information elements in the ATTACH REQUEST message differ from the ones received within the previous ATTACH REQUEST message, the previously initiated attach procedure shall be aborted if the ATTACH COMPLETE message has not been received and the new attach procedure shall be progressed; or

- if the information elements do not differ, then the ATTACH ACCEPT message shall be resent and the timer T3450 shall be restarted if an ATTACH COMPLETE message is expected. In that case, the retransmission counter related to T3450 is not incremented.

e) More than one ATTACH REQUEST received and no ATTACH ACCEPT or ATTACH REJECT message has been sent

- If one or more of the information elements in the ATTACH REQUEST message differs from the ones received within the previous ATTACH REQUEST message, the previously initiated attach procedure shall be aborted and the new attach procedure shall be executed;

- if the information elements do not differ, then the network shall continue with the previous attach procedure and shall ignore the second ATTACH REQUEST message.

f) ATTACH REQUEST received in state EMM-REGISTERED

If an ATTACH REQUEST message is received in state EMM-REGISTERED the network may initiate the EMM common procedures; if it turned out that the ATTACH REQUEST message was sent by a UE that has already been attached, the EMM context, EPS bearer contexts, if any, are deleted and the new ATTACH REQUEST is progressed.

g) TRACKING AREA UPDATE REQUEST message received before ATTACH COMPLETE message.

Timer T3450 shall be stopped. The allocated GUTI shall be considered as valid and the tracking area updating procedure shall be executed as described in subclause 5.5.3.

5.5.1.3 Combined attach procedure for EPS services and non-EPS services

5.5.1.3.1 General

The combined EPS attach procedure is used by a UE in CS/PS mode 1 or CS/PS mode 2 of operation to attach for both EPS and non-EPS services.

When the UE initiates a combined EPS attach procedure, the UE shall indicate "combined EPS/IMSI attach" in the EPS attach type IE.

The combined EPS attach procedure follows the attach procedure for EPS described in subclause 5.5.1.2.

5.5.1.3.2 Combined attach procedure initiation

If the UE is in EMM state EMM-DEREGISTERED, the UE initiates the combined attach procedure by sending an ATTACH REQUEST message to the network, starting timer T3410 and entering state EMM-REGISTERED-INITIATED (see example in figure 5.5.1.2.2.1).

The UE shall include the TMSI status IE if no valid TMSI is available. Furthermore, if the UE has stored a valid location area identification, the UE shall include it in the Old location area identification IE in the ATTACH REQUEST message.

5.5.1.3.3 EMM common procedure initiation

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

5.5.1.3.4 Combined attach accepted by the network

5.5.1.3.4.1 General

Depending on the value of the EPS attach result IE received in the ATTACH ACCEPT message, two different cases can be distinguished:

1) The EPS attach result IE value indicates "combined EPS/IMSI attach": attach for EPS and non-EPS services have been successful.

2) The EPS attach result IE value indicates "EPS only": attach for EPS services has been successful but attach for non-EPS services has failed.

5.5.1.3.4.2 Combined attach successful

The description for attach for EPS services as specified in subclause 5.5.1.2.4 shall be followed. In addition, the following description for attach for non-EPS services applies.

The TMSI reallocation may be part of the combined attach procedure. The TMSI allocated is then included in the ATTACH ACCEPT message, together with the location area identification (LAI). In this case the MME shall start timer T3450 and enter state EMM-COMMON-PROCEDURE-INITIATED as described in subclause 5.4.1.

The UE, receiving an ATTACH ACCEPT message, stores the received location area identification, stops timer T3410, resets the location update attempt counter and sets the update status to U1 UPDATED. If the message contains a mobile identity, the UE shall use this mobile identity as the new temporary identity. The UE shall delete its old mobile identity and shall store the new mobile identity. If no mobile identity has been included by the network in the ATTACH ACCEPT message, the old mobile identity, if any available, shall be kept.

The UE, when receiving the ATTACH ACCEPT message combined with the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, shall send an ATTACH COMPLETE message combined with an ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message to the network after which it shall enter state EMM-REGISTERED and MM state MM-IDLE and set the EPS update status to EU1 UPDATED.

Upon receiving an ATTACH COMPLETE message, the MME shall stop timer T3450, enter state EMM-REGISTERED and consider the new TMSI sent in the ATTACH ACCEPT message as valid.

5.5.1.3.4.3 Combined attach successful for EPS services only

The description for attach for EPS services as specified in subclause 5.5.1.2.4 shall be followed. In addition, the following description for attach for non-EPS services applies.

The UE receiving the ATTACH ACCEPT message takes one of the following actions depending on the EMM cause value:

#2 (IMSI unknown in HSS)

The UE shall stop T3410 if still running. The UE shall set the update status to U3 ROAMING NOT ALLOWED and shall delete any TMSI, LAI and ciphering key sequence number. The UE shall enter state EMM-REGISTERED.NORMAL-SERVICE. The new MM state is MM IDLE. The USIM shall be considered as invalid for non-EPS services until switching off or the UICC containing the USIM is removed.

#16 (MSC temporarily not reachable);

#17 (Network failure); or

#22 (Congestion)

The UE shall stop timer T3410 if still running. The tracking area updating attempt counter shall be incremented, unless it was already set to 5.

If the tracking area updating attempt counter is less than 5:

- the UE shall start timer T3411, shall set the EPS update status to EU1 UPDATED and shall enter state EMM-REGISTERED.ATTEMPTING-TO-UPDATE-MM. When timer T3411 expires the combined tracking area updating procedure indicating "combined TA/LA updating with IMSI attach" is triggered.

If the tracking area updating attempt counter is equal to 5:

- the UE shall start timer T3402, shall set the EPS update status to EU1 UPDATED and shall enter state EMM-REGISTERED.ATTEMPTING-TO-UPDATE-MM. When timer T3402 expires the combined tracking area updating procedure indicating "combined TA/LA updating with IMSI attach" is triggered;
- a UE operating in CS/PS mode 1 of operation shall select GERAN or UTRAN radio access technology and proceed with appropriate MM or GMM specific procedures.

Editor's note: the conditions for the UE to reselect E-UTRAN radio access technology are FFS.

#18 (CS domain not available)

The UE shall stop timer T3410 if still running, shall set the EPS update status to EU1 UPDATED and shall enter state EMM-REGISTERED.NORMAL-SERVICE.

The UE shall set the update status to U2 NOT UPDATED.

A UE in CS/PS mode 1 of operation shall select GERAN or UTRAN radio access technology and proceed with appropriate MM or GMM specific procedures. The UE shall not reselect E-UTRAN radio access technology for the duration the UE is on the PLMN or an equivalent PLMN.

Other EMM cause values and the case that no EMM cause IE was received are considered as abnormal cases. The combined attach procedure shall be considered as failed for EPS and non-EPS services. The behaviour of the UE in those cases is specified in subclause 5.5.1.3.6.

5.5.1.3.5 Combined attach not accepted by the network

If the attach request can neither be accepted by the network for EPS nor for non-EPS services, the MME shall send an ATTACH REJECT message to the UE including an appropriate EMM cause value. If the attach procedure fails due to a default EPS bearer setup failure or an ESM procedure failure, the MME shall combine the ATTACH REJECT message with a PDN CONNECTIVITY REJECT message. In this case the EMM cause value in the ATTACH REJECT message shall be set to #19, "ESM failure".

Upon receiving the ATTACH REJECT message, the UE shall stop timer T3410, enter MM state MM IDLE, and take the following actions depending on the EMM cause value received.

#3 (Illegal UE);

#6 (Illegal ME); or

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI.

The UE shall consider the USIM as invalid for EPS and non-EPS services until switching off or the UICC containing the USIM is removed. Additionally, the UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the MM parameters update status, TMSI, LAI and ciphering key sequence number, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the combined attach procedure is rejected with this cause value.

#7 (EPS services not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. Additionally, the UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the combined attach procedure is rejected with this cause value.

A UE which is not yet IMSI attached for non-EPS services shall select GERAN or UTRAN radio access technology and perform an IMSI attach for non-EPS services, using the MM IMSI attach procedure as described in 3GPP TS 24.008 [13]. The UE shall not reselect E-UTRAN radio access technology until switching off or the UICC containing the USIM is removed.

A UE which is already attached for non-EPS services is still attached for non-EPS services in the network. The UE shall select GERAN or UTRAN radio access technology and shall proceed with the appropriate MM specific procedure according to the MM service state. The UE shall not reselect E-UTRAN radio access technology until switching off or the UICC containing the USIM is removed.

#11 (PLMN not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, and KSI, and reset the attach attempt counter. The UE shall delete the list of equivalent PLMNs and enter the state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMN list".

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the MM parameters update status, TMSI, LAI, ciphering key sequence number and location update attempt counter, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined attach procedure is rejected with this cause value and no RR connection exists.

#12 (Tracking area not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. The UE shall reset the attach attempt counter and enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for regional provision of service".

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the MM parameters update status, TMSI, LAI, ciphering key sequence number and location update attempt counter, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined attach procedure is rejected with this cause value.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. The UE shall delete the list of equivalent PLMNs and reset the attach attempt counter. Additionally the UE enter the state EMM-DEREGISTERED.LIMITED-SERVICE or optionally EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming".

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the MM parameters update status, TMSI, LAI, ciphering key sequence number and location update attempt counter, and the GMM

parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined attach procedure is rejected with this cause value.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. Additionally the UE shall reset the attach attempt counter and enter the state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list.

A UE operating in CS/PS mode 1 which is not yet IMSI attached for non-EPS services may select GERAN or UTRAN radio access technology and perform an IMSI attach for non-EPS services, using the MM IMSI attach procedure as described in 3GPP TS 24.008 [13]. In this case the UE shall not reselect E-UTRAN radio access technology for the duration the UE is on the PLMN or an equivalent PLMN.

A UE operating in CS/PS mode 1 which is already IMSI attached for non-EPS services in the network is still IMSI attached for non-EPS services in the network. The UE may select GERAN or UTRAN radio access technology and proceed with the appropriate MM specific procedure according to the MM service state. In this case the UE shall not reselect E-UTRAN radio access technology for the duration the UE is on the PLMN or an equivalent PLMN.

A UE in CS/PS mode 1 of operation may perform a PLMN selection according to 3GPP TS 23.122 [6].

A UE operating in CS/PS mode 2 which is already IMSI attached for non-EPS services in the network is still IMSI attached for non-EPS services in the network.

A UE operating in CS/PS mode 2 of operation shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined attach procedure is rejected with this cause value.

#15 (No suitable cells in tracking area);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI and KSI. Additionally the UE shall reset the attach attempt counter and enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming".

The UE shall search for a suitable cell in another tracking area or in another location area in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the MM parameters update status, TMSI, LAI, ciphering key sequence number and location update attempt counter, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined attach procedure is rejected with this cause value.

#25 (Not authorized for this CSG);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). Additionally, the UE shall reset the attach attempt counter and shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall remove the CSG ID of the cell where the UE has sent the ATTACH REQUEST message from the Allowed CSG list.

The UE shall search for a suitable cell in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the MM parameters update status and location update attempt counter, and GMM parameters GMM state, GPRS update status and GPRS

attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined attach procedure is rejected with this cause value.

Other values are considered as abnormal cases. The behaviour of the UE in those cases is specified in subclause 5.5.1.3.6.

5.5.1.3.6 Abnormal cases in the UE

The UE shall proceed as follows:

- if the combined attach was successful for EPS services only and the ATTACH ACCEPT message contained a cause value not treated in subclause 5.5.1.3.4.3 or the EMM cause IE is not included in the message, the UE shall follow the procedure specified in subclause 5.5.1.2.6 item d, with the following modification;
- otherwise, the abnormal cases specified in subclause 5.5.1.2.6 apply with the following modification.

If the EPS attach attempt counter is incremented according to subclause 5.5.1.2.6 the next actions depend on the value of the attach attempt counter:

- if the update status is U1 UPDATED and the attach attempt counter is less than 5, then the UE shall keep the update status to U1 UPDATED, the new MM state is MM IDLE substate NORMAL SERVICE;
- if the attach attempt counter is less than 5 and, additionally, the update status is different from U1 UPDATED, then the UE shall delete any LAI, TMSI, ciphering key sequence number and list of equivalent PLMNs and set the update status to U2 NOT UPDATED. The MM state remains MM LOCATION UPDATING PENDING; or
- if the attach attempt counter is equal to 5, then the UE shall delete any LAI, TMSI, ciphering key sequence number and list of equivalent PLMNs and set the update status to U2 NOT UPDATED. A UE operating in CS/PS mode 1 of operation shall select GERAN or UTRAN radio access technology and proceed with appropriate MM or GMM specific procedures.

Editor's note: the conditions for the UE to reselect E-UTRAN radio access technology are FFS.

5.5.1.3.7 Abnormal cases on the network side

The abnormal cases specified in subclause 5.5.1.2.7 apply with the exceptions for cases a and c in which in addition to the GUTI the old TMSI shall be considered occupied until the new TMSI is used by the UE in a subsequent message.

5.5.2 Detach procedure

5.5.2.1 General

The detach procedure is used:

- by the UE to detach for EPS services only;
- by the UE to disconnect from the last PDN it is connected to;
- by the UE in CS/PS mode 1 or CS/PS mode 2 of operation to detach for both EPS services and non-EPS services or for non-EPS services only via a combined detach procedure; 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 or CS Fallback 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.

5.5.2.2 UE initiated detach procedure

5.5.2.2.1 UE initiated detach procedure initiation

The detach procedure is initiated by the UE by sending a DETACH REQUEST message (see example in figure 5.5.2.2.1.1). The Detach type IE included in the message indicates whether detach is due to a "switch off" or not. The Detach type IE also indicates whether the detach is for EPS services only, for non-EPS services only, or for both.

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. If the detach type indicates that the detach is for non-EPS services only the UE shall enter the state EMM-REGISTERED.IMSI-DETACH-INITIATED, otherwise the UE shall enter the state EMM-DEREGISTERED-INITIATED. If the detach type indicates that the detach is for non-EPS services or both EPS and non-EPS services, the UE shall enter the state MM IMSI DETACH PENDING.

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. After transmission of the message, the UE shall delete the KSI, if any.

Editor's note: Details for the case the UE detaches from EPS services only when it has already registered to both EPS and non-EPS services are FFS.

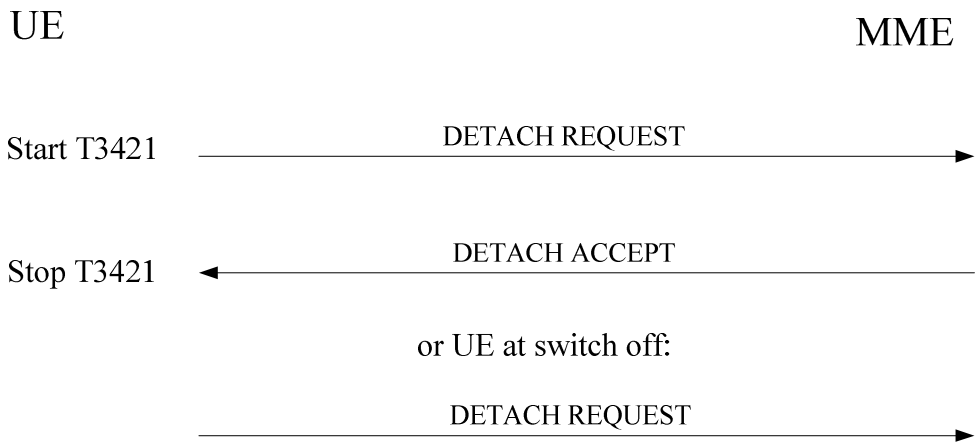

Figure 5.5.2.2.1.1: UE initiated detach procedure

5.5.2.2.2 UE initiated detach procedure completion for EPS services only

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. On reception of a DETACH REQUEST message indicating "switch off", the MME shall delete the KSI, if any.

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.

5.5.2.2.3 UE initiated combined detach procedure completion

When the DETACH REQUEST message is received by the network, a DETACH ACCEPT message shall be sent to the UE, if the Detach type IE value indicates that the detach request has not been sent due to switching off. Depending on the value of the Detach type IE the following applies:

- combined EPS/IMSI detach:

  The UE is marked as inactive in the network for EPS and for non-EPS services. The states EMM-DEREGISTERED and MM-NULL are entered in both the UE and the network.

- IMSI detach:

  The UE is marked as inactive in the network for non-EPS services. The states MM-NULL and EMM-REGISTERED are entered in both the UE and the network.

5.5.2.2.4 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Access barred because of access class barring or NAS signalling connection establishment rejected by the network

   If access is barred for "signalling" (see 3GPP TS 36.331 [22]), the detach procedure shall not be started. The UE stays in the current serving cell and applies the normal cell reselection process. The detach procedure is started as soon as possible and if still necessary, i.e. when access for "signalling" is granted on the current cell or when the UE moves to a cell where access for "signalling" is granted. The UE may perform a local detach either immediately or after an implementation dependent time.

b) Lower layer failure or release of the NAS signalling connection before reception of DETACH ACCEPT message

   The detach procedure shall be aborted, and the UE shall enter state:

   - EMM-REGISTERED.NORMAL-SERVICE and MM-NULL if "IMSI detach" was requested;
   - EMM-DEREGISTERED if "EPS detach" was requested;
   - EMM-DEREGISTERED and MM-NULL if "combined EPS/IMSI detach" was requested.

c) T3421 timeout

   On the first four expiries of the timer, the UE shall retransmit the DETACH REQUEST message and shall reset and restart timer T3421. On the fifth expiry of timer T3421, the detach procedure shall be aborted and the UE shall change to state:

   - EMM-REGISTERED.NORMAL-SERVICE and MM-NULL if "IMSI detach" was requested;
   - EMM-DEREGISTERED if "EPS detach" was requested;
   - EMM-DEREGISTERED and MM-NULL if "combined EPS/IMSI detach" was requested.

d) Detach procedure collision

   If the UE receives a DETACH REQUEST message before the UE initiated detach procedure has been completed, it shall send a DETACH ACCEPT message to the network.

e) Detach and EMM common procedure collision

   Detach containing cause "switch off":

   - If the UE receives a message used in an EMM common procedure before the detach procedure has been completed, this message shall be ignored and the detach procedure shall continue

   Detach containing other causes than "switch off":

   - If the UE receives a GUTI REALLOCATION COMMAND, an EMM STATUS or an EMM INFORMATION message before the detach procedure is completed, this message shall be ignored and the detach procedure shall continue.
   - If the UE receives an AUTHENTICATION REQUEST, SECURITY MODE COMMAND or IDENTITY REQUEST message before the detach procedure has been completed, the UE shall respond to it as described in subclause 5.4.2, 5.4.3 and 5.4.4 respectively and the detach procedure shall continue.

f) Change of cell into a new tracking area

If a cell change into a new tracking area that is not in the stored TAI list occurs before the UE initiated detach procedure is completed, the detach procedure shall be aborted and re-initiated after successfully performing a tracking area updating procedure. If the detach procedure was initiated due to removal of the USIM, the UE shall abort the detach procedure and enter the state EMM-DEREGISTERED.

g) Transmission failure of DETACH REQUEST message indication with TAI change from lower layers

If the current TAI is not in the TAI list, the detach procedure shall be aborted and re-initiated after successfully performing a tracking area updating procedure.

If the current TAI is still part of the TAI list, the UE shall restart the detach procedure.

h) Transmission failure of DETACH REQUEST message indication without TAI change from lower layers

The UE shall restart the detach procedure.

i) Access barred because the CSG ID is not in the UE's Allowed CSG list

If access is barred because the CSG ID is not in the UE's Allowed CSG list, the detach procedure shall not be started. The UE stays in the current serving cell and applies the normal cell reselection process. The detach procedure is started as soon as possible and if still necessary, e.g. when the UE moves to a cell where access is granted. The UE may perform a local detach either immediately or after an implementation dependent time.

5.5.2.2.5 Abnormal cases on the network side

The following abnormal cases can be identified:

a) CSG ID of the CSG cell is not in the Allowed CSG list of the UE which sends the detach request

If the UE initiates a detach procedure in a CSG cell the CSG ID of which is not in the UE's Allowed CSG list, the network shall initiate the detach procedure. The MME shall send a DETACH REQUEST message including the EMM cause value #25,"not authorized for this CSG", to indicate to the UE to remove the CSG ID of the cell where the UE has sent the DETACH REQUEST message from the Allowed CSG list.

5.5.2.3 Network initiated detach procedure

5.5.2.3.1 Network initiated detach procedure initiation

The network initiates the detach procedure by sending a DETACH REQUEST message to the UE (see example in figure 5.5.2.3.1). The network may include an EMM cause IE to specify the reason for the detach request. The network shall start timer T3422. If the detach type IE indicates "re-attach not required" or "re-attach required", the network shall deactivate the EPS bearer context(s) for the UE locally and enter state EMM-DEREGISTERED-INITIATED.

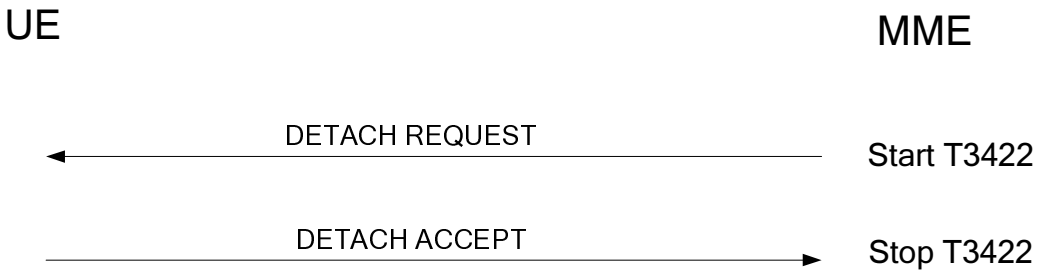

Figure 5.5.2.3.1: Network initiated detach procedure

5.5.2.3.2 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 default EPS 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, using the existing NAS signalling connection.

A UE which receives a DETACH REQUEST message with detach type indicating "re-attach required" or "re-attach not required" and no EMM cause IE, is detached only for EPS services.

When receiving the DETACH REQUEST message and the Detach type IE indicates "IMSI detach", the UE shall not deactivate the EPS bearer context(s) including the default EPS bearer context. The UE shall set the MM update status to U2 NOT UPDATED. A UE may send a DETACH ACCEPT message to the network, and shall re-attach to non-EPS services by performing the combined tracking area updating procedure according to subclause 5.5.3.3, sending a TRACKING AREA UPDATE REQUEST message with EPS update type IE indicating "combined TA/LA updating with IMSI attach".

If the Detach type IE indicates "re-attach required" or "re-attach not required" and the UE is attached for EPS and non-EPS services, then if in the UE 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 value is not #2, "IMSI unknown in HSS", the UE shall deactivate the EPS bearer context(s) including the default EPS 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.

If the detach type IE indicates "IMSI detach" or "re-attach required", then the UE shall ignore the EMM cause IE if received.

If the detach type IE indicates "re-attach not required", the UE shall take the following actions depending on the received EMM cause value:

#2 (IMSI unknown in HSS);

The UE shall handle the MM parameters update status, TMSI, LAI and ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required". The USIM shall be considered as invalid for non-EPS services until switching off or the UICC containing the USIM is removed.

The UE is still attached for EPS services in the network.

#3 (Illegal UE); or

#6 (Illegal ME);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the MM parameters update status, TMSI, LAI and ciphering key sequence number and the GMM parameters GMM state, RAI, P-TMSI, P-TMSI signature, GPRS ciphering key sequence number and GPRS update status as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required". The USIM shall also be considered as invalid for non-EPS services until switching off or the UICC containing the USIM is removed.

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 (EPS services not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, RAI, P-TMSI, P-TMSI signature, GPRS ciphering key sequence number and GPRS update status as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

A UE operating in CS/PS mode 1 or CS/PS mode 2 of operation shall set the timer T3212 to its initial value and restart it, if not already running. The UE operating in CS/PS mode 1 or CS/PS mode 2 of operation is still attached for non-EPS services in the network. The UE operating in CS/PS mode 1 or CS/PS mode 2 of operation shall select GERAN or UTRAN access technology and shall proceed with the appropriate MM specific procedure according to the MM service state. The UE shall not reselect E-UTRAN radio access technology until switching off or the UICC containing the USIM is removed.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the MM parameters update status, TMSI, LAI and ciphering key sequence number and the GMM parameters GMM state, RAI, P-TMSI, P-TMSI signature, GPRS ciphering key sequence number and GPRS update status as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required". The USIM shall also be considered as invalid for non-EPS services until switching off or the UICC containing the USIM is removed.

#11 (PLMN not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall delete the list of equivalent PLMNs, shall reset the attach attempt counter and enter the state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMN list".

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the MM parameters update status, TMSI, LAI and ciphering key sequence number and the GMM parameters GMM state, RAI, P-TMSI, P-TMSI signature, GPRS ciphering key sequence number, GPRS update status and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

#12 (Tracking area not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall reset the attach attempt counter and shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for regional provision of service".

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, RAI, P-TMSI, P-TMSI signature, GPRS ciphering key sequence number, GPRS update status and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required". If the UE is attached for non-EPS services, the UE shall in addition handle the MM parameters update status, TMSI, LAI, ciphering key sequence number and location update attempt counter as specified in 3GPP TS 24.008 [13] 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 tracking area);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall delete the list of equivalent PLMNs, reset the attach attempt counter and shall change to state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming".

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6]

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, RAI, P-TMSI, P-TMSI signature, GPRS ciphering key sequence number, GPRS update status and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required". If the UE is attached for non-EPS services, the UE shall in addition handle the MM parameters update status, TMSI, LAI, ciphering key sequence number and location update attempt counter and as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). Furthermore the UE shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall reset the attach attempt counter and shall enter the state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list.

A UE operating in CS/PS mode 1 or CS/PS mode 2 of operation is still IMSI attached for non-EPS services. If the timer T3212 is not already running in the UE, the UE shall set the timer T3212 to its initial value and restart it.

A UE operating in CS/PS mode 1 of operation may select GERAN or UTRAN radio access technology and proceed with the appropriate MM specific procedure according to the MM service state. In this case the UE shall not reselect E-UTRAN radio access technology for the duration the UE is on the PLMN or an equivalent PLMN.

A UE in CS/PS mode 1 of operation may perform a PLMN selection according to 3GPP TS 23.122 [6].

A UE in PS mode of operation or in CS/PS mode 2 of operation shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, RAI, P-TMSI, P-TMSI signature, GPRS ciphering key sequence number and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] 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 tracking area);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall reset the attach attempt counter and shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming".

The UE shall search for a suitable cell in another tracking area or in another location area in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, RAI, P-TMSI, P-TMSI signature, GPRS ciphering key sequence number, GPRS update status and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required". If the UE is attached for non-EPS services, the UE shall in addition handle the MM parameters update status, TMSI, LAI, ciphering key sequence number and location update attempt counter as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

#25 (Not authorized for this CSG);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). The UE shall reset the attach attempt counter and shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall remove the CSG ID of the cell where the UE has received the DETACH REQUEST message from the Allowed CSG list.

The UE shall search for a suitable cell in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status and GPRS attach attempt counter as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required". If the UE is attached for non-EPS services, the UE shall in addition handle the MM parameters update status and location update attempt counter as specified in 3GPP TS 24.008 [13] for the case when a DETACH REQUEST is received with this cause value and with detach type set to "re-attach not required".

Other cause values or if no EMM cause IE is included is considered as abnormal cases. The behaviour of the UE in those cases is described in subclause 5.5.2.3.4.

5.5.2.3.3 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.

5.5.2.3.4 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of DETACH ACCEPT message indication from lower layers

The detach procedure shall be progressed and the UE shall send the DETACH ACCEPT message.

b) DETACH REQUEST, other cause values than those treated in subclause 5.5.2.3.2 or no EMM cause IE is included, and the Detach type IE indicates "re-attach not required"

The UE shall delete any GUTI, TAI list, last visited registered TAI, list of equivalent PLMNs, KSI, shall set the update status to EU2 NOT UPDATED and shall start timer T3402. The UE may enter the state EMM-DEREGISTERED.PLMN-SEARCH in order to perform a PLMN selection according to 3GPP TS 23.122 [6]; otherwise the UE shall enter the state EMM-DEREGISTERED.ATTEMPTING-TO-ATTACH.

If A/Gb mode or Iu mode is supported by the UE, the UE shall delete the GMM parameters GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and shall enter the state GMM-DEREGISTERED.

5.5.2.3.5 Abnormal cases on the network side

The following abnormal cases can be identified:

a) T3422 time-out

On the first expiry of the timer, the network shall retransmit the DETACH REQUEST message and shall start timer T3422. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3422, the detach procedure shall be aborted and the network changes to state EMM-DEREGISTERED.

b) Lower layer failure

The detach procedure is aborted and the network changes to state EMM-DEREGISTERED.

c) Detach procedure collision

If the network receives a DETACH REQUEST message with "switch off" indication, before the network initiated GPRS detach procedure has been completed, both procedures shall be considered completed.

If the network receives a DETACH REQUEST message without "switch off" indication, before the network initiated detach procedure has been completed, the network shall send a DETACH ACCEPT message to the UE.

If the network receives a DETACH REQUEST message without "switch off" indication from a CSG cell the CSG ID of which is not in the UE's Allowed CSG list, the network shall send a DETACH REQUEST message including the EMM cause value #25,"not authorized for this CSG", to the UE. Upon reception the DETACH REQUEST message, the behaviour of the UE is specified in subclause 5.5.2.3.2.

d) Detach and attach procedure collision

If the network receives an ATTACH REQUEST message before the network initiated detach procedure with detach type "re-attach not required" has been completed, the network shall ignore the ATTACH REQUEST message. If the Detach type IE, sent in the DETACH REQUEST message, indicates "re-attach required" the detach procedure is aborted and the attach procedure shall be progressed after the EPS bearer context(s) have been deleted. If the Detach type IE, sent in DETACH REQUEST message, indicates "IMSI detach" the detach procedure is aborted and the attach procedure shall be progressed.

e) Detach and tracking area updating procedure collision

If the Detach type IE, sent in DETACH REQUEST message, indicates "re-attach required" or "re-attach not required" and the network receives a TRACKING AREA UPDATE REQUEST message before the network initiated detach procedure has been completed, the detach procedure shall be progressed, i.e. the TRACKING AREA UPDATE REQUEST message shall be ignored.

If the Detach type IE, sent in DETACH REQUEST message, indicates "IMSI detach" and the network receives a TRACKING AREA UPDATE REQUEST message before the network initiated detach procedure has been completed, the network shall abort the detach procedure, shall stop T3422 and shall progress the tracking area updating procedure.

f) Detach and service request procedure collision

If the network receives a SERVICE REQUEST message before the network initiated detach procedure has been completed, the network shall ignore the SERVICE REQUEST message.

5.5.3 Tracking area updating procedure (S1 mode only)

5.5.3.1 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 inter-system change and A/Gb mode to S1 mode inter-system change;
- S101 mode to S1 mode inter-system change;
- NAS signalling connection recovery;
- MME load balancing;
- to update the network of a change of the UE core network capability information or the UE specific DRX parameter or both;
- to indicate to the network that the UE radio capability information has changed.

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.

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.

In a shared network, the UE shall choose one of the PLMN identities as specified in 3GPP TS 23.122 [6]. The UE shall construct the TAI of the cell from this chosen PLMN identity and the TAC received on the broadcast system information. The chosen PLMN identity shall be indicated to the E-UTRAN (see 3GPP TS 36.331 [22]). Whenever a TRACKING AREA UPDATING REJECT message with the cause "PLMN not allowed" is received by the UE, the chosen PLMN identity shall be stored in the "forbidden PLMN list". Whenever a TRACKING AREA UPDATING REJECT message is received by the UE with the cause "Roaming not allowed in this tracking area", "Tracking area not allowed", or "No suitable cells in tracking Area", the constructed TAI shall be stored in the suitable list.

A tracking area updating attempt counter is used to limit the number of subsequently rejected tracking area update attempts. The tracking area updating attempt counter shall be incremented as specified in subclause 5.5.3.2.6. Depending on the value of the tracking area updating attempt counter, specific actions shall be performed. The tracking area updating attempt counter shall be reset when:

- a normal or combined attach procedure is successfully completed;
- a normal or periodic tracking area updating or a combined tracking area updating procedure is successfully completed; or
- a normal or periodic tracking area updating or a combined tracking area updating procedure is rejected with cause value #11, #12, #13, #14, #15 or #25.

Additionally the tracking area updating attempt counter shall be reset when the UE is in substate EMM-REGISTERED.ATTEMPTING-TO-UPDATE and:

- a new tracking area is entered; or
- timer T3402 expires.

5.5.3.2 Normal and periodic tracking area updating procedure

5.5.3.2.1 General

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 5.3.2.

5.5.3.2.2 Normal and periodic 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,

a) 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;

b) when the periodic tracking area updating timer T3412 expires;

c) when the UE with ISR active moves to E-UTRAN and the UE's TIN indicates "P-TMSI";

d) when the UE performs an inter-system change from S101 mode to S1 mode and has no user data pending;

e) when the UE receives an indication from the lower layers that the RRC connection was released with cause "load balancing TAU required";

f) when the UE deactivated EPS bearer context(s) locally while out of coverage, and then returns to E-UTRAN coverage;

g) when the UE changes the UE core network capability information or the UE specific DRX parameter or both;

h) when the UE receives an indication of "RRC Connection failure" from the lower layers and has no user uplink data pending.

Editor's note: It is FFS how the "ON-OFF" indication for NAS signalling connection recovery is provided by the network.

When the UE has user data pending and performs an inter-system change from S101 mode to S1 mode to a tracking area included in the TAI list stored in the UE, the UE shall perform a service request procedure instead of a tracking area updating procedure.

When initiating a tracking area updating procedure as a result of an Iu mode to S1 mode or A/Gb mode to S1 mode inter-system change, the UE shall handle the GUTI as follows:

- if the TIN indicates "P-TMSI" and the UE holds a valid P-TMSI and RAI, the UE shall map the P-TMSI and RAI into the old GUTI IE. Additionally, if the UE holds a valid GUTI, the UE shall indicate the GUTI in the Additional GUTI IE.

NOTE: Mapping the P-TMSI and RAI to the GUTI is specified in Annex H of 3GPP TS 23.401 [10].

- if the TIN indicates "GUTI" or "RAT-related TMSI" and the UE holds a valid GUTI, the UE shall indicate the GUTI in the Old GUTI IE.

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 (see example in figure 5.5.3.2.2). If timer T3402 is currently running, the UE shall stop timer T3402. If timer T3411 is currently running, the UE shall stop timer T3411. If timer T3442 is currently running, the UE shall stop timer T3442.

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 the UE's TIN indicates "P-TMSI" the UE shall map the valid P-TMSI and RAI into the old GUTI. If a UE in EMM-IDLE mode has uplink user data pending when it initiates the tracking area updating procedure, or uplink signalling not related to the tracking area updating procedure, it may also set an "active" flag in the TRACKING AREA UPDATE REQUEST message to indicate the request to establish the user plane to the network and to keep the NAS signalling connection after the completion of the tracking area updating procedure.

If the UE has an EPS security context, the UE shall include the KSI_{ASME} in the TRACKING AREA UPDATE REQUEST message. Otherwise, the UE shall set the KSI_{ASME} to the value "no key is available". The UE shall set the KSI_{SGSN} to the value "no key is available".

When the tracking area updating procedure is initiated to perform an inter-system change from A/Gb mode or Iu mode to S1 mode, the UE shall include the KSI_{ASME} in the TRACKING AREA UPDATE REQUEST message if the UE has a cached EPS security context. Otherwise, the UE shall set the KSI_{ASME} to the value "no key is available".

When the tracking area updating procedure is initiated in EMM-IDLE mode to perform an inter-system change from A/Gb mode or Iu mode to S1 mode, the UE shall include the KSI_{SGSN} in the TRACKING AREA UPDATE REQUEST message. If the UE does not have a cached EPS security context, the UE shall include the $Nonce_{UE}$ IE in the TRACKING AREA UPDATE REQUEST message. The TRACKING AREA UPDATE REQUEST message shall be integrity protected with the cached EPS security context if the UE has one. If the UE does not have a cached EPS security context, the TRACKING AREA UPDATE REQUEST message shall not be integrity protected.

When the tracking area updating procedure is initiated in EMM-CONNECTED mode to perform an inter-system change from A/Gb mode or Iu mode to S1 mode, the UE shall take one of the following actions:

- If the MME has indicated the KSI_{ASME} in the handover command through the lower layer and the UE has a cached EPS security context identified by the KSI_{ASME}, the UE shall provide the KSI_{ASME} to lower layers and send the TRACKING AREA UPDATE REQUEST message including the KSI_{SGSN} IE and integrity protect the message with the cached EPS security context; or

- if the UE does not have any cached EPS security, the UE shall provide the KSI_{SGSN} to lower layers context and send the TRACKING AREA UPDATE REQUEST message including the KSI_{SGSN} IE and shall not integrity protect the message.

Editor's note: if the SA3 revisits the issue of the key freshness during inter-system change, CT1 would have to align accordingly.

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.

If the UE initiates the first tracking area updating procedure following an attach in A/Gb mode or Iu mode, the UE shall include a UE radio capability information update needed IE in the TRACKING AREA UPDATE REQUEST message.

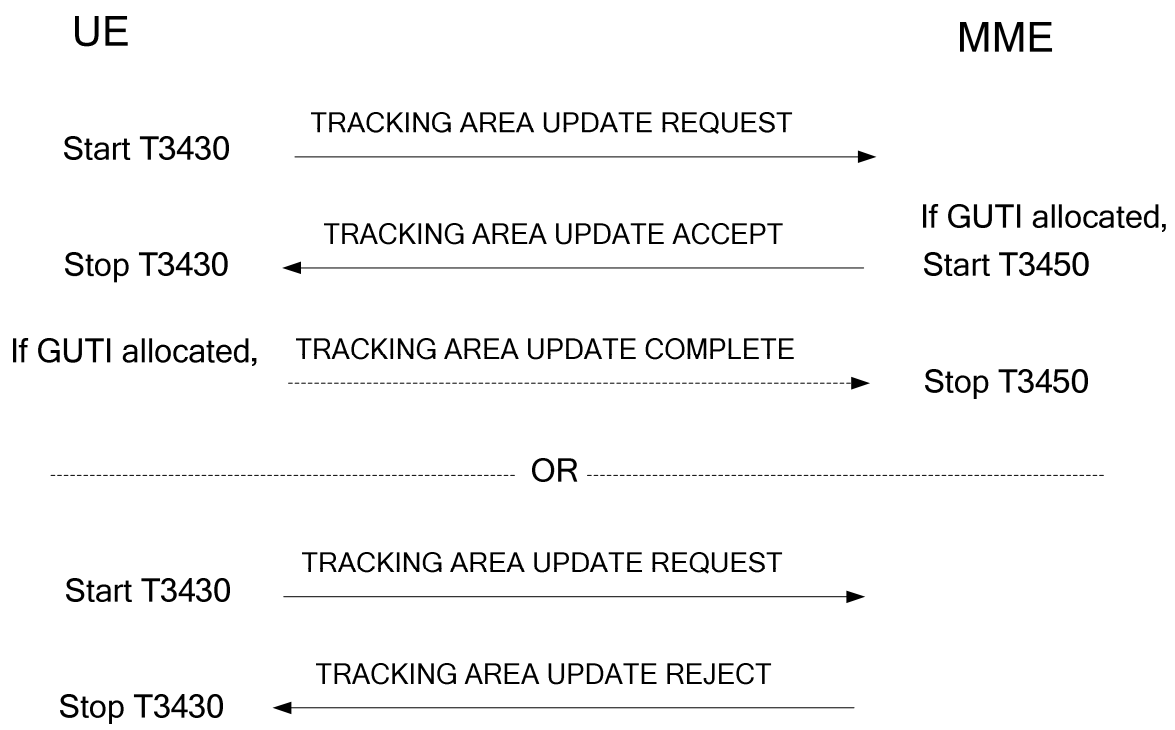

Figure 5.5.3.2.2.1: Tracking area updating procedure

5.5.3.2.3 EMM common procedure initiation

The network may initiate EMM common procedures, e.g. the EMM authentication and security mode control procedures.

5.5.3.2.4 Normal and periodic 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 5.4.1. 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 "list of emergency numbers" are included in the TRACKING AREA UPDATE ACCEPT message.

If the UE has included the UE network capability IE or the MS network capability IE or both in the TRACKING AREA UPDATE REQUEST message, the MME shall store all octets received from the UE, up to the maximum length defined for the respective information element.

NOTE: This information is forwarded to the new MME during inter-MME handover or to the new SGSN during inter-system handover to A/Gb mode or Iu mode.

If a UE radio capability information update needed IE is included in the TRACKING AREA UPDATE REQUEST message, the MME shall delete the stored UE radio capability information, if any.

If an EPS bearer context status IE is included in the 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.

For a shared network, the TAIs included in the TAI list can contain different PLMN identities.

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 tracking 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.

The MME may also include of list of equivalent PLMNs in the TRACKING AREA UPDATE ACCEPT message. Each entry in the list contains a PLMN code (MCC+MNC). The UE shall store the list as provided by the network, after having removed from the list any PLMN code that is already in the list of forbidden PLMNs. In addition, the UE shall add to the stored list the PLMN code of the registered PLMN that sent the list. The UE shall replace the stored list on each receipt of the TRACKING AREA UPDATE ACCEPT message. If the TRACKING AREA UPDATE ACCEPT message does not contain a list, then the UE shall delete the stored list.

The network may also indicate in the EPS update result IE in the TRACKING AREA UPDATE ACCEPT message that ISR is active. If the TRACKING AREA UPDATE ACCEPT message contains:

i) no indication that ISR is activated, the UE shall regard any P-TMSI and RAI previously assigned to the UE as invalid and set the TIN to "GUTI";

ii) an indication that ISR is activated, the UE shall regard a previously assigned P-TMSI and RAI as valid and registered with the network. If the TIN currently indicates "P-TMSI", the UE shall set the TIN to "RAT-related TMSI".

For manual update of the Allowed CSG list, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSD ID to the Allowed CSG list.

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.

5.5.3.2.5 Normal and periodic 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 EMM cause value.

Upon receiving the TRACKING AREA UPDATE REJECT message, the UE shall stop timer T3430, stop any transmission of user data, and take the following actions depending on the EMM cause value received.

#3 (Illegal UE); or

#6 (Illegal ME);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number and the MM parameters update status, TMSI, LAI and ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the normal routing area updating procedure is rejected with this cause value. The USIM shall

be considered as invalid also for non-EPS services until switching off or the UICC containing the USIM is removed.

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 (EPS services not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the normal routing area updating procedure is rejected with this cause value.

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

The UE shall set the EPS update status to EU2 NOT UPDATED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

Subsequently, the UE shall automatically initiate the attach procedure.

#10 (Implicitly detached);

The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.NORMAL-SERVICE. The UE shall then perform a new attach procedure.

#11 (PLMN not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall reset the tracking area updating attempt counter, delete the list of equivalent PLMNs and enter the state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMN list".

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and routing area updating attempt counter and the MM parameters update status, TMSI, LAI, ciphering key sequence number and the location update attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal routing area updating procedure is rejected with this cause value and no RR connection exists.

#12 (Tracking area not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall reset the tracking area updating attempt counter and shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for regional provision of service".

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal routing area updating procedure is rejected with this cause value.

Editor's note: If RAN2 is going to abandon the additional cell re-selection hysteresis at tracking area boundaries, the behaviour described above may need to be changed: the UE could remain in EMM-REGISTERED state, GUTI and all EPS bearer contexts could be kept.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete the list of equivalent PLMNs. The UE shall reset the tracking area updating attempt counter and shall change to state EMM-REGISTERED.PLMN-SEARCH.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming" and shall remove the current TAI from the stored TAI list if present.

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal routing area updating procedure is rejected with this cause value.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). Furthermore the UE shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall reset the tracking area updating attempt counter and shall enter the state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list.

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal routing area updating procedure is rejected with this cause value.

#15 (No suitable cells in tracking area);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). The UE shall reset the tracking area updating attempt counter and shall enter the state EMM-REGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming" and shall remove the current TAI from the stored TAI list if present.

The UE shall search for a suitable cell in another tracking area or in another location area in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal routing area updating procedure is rejected with this cause value.

#25 (Not authorized for this CSG);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). The UE shall reset the tracking area updating attempt counter and shall enter the state EMM-REGISTERED.LIMITED-SERVICE.

The UE shall remove the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message from the Allowed CSG list.

The UE shall search for a suitable cell in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the normal routing area updating procedure is rejected with this cause value.

#40 (No EPS bearer context activated);

The UE shall delete the list of equivalent PLMNs and deactivate all the EPS bearer contexts locally, if any, and shall enter the state EMM-DEREGISTERED.NORMAL-SERVICE. The UE shall then perform a new attach procedure.

Other values are considered as abnormal cases. The specification of the UE behaviour in those cases is described in subclause 5.5.3.2.6.

5.5.3.2.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Access barred because of access class barring or NAS signalling connection establishment rejected by the network

   If access is barred for "signalling" (see 3GPP TS 36.331 [22]), the tracking area updating procedure shall not be started. The UE stays in the current serving cell and applies the normal cell reselection process. The tracking area updating procedure is started as soon as possible and if still necessary, e.g. when access for "signalling" is granted on the current cell or when the UE moves to a cell where access for "signalling" is granted.

b) Lower layer failure or release of the NAS signalling connection before the TRACKING AREA UPDATE ACCEPT or TRACKING AREA UPDATE REJECT message is received

   The tracking area updating procedure shall be aborted, and the UE shall proceed as described below.

c) T3430 timeout

   The UE shall abort the procedure and proceed as described below. The NAS signalling connection shall be released locally.

d) TRACKING AREA UPDATE REJECT, other causes than those treated in subclause 5.5.3.2.5

   Upon reception of the cause values #95, #96, #97, #99 and #111 the UE should set the tracking area updating attempt counter to 5. The UE shall proceed as described below.

e) Change of cell into a new tracking area

   If a cell change into a new tracking area occurs before the tracking area updating procedure is completed, the tracking area updating procedure shall be aborted and re-initiated immediately. The UE shall set the update status to EU2 NOT UPDATED.

f) Tracking area updating and detach procedure collision

   If the UE receives a DETACH REQUEST message before the tracking area updating procedure has been completed, the tracking area updating procedure shall be aborted and the detach procedure shall be progressed.

g) Tracking area updating and GUTI reallocation procedure collision

   If the UE receives a GUTI REALLOCATION COMMAND message before the tracking area updating procedure has been completed, this message shall be ignored and the tracking area updating procedure shall be progressed.

h) Transmission failure of TRACKING AREA UPDATE REQUEST message indication from lower layers

   The tracking area updating procedure shall be aborted and re-initiated immediately. The UE shall set the update status to EU2 NOT UPDATED.

i) Transmission failure of TRACKING AREA UPDATE COMPLETE message indication with TAI change from lower layers

   If the current TAI is not in the TAI list, the tracking area updating procedure shall be aborted and re-initiated immediately. The UE shall set the update status to EU2 NOT UPDATED.

   If the current TAI is still part of the TAI list, it is up to the UE implementation how to re-run the ongoing procedure.

j) Transmission failure of TRACKING AREA UPDATE COMPLETE message indication without TAI change from lower layers

It is up to the UE implementation how to re-run the ongoing procedure.

k) Access barred because the CSG ID is not in the UE's Allowed CSG list

If access is barred because the CSG ID is not in the UE's Allowed CSG list, the tracking area updating procedure shall not be started. The UE stays in the current serving cell and applies the normal cell reselection process. The tracking area updating procedure is started as soon as possible and if still necessary, e.g. when the UE moves to a cell where access is granted.

For the cases b, c, d, e, and f, the UE shall stop any ongoing transmission of user data.

For the cases b, c and d the UE shall proceed as follows:

Timer T3430 shall be stopped if still running. The tracking area updating attempt counter shall be incremented, unless it was already set to 5 due to case d.

If the tracking area updating attempt counter is less than 5, and the TAI of the current serving cell is included in the TAI list and the update status is equal to EU1 UPDATED:

- the UE shall keep the update status to EU1 UPDATED and enter state EMM-REGISTERED.NORMAL-SERVICE. The UE shall start timer T3411. When timer T3411 expires the tracking area updating procedure is triggered again.

If the tracking area updating attempt counter is less than 5, and the TAI of the current serving cell is not included in the TAI list or the update status is different to EU1 UPDATED:

- the UE shall start timer T3411, shall set the update status to EU2 NOT UPDATED and change to state EMM-REGISTERED.ATTEMPTING-TO-UPDATE. When timer T3411 expires the tracking area updating procedure is triggered again.

  If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GPRS update status as specified in 3GPP TS 24.008 [13] for the abnormal case when a normal or periodic routing area updating procedure fails and the routing area updating attempt counter is less than 5.

If the tracking area updating attempt counter is equal to 5:

- the UE shall start timer T3402, shall set the update status to EU2 NOT UPDATED, shall delete the list of equivalent PLMNs and shall change to state EMM-REGISTERED.ATTEMPTING-TO-UPDATE or optionally to EMM-REGISTERED.PLMN-SEARCH in order to perform a PLMN selection according to 3GPP TS 23.122 [6].

  If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GPRS update status as specified in 3GPP TS 24.008 [13] for the abnormal case when a normal or periodic routing area updating procedure fails and the routing area updating attempt counter is equal to 5.

5.5.3.2.7 Abnormal cases on the network side

The following abnormal cases can be identified:

a) If a lower layer failure occurs before the message TRACKING AREA UPDATE COMPLETE has been received from the UE and a GUTI has been assigned, the network shall abort the procedure and shall consider both, the old and new GUTI as valid until the old GUTI can be considered as invalid by the network (see subclause 5.4.1.4). During this period the network may use the identification procedure followed by a GUTI reallocation procedure if the old GUTI is used by the UE in a subsequent message.

The network may page with IMSI if paging with old and new S-TMSI fails. Paging with IMSI causes the UE to re-attach as described in subclause 5.6.2.2.2.

b) Protocol error

If the TRACKING AREA UPDATE REQUEST message has been received with a protocol error, the network shall return a TRACKING AREA UPDATE REJECT message with one of the following EMM cause values:

#96: invalid mandatory information element error;

#99: information element non-existent or not implemented;

#100: conditional IE error; or

#111: protocol error, unspecified.

c) T3450 time-out

On the first expiry of the timer, the network shall retransmit the TRACKING AREA UPDATE ACCEPT message and shall reset and restart timer T3450. The retransmission is performed four times, i.e. on the fifth expiry of timer T3450, the tracking area updating procedure is aborted. Both, the old and the new GUTI shall be considered as valid until the old GUTI can be considered as invalid by the network (see subclause 5.4.1.4). During this period the network acts as described for case a above.

d) TRACKING AREA UPDATE REQUEST received after the TRACKING AREA UPDATE ACCEPT message has been sent and before the TRACKING AREA UPDATE COMPLETE message is received

- If one or more of the information elements in the TRACKING AREA UPDATE REQUEST message differ from the ones received within the previous TRACKING AREA UPDATE REQUEST message, the previously initiated tracking area updating procedure shall be aborted if the TRACKING AREA UPDATE COMPLETE message has not been received and the new tracking area updating procedure shall be progressed; or

- if the information elements do not differ, then the TRACKING AREA UPDATE ACCEPT message shall be resent and the timer T3450 shall be restarted if an TRACKING AREA UPDATE COMPLETE message is expected. In that case, the retransmission counter related to T3450 is not incremented.

e) More than one TRACKING AREA UPDATE REQUEST received and no TRACKING AREA UPDATE ACCEPT or TRACKING AREA UPDATE REJECT message has been sent

- If one or more of the information elements in the TRACKING AREA UPDATE REQUEST message differs from the ones received within the previous TRACKING AREA UPDATE REQUEST message, the previously initiated tracking area updating procedure shall be aborted and the new tracking area updating procedure shall be progressed;

- if the information elements do not differ, then the network shall continue with the previous tracking area updating procedure and shall not treat any further this TRACKING AREA UPDATE REQUEST message.

5.5.3.3 Combined tracking area updating procedure

5.5.3.3.1 General

Within a combined tracking area updating procedure the messages TRACKING AREA UPDATE ACCEPT and TRACKING AREA UPDATE COMPLETE carry information for the tracking area updating and the location area updating.

The combined tracking area updating procedure follows the normal tracking area updating procedure described in subclause 5.5.3.2.

5.5.3.3.2 Combined tracking area updating procedure initiation

To initiate a combined tracking area updating procedure the UE sends the message TRACKING AREA UPDATE REQUEST to the network, starts timer T3430 and changes to state EMM-TRACKING-AREA-UPDATING-INITIATED. The value of the EPS update type IE in the message shall indicate "combined TA/LA updating" unless explicitly specified otherwise.

The UE shall include the TMSI status IE if no valid TMSI is available. Furthermore, if the UE has stored a valid location area identification, the UE shall include it in the Old location area identification IE in the TRACKING AREA UPDATE REQUEST message.

5.5.3.3.3 EMM common procedure initiation

The network may initiate EMM common procedures, e.g. the EMM authentication and security mode control procedures.

5.5.3.3.4 Combined tracking area updating procedure accepted by the network

5.5.3.3.4.1 General

Depending on the value of the EPS update result IE received in the TRACKING AREA UPDATE ACCEPT message, two different cases can be distinguished:

1) The EPS update result IE value indicates "combined TA/LA updated": Tracking and location area updating is successful;

2) The EPS update result IE value indicates "TA updated": Tracking area updating is successful, but location area updating is not successful.

A TRACKING AREA UPDATE COMPLETE message shall be returned to the network if the TRACKING AREA UPDATE ACCEPT message contains a GUTI or a mobile identity or both.

5.5.3.3.4.2 Combined tracking area updating successful

The description for normal tracking area update as specified in subclause 5.5.3.2.4 shall be followed. In addition, the following description for location area updating applies.

The TMSI reallocation may be part of the combined tracking area updating procedure. The TMSI allocated is then included in the TRACKING AREA UPDATE ACCEPT message together with the location area identification (LAI). In this case the MME shall change to state EMM-COMMON-PROCEDURE-INITIATED and shall start the timer T3450 as described in subclause 5.4.1. The LAI may be included in the TRACKING AREA UPDATE ACCEPT message without TMSI.

The UE, receiving a TRACKING AREA UPDATE ACCEPT message, stores the received location area identification, resets the location update attempt counter, sets the update status to U1 UPDATED and enters MM state MM IDLE.

How to handle the old TMSI stored in the UE depends on the mobile identity included in the TRACKING AREA UPDATE ACCEPT message.

- If the TRACKING AREA UPDATE ACCEPT message contains an IMSI, the UE is not allocated any TMSI, and shall delete any old TMSI accordingly.

- If the TRACKING AREA UPDATE ACCEPT message contains a TMSI, the UE shall use this TMSI as new temporary identity. The UE shall delete its old TMSI and shall store the new TMSI. In this case, a TRACKING AREA UPDATE COMPLETE message is returned to the network to confirm the received TMSI.

- If neither a TMSI nor an IMSI has been included by the network in the TRACKING AREA UPDATE ACCEPT message, the old TMSI, if any is available, shall be kept.

The network receiving a TRACKING AREA UPDATE COMPLETE message stops timer T3450, changes to state EMM-REGISTERED and considers the new TMSI as valid.

5.5.3.3.4.3 Combined tracking area updating successful for EPS services only

The description for tracking area for EPS services as specified in subclause 5.5.3.2.4 shall be followed. In addition, the following description for location updating for non-EPS services applies.

The UE receiving the TRACKING AREA UPDATE ACCEPT message takes one of the following actions depending on the EMM cause value:

#2 (IMSI unknown in HSS)

The UE shall stop T3430 if still running. The UE shall set the update status to U3 ROAMING NOT ALLOWED and shall delete any TMSI, LAI and ciphering key sequence number. The UE shall enter state

EMM-REGISTERED.NORMAL-SERVICE. The new MM state is MM IDLE. The USIM shall be considered as invalid for non-EPS services until switching off or the UICC containing the USIM is removed.

#16 (MSC temporarily not reachable);

#17 (Network failure); or

#22 (Congestion)

The UE shall stop timer T3430 if still running. The tracking area updating attempt counter shall be incremented, unless it was already set to 5.

If the tracking area updating attempt counter is less than 5:

- the UE shall start timer T3411, shall set the EMM update status to EU1 UPDATED and shall enter state EMM-REGISTERED.ATTEMPTING-TO-UPDATE-MM. When timer T3411 expires the combined tracking area updating procedure indicating "combined TA/LA updating with IMSI attach" is triggered again.

If the tracking area updating attempt counter is equal to 5:

- the UE shall start timer T3402, shall set the EPS update status to EU1 UPDATED and shall enter state EMM-REGISTERED.ATTEMPTING-TO-UPDATE-MM. When timer T3402 expires the combined tracking area updating procedure indicating "combined TA/LA updating with IMSI attach" is triggered again;

- a UE operating in CS/PS mode 1 of operation shall select GERAN or UTRAN radio access technology and proceed with appropriate MM or GMM specific procedures.

Editor's note: the conditions for the UE to reselect E-UTRAN radio access technology are FFS.

#18 (CS domain not available)

The UE shall stop timer T3430 if still running, shall set the EPS update status to EU1 UPDATED and shall enter state EMM-REGISTERED.NORMAL-SERVICE.

The UE shall set the update status to U2 NOT UPDATED.

A UE in CS/PS mode 1 of operation shall select GERAN or UTRAN radio access technology and proceed with appropriate MM or GMM specific procedures. The UE shall not reselect E-UTRAN radio access technology for the duration the UE is on the PLMN or an equivalent PLMN.

Other EMM cause values and the case that no EMM cause IE was received are considered as abnormal cases. The combined tracking area updating procedure shall be considered as failed for EPS and non-EPS services. The behaviour of the UE in those cases is specified in subclause 5.5.3.3.6.

5.5.3.3.5 Combined tracking area updating procedure not accepted by the network

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

Upon receiving the TRACKING AREA UPDATE REJECT message, the UE shall stop timer T3430, stop any transmission of user data, enter state MM IDLE, and take the following actions depending on the EMM cause value received.

#3 (Illegal UE);

#6 (Illegal ME); or

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI Listand KSI.

The UE shall consider the USIM as invalid for EPS and non-EPS services until switching off or the UICC containing the USIM is removed. Additionally, the UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the MM parameters update status, TMSI, LAI and ciphering key sequence number, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the combined routing area updating procedure is rejected with this cause value.

#7 (EPS services not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI List and KSI. The UE shall consider then USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

Editor's note: The handling of timer T3212 for non-EPS service is FFS.

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the combined routing area updating procedure is rejected with this cause value.

A UE in CS/PS mode 1 or CS/PS mode 2 of operation is still IMSI attached for non-EPS services. The UE shall select GERAN or UTRAN radio access technology and proceed with appropriate MM specific procedure according to the MM service state. The UE shall not reselect E-UTRAN radio access technology until switching off or the UICC containing the USIM is removed.

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

The UE shall set the EPS update status to EU2 NOT UPDATED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI List and KSI. The UE shall delete the list of equivalent PLMNs and enter the state EMM-DEREGISTERED.

Subsequently, the UE shall automatically initiate the attach procedure.

#10 (Implicitly detached);

The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.NORMAL-SERVICE. The UE shall then perform a new attach procedure.

#11 (PLMN not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI List and KSI, and reset the tracking area updating attempt counter. The UE shall delete the list of equivalent PLMNs and enter the state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMN list".

The UE shall then perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle and the MM parameters update status, TMSI, LAI, ciphering key sequence number and the location update attempt counter, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined routing area updating procedure is rejected with this cause value and no RR connection exists.

#12 (Tracking area not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to clause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI List and KSI. The UE shall reset the tracking area updating attempt counter and shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for regional provision of service".

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the MM parameters update status, TMSI, LAI, ciphering key sequence number and the location update attempt counter, and the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined routing area updating procedure is rejected with this cause value.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete the list of equivalent PLMNs. The UE shall reset the tracking area updating attempt counter and shall change to state EMM-REGISTERED.PLMN-SEARCH.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming" and shall remove the current TAI from the stored TAI list if present.

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

The UE shall indicate the Update type IE "combined TA/LA updating with IMSI attach" when performing the tracking area updating procedure following the PLMN selection.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the MM parameters update status and the location update attempt counter, and the GMM parameters GMM state, GPRS update status and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined routing area updating procedure is rejected with this cause value.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). Furthermodre the UE shall delete any GUTI, last visited registered TAI, TAI List and KSI. The UE shall reset the tracking area updating attempt counter and shall enter the state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list.

A UE operating in CS/PS mode 1 or CS/PS mode 2 of operation is still IMSI attached for non-EPS services. If the timer T3212 is not already running in the UE, the UE shall set the timer T3212 to its initial value and restart it.

A UE operating in CS/PS mode 1 of operation may select GERAN or UTRAN radio access technology and proceed with the appropriate MM specific procedure according to the MM service state. In this case the UE shall not reselect E-UTRAN radio access technology for the duration the UE is on the PLMN or equivalent PLMN.

A UE in CS/PS mode 1 of operation may perform a PLMN selection according to 3GPP TS 23.122 [6].

A UE operating in CS/PS mode 2 of operation shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, GPRS ciphering key sequence number and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined routing area updating procedure is rejected with this cause value.

#15 (No suitable cells in tracking area);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). The UE shall reset the tracking area updating attempt counter and shall enter the state EMM-REGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming" and shall remove the current TAI from the stored TAI list if present.

The UE shall search for a suitable cell in another tracking area or in another location area in the same PLMN according to 3GPP TS 36.304 [21].

The UE shall indicate the Update type IE "combined TA/LA updating with IMSI attach" when performing the tracking area updating procedure.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the MM parameters update status and the location update attempt counter, and the GMM parameters GMM state, GPRS update status and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined routing area updating procedure is rejected with this cause value.

#25 (Not authorized for this CSG);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). The UE shall reset the tracking area updating attempt counter and shall enter the state EMM-REGISTERED.LIMITED-SERVICE.

The UE shall remove the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message from the Allowed CSG list.

The UE shall search for a suitable cell in the same PLMN according to 3GPP TS 36.304 [21].

The UE shall indicate the Update type IE "combined TA/LA updating with IMSI attach" when performing the tracking area updating procedure.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the MM parameters update status and the location update attempt counter, and the GMM parameters GMM state, GPRS update status and routing area updating attempt counter as specified in 3GPP TS 24.008 [13] for the case when the combined routing area updating procedure is rejected with this cause value.

Other values are considered as abnormal cases. The behaviour of the UE in those cases is specified in subclause 5.5.3.3.6.

5.5.3.3.6 Abnormal cases in the UE

The UE shall proceed as follows:

- if the combined tracking area update was successful for EPS services only and the TRACKING AREA UPDATE ACCEPT message contained a cause value not treated in subclause 5.5.3.3.4.3 or the EMM Cause IE is not included in the message, the UE shall follow the procedure specified in subclause 5.5.3.2.6, item d with the following modification;

- otherwise, the abnormal cases specified in subclause 5.5.3.2.6 apply with the following modification.

If the EPS tracking area updating attempt counter is incremented according to subclause 5.5.3.2.6 the next actions depend on the value of the tracking area updating attempt counter.

- if the update status is U1 UPDATED and the tracking area updating attempt counter is less than 5, then the UE shall keep the update status to U1 UPDATED, the new MM state is MM IDLE substate NORMAL SERVICE;

- if the tracking area updating attempt counter is less than 5 and, additionally, the update status is different from U1 UPDATED UE shall delete any LAI, TMSI, ciphering key sequence number and list of equivalent PLMNs and set the update status to U2 NOT UPDATED. The MM state remains MM LOCATION UPDATING PENDING; or

- if the tracking area updating attempt counter is equal to 5, the UE shall delete any LAI, TMSI, ciphering key sequence number and list of equivalent PLMNs and set the update status to U2 NOT UPDATED. A UE operating in CS/PS mode 1 of operation shall select GERAN or UTRAN radio access technology and proceed with appropriate MM or GMM specific procedures.

Editor's note: the conditions for the UE to reselect E-UTRAN radio access technology are FFS.

5.5.3.3.7 Abnormal cases on the network side

The abnormal cases specified in subclause 5.5.3.2.7 apply with the exceptions for cases a and c in which in addition to the GUTI the old TMSI shall be considered occupied until the new TMSI is used by the UE in a subsequent message.

5.6 EMM connection management procedures (S1 mode only)

5.6.1 Service request procedure

5.6.1.1 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 or signalling is to be sent. Another purpose of this procedure is to invoke MO/MT CS fallback procedures.

This procedure is used when:

- the network has downlink signalling pending;
- the UE has uplink signalling pending;
- the UE or the network has user data pending and the UE is in EMM-IDLE mode;
- the UE in EMM-IDLE or EMM-CONNECTED mode has requested to perform mobile originating/terminating CS fallback; or
- the UE has uplink cdma2000® signalling pending.

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 5.6.2).

The UE shall invoke the service request procedure when:

a) the UE receives a paging request from the network in EMM-IDLE mode;

b) the UE, in EMM-IDLE mode, has pending user data to be sent;

c) the UE, in EMM-IDLE mode, has uplink signalling pending;

d) the UE, in EMM-IDLE or EMM-CONNECTED mode, has a mobile originating CS fallback request;

e) the UE, in EMM-IDLE or EMM-CONNECTED mode, has a CS fallback response to be sent to the network; or

f) the UE, in EMM-IDLE mode, has uplink cdma2000® signalling pending.

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

5.6.1.2 Service request procedure initiation

If the UE has pending uplink data or uplink signalling in EMM-IDLE mode to be transmitted or it responds to paging with CN domain indicator set to "PS", 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.

The UE shall send an EXTENDED SERVICE REQUEST message,

- regardless of the EMM mode, if the UE has a mobile originating CS fallback request; and
- regardless of the EMM mode, if the UE has a CS fallback response to be sent as a response to a paging for CS fallback.

5.6.1.3 EMM common procedure initiation

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

5.6.1.4 Service request procedure accepted by the network

For cases a, b and c in subclause 5.6.1.1, the UE shall treat the indication from the lower layers that the user plane radio bearer is set up as successful completion of the procedure.

For cases d and e in subclause 5.6.1.1, the UE shall treat the indication from the lower layers that the inter-system change from S1 mode to A/Gb or Iu mode is completed as successful completion of the procedure.

The EMM sublayer in the UE shall indicate to the MM sublayer that the CS fallback procedure has succeeded.

If the service type information element in the EXTENDED SERVICE REQUEST message indicates "mobile terminating CS fallback" the network initiates CS fallback procedures.

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

The UE shall locally deactivate the EPS bearer contexts that do not have a user plane radio bearer established after the successful completion of the service request procedure.

When the E-UTRAN fails to establish radio bearers for one or more EPS bearer contexts, then the MME shall locally deactivate the EPS bearer contexts corresponding to the failed radio bearers based on the lower layer indication from the E-UTRAN, without notifying the UE.

For manual update of the Allowed CSG list, the UE, after a successful completion of the procedure, shall check whether the CSG ID of the cell where the UE has sent the SERVICE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSD ID to the Allowed CSG list.

5.6.1.5 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 including an appropriate EMM cause value. When the EMM cause value is #39, "CS domain temporarily not available", the MME shall include a value for timer T3442 in the SERVICE REJECT message.

On receipt of the SERVICE REJECT message, the UE shall stop timer T3417 and take the following actions depending on the received EMM cause value.

#3 (Illegal UE); or

#6 (Illegal ME);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. The UE shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number and the MM parameters update status, TMSI, LAI and ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with this cause value. The USIM shall be considered as invalid also for non-EPS services until switching off or the UICC containing the USIM is removed.

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 (EPS services not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed. The UE shall enter the state EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with this cause value.

A UE operating in CS/PS mode 1 or CS/PS mode 2 of operation is still IMSI attached for non-EPS services. The UE shall select GERAN or UTRAN radio access technology and proceed with appropriate MM specific procedure according to the MM service state. The UE shall not reselect E-UTRAN radio access technology until switching off or the UICC containing the USIM is removed.

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

The UE shall set the EPS update status to EU2 NOT UPDATED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall enter the state EMM-DEREGISTERED.

Subsequently, the UE shall automatically initiate the attach procedure.

#10 (Implicitly detached);

The UE shall enter the state EMM-DEREGISTERED.NORMAL-SERVICE. The UE shall then perform a new attach procedure.

Editor's note: The need to re-establish any previously activated EPS bearer context is FFS.

#11 (PLMN not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall enter the state EMM-DEREGISTERED.PLMN-SEARCH.

The UE shall store the PLMN identity in the "forbidden PLMN list".

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number and the MM parameters update status, TMSI, LAI, ciphering key sequence number and the location update attempt counter as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with this cause value.

#12 (Tracking area not allowed);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and KSI. The UE shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for regional provision of service".

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with this cause value.

Editor's note: If RAN2 is going to abandon the additional cell re-selection hysteresis at tracking area boundaries, the behaviour described above may need to be changed: the UE could remain in EMM-REGISTERED state, GUTI and all EPS bearer contexts could be kept.

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

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). The UE shall enter the state EMM-REGISTERED.PLMN-SEARCH.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming".

The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state and GPRS update status as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with this cause value.

#15 (No suitable cells in tracking area);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). The UE shall enter the state EMM-REGISTERED.LIMITED-SERVICE.

The UE shall store the current TAI in the list of "forbidden tracking areas for roaming".

The UE shall search for a suitable cell in another tracking area or in another location area in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state and GPRS update status as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with this cause value.

#25 (Not authorized for this CSG);

The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3). The UE shall enter the state EMM-REGISTERED.LIMITED-SERVICE.

The UE shall remove the CSG ID of the cell where the UE has sent the SERVICE REQUEST message from the Allowed CSG list.

The UE shall search for a suitable cell in the same PLMN according to 3GPP TS 36.304 [21].

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state and GPRS update status as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with this cause value.

#38 (CS fallback call establishment not allowed);

The UE shall cancel upper layer actions related to CS fallback. The UE shall enter the state EMM-REGISTERED.NORMAL-SERVICE, and the EMM sublayer in the UE shall indicate to the MM sublayer that the CS fallback procedure has failed.

#39 (CS domain temporarily not available);

The UE shall start timer T3442 and shall set the EPS update status to EU2 NOT UPDATED (and shall store it according to subclause 5.1.3.3). The UE shall enter the state EMM-REGISTERED.NORMAL-SERVICE.

The UE shall not try to send an EXTENDED SERVICE REQUEST message for mobile originating services to the network until timer T3442 expires or the UE sends a TRACKING AREA UPDATE REQUEST message.

Other values are considered as abnormal cases. The specification of the UE behaviour in those cases is described in subclause 5.6.1.6.

5.6.1.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Access barred because of access class barring or NAS signalling connection establishment rejected by the network

If the service request procedure is started in response to a paging request from the network, access class barring is not applicable.

If the trigger for the service request procedure is the response to a paging request from the network and the NAS signalling connection establishment is rejected by the network, the service request procedure shall not be started. The UE stays in the current serving cell and applies normal cell reselection process. The service request procedure may be started if it is still necessary, i.e. when access for "terminating calls" is granted or because of a cell change.

Otherwise, if access is barred for "originating calls" (see 3GPP TS 36.331 [22]), the service request procedure shall not be started. The UE stays in the current serving cell and applies normal cell reselection process. The service request procedure may be started if it is still necessary, i.e. when access for "originating calls" is granted or because of a cell change.

b) Lower layer failure before the NAS security mode control procedure is completed or SERVICE REJECT message is received

The UE shall enter state EMM-REGISTERED. The UE shall abort the service request procedure, stop timer T3417 and locally release any resources allocated for the service request procedure.

c) T3417 expired

If the service request procedure was initiated for CS fallback:

The EMM sublayer shall abort the procedure and indicate to the MM sublayer that the CS fallback procedure has failed, and then enter the state EMM-REGISTERED.

If the service request procedure was initiated for EPS services:

The UE shall enter state EMM-REGISTERED.

If the UE is in EMM-IDLE mode then the procedure shall be aborted and the UE shall release locally any resources allocated for the service request procedure.

If the UE is in EMM-CONNECTED mode, then the procedure shall be aborted.

d) SERVICE REJECT received, other cause values than those treated in subclause 5.6.1.5

The procedure shall be aborted.

e) Tracking area updating procedure is triggered

The UE shall abort the service request procedure, stop timer T3417 and perform the tracking area updating procedure. The "active" flag shall be set in the TRACKING AREA UPDATE REQUEST message.

f) Power off

If the UE is in state EMM-SERVICE-REQUEST-INITIATED at power off, the EPS detach procedure shall be performed.

g) Procedure collision

If the UE receives a DETACH REQUEST message from the network in state EMM-SERVICE-REQUEST-INITIATED, the EPS detach procedure shall be progressed and the service request procedure shall be aborted. If the Detach type IE in the DETACH REQUEST message indicated "re-attach required", the EPS attach procedure shall be performed.

h) Transmission failure of SERVICE REQUEST message indication with TAI change from lower layers

If the current TAI is not in the TAI list, the service request procedure shall be aborted to perform the tracking area updating procedure. The "active" flag shall be set in the TRACKING AREA UPDATE REQUEST message.

If the current TAI is still part of the TAI list, the UE shall restart the service request procedure.

i) Transmission failure of SERVICE REQUEST message indication without TAI change from lower layers

The UE shall restart the service request procedure.

j) Access barred because the CSG ID is not in the UE's Allowed CSG list

If the service request procedure is started in response to a paging request from the network, access class barring is not applicable.

Otherwise, if access is barred for "originating calls" (see 3GPP TS 36.331 [22]), the service request procedure shall not be started. The UE stays in the current serving cell and applies normal cell reselection process. The service request procedure may be started if it is still necessary, i.e. because of a cell change.

5.6.1.7 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure

If a lower layer failure occurs before the security mode control procedure is completed, a SERVICE REJECT message has been sent to the UE or the service request procedure has been accepted by the network, the network enters/stays in EMM-IDLE.

b) Protocol error

If the SERVICE REQUEST message is received with a protocol error, the network shall return a SERVICE REJECT message with one of the following EMM cause values:

#96: invalid mandatory information;

#99: information element non-existent or not implemented;

#100: conditional IE error; or

#111: protocol error, unspecified.

The network stays in EMM-IDLE mode.

c) More than one SERVICE REQUEST received and the procedure has not been completed (i.e., the security mode control procedure has not been completed or SERVICE REJECT message has not been sent or service request procedure has not been completed)

- If one or more of the information elements in the SERVICE REQUEST message differs from the ones received within the previous SERVICE REQUEST message, the previously initiated service request procedure shall be aborted and the new service request procedure shall be progressed;

- If the information elements do not differ, then the network shall continue with the previous service request procedure and shall not treat any further this SERVICE REQUEST message.

d) ATTACH REQUEST received before the security mode control procedure has been completed or a SERVICE REJECT message has been sent or the service request procedure has been completed

If an ATTACH REQUEST message is received and the security mode control procedure has not been completed or the service request procedure has not been completed or a SERVICE REJECT message has not been sent, the network may initiate the EMM common procedures, e.g. the EMM authentication and ciphering procedure. The network may e.g. after a successful EMM authentication and ciphering procedure execution, abort the service request procedure, the EMM context, EPS bearer contexts, if any, are deleted and the new ATTACH REQUEST is progressed.

e) TRACKING AREA UPDATE REQUEST message received before the security mode control procedure has been completed or the service request procedure has been completed or a SERVICE REJECT message has been sent

If a TRACKING AREA UPDATE REQUEST message is received and the security mode control procedure has not been completed or the service request procedure has not been completed or a SERVICE REJECT message has not been sent, the network may initiate the EMM common procedures, e.g. the EMM authentication and ciphering procedure. The network may e.g. after a successful EMM authentication and ciphering procedure execution, abort the service request procedure and progress the tracking area updating procedure.

5.6.2 Paging procedure

5.6.2.1 General

The paging procedure is used by the network to request the establishment of a NAS signalling connection to the UE. The NAS signalling connection thus established can also be used to transport cdma2000® signalling messages to the UE. Another purpose of the paging procedure is to initiate the mobile terminating CS fallback procedure.

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

5.6.2.2 Paging for EPS services

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

The network shall initiate the paging procedure for EPS services using S-TMSI with CN domain indicator set to "PS" when NAS signalling messages, cdma2000® 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 [20], 3GPP TS 36.413 [23]) and starts the timer T3413 for this paging procedure. Upon reception of a paging indication, the UE shall respond to the paging with a SERVICE REQUEST message (see 3GPP TS 23.401 [10] and 3GPP TS 36.413 [23]). If the paging for EPS services was received during an ongoing UE initiated EMM specific procedure or service request procedure, then the UE shall ignore the paging and the UE and the network shall proceed with the EMM specific procedure or the service request procedure.

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

5.6.2.2.2 Paging for EPS services through E-UTRAN using IMSI

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

The network may initiate paging for EPS services using IMSI with CN domain indicator set to "PS" if the S-TMSI is not available due to a network failure.

In S1 mode, to initiate the procedure the EMM entity in the network requests the lower layer to start paging (see 3GPP TS 36.331 [22] and 3GPP TS 36.413 [23]).

When a UE receives a paging for EPS services using IMSI from the network before a UE initiated EMM specific procedure has been completed, then the UE shall abort the EMM specific procedure and proceed according to the description in this clause.

Upon reception of a paging for EPS services using IMSI, the UE shall locally deactivate any EPS bearer context(s) and locally detach from EPS. Additionally the UE shall delete the following parameters: last visited registered TAI, TAI list, GUTI and KSI_{ASME}. The UE shall set the EPS update status to EU2 NOT UPDATED and change the state to EMM-DEREGISTERED.

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI, and GPRS ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when a paging for GPRS services using IMSI is received.

After performing the local detach, the UE shall then perform an EPS attach procedure as described in subclause 5.5.1.2. If the UE is operating in CS/PS mode 1 or CS/PS mode 2 of operation, then the UE shall perform a combined EPS attach procedure as described in subclause 5.5.1.3.

NOTE 1: In some cases, user interaction can be required, thus the UE cannot activate the dedicated bearer context(s) automatically.

NOTE 2: The UE does not respond to the paging except with the attach request, hence timer T3413 in the network is not used when paging with IMSI.

NOTE 3: Paging without DRX parameters can require a considerable extension of the paging duration.

Editor's note: It is FFS if NOTE 3 is applicable for EPS.

5.6.2.3 Paging for CS fallback to A/Gb or Iu mode

The network may initiate the paging procedure for non-EPS services when the UE is IMSI attached for non-EPS services.

To initiate the procedure when no NAS signalling connection exists, the EMM entity in the network requests the lower layer to start paging (see 3GPP TS 36.300 [20], 3GPP TS 36.413 [23]) and starts the timer T3413 for this paging procedure. The paging message includes a CN domain indicator set to "CS" in order to indicate that this is paging for CS fallback. Upon reception of a paging indication, the UE may respond to the paging immediately or may request

upper layers input i.e. to accept or reject CS fallback. The response is indicated in the CSFB response information element in the EXTENDED SERVICE REQUEST message in both EMM-IDLE and EMM-CONNECTED modes.

The network shall stop the timer T3413 for the paging procedure when a response is received from the UE.

To notify the UE about an incoming mobile terminating CS service when a NAS signalling connection exists, the EMM entity in the network shall send a CS SERVICE NOTIFICATION message.

Editor's note: The information which needs to be contained in the CS SERVICE NOTIFICATION message is FFS.

5.6.3 Transport of NAS messages procedure

5.6.3.1 General

The purpose of the transport of NAS messages procedure is to carry SMS messages in an encapsulated form between the MME and the UE. The procedure may be initiated by the UE or the network and can only be used when the UE is IMSI attached for non-EPS services.

5.6.3.2 Transport of NAS messages procedure initiation by the UE

The UE initiates the procedure by sending an UL NAS TRANSPORT message.

5.6.3.3 Transport of NAS messages procedure initiation by the network

The network initiates the procedure by sending a DL NAS TRANSPORT message.

5.7 Reception of 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 (see example in figure 5.7.1).

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.

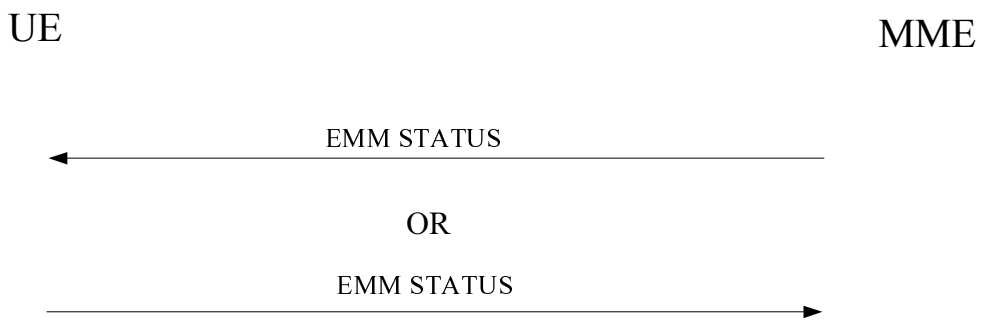

Figure 5.7.1: EMM status procedure

6 Elementary procedures for EPS session management

6.1 Overview

6.1.1 General

6.1.2 Types of ESM procedures

6.1.3 ESM sublayer states

6.1.3.1 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 is FFS.

6.1.3.2 ESM sublayer states in the UE

6.1.3.2.1 BEARER CONTEXT INACTIVE

No EPS bearer context exists.

6.1.3.2.2 BEARER CONTEXT ACTIVE

The EPS bearer context is active in the UE.

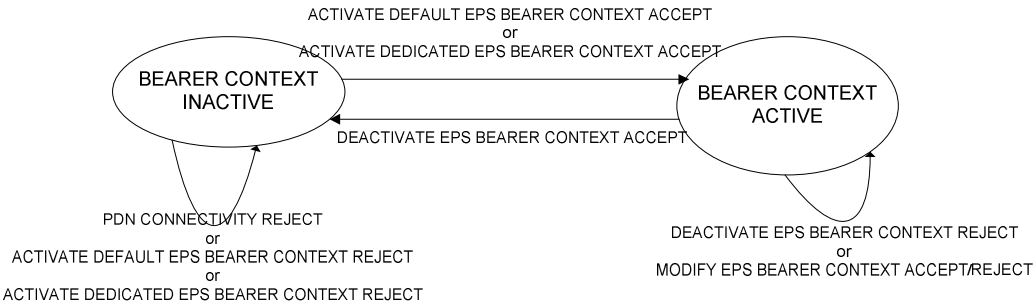

Figure 6.1.3.2.2.1: The ESM sublayer states for EPS bearer context handling in the UE (overview)

6.1.3.2.3 PROCEDURE TRANSACTION INACTIVE

No procedure transaction exists.

6.1.3.2.4 PROCEDURE TRANSACTION PENDING

The UE has initiated a procedure transaction towards the network.

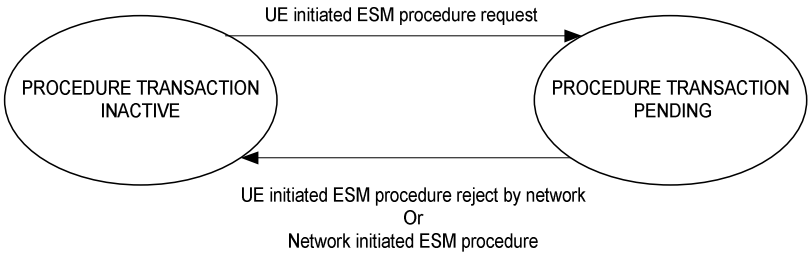

Figure 6.1.3.2.4.1: The procedure transaction states in the UE (overview)

6.1.3.3 ESM sublayer states in the MME

6.1.3.3.1 BEARER CONTEXT INACTIVE

No EPS bearer context exists.

6.1.3.3.2 BEARER CONTEXT ACTIVE PENDING

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

6.1.3.3.3 BEARER CONTEXT ACTIVE

The EPS bearer context is active in the network.

6.1.3.3.4 BEARER CONTEXT INACTIVE PENDING

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

6.1.3.3.5 BEARER CONTEXT MODIFY PENDING

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

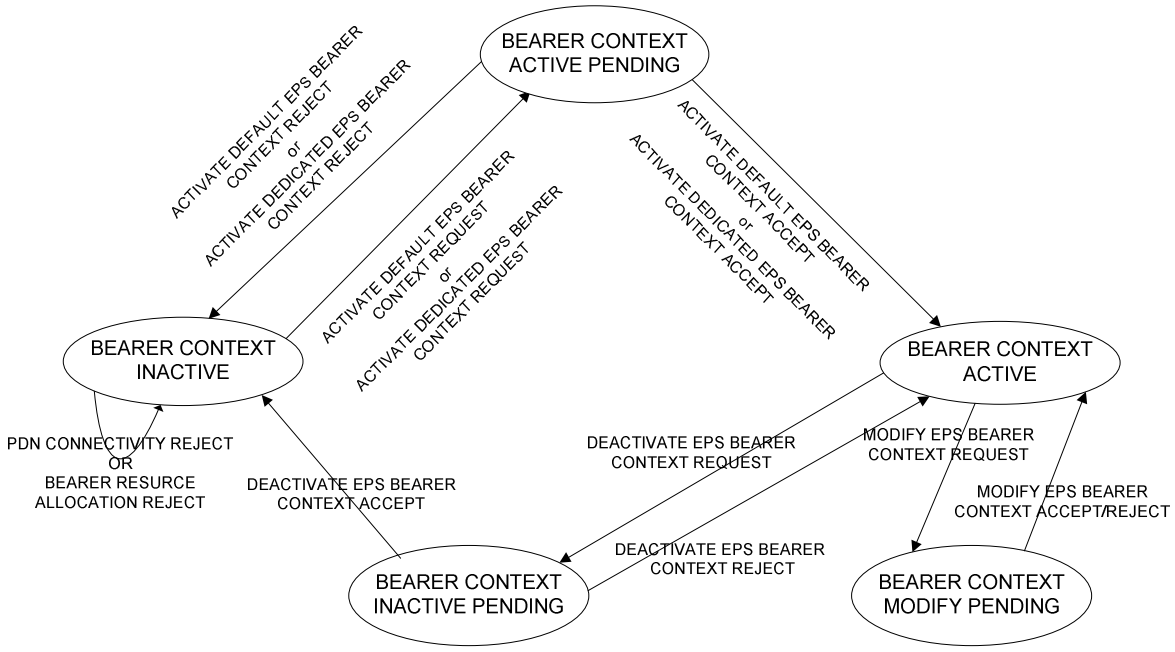

Figure 6.1.3.3.5.1: The ESM sublayer states for EPS bearer context handling in the network (overview)

6.1.4 Coordination between ESM and SM

This section applies for a UE supporting A/Gb mode or Iu mode, and S1 mode.

For inter-system change from S1 mode to A/Gb mode or Iu mode, SM uses the following parameters from each active EPS bearer context: EPS bearer identity to map to NSAPI, linked EPS bearer identity (if available) to map to linked NSAPI, PDN address, APN, TFT (if available), APN-AMBR if it is the default EPS bearer context, GERAN/UTRAN parameters as provided while on E-UTRAN access, i.e. R99 QoS, LLC SAPI, radio priority, packet flow identifier, transaction identifier and BCM (if available). The mapping from EPS to pre-Rel-8 QoS parameters is given in 3GPP TS 23.401 [10], Annex E.

For inter-system change from A/Gb mode or Iu mode to S1 mode, ESM uses the following parameters from each active PDP context: NSAPI to map to EPS bearer identity, linked NSAPI (if available) to map to linked EPS bearer identity, PDP address, APN, TFT (if available), APN-AMBR if it is the default PDP context, and R99 QoS. The mapping from pre-Rel-8 to EPS QoS parameters is given in 3GPP TS 23.401 [10], Annex E.

6.2 IP address allocation

6.2.1 General

The UE can configure an IPv4 address during the establishment of a default EPS bearer context. The UE can obtain an IPv4 address or an IPv6 prefix or both via an IETF-based IP address allocation mechanism once the default bearer is established.

The following IETF-based IP address/prefix allocation methods are specified for EPS:

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.

NOTE: From the perspective of the UE, the procedure used to allocate a static IP address via NAS signalling is the same as the procedure used to allocate a dynamic IP address specified in subclause 6.2.2.

Upon deactivation of the default bearer of a PDN connection, the UE shall locally release any IPv4 address or IPv6 prefix allocated to the UE for the corresponding PDN connection.

6.2.2 IP address allocation via NAS signalling

The UE shall set the PDN type IE in the PDN CONNECTIVITY REQUEST message based on its IP stack configuration as follows:

- A UE, which is IPv6 and IPv4 capable, shall set the PDN type IE to IPv4v6.
- A UE, which is only IPv4 capable, shall set the PDN type IE to IPv4.
- A UE, which is only IPv6 capable, shall set the PDN type IE to IPv6.
- When the IP version capability of the UE is unknown in the UE (as in the case when the MT and TE are separated and the capability of the TE is not known in the MT), the UE shall set the PDN type IE to IPv4v6.

If the UE wants to use DHCPv4 for IPv4 address assignment, it shall indicate that to the network within the Protocol Configuration Options IE in the PDN CONNECTIVITY REQUEST.

On receipt of the PDN CONNECTIVITY REQUEST message sent by the UE, the network when allocating an IP address shall take into account the PDN type IE, the operator policies of the home and visited network, and the user's subscription data.

- If the UE requests for PDN type IPv4v6, but the subscription is limited to IPv4 only or IPv6 only for the requested APN, the network shall override the PDN type requested by the UE to be limited to a single address PDN type (IPv4 or IPv6). In the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message sent to the UE, the network shall set the PDN type value to either "IPv4" or "IPv6" and the ESM cause value to #50,

"PDN type IPv4 only allowed", or #51, "PDN type IPv6 only allowed", respectively. The UE shall not subsequently initiate another UE requested PDN connectivity procedure to the same APN to obtain a PDN type different from the one allowed by the network.

- If the UE requests PDN type IPv4v6, but the PDN GW configuration dictates the use of IPv4 addressing only or IPv6 addressing only for this APN, the network shall override the PDN type requested by the UE to limit it to a single address PDN type (IPv4 or IPv6). In the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message sent to the UE, the network shall set the PDN type value to either "IPv4" or "IPv6" and the ESM cause value to #50, "PDN type IPv4 only allowed", or #51, "PDN type IPv6 only allowed", respectively. The UE shall not subsequently initiate another UE requested PDN connectivity procedure to the same APN to obtain a PDN type different from the one allowed by the network.

- If the UE requests PDN type IPv4v6, but the operator uses single addressing per bearer, e.g. due to interworking with nodes of earlier releases, the network shall override the PDN type requested by the UE to a single IP version only. In the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message sent to the UE, the network shall set the PDN type value to either "IPv4" or "IPv6" and the ESM cause value to #52, "single address bearers only allowed". The UE may subsequently request another PDN connection for the other IP version using the UE requested PDN connectivity procedure to the same APN with a single address PDN type (IPv4 or IPv6) other than the one already activated.

- If the network sets the PDN type to IPv4 or IPv4v6, the network shall include an IPv4 address in the PDN address information. In this case, if the IPv4 address is to be configured using DHCPv4, the network shall set the IPv4 address to 0.0.0.0.

- If the network sets the PDN type to IPv6 or IPv4v6, the network shall include the interface identifier that the UE shall use for the link local address in the PDN address information.

The network shall include the PDN type and the PDN address information within the PDN address IE in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message sent to the UE.

6.2.3 IPv6 stateless address autoconfiguration

The IPv6 stateless address autoconfiguration procedure is defined in IETF RFC 4862 [28]. This subclause provides some specific handling which applies in the context of this specification.

After a default bearer has been established, the UE can send a Router Solicitation message to trigger the network to send a Router Advertisement (see IETF RFC 4861 [27]). The network (PDN GW or the Serving GW if S5-PMIP reference point is used) periodically sends 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 UE that stateless address autoconfiguration is performed, the Router Advertisement has the M flag ("Managed Address Configuration" flag) cleared. The O flag ("Other Configuration" flag) can be set if additional parameters can be provided via DHCPv6 (see subclause 6.2.5).

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

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

When creating a global IPv6 address, the UE can 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 network guarantees that the prefixes in the Router Advertisements are unique, the UE does not perform the Duplicate Address Detection procedure.

6.2.4 IPv4 address allocation via DHCPv4

If the UE wants to configure the IPv4 address and additional IPv4 parameters that were not provided during the establishment of the default EPS bearer context (e.g. the DNS server address), the UE sends a DHCPDISCOVER message and uses DHCPv4 as specified in IETF RFC 2131 [24].

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 establishment of the default EPS bearer context and the UE needs additional parameters which were not provided, the UE uses DHCPv4 for configuring the remaining additional IPv4 parameters.

The network, acting as DHCPv4 server, replies with the options requested by the UE.

The UE can use the Rapid Commit option as specified in IETF RFC 4039 [26]. 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 [24] will be followed.

6.2.5 IPv6 parameter configuration via stateless DHCPv6

If the O flag ("Other Configuration" flag) is set in the Router Advertisement (see IETF RFC 4861 [27]) and the UE needs to configure additional IP parameters (e.g. the DNS server address) that were not provided during the establishment of the default EPS bearer context or the IPv6 address allocation procedure, the UE sends a DHCPv6 Information-Request message including the options it wishes to receive, as specified in IETF RFC 3736 [25].

The network replies with the options requested by the UE. Any interaction between the network and any external DHCPv6 server are specified in 3GPP TS 29.061 [16].

6.3 General on elementary ESM procedures

6.3.1 Services provided by lower layers

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.

6.3.2 Abnormal cases in the UE

The following generic abnormal case can be identified:

a) ESM uplink message transmission failure indication by lower layers

If lower layers indicate a TAI change, but the current TAI is not in the TAI list, the ESM procedure shall be aborted and re-initiated after successfully performing a tracking area updating procedure.

If lower layers indicate a TAI change, but the current TAI is still part of the TAI list, it is up to the UE implementation how the ESM procedure is re-initiated.

If lower layers indicate the TAI has not changed, it is up to the UE implementation how the ESM procedure is re-initiated.

NOTE: The ESM procedure can typically be re-initiated using a retransmission mechanism of the uplink message (the one that has previously failed to be transmitted) with new sequence number and message authentication code information thus avoiding to restart the whole procedure.

6.4 Network initiated ESM procedures

6.4.1 Default EPS bearer context activation procedure

6.4.1.1 General

The purpose of the default bearer context activation procedure is to establish a default EPS bearer context between the UE and the EPC. The default EPS bearer context activation procedure is initiated by the network as a response to the PDN CONNECTIVITY REQUEST message from the UE. The default bearer context activation procedure can be part of the attach procedure, and if the attach procedure fails, the UE shall consider that the default bearer activation has implicitly failed. The default EPS bearer context does not have any TFT, i.e. it uses a match-all packet filter.

6.4.1.2 Default EPS bearer context activation initiated by the network

The MME shall initiate the default bearer context activation procedure by sending an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message and enter the state BEARER CONTEXT ACTIVE PENDING (see example in figure 6.4.1.2.1). When the default bearer is activated as part of the attach procedure, the MME shall send the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message together with ATTACH ACCEPT and shall not start the timer T3485. When the default bearer is activated as the response to a stand-alone PDN CONNECTIVITY REQUEST message apart from the attach procedure, the MME shall send the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message alone, and start the timer T3485.

The MME shall assign and include an EPS bearer identity in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message. The MME shall retrieve the PTI from the PDN CONNECTIVITY REQUEST message and include it in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message. Both the network identifier part and the operator identifier part shall be included in the Access Point Name IE.

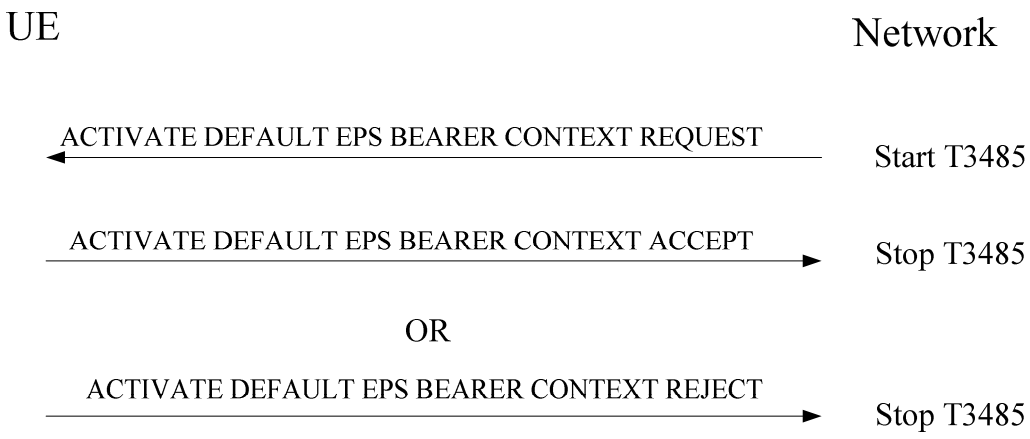

Figure 6.4.1.2.1: Default EPS bearer context activation procedure

6.4.1.3 Default EPS bearer context activation accepted by the UE

Upon receipt of the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, the UE shall send an ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message and enter the state BEARER CONTEXT ACTIVE. When the default bearer is activated as part of the attach procedure, the UE shall send the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message together with ATTACH COMPLETE message. When the default bearer is activated as the response to the stand-alone PDN CONNECTIVITY REQUEST message, the UE shall send the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message alone.

The UE checks the PTI in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message to identify the UE requested PDN connectivity procedure to which the default bearer context activation is related (see subclause 6.5.1).

Upon receipt of the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message, the MME shall enter the state BEARER CONTEXT ACTIVE and stop the timer T3485, if the timer is running.

6.4.1.4 Default EPS bearer context activation not accepted by the UE

If the default EPS bearer context activation is part of the attach procedure, the ESM sublayer shall notify the EMM sublayer of an ESM failure.

If the default EPS bearer context activation is not part of the attach procedure, the UE shall send an ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message and enter the state BEARER CONTEXT INACTIVE.

The ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message contains an ESM cause that typically indicates one of the following cause values:

#26: insufficient resources;

#31: activation rejected, unspecified;

#41: semantic error in the TFT operation;

#42: syntactical error in the TFT operation;

#44: semantic error(s) in packet filter(s);

#45: syntactical error(s) in packet filter(s); or

#95 – 111: protocol errors.

The UE shall check the TFT in the request message for different types of TFT IE errors as follows:

- semantic errors in the TFT operations;
- syntactical errors in the TFT operations;
- semantic errors in packet filters; and
- syntactical errors in packet filters,

as indicated in 3GPP TS 24.008 [13], subclause 6.1.3.2.3, and shall reject the request message if TFT IE errors are detected.

Upon receipt of the ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message, the MME shall enter the state BEARER CONTEXT INACTIVE and stop the timer T3485, if the timer is running.

6.4.1.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Default EPS bearer context activation request for an already activated default EPS bearer context:

   If the UE receives an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message with an EPS bearer identity identical to the EPS bearer identity of an already activated default EPS bearer context, the UE shall locally deactivate the existing default EPS bearer context and all the associated dedicated EPS bearer contexts, if any, and proceed with the requested default EPS bearer context activation.

b) Default EPS bearer context activation request for an already activated dedicated EPS bearer context:

   If the UE receives an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message with an EPS bearer identity identical to the EPS bearer identity of an already activated dedicated EPS bearer context, the UE shall locally deactivate the existing dedicated EPS bearer context and proceed with the requested default EPS bearer context activation.

6.4.1.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3485:

   On the first expiry of the timer T3485, the MME shall resend the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST and shall reset and restart timer T3485. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3485, the MME shall release possibly allocated resources for this activation and shall abort the procedure.

6.4.2 Dedicated EPS bearer context activation procedure

6.4.2.1 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 modification procedure. The dedicated bearer context activation procedure can be part of the attach procedure, and if the attach procedure fails, the UE shall consider that the dedicated bearer activation has implicitly failed.

6.4.2.2 Dedicated EPS 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, start the timer T3485, and enter the state BEARER CONTEXT ACTIVE PENDING (see example in figure 6.4.2.2.1).

The MME allocates the EPS bearer identity and includes it in the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message. The MME shall include the EPS bearer identity of the associated default bearer as the linked EPS bearer identity in the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message. 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 modification procedure (see subclause 6.5.3).

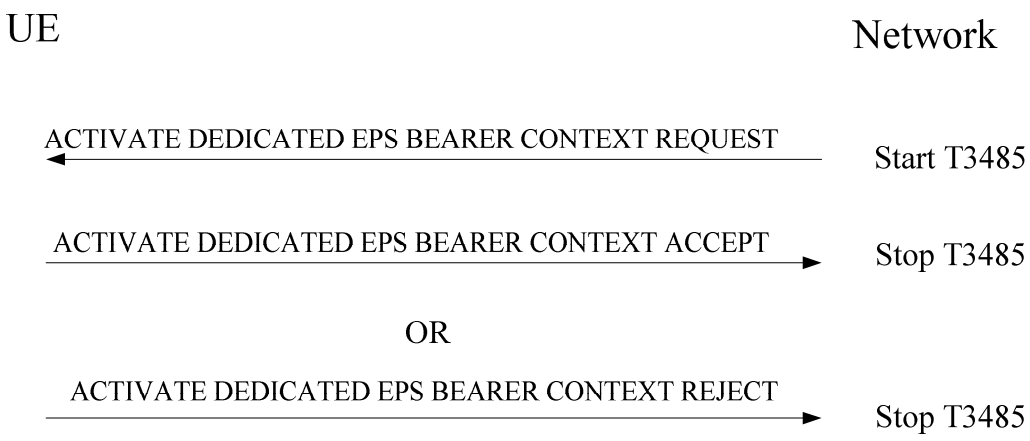

Figure 6.4.2.2.1: Dedicated EPS bearer context activation procedure

6.4.2.3 Dedicated EPS 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 uplink TFT before taking it into use. Then the UE shall send an ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message and enter the state BEARER CONTEXT ACTIVE. The ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message shall include the EPS bearer identity.

The linked EPS bearer identity 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 modification procedure to which the dedicated bearer context activation is related (see subclause 6.5.3).

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

Upon receipt of the ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message, the MME shall stop the timerT3485 and enter the state BEARER CONTEXT ACTIVE.

6.4.2.4 Dedicated EPS 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.

The ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message contains an ESM cause that typically indicates one of the following cause values:

#26: insufficient resources;

#31: activation rejected, unspecified;

#41: semantic error in the TFT operation;

#42: syntactical error in the TFT operation;

#43: unknown EPS bearer context;

#44: semantic error(s) in packet filter(s);

#45: syntactical error(s) in packet filter(s);

#46: EPS bearer context without TFT already activated; or

#95 – 111: protocol errors.

The UE shall check the TFT in the request message for different types of TFT IE errors as follows:

- semantic errors in the TFT operations;
- syntactical errors in the TFT operations;
- semantic errors in packet filters; and
- syntactical errors in packet filters,

as indicated in 3GPP TS 24.008 [13], subclause 6.1.3.2.3, and shall reject the request message if TFT IE errors are detected.

Upon receipt of the ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message in state BEARER CONTEXT ACTIVE PENDING, the MME shall stop the timer T3485, enter the state BEARER CONTEXT INACTIVE and abort the dedicated EPS bearer context activation procedure.

6.4.2.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Dedicated EPS bearer context activation request for an already activated dedicated EPS bearer context

If the UE receives an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message with an EPS bearer identity identical to the EPS bearer identity of an already activated dedicated EPS bearer context, the UE shall locally deactivate the existing dedicated EPS bearer context and proceed with the requested dedicated EPS bearer context activation.

b) No default EPS bearer context with linked EPS bearer identity activated

If the linked EPS bearer identity included in the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message does not match the EPS bearer identity of any activated default EPS bearer context, the UE shall reply with an ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message with cause value #43, "unknown EPS bearer context".

6.4.2.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3485:

On the first expiry of the timer T3485, the MME shall resend the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST and shall reset and restart timer T3485. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3485, the MME shall abort the procedure, release any resources allocated for this activation and enter the state BEARER CONTEXT INACTIVE.

b) Collision of UE requested PDN disconnect procedure and dedicated EPS bearer context activation procedure:

When the MME receives a PDN DISCONNECT REQUEST message during the dedicated EPS bearer context activation procedure, and the EPS bearer to be activated belongs to the PDN connection the UE wants to

disconnect, the MME shall terminate the dedicated bearer context activation procedure locally, release any resources related to this procedure and proceed with the PDN disconnect procedure.

6.4.3 EPS bearer context modification procedure

6.4.3.1 General

The purpose of the EPS bearer context modification procedure is to modify an EPS bearer context with a specific QoS and TFT. The EPS bearer context modification procedure is initiated by the network, but it may also be initiated as part of the UE requested bearer resource modification procedure.

6.4.3.2 EPS bearer context modification initiated by the network

The MME shall initiate the EPS bearer context modification procedure by sending a MODIFY EPS BEARER CONTEXT REQUEST message to the UE, starting the timer T3486, and entering the state BEARER CONTEXT MODIFY PENDING (see example in figure 6.4.3.2.1).

The MME shall include an EPS bearer identity that identifies the EPS bearer context to be modified in the MODIFY EPS BEARER CONTEXT REQUEST message.

The MODIFY EPS BEARER CONTEXT REQUEST message shall include also a procedure transaction identity (PTI), if this procedure was initiated by a UE requested bearer resource modification procedure.

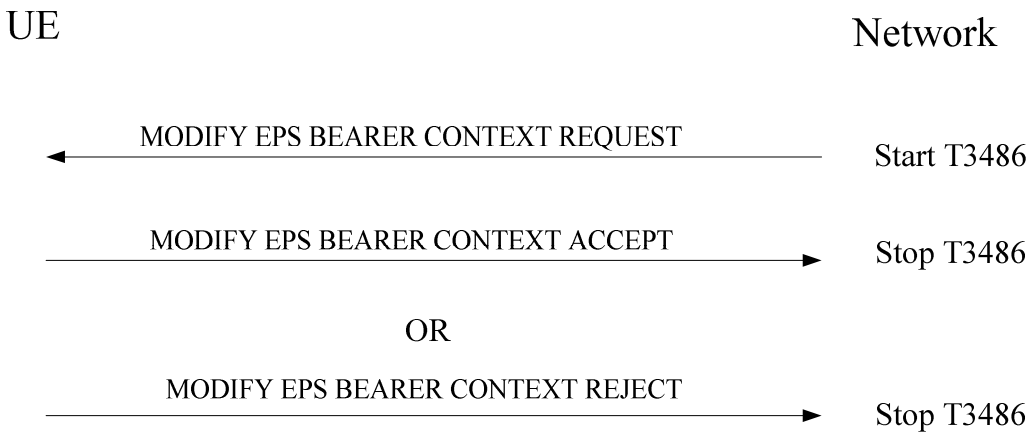

Figure 6.4.3.2.1: EPS bearer context modification procedure

6.4.3.3 EPS bearer context modification accepted by the UE

Upon receipt of the MODIFY EPS BEARER CONTEXT REQUEST message, the UE shall first check the received uplink TFT before taking it into use and then send a MODIFY EPS BEARER CONTEXT ACCEPT message to the MME.

If the PTI is included in the MODIFY EPS BEARER CONTEXT REQUEST message, the UE uses the PTI to identify the UE requested bearer resource modification procedure to which the EPS bearer context modification is related.

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

Upon receipt of the MODIFY EPS BEARER CONTEXT ACCEPT message, the MME shall stop the timer T3486 and enter the state BEARER CONTEXT ACTIVE.

6.4.3.4 EPS bearer context modification not accepted by the UE

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

The MODIFY EPS BEARER CONTEXT REJECT message contains an ESM cause that typically indicates one of the following cause values:

#26: insufficient resources;

#41: semantic error in the TFT operation;

#42: syntactical error in the TFT operation;

#44: semantic error(s) in packet filter(s);

#45: syntactical error(s) in packet filter(s);

#46: EPS bearer context without TFT already activated; or

#95 – 111: protocol errors.

The UE shall check the TFT in the request message for different types of TFT IE errors as follows:

- semantic errors in the TFT operations;
- syntactical errors in the TFT operations;
- semantic errors in packet filters; and
- syntactical errors in packet filters,

as indicated in 3GPP TS 24.008 [13], subclause 6.1.3.3.3, and shall reject the request message if TFT IE errors are detected.

Upon receipt of the MODIFY EPS BEARER CONTEXT REJECT message in state BEARER CONTEXT MODIFY PENDING, the MME shall stop the timer T3486, enter the state BEARER CONTEXT ACTIVE and abort the EPS bearer context modification procedure. When the MME detects that after the failed EPS bearer context modification there is a misalignment between the EPS bearer configuration and the EPS bearer context configuration or between the QoS on NAS and AS level, the MME should initiate the necessary procedures to achieve a re-alignment.

6.4.3.5 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE are FFS.

6.4.3.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3486:

On the first expiry of the timer T3486, the MME shall resend the MODIFY EPS BEARER CONTEXT REQUEST and shall reset and restart timer T3486. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3486, the MME shall abort the procedure and enter the state BEARER CONTEXT ACTIVE.

The MME may continue to use the previous configuration of the EPS bearer context or initiate an EPS bearer context deactivation procedure.

b) Collision of UE requested PDN disconnect procedure and EPS bearer context modification:

When the MME receives a PDN DISCONNECT REQUEST message during an EPS bearer context modification procedure, and the EPS bearer to be modified belongs to the PDN connection the UE wants to disconnect, the MME shall terminate the EPS bearer context modification procedure locally, release any resources related to this procedure and proceed with the PDN disconnect procedure.

6.4.4 EPS bearer context deactivation procedure

6.4.4.1 General

The purpose of the EPS bearer context deactivation procedure is to deactivate an EPS bearer context or disconnect from a PDN by deactivating all EPS bearer contexts to the PDN. The EPS bearer context deactivation procedure is initiated by the network, and it may be triggered by the UE by means of the UE requested bearer resource modification procedure or UE requested PDN disconnect procedure.

6.4.4.2 EPS bearer context deactivation initiated by the network

If a NAS signalling connection exists when the MME initiates the EPS bearer context deactivation procedure, the MME shall initiate the EPS bearer context deactivation procedure by sending a DEACTIVATE EPS BEARER CONTEXT REQUEST message to the UE, start the timer T3495, and enter the state BEARER CONTEXT INACTIVE PENDING (see example in figure 6.4.4.2.1).

The procedure transaction identity (PTI) shall also be included if the deactivation is triggered by a UE initiated bearer resource modification procedure.

When the MME wants to deactivate all EPS bearer contexts to a PDN and thus disconnect the UE from the PDN, the MME shall include the EPS bearer identity of the default bearer associated to the PDN in the DEACTIVATE EPS BEARER CONTEXT REQUEST message.

If no NAS signalling connection exists when the MME initiates the EPS 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.

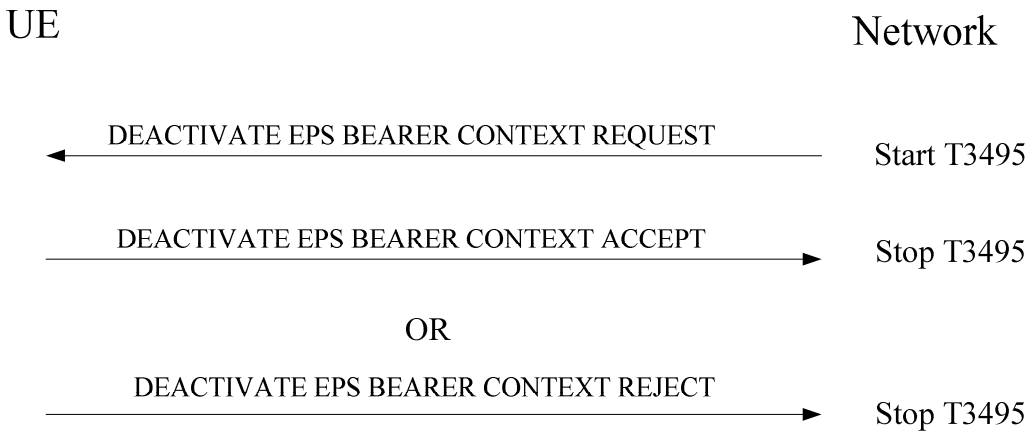

Figure 6.4.4.2.1: EPS bearer context deactivation procedure

6.4.4.3 EPS bearer context deactivation accepted by the UE

Upon receipt of the DEACTIVATE EPS BEARER CONTEXT REQUEST message, 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 DEACTIVATE EPS BEARER CONTEXT ACCEPT.

If the EPS bearer identity indicated in the DEACTIVATE EPS BEARER CONTEXT REQUEST does not point to an existing EPS bearer context, the UE shall respond with a DEACTIVATE EPS BEARER CONTEXT ACCEPT with the EPS bearer identity set to the received EPS bearer identity.

If the EPS bearer identity indicated in the DEACTIVATE EPS BEARER CONTEXT REQUEST is that of the default bearer to a PDN, the UE shall delete all EPS bearer contexts associated to the PDN. After deactivating all EPS bearer contexts, the UE shall respond to the MME with the DEACTIVATE EPS BEARER CONTEXT ACCEPT.

Upon receipt of the DEACTIVATE EPS BEARER CONTEXT ACCEPT message, the MME shall enter the state BEARER CONTEXT INACTIVE and stop the timer T3495.

6.4.4.4 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE are FFS.

6.4.4.5 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3495:

On the first expiry of the timer T3495, the MME shall resend the DEACTIVATE EPS BEARER CONTEXT REQUEST and shall reset and restart timer T3495. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3495, the MME shall abort the procedure and deactivate the EPS bearer context locally without any peer-to-peer ESM signalling between the MME and the UE.

b) Collision of UE requested PDN disconnect procedure and EPS bearer context deactivation:

When the MME receives a PDN DISCONNECT REQUEST message during the EPS bearer context deactivation procedure, and the EPS bearer indicated in the DEACTIVATE EPS BEARER CONTEXT REQUEST message is a dedicated EPS bearer belonging to the PDN connection the UE wants to disconnect, the MME shall proceed with both procedures. If the EPS bearer indicated in the DEACTIVATE EPS BEARER CONTEXT REQUEST message is the default EPS bearer, the MME shall proceed with the EPS bearer context deactivation procedure.

6.4.4.6 Local EPS bearer context deactivation without ESM signalling

The UE and the MME deactivate EPS bearer contexts locally without peer-to-peer ESM signalling in the following cases:

- during the service request procedure, if the E-UTRAN fails to establish the user plane radio bearers for one or more EPS bearer contexts e.g. due to radio access control;
- during handover, if the target E-UTRAN cannot establish all the user plane radio bearers for the UE; or
- if the E-UTRAN releases one or more user plane bearers of the UE due to E-UTRAN specific reasons.

For those cases, based on the indication from the lower layers, the UE and the MME shall locally deactivate the EPS bearer contexts for which no user plane radio bearers are set up.

NOTE: The lower layers in the UE provide the user plane radio bearer context status to the ESM sublayer when a change in the user plane radio bearers is detected by the lower layers including establishment and release of user plane radio bearers for the UE in connected mode. This does not apply to the release of the RRC connection due to an S1-release procedure or due to radio link failure.

When the user plane radio bearer for a default EPS bearer context is not established during the service request procedure, the UE shall locally deactivate all EPS bearer contexts associated to the PDN connection with the default EPS bearer context. The MME shall locally deactivate all EPS bearer contexts associated to the PDN connection with the default EPS bearer context without peer-to-peer ESM signalling to the UE.

Opon completion of the service request procedure, if the UE locally deactivates all EPS bearer contexts, the UE shall perform a local detach, enter state EMM-DEREGISTERED and initiate an attach procedure.

If no NAS signalling connection exists when the MME initiates the EPS bearer context deactivation, the MME locally deactivates the EPS bearer contexts without peer-to-peer ESM signalling.

6.5 UE requested ESM procedures

6.5.1 UE requested PDN connectivity procedure

6.5.1.1 General

The purpose of the UE requested PDN connectivity procedure is for a UE to request the setup of a default EPS bearer to a PDN. If accepted by the network, this procedure initiates the establishment of a default EPS bearer context. The procedure is used either to establish the first default bearer by inclusion into the initial attach message or to establish subsequent default bearers to additional PDNs in order to allow the UE simultaneous access to multiple PDNs.

6.5.1.2 UE requested PDN connectivity procedure initiation

In order to request connectivity to the default PDN, the UE shall not include any APN in the PDN CONNECTIVITY REQUEST message.

In order to request connectivity to an additional PDN, the UE shall send a PDN CONNECTIVITY REQUEST message to the MME, start timer T3482 and enter the state PROCEDURE TRANSACTION PENDING (see example in figure 6.5.1.2.1). This message shall include the requested APN, if available. In the PDN type information element the UE shall indicate the IP version capability of the IP stack associated with the UE as specified in subclause 6.4.1

The UE shall set the request type to "initial attach" when the UE is establishing connectivity to a PDN for the first time, i.e. when it is an initial attach to that PDN. The UE shall set the request type to "handover" when the connectivity to a PDN is established upon handover from a non-3GPP access network and the UE was connected to that PDN before the handover to the 3GPP access network.

If the UE supports DSMIPv6, the UE may include a request for obtaining the IPv6 address and optionally the IPv4 address of the home agent in the Protocol configuration options IE in the PDN CONNECTIVITY REQUEST message. The UE may also include a request for obtaining the IPv6 Home Network Prefix.

The UE may set the ESM information transfer flag in the PDN CONNECTIVITY REQUEST message to indicate that it has ESM information, i.e. protocol configuration options, APN, or both, that needs to be sent after the NAS signalling security has been activated between the UE and the MME.

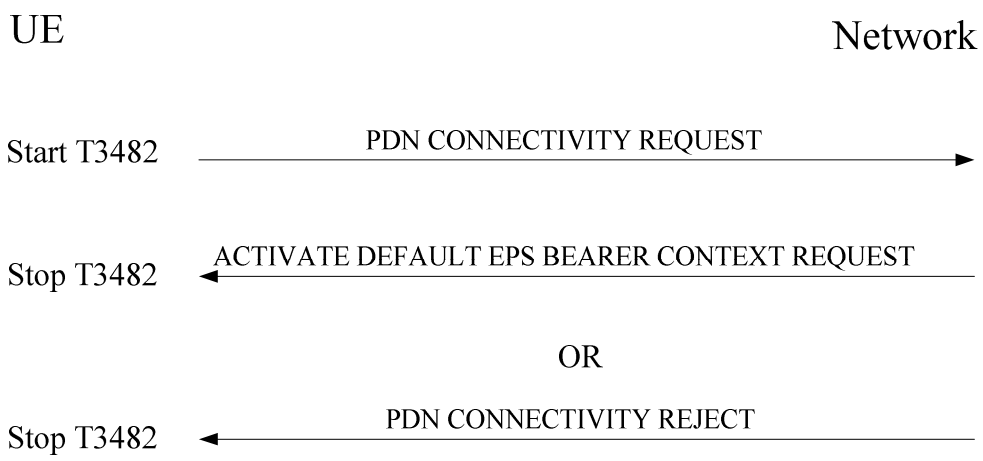

Figure 6.5.1.2.1: UE requested PDN connectivity procedure

6.5.1.3 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 no requested APN is included in the PDN CONNECTIVITY REQUEST message, the MME shall use the default APN as requested APN.

If connectivity with the requested PDN is accepted by the network, the MME shall initiate the default EPS bearer context activation procedure (see subclause 6.4.1).

If connectivity with the requested PDN is accepted, but with a restriction of IP version (i.e. both an IPv4 address and an IPv6 prefix is requested, but only one particular IP version, or only single IP version bearers are supported/allowed by the network), cause value #50, "PDN type IPv4 only supported", #51, "PDN type IPv6 only allowed", or #52, "single address bearers only allowed", respectively, as listed in subclause 6.5.1.4, shall be included in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message.

Upon receipt of the message ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST, the UE shall stop timer T3482 and enter the state PROCEDURE TRANSACTION INACTIVE.

6.5.1.4 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.

Upon receipt of the PDN CONNECTIVITY REJECT message, the UE shall stop timer T3482 and enter the state PROCEDURE TRANSACTION INACTIVE.

The PDN CONNECTIVITY REJECT message contains an ESM cause that typically indicates one of the following cause values:

#8: operator determined barring;

#26: insufficient resources;

#27: missing or unknown APN;

#28: unknown PDN type;

#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;

#35: PTI already in use;

#38: network failure;

#50: PDN type IPv4 only allowed;

#51: PDN type IPv6 only allowed;

#52: single address bearers only allowed;

#54: PDN connection does not exist;

#95 – 111: protocol errors;

#112: APN restriction value incompatible with active EPS bearer context.

6.5.1.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) T3482 expired

On the first expiry of the timer T3482, the UE shall resend the PDN CONNECTIVITY REQUEST and shall reset and restart timer T3482. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3482, the UE shall abort the procedure, release the PTI allocated for this invocation and enter the state PROCEDURE TRANSACTION INACTIVE;

6.5.1.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) UE initiated PDN connectivity request for an already existing PDN connection:

   If the network receives a PDN CONNECTIVITY REQUEST message with the same combination of APN and PDN type as an already existing PDN connection, the network shall deactivate the existing EPS bearer contexts for the PDN connection locally without notification to the UE and proceed with the requested PDN connectivity procedure.

b) UE initiated PDN connectivity request with request type "handover" for a PDN connection that does not exist:

   If the network receives a PDN CONNECTIVITY REQUEST message for either a default APN or a specific APN with request type set to "handover" and the MME does not have any information about that PDN connection, then MME shall reject the PDN connectivity request procedure including the cause value #54, "PDN connection does not exist", in the PDN CONNECTIVITY REJECT message.

c) ESM information not received:

   If the ESM information transfer flag in the PDN CONNECTIVITY REQUEST message has been set and the ESM information is not received before the final expiry of timer T3489 as described in subclause 6.6.1.2.6, the MME shall reject the PDN connectivity request procedure including the cause value #53, "ESM information not received", in the PDN CONNECTIVITY REJECT message.

6.5.2 UE requested PDN disconnect procedure

6.5.2.1 General

The purpose of the UE requested PDN disconnection procedure is for a UE to request disconnection from one PDN. The UE can initiate this procedure to disconnect from a PDN (including the default PDN) as long as it is connected to at least one other PDN. With this procedure, all EPS bearer contexts established towards this PDN, including the default EPS bearer context, are released.

6.5.2.2 UE requested PDN disconnection procedure initiation

In order to request PDN disconnection from a PDN, the UE shall send a PDN DISCONNECT REQUEST message to the MME, start the timer T3492 and enter the state PROCEDURE TRANSACTION PENDING (see example in figure 6.5.2.2.1). The PDN DISCONNECT REQUEST message shall include the EPS bearer identity of the default bearer associated with the PDN to disconnect from as the linked EPS bearer identity in the PDN DISCONNECT REQUEST message. The UE shall also set the EPS bearer identity in the PDN DISCONNECT REQUEST message to the value "no EPS bearer identity assigned" and include a procedure transaction identity (PTI).

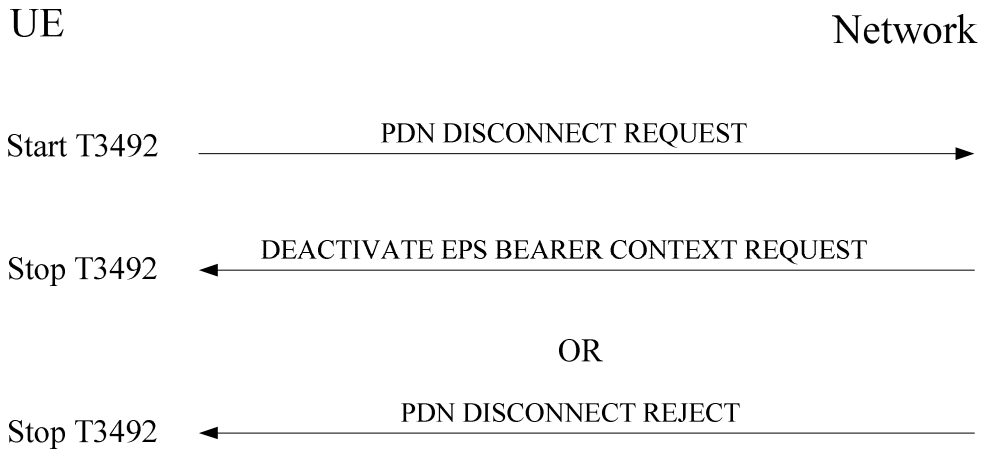

Figure 6.5.2.2.1: UE requested PDN disconnection procedure

6.5.2.3 UE requested PDN disconnection procedure accepted by the network

Upon receipt of the PDN DISCONNECT REQUEST message, if it is accepted by the network, the MME shall initiate the bearer context deactivation procedure by sending the DEACTIVATE EPS BEARER CONTEXT REQUEST message including the linked EPS bearer identity of the default bearer associated with the PDN to disconnect from and the PTI. The behaviour of the MME is described in subclause 6.4.4.

Upon receipt of the DEACTIVATE EPS BEARER CONTEXT REQUEST message, the UE shall stop the timer T3492 and enter the state PROCEDURE TRANSACTION INACTIVE. The behaviour of the UE is described in subclause 6.4.4.

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.

6.5.2.4 UE requested PDN disconnection procedure not accepted by the network

Upon receipt of the PDN DISCONNECT REQUEST message, if it is not accepted by the network, the MME shall send a PDN DISCONNECT REJECT message to the UE. The PDN DISCONNECT REJECT message shall contain the PTI and an ESM cause that typically indicates one of the following cause values:

#35: PTI already in use;

#43: unknown EPS bearer context;

#49: last PDN disconnection not allowed;

#95 – 111: protocol errors.

Upon receipt of the PDN DISCONNECT REJECT message, the UE shall stop the timer T3492, enter the state PROCEDURE TRANSACTION INACTIVE and abort the PDN disconnection procedure. Additionally, in all cases with the exception of the UE having received cause value #49, the UE shall deactivate all EPS bearer contexts for this PDN connection locally without peer-to-peer signalling between the UE and the MME.

6.5.2.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Expiry of timer T3492:

On the first expiry of the timer T3492, the UE shall resend the PDN DISCONNECT REQUEST and shall reset and restart timer T3492. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3492, the UE shall abort the procedure, deactivate all EPS bearer contexts for this PDN connection locally without peer-to-

peer signalling between the UE and the MME, and enter the state PROCEDURE TRANSACTION INACTIVE. In order to synchronize EPS bearer contexts status with the MME, on indication of "back to E-UTRAN coverage" from the lower layers, the UE shall send a TRACKING AREA UPDATE REQUEST message to the MME.

b) Collision of UE requested PDN disconnect procedure and dedicated EPS bearer context activation procedure:

When the UE receives an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message during the PDN disconnect procedure, and the EPS bearer to be activated belongs to the PDN connection the UE wants to disconnect, the UE shall ignore the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message and proceed with the PDN disconnect procedure.

c) Collision of UE requested PDN disconnect procedure and EPS bearer context modification:

When the UE receives a MODIFY EPS BEARER CONTEXT REQUEST message during the PDN disconnect procedure, and the EPS bearer to be modified belongs to the PDN connection the UE wants to disconnect, the UE shall ignore the MODIFY BEARER CONTEXT REQUEST message and proceed with the PDN disconnect procedure.

d) Collision of UE requested PDN disconnect procedure and EPS bearer context deactivation procedure:

When the UE receives a DEACTIVATE EPS BEARER CONTEXT REQUEST message during the PDN disconnect procedure, and the EPS bearer indicated in the DEACTIVATE EPS BEARER CONTEXT REQUEST message is a dedicated EPS bearer belonging to the PDN connection the UE wants to disconnect, the UE shall proceed with both procedures.

6.5.2.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) No PDN connection with the linked EPS bearer identity activated:

If the linked EPS bearer identity included in the PDN DISCONNECT REQUEST message does not belong to the default EPS bearer context of an established PDN connection, the MME shall reply with a PDN DISCONNECT REJECT message with cause value #43, "unknown EPS bearer context".

6.5.3 UE requested bearer resource modification procedure

6.5.3.1 General

The purpose of the UE requested bearer resource modification procedure is for a UE to request a modification (e.g. allocation or release) of bearer resources for a traffic flow aggregate. The UE can request or modify a specific QoS demand (QCI) and optionally it can either send a GBR requirement, for a new traffic flow aggregate, or modify the existing GBR. If accepted by the network, this procedure invokes a dedicated EPS bearer context activation procedure (see subclause 6.4.2),an EPS bearer context modification procedure (see subclause 6.4.3), or an EPS bearer context deactivation procedure (see subclause 6.4.4).

6.5.3.2 UE requested bearer resource modification procedure initiation

In order to request the modification of bearer resources for one traffic flow aggregate, the UE shall send a BEARER RESOURCE MODIFICATION REQUEST message to the MME, start timer T3480 and enter the state PROCEDURE TRANSACTION PENDING (see example in figure 6.5.3.2.1).

If the UE requests the release of bearer resources, the cause value typically indicates one of the following:

#36: regular deactivation.

Editor's note: Other cause values are FFS.

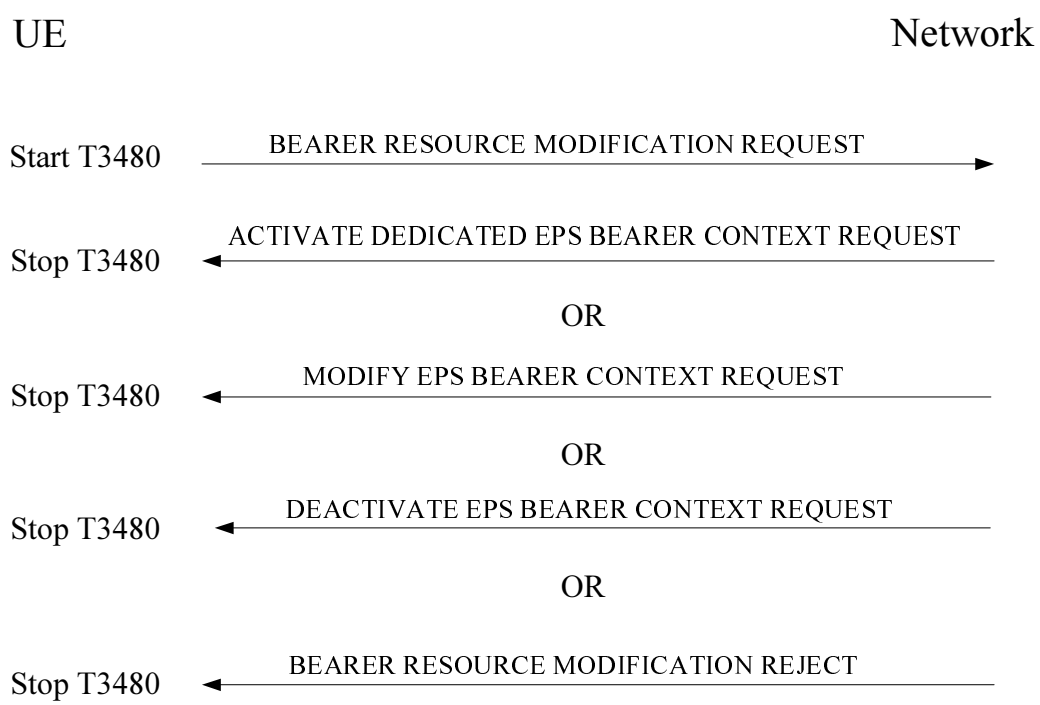

Figure 6.5.3.2.1: UE requested bearer resource modification procedure

6.5.3.3 UE requested bearer resource modification procedure accepted by the network

Upon receipt of the BEARER RESOURCE MODIFICATION REQUEST message, the MME checks whether the resources requested by the UE can be established, modified or released by verifying the bearer identity given in the Linked EPS bearer identity IE to be any of the active default EPS bearer context(s).

If the bearer resource modification requested is accepted by the network, the MME shall initiate either a dedicated EPS bearer context activation procedure, an EPS bearer context modification procedure or an EPS bearer context deactivation procedure. Upon receipt of an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST, MODIFY EPS BEARER CONTEXT REQUEST or DEACTIVATE EPS BEARER CONTEXT REQUEST with a PTI which matches the value used for the BEARER RESOURCE MODIFICATION REQUEST, the UE shall stop timer T3480 and enter the state PROCEDURE TRANSACTION INACTIVE.

If the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST is received, the UE shall enter the state BEARER CONTEXT ACTIVE and verify that the bearer identity given in the EPS bearer identity IE is not already used by any dedicated EPS bearer contexts associated with the included linked EPS bearer identity.

If the MODIFY EPS BEARER CONTEXT REQUEST is received, the UE verifies that the bearer identity given in the EPS bearer identity IE is any of the active EPS bearer contexts.

If the DEACTIVATE EPS BEARER CONTEXT REQUEST is received, the UE verifies that the bearer identity given in the EPS bearer identity IE is any of the active EPS bearer contexts associated with the included linked EPS bearer identity and enters the state BEARER CONTEXT INACTIVE.

6.5.3.4 UE requested bearer resource modification procedure not accepted by the network

If the bearer resource modification requested cannot be accepted by the network, the MME shall send a BEARER RESOURCE MODIFICATION 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 modification.

The cause value typically indicates one of the following:

#26: insufficient resources;

#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;

#35: PTI already in use;

#37: EPS 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(s) in packet filter(s);

#45: syntactical error(s) in packet filter(s);

#46: EPS bearer context without TFT already activated; or

#95 – 111: protocol errors.

If the requested new TFT is not available, then the BEARER RESOURCE MODIFICATION REJECT shall be sent.

The TFT in the request message is checked by the network for different types of TFT IE errors as follows:

a) semantic errors in the TFT operations;

b) syntactical errors in the TFT operations;

c) semantic errors in packet filters; and

d) syntactical errors in packet filters,

as indicated in 3GPP TS 24.008 [13], subclause 6.1.3.3.3.

Upon receipt of a BEARER RESOURCE MODIFICATION REJECT message, the UE shall stop the timer T3480 and enter the state PROCEDURE TRANSACTION INACTIVE.

The further actions to be performed by the UE are implementation dependent as part of upper layers responsibility.

6.5.3.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Expiry of timer T3480:

On the first expiry of the timer T3480, the UE shall resend the BEARER RESOURCE MODIFICATION REQUEST and shall reset and restart timer T3480. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3480, the UE shall abort the procedure, release the PTI allocated for this activation and enter the state PROCEDURE TRANSACTION INACTIVE. In addition, if the UE had initiated resource release for all the traffic flows for the bearer, it shall deactivate the dedicated bearer context locally without peer-to-peer signalling between the UE and the MME. In order to synchronize the EPS bearer context status with the MME, on indication of "back to E-UTRAN coverage" from the lower layers, the UE shall send a TRACKING AREA UPDATE REQUEST message to the MME.

b) Unknown EPS bearer context

Upon receipt of the BEARER RESOURCE MODIFICATION REJECT message including cause value #43, "unknown EPS bearer context", the UE shall deactivate the existing default EPS bearer context locally without peer-to-peer signalling between the UE and the MME.

c) Collision of UE and network initiated dedicated EPS bearer context deactivation procedures.

When the UE receives a DEACTIVATE EPS BEARER CONTEXT REQUEST message during the bearer resource modification procedure, and the EPS bearer indicated in the DEACTIVATE EPS BEARER CONTEXT REQUEST message is a dedicated EPS bearer context the UE wants to release, the UE shall abort the bearer resource modification procedure and proceed with the network initiated dedicated EPS bearer context deactivation procedure.

6.5.3.6 Abnormal cases on the network side

Editor's note: The abnormal cases on the network side are FFS.

6.6 Miscellaneous procedures

6.6.1 Exchange of protocol configuration options

6.6.1.1 General

The UE and the PDN-GW can exchange protocol configuration options via the dedicated ESM information request procedure or via other ESM procedures.

6.6.1.2 ESM information request procedure

6.6.1.2.1 General

The ESM information request procedure is used by the network to retrieve ESM information, i.e. protocol configuration options, APN, or both from the UE during the attach procedure if the UE indicated in the PDN CONNECTIVITY REQUEST message that it has ESM information that needs to be sent security protected. The purpose of this procedure is to provide privacy for the ESM information if ciphering is enabled in the network.

6.6.1.2.2 ESM information request initiated by the network

The network intiates the protocol configuration options request procedure by sending a ESM INFORMATION REQUEST message to the UE and starting timer T3489 (see example in figure 6.6.1.2.2.1). This message shall be sent only after the security context has been setup, and if the ESM information transfer flag has been set in the PDN CONNECTIVITY REQUEST message. The MME shall set the EPS bearer identity of the ESM INFORMATION REQUEST message to the value "no EPS bearer identity assigned" and include the PTI from the associated PDN CONNECTIVITY REQUEST message.

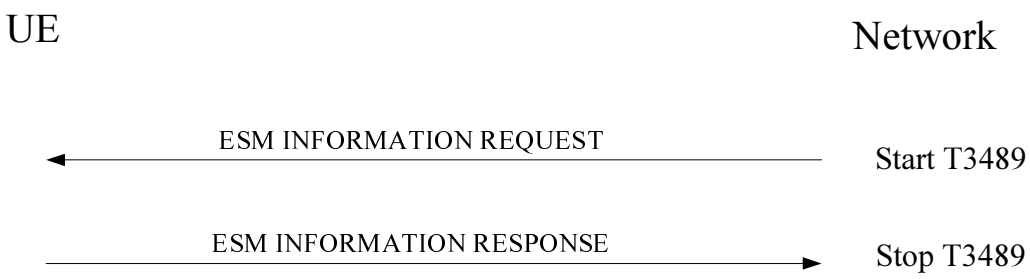

Figure 6.6.1.2.2.1: ESM information request procedure

6.6.1.2.3 ESM information request completion by the UE

Upon receipt of the ESM INFORMATION REQUEST message, the UE shall send an ESM INFORMATION RESPONSE message to the network .The UE shall include all the protocol configuration options that need to be

transferred security protected, and APN if required, to the network in the ESM INFORMATION RESPONSE message. The UE shall set the EPS bearer identity of the ESM INFORMATION RESPONSE message to the value "no EPS bearer identity assigned" and include the PTI from the ESM INFORMATION REQUEST message.

6.6.1.2.4 ESM information request completion by the network

Upon receipt of the ESM INFORMATION RESPONSE message, the network shall stop timer T3489.

6.6.1.2.5 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE are FFS.

6.6.1.2.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3489:

On the first expiry of the timer T3489, the MME shall resend the ESM INFORMATION REQUEST message and shall reset and restart timer T3489. This retransmission is repeated two times, i.e. on the third expiry of timer T3489, the MME shall abort the procedure, release any resources for this procedure and reject the associated PDN connectivity procedure including the cause value #53, "ESM information not received", in the PDN CONNECTIVITY REJECT message.

6.6.1.3 Exchange of protocol configuration options in other messages

The UE may include a Protocol configuration options IE on EPS bearer context activation, EPS bearer context deactivation, EPS bearer context modification, PDN connectivity request, PDN disconnect request, and bearer resource modification request if the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the PDN-GW.

The PDN-GW may include a Protocol configuration options IE on EPS bearer context activation, EPS bearer context deactivation, EPS bearer context modification, PDN connectivity reject, PDN disconnect reject, and bearer resource modification reject if the PDN-GW wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

6.7 Reception of an ESM STATUS message by an ESM entity

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

On receipt of an ESM 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 ESM STATUS message are implementation dependent.

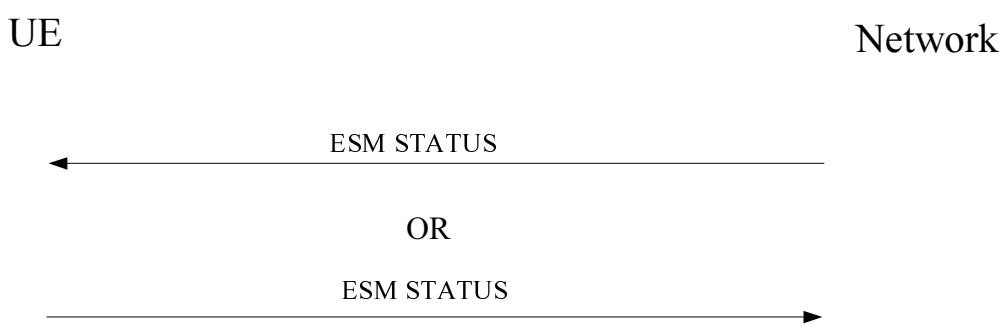

Figure 6.7.1: ESM status procedure

7 Handling of unknown, unforeseen, and erroneous protocol data

7.1 General

The procedures specified in the present document apply to those messages which pass the checks described in this subclause.

This subclause also specifies procedures for the handling of unknown, unforeseen, and erroneous protocol data by the receiving entity. These procedures are called "error handling procedures", but in addition to providing recovery mechanisms for error situations they define a compatibility mechanism for future extensions of the protocols.

Subclauses 7.1 to 7.8 shall be applied in order of precedence.

Most error handling procedures are mandatory for the UE.

Detailed error handling procedures in the network are implementation dependent and may vary from PLMN to PLMN. However, when extensions of this protocol are developed, networks will be assumed to have the error handling that is indicated in this subclause as mandatory ("shall") and that is indicated as strongly recommended ("should").

Also, the error handling of the network is only considered as mandatory or strongly recommended when certain thresholds for errors are not reached during a dedicated connection.

For definition of semantical and syntactical errors see 3GPP TS 24.007 [12], subclause 11.4.2.

7.2 Message too short

When a message is received that is too short to contain a complete message type information element, that message shall be ignored, cf. 3GPP TS 24.007 [12].

7.3 Unknown or unforeseen procedure transaction identity or EPS bearer identity

7.3.1 Procedure transaction identity

The following network procedures shall apply for handling an unknown, erroneous, or unforeseen PTI received in an ESM message:

a) If the network receives a PDN CONNECTIVITY REQUEST message with an unassigned or reserved PTI value, the network shall respond with a PDN CONNECTIVITY REJECT message including cause value #81, "invalid PTI value".

b) If the network receives a PDN DISCONNECT REQUEST message with an unassigned or reserved PTI value, the network shall respond with a PDN DISCONNECT REJECT message including cause value #81, "invalid PTI value".

c) If the network receives a BEARER RESOURCE MODIFICATION REQUEST message with an unassigned or reserved PTI value, the network shall respond with a BEARER RESOURCE MODIFICATION REJECT message including cause value #81, "invalid PTI value".

d) If the network receives an ESM message other than those listed in items a) through c) above with a reserved PTI value, the network shall ignore the message.

The following UE procedures shall apply for handling an unknown, erroneous, or unforeseen PTI received in an ESM message:

a) If the UE receives a PDN CONNECTIVITY REJECT message in which the PTI value is an assigned value that does not match any PTI in use, the UE shall ignore the message.

b) If the UE receives an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message in which the PTI value is an assigned value that does not match any PTI in use, the UE shall respond with an ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message including cause value #47, "PTI mismatch".

c) If the UE receives an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message which contains a reserved PTI value, the UE shall respond with an ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message including cause value #81, "invalid PTI value".

d) If the UE receives a PDN DISCONNECT REJECT message in which the PTI value is an assigned value that does not match any PTI in use, the UE shall ignore the message.

e) If the UE receives a BEARER RESOURCE MODIFICATION REJECT message in which the PTI value is an assigned value that does not match any PTI in use, the UE shall ignore the message.

f) If the UE receives a MODIFY EPS BEARER CONTEXT REQUEST message in which the PTI value is an assigned value that does not match any PTI in use, the UE shall respond with a MODIFY EPS BEARER CONTEXT REJECT message including cause value #47, "PTI mismatch".

g) If the UE receives a MODIFY EPS BEARER CONTEXT REQUEST message which contains a reserved PTI value, the UE shall respond with a MODIFY EPS BEARER CONTEXT REJECT message including cause value #81, "invalid PTI value".

h) If the UE receives an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message in which the PTI value is an assigned value that does not match any PTI in use, the UE shall respond with an ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message including cause value #47, "PTI mismatch".

i) If the UE receives an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message which contains a reserved PTI value, the UE shall respond with an ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message including cause value #81, "invalid PTI value".

j) If the UE receives a DEACTIVATE EPS BEARER CONTEXT REQUEST message in which the PTI value is an assigned value that does not match any PTI in use, the UE shall ignore the message.

k) If the UE receives an ESM INFORMATION REQUEST message in which the PTI value is an assigned value that does not match a PTI in use for a pending UE requested PDN connectivity procedure for which the ESM information transfer flag was set in the PDN CONNECTIVITY REQUEST message, the UE shall ignore the message.

l) If the UE receives an ESM message other than those listed in items a) through k) with a reserved PTI value, the UE shall ignore the message.

7.3.2 EPS bearer identity

The following network procedures shall apply for handling an unknown, erroneous, or unforeseen EPS bearer identity received in an ESM message:

a) If the network receives a PDN CONNECTIVITY REQUEST message which includes an assigned or reserved EPS bearer identity value, the network shall respond with a PDN CONNECTIVITY REJECT message including cause value #43, "unknown EPS bearer context".

b) If the network receives a PDN DISCONNECT REQUEST message which includes an unassigned or reserved EPS bearer identity value or a value that does not match the default EPS bearer context of an established PDN connection, the network shall respond with a PDN DISCONNECT REJECT message including cause value #43, "unknown EPS bearer context".

c) If the network receives a BEARER RESOURCE MODIFICATION REQUEST message which includes an unassigned or reserved EPS bearer identity value or a value that does not match an EPS bearer context of an established PDN connection, the network shall respond with a BEARER RESOURCE MODIFICATION REJECT message including cause value #43, "unknown EPS bearer context".

d) If the network receives an ESM message other than those listed in items a) through c) above in which the message includes an unassigned or reserved EPS bearer identity value or a value that does not match an EPS bearer context of an established PDN connection, the network shall ignore the message.

The following UE procedures shall apply for handling an unknown, erroneous, or unforeseen EPS bearer identity received in an ESM message:

a) If the UE receives an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message which includes an unassigned or reserved EPS bearer identity value, the UE shall respond with an ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message including cause value #43, "unknown EPS bearer context".

b) If the UE receives an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message which includes an unassigned or reserved EPS bearer identity value, the UE shall respond with an ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message including cause value #43, "unknown EPS bearer context".

c) If the UE receives a MODIFY EPS BEARER CONTEXT REQUEST message which includes an unassigned or reserved EPS bearer identity value, the UE shall respond with a MODIFY EPS BEARER CONTEXT REJECT message including cause value #43, "unknown EPS bearer context".

d) If the UE receives an ESM message other than those listed in items a) through c) in which the message includes an unassigned or reserved EPS bearer identity value or a value that does not match an EPS bearer context of an established PDN connection, the UE shall ignore the message.

7.4 Unknown or unforeseen message type

If UE receives an EMM message or ESM message with message type not defined for the protocol discriminator (PD) or not implemented by the receiver, it shall return a status message (EMM STATUS or ESM STATUS depending on the PD) with cause value #97, "message type non-existent or not implemented".

If the network receives an EMM or ESM message with message type not defined for the PD or not implemented by the receiver in a protocol state where reception of an unsolicited message with the given PD from the UE is not foreseen in the protocol, the network actions are implementation dependent. Otherwise, if the network receives a message with message type not defined for the PD or not implemented by the receiver, it shall ignore the message except that it should return a status message (EMM STATUS or ESM STATUS depending on the PD) with cause value #97, "message type non-existent or not implemented".

NOTE: A message type not defined for the PD in the given direction is regarded by the receiver as a message type not defined for the PD, see 3GPP TS 24.007 [12].

If the UE receives a message not compatible with the protocol state, the UE shall return a status message (EMM STATUS or ESM STATUS depending on the PD) with cause value #98, "message type not compatible with protocol state".

If the network receives a message not compatible with the protocol state, the network actions are implementation dependent.

7.5 Non-semantical mandatory information element errors

7.5.1 Common procedures

When on receipt of a message,

- an "imperative message part" error; or
- a "missing mandatory IE" error

is diagnosed or when a message containing:

- a syntactically incorrect mandatory IE;
- an IE unknown in the message, but encoded as "comprehension required" (see 3GPP TS 24.007 [12]); or
- an out of sequence IE encoded as "comprehension required" (see 3GPP TS 24.007 [12]) is received,

the UE shall proceed as follows:

If the message is not one of the messages listed in subclause 7.5.3, item a), c), d) or h), the UE shall return a status message (EMM STATUS or ESM STATUS depending on the PD) with cause value #96, "invalid mandatory information"; and

the network shall proceed as follows:

If the message is not one of the messages listed in subclause 7.5.3, item b), e), f), or g), the network shall either:

- try to treat the message (the exact further actions are implementation dependent); or
- ignore the message except that it should return a status message (EMM STATUS or ESM STATUS depending on the PD) with cause value #96, "invalid mandatory information".

7.5.2 EPS mobility management

No exceptional cases are described for mobility management messages.

No semantical or syntactical diagnosis other than presence and length shall be performed on the ESM message container information element in the ATTACH REQUEST, ATTACH ACCEPT and ATTACH COMPLETE messages.

7.5.3 EPS session management

a) If the message is a DEACTIVATE EPS BEARER CONTEXT REQUEST, a DEACTIVATE EPS BEARER CONTEXT ACCEPT message shall be returned. All resources associated with that EPS bearer shall be released.

b) If the message is a PDN DISCONNECT REQUEST, a DEACTIVATE EPS BEARER CONTEXT REQUEST message shall be returned. All EPS bearers associated shall be released.

c) If the message is an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST, an ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message with cause value #96, "invalid mandatory information", shall be returned.

d) If the message is an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST, an ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message with cause value #96, "invalid mandatory information", shall be returned.

e) If the message is a PDN CONNECTIVITY REQUEST, a PDN CONNECTIVITY REJECT message with cause value #96, "invalid mandatory information", shall be returned.

f) If the message is a BEARER RESOURCE MODIFICATION REQUEST, a BEARER RESOURCE MODIFICATION REJECT message with cause value #96, "invalid mandatory information", shall be returned.

g) If the message is a MODIFY EPS BEARER CONTEXT REQUEST, a MODIFY EPS BEARER CONTEXT REJECT message with cause value #96, "invalid mandatory information", shall be returned.

7.6 Unknown and unforeseen IEs in the non-imperative message part

7.6.1 IEIs unknown in the message

The UE shall ignore all IEs unknown in a message which are not encoded as "comprehension required" (see 3GPP TS 24.007 [12]).

The network shall take the same approach.

7.6.2 Out of sequence IEs

The UE shall ignore all out of sequence IEs in a message which are not encoded as "comprehension required" (see 3GPP TS 24.007 [12]).

The network should take the same approach.

7.6.3 Repeated IEs

If an information element with format T, TV, TLV, or TLV-E is repeated in a message in which repetition of the information element is not specified in clause 8 of the present document, the UE shall handle only the contents of the information element appearing first and shall ignore all subsequent repetitions of the information element. When repetition of information elements is specified, the UE shall handle only the contents of specified repeated information elements. If the limit on repetition of information elements is exceeded, the UE shall handle the contents of information elements appearing first up to the limit of repetitions and shall ignore all subsequent repetitions of the information element.

The network should follow the same procedures.

7.7 Non-imperative message part errors

This category includes:

- syntactically incorrect optional IEs; and
- conditional IE errors.

7.7.1 Syntactically incorrect optional IEs

The UE shall treat all optional IEs that are syntactically incorrect in a message as not present in the message.

The network shall take the same approach.

7.7.2 Conditional IE errors

When upon receipt of a EMM or ESM message the UE diagnoses a "missing conditional IE" error or an "unexpected conditional IE" error, or when it receives a EMM or ESM message containing at least one syntactically incorrect conditional IE, the UE shall ignore the message and shall return a status message (EMM STATUS or ESM STATUS depending on the PD) with cause value #100, "conditional IE error".

When the network receives a message and diagnoses a "missing conditional IE" error or an "unexpected conditional IE" error or when it receives a message containing at least one syntactically incorrect conditional IE, the network shall either:

- try to treat the message (the exact further actions are implementation dependent); or
- ignore the message except that it should return a status message (EMM STATUS or ESM STATUS depending on the PD) with cause value # 100, "conditional IE error".

7.8 Messages with semantically incorrect contents

When a message with semantically incorrect contents is received, the UE shall perform the foreseen reactions of the procedural part of the present document (i.e. of clauses 4, 5 and 6). If however no such reactions are specified, the UE shall ignore the message except that it shall return a status message (EMM STATUS or ESM STATUS depending on the PD) with cause value #95, "semantically incorrect message".

The network should follow the same procedure except that a status message is not normally transmitted.

8 Message functional definitions and contents

8.1 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 [12].

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, TLV and TLV-E formatted IEs which compose the non-imperative part of the message, see 3GPP TS 24.007 [12]). 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, TLV or TLV-E. 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 can 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 clause 9 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 [12].

   5. The format of the information element (T, V, TV, LV, TLV or TLV-E) as defined in 3GPP TS 24.007 [12].

   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 or non-presence of the IEs or for both cases (see 3GPP TS 24.007 [12]).

8.2 EPS mobility management 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, 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.

8.2.1 Attach accept

8.2.1.1 Message definition

This message is sent by the network to the UE to indicate that the corresponding attach request has been accepted. See table 8.2.1.1.

Message type: ATTACH ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.1.1: ATTACH ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach accept message identity	Message type 9.8	M	V	1
	EPS attach result	EPS attach result 9.9.3.10	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2
	T3412 value	GPRS timer 9.9.3.16	M	V	1
	TAI list	Tracking area identity list 9.9.3.33	M	LV	7-97
	ESM message container	ESM message container 9.9.3.15	M	LV-E	2-n
50	GUTI	EPS mobile identity 9.9.3.12	O	TLV	13
13	Location area identification	Location area identification 9.9.2.2	O	TV	6
23	MS identity	Mobile identity 9.9.2.3	O	TLV	7-10
53	EMM cause	EMM cause 9.9.3.9	O	TV	2
17	T3402 value	GPRS timer 9.9.3.16	O	TV	2
59	T3423 value	GPRS timer 9.9.3.16	O	TV	2
4A	Equivalent PLMNs	PLMN list 9.9.2.6	O	TLV	5-47

8.2.1.2 GUTI

This IE may be included to assign a GUTI to the UE during attach or combined EPS/IMSI attach.

8.2.1.3 Location area identification

This IE may be included to assign a new location area identification to a UE during a combined attach.

8.2.1.4 MS identity

This IE may be included to assign or unassign a new TMSI to a UE during a combined attach.

8.2.1.5 EMM cause

This IE shall be included when IMSI attach for non-EPS services is not successful during a combined EPS/IMSI attach procedure.

8.2.1.6 T3402 value

This IE may be included to indicate a value for timer T3402.

If this IE is not included, the UE shall use the default value.

8.2.1.7 T3423 value

This IE may be included to indicate a value for timer T3423.

If this IE is not included, the UE shall use the default value.

8.2.1.8 Equivalent PLMNs

This IE may be included in order to assign a new equivalent PLMNs list to a UE.

8.2.2 Attach complete

This message is sent by the UE to the network in response to an ATTACH ACCEPT message. See table 8.2.2.1.

Message type: ATTACH COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.2.1: ATTACH COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach complete message identity	Message type 9.8	M	V	1
	ESM message container	ESM message container 9.9.3.15	M	LV-E	2-n

8.2.3 Attach reject

8.2.3.1 Message definition

This message is sent by the network to the UE to indicate that the corresponding attach request has been rejected. See table 8.2.3.1.

Message type: ATTACH REJECT

Significance: dual

Direction: network to UE

Table 8.2.3.1: ATTACH REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach reject message identity	Message type 9.8	M	V	1
	EMM cause	EMM cause 9.9.3.9	M	V	1
78	ESM message container	ESM message container 9.9.3.15	O	TLV-E	4-n

8.2.3.2 ESM message container

This IE is included to carry a single ESM message.

8.2.4 Attach request

8.2.4.1 Message definition

This message is sent by the UE to the network in order to perform an attach procedure. See table 8.2.4.1.

Message type: ATTACH REQUEST

Significance: dual

Direction: UE to network

Table 8.2.4.1: ATTACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Attach request message identity	Message type 9.8	M	V	1
	EPS attach type	EPS attach type 9.9.3.11	M	V	1/2
	NAS key set identifier	NAS key set identifier 9.9.3.21	M	V	1/2
	Old GUTI or IMSI	EPS mobile identity 9.9.3.12	M	LV	5-12
	UE network capability	UE network capability 9.9.3.34	M	LV	3-14
	ESM message container	ESM message container 9.9.3.15	M	LV-E	2-n
52	Last visited registered TAI	Tracking area identity 9.9.3.32	O	TV	6
5C	DRX parameter	DRX parameter 9.9.3.8	O	TV	3
31	MS network capability	MS network capability 9.9.3.20	O	TLV	4-10
13	Old location area identification	Location area identification 9.9.2.2	O	TV	6
9-	TMSI status	TMSI status 9.9.3.31	O	TV	1
11	Mobile station classmark 2	Mobile station classmark 2 9.9.2.4	O	TLV	5
20	Mobile station classmark 3	Mobile station classmark 3 9.9.2.5	O	TLV	2-34
40	Supported Codecs	Supported Codec List 9.9.2.8	O	TLV	5-n

Editor's note: The length of the TAI is FFS.

8.2.4.2 Last visited registered TAI

This IE shall be included if the UE holds a valid last visited registered TAI.

8.2.4.3 DRX parameter

This IE is included by the UE if it wants to indicate UE specific DRX parameters to the network.

8.2.4.4 MS network capability

A UE supporting A/Gb mode or Iu mode shall include this IE to indicate its capabilities to the network.

8.2.4.5 Old location area identification

The UE shall include this IE during a combined attach procedure if it has a valid location area identification.

8.2.4.6 TMSI status

The UE shall include this IE during combined attach procedure if it has no valid TMSI available.

8.2.4.7 Mobile station classmark 2

This IE shall be included if the UE supports SRVCC to GERAN or UTRAN (see 3GPP TS 23.216 [8]).

8.2.4.8 Mobile station classmark 3

This IE shall be included if the UE supports SRVCC to GERAN.

8.2.4.9 Supported Codecs

This IE shall be included if the UE supports SRVCC to GERAN or UTRAN to indicate its supported speech codecs for CS speech calls.

8.2.5 Authentication failure

8.2.5.1 Message definition

This message is sent by the UE to the network to indicate that authentication of the network has failed. See table 8.2.5.1.

Message type: AUTHENTICATION FAILURE

Significance: dual

Direction: UE to network

Table 8.2.5.1: AUTHENTICATION FAILURE message content

IEI	Information element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Authentication failure message type	Message type 9.8	M	V	1
	EMM cause	EMM cause 9.9.3.9	M	V	1
30	Authentication failure parameter	Authentication failure parameter 9.9.3.1	O	TLV	16

8.2.5.2 Authentication failure parameter

This IE shall be sent if and only if the EMM cause was "Synch failure". It shall include the response to the authentication challenge from the USIM, which is made up of the AUTS parameter (see 3GPP TS 33.102 [18]).

8.2.6 Authentication reject

This message is sent by the network to the UE to indicate that the authentication procedure has failed and that the UE shall abort all activities. See table 8.2.6.1.

Message type: AUTHENTICATION REJECT

Significance: dual

Direction: network to UE

Table 8.2.6.1: AUTHENTICATION REJECT message content

IEI	Information element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Authentication reject message type	Message type 9.8	M	V	1

8.2.7 Authentication request

This message is sent by the network to the UE to initiate authentication of the UE identity. See table 8.2.7.1.

Message type: AUTHENTICATION REQUEST

Significance: dual

Direction: network to UE

Table 8.2.7.1: AUTHENTICATION REQUEST message content

IEI	Information element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Authentication request message type	Message type 9.8	M	V	1
	NAS key set identifier$_{ASME}$	NAS key set identifier 9.9.3.21	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2
	Authentication parameter RAND (EPS challenge)	Authentication parameter RAND 9.9.3.3	M	V	16
	Authentication parameter AUTN (EPS challenge)	Authentication parameter AUTN 9.9.3.2	M	LV	17

8.2.8 Authentication response

This message is sent by the UE to the network to deliver a calculated authentication response to the network. See table 8.2.8.1.

Message type: AUTHENTICATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.8.1: AUTHENTICATION RESPONSE message content

IEI	Information element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Authentication response message type	Message type 9.8	M	V	1
	Authentication response parameter	Authentication response parameter 9.9.3.4	M	LV	5-17

8.2.9 Detach accept

8.2.9.1 Detach accept (UE originating detach)

This message is sent by the network to indicate that the detach procedure has been completed. See table 8.2.9.1.1.

Message type: DETACH ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.9.1.1: DETACH ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Detach accept message identity	Message type 9.8	M	V	1

8.2.9.2 Detach accept (UE terminated detach)

This message is sent by the UE to indicate that the detach procedure has been completed. See table 8.2.9.2.1.

Message type: DETACH ACCEPT

Significance: dual

Direction: UE to network

Table 8.2.9.2.1: DETACH ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Detach accept message identity	Message type 9.8	M	V	1

8.2.10 Detach request

8.2.10.1 Detach request (UE originating detach)

This message is sent by the UE to request the release of an EMM context. See table 8.2.10.1.1.

Message type: DETACH REQUEST

Significance: dual

Direction: UE to network

Table 8.2.10.1.1: DETACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Detach request message identity	Message type 9.8	M	V	1
	Detach type	Detach type 9.9.3.7	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2
	GUTI or IMSI	EPS mobile identity 9.9.3.12	M	LV	5-12

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

8.2.10.2 Detach request (UE terminated detach)

8.2.10.2.1 Message definition

This message is sent by the network to request the release of an EMM context. See table 8.2.10.2.1.

Message type: DETACH REQUEST

Significance: dual

Direction: network to UE

Table 8.2.10.2.1: DETACH REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Detach request message identity	Message type 9.8	M	V	1
	Detach type	Detach type 9.9.3.7	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2
53	EMM cause	EMM cause 9.9.3.9	O	TV	2

8.2.10.2.2 EMM cause

This information element is included if an EMM cause is provided.

8.2.11 Downlink NAS Transport

This message is sent by the network to the UE in order to carry an SMS message in encapsulated format. See table 8.2.11.1.

Message type: DOWNLINK NAS TRANSPORT

Significance: dual

Direction: network to UE

Table 8.2.11.1: DOWNLINK NAS TRANSPORT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Downlink NAS transport message identity	Message type 9.8	M	V	1
	NAS message container	NAS message container 9.9.3.22	M	LV	3-252

8.2.12 EMM information

8.2.12.1 Message definition

This message is sent by the network at any time during EMM context is established to send certain information to the UE. See table 8.2.12.1.

Message type: EMM INFORMATION

Significance: local

Direction: network to UE

Table 8.2.12.1: EMM INFORMATION message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	EMM information message identity	Message type 9.8	M	V	1
43	Full name for network	Network name 9.9.3.24	O	TLV	3-?
45	Short name for network	Network name 9.9.3.24	O	TLV	3-?
46	Local time zone	Time zone 9.9.3.29	O	TV	2
47	Universal time and local time zone	Time zone and time 9.9.3.30	O	TV	8
49	Network daylight saving time	Daylight saving time 9.9.3.6	O	TLV	3

8.2.12.2 Full name for network

This IE may be sent by the network. If this IE is sent, the contents of this IE indicate the "full length name of the network" that the network wishes the UE to associate with the MCC and MNC contained in the last visited tracking area identification.

8.2.12.3 Short name for network

This IE may be sent by the network. If this IE is sent, the contents of this IE indicate the "abbreviated name of the network" that the network wishes the UE to associate with the MCC and MNC contained in the last visited tracking area identification.

8.2.12.4 Local time zone

This IE may be sent by the network. The UE should assume that this time zone applies to the tracking area of the current cell, and also applies to the tracking area list if available in the UE.

NOTE: The time information can be inaccurate, especially when the TAI list includes tracking areas belonging to different time zones.

If the local time zone has been adjusted for daylight saving time, the network shall indicate this by including the Network daylight saving time IE.

8.2.12.5 Universal time and local time zone

This IE may be sent by the network. The UE should assume that this time zone applies to the tracking area the UE is currently in, and also applies to the tracking area list if available in the UE. The UE shall not assume that the time information is accurate.

NOTE: The time information can be inaccurate, especially when the TAI list includes tracking areas belonging to different time zones.

If the local time zone has been adjusted for daylight saving time, the network shall indicate this by including the Network daylight saving time IE.

8.2.12.6 Network daylight saving time

This IE may be sent by the network. If this IE is sent, the contents of this IE indicates the value that has been used to adjust the local time zone.

8.2.13 EMM status

This message is sent by the UE or by the network at any time to report certain error conditions listed in clause 7. See table 8.2.13.1.

Message type: EMM STATUS

Significance: local

Direction: both

Table 8.2.13.1: EMM STATUS message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	EMM status message identity	Message type 9.8	M	V	1
	EMM cause	EMM cause 9.9.3.9	M	V	1

8.2.14 Extended service request

8.2.14.1 Message definition

This message is sent by the UE to the network to initiate a CS fallback call or respond to a mobile terminated CS fallback request from the network. See table 8.2.14.1.

Message type: EXTENDED SERVICE REQUEST

Significance: dual

Direction: UE to network

Table 8.2.14.1: EXTENDED SERVICE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Extended service request message identity	Message type 9.8	M	V	1
	Service type	Service type 9.9.3.27	M	V	1/2
	NAS key set identifier	NAS key set identifier 9.9.3.21	M	V	1/2
	M-TMSI	Mobile identity 9.9.2.3	M	LV	6
B-	CSFB response	CSFB response 9.9.3.5	C	TV	1

8.2.14.2 CSFB response

The UE shall include this IE only if the Service type information element indicates "mobile terminating CS fallback".

8.2.15 GUTI reallocation command

8.2.15.1 Message definition

This message is sent by the network to the UE to reallocate a GUTI and optionally to provide a new TAI list. See table 8.2.15.1.

Message type: GUTI REALLOCATION COMMAND

Significance: dual

Direction: network to UE

Table 8.2.15.1: GUTI REALLOCATION COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	GUTI reallocation command message identity	Message type 9.8	M	V	1
	GUTI	EPS mobile identity 9.9.3.12	M	LV	12
54	TAI list	Tracking area identity list 9.9.3.33	O	TLV	8-98

8.2.15.2 TAI list

This IE may be included to assign a TAI list to the UE.

8.2.16 GUTI reallocation complete

This message is sent by the UE to the network to indicate that reallocation of a GUTI has taken place. See table 8.2.16.1.

Message type: GUTI REALLOCATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.16.1: GUTI REALLOCATION COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	GUTI reallocation complete message identity	Message type 9.8	M	V	1

8.2.17 Identity request

This message is sent by the network to the UE to request the UE to provide the specified identity. See table 8.2.17.1.

Message type: IDENTITY REQUEST

Significance: dual

Direction: network to UE

Table 8.2.17.1: IDENTITY REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Identity request message identity	Message type 9.8	M	V	1
	Identity type	Identity type 2 9.9.3.17	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2

Editor's note: It is for further study whether when the IMEI is included that Message authentication code becomes mandatory.

8.2.18 Identity response

This message is sent by the UE to the network in response to an IDENTITY REQUEST message and provides the requested identity. See table 8.2.18.1.

Message type: IDENTITY RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.18.1: IDENTITY RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Identity response message	Message type 9.8	M	V	1
	Mobile identity	Mobile identity 9.9.2.3	M	LV	4-10

8.2.19 NAS CS service notification

Editor's note: This message is needed for CS fallback. The definition of the message is FFS.

8.2.20 Security mode command

8.2.20.1 Message definition

This message is sent by the network to the UE to establish NAS signalling security. See table 8.2.20.1.

Message type: SECURITY MODE COMMAND

Significance: dual

Direction: network to UE

Table 8.2.20.1: SECURITY MODE COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Security mode command message identity	Message type 9.8	M	V	1
	Selected NAS security algorithms	NAS security algorithms 9.9.3.23	M	V	1
	NAS key set identifier$_{ASME}$	NAS key set identifier 9.9.3.21	M	V	1/2
	NAS key set identifier$_{SGSN}$	NAS key set identifier 9.9.3.21	M	V	1/2
	Replayed UE security capabilities	UE security capability 9.9.3.36	M	LV	3-6
C-	IMEISV request	IMEISV request 9.9.3.18	O	TV	1
55	Replayed nonce$_{UE}$	Nonce 9.9.3.25	O	TV	5
56	Nonce$_{MME}$	Nonce 9.9.3.25	O	TV	5

8.2.20.2 IMEISV request

The MME may include this information element to request the UE to send its IMEISV with the corresponding SECURITY MODE COMPLETE message.

8.2.20.3 Replayed nonce$_{UE}$

The MME may include this information element to indicate to the UE to use the replayed nonce$_{UE}$.

8.2.20.4 $Nonce_{MME}$

The MME may include this information element to indicate to the UE to use the $nonce_{MME}$.

8.2.21 Security mode complete

8.2.21.1 Message definition

This message is sent by the UE to the network in response to a SECURITY MODE COMMAND message. See table 8.2.21.1.

Message type: SECURITY MODE COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.21.1: SECURITY MODE COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Security mode complete message identity	Message type 9.8	M	V	1
23	IMEISV	Mobile identity 9.9.2.3	O	TLV	11

8.2.21.2 IMEISV

The UE shall include this information element, if the IMEISV was requested within the corresponding SECURITY MODE COMMAND message.

8.2.22 Security mode reject

This message is sent by the UE to the network to indicate that the corresponding security mode command has been rejected. See table 8.2.22.1.

Message type: SECURITY MODE REJECT

Significance: dual

Direction: UE to network

Table 8.2.22.1: SECURITY MODE REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Security mode reject message identity	Message type 9.8	M	V	1
	EMM cause	EMM cause 9.9.3.9	M	V	1

8.2.23 Security protected NAS message

This message is sent by the UE or the network to transfer a NAS message together with the sequence number and the message authentication code protecting the message. See table 8.2.23.1.

Message type: SECURITY PROTECTED NAS MESSAGE

Significance: dual

Direction: both

Table 8.2.23.1: SECURITY PROTECTED NAS MESSAGE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Message authentication code	Message authentication code 9.5	M	V	4
	Sequence number	Sequence number 9.6	M	V	1
	NAS message	NAS message 9.7	M	V	1-n

8.2.24 Service reject

8.2.24.1 Message definition

This message is sent by the network to the UE in order to reject the service request procedure. See table 8.2.24.1.

Message type: SERVICE REJECT

Significance: dual

Direction: network to UE

Table 8.2.24.1: SERVICE REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Service reject message identity	Message type 9.8	M	V	1
	EMM cause	EMM cause 9.9.3.9	M	V	1
5B	T3442 value	GPRS timer 9.9.3.16	C	TV	2

8.2.24.2 T3442 value

The MME shall include this IE when the EMM cause value is #39, "CS domain temporarily not available".

8.2.25 Service request

This message is sent by the UE to the network to request the establishment of a NAS signalling connection and of the radio and S1 bearers. Its structure does not follow the structure of a standard layer 3 message. See table 8.2.25.1.

Message type: SERVICE REQUEST

Significance: dual

Direction: UE to network

Table 8.2.25.1: SERVICE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	KSI and sequence number	KSI and sequence number 9.9.3.19	M	V	1
	Message authentication code (short)	Short MAC 9.9.3.28	M	V	2

8.2.26 Tracking area update accept

8.2.26.1 Message definition

This message is sent by the network to the UE to provide the UE with EPS mobility management related data in response to a tracking area update request message. See table 8.2.26.1.

Message type: TRACKING AREA UPDATE ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.26.1: TRACKING AREA UPDATE ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Tracking area update accept message identity	Message type 9.8	M	V	1
	EPS update result	EPS update result 9.9.3.13	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2
5A	T3412 value	GPRS timer 9.9.3.16	O	TV	2
50	GUTI	EPS mobile identity 9.9.3.12	O	TLV	13
54	TAI list	Tracking area identity list 9.9.3.33	O	TLV	8-98
57	EPS bearer context status	EPS bearer context status 9.9.2.1	O	TLV	4
13	Location area identification	Location area identification 9.9.2.2	O	TV	6
23	MS identity	Mobile identity 9.9.2.3	O	TLV	7-10
53	EMM cause	EMM cause 9.9.3.9	O	TV	2
17	T3402 value	GPRS timer 9.9.3.16	O	TV	2
59	T3423 value	GPRS timer 9.9.3.16	O	TV	2
4A	Equivalent PLMNs	PLMN list 9.9.2.6	O	TLV	5-47

8.2.26.2 T3412 value

This IE may be included to indicate a value for timer T3412.

If this IE is not included, the UE shall use the value currently stored, e.g. from a prior ATTACH ACCEPT message.

8.2.26.3 GUTI

This IE may be included to assign a GUTI to a UE.

8.2.26.4 TAI list

This IE may be included to assign a TAI list to a UE.

8.2.26.5 EPS bearer context status

This IE shall be included if the network wants to indicate the EPS bearer contexts that are active for the UE in the network.

8.2.26.6 Location area identification

This IE may be included to assign a new location area identification to a UE during a combined TA/LA update.

8.2.26.7 MS identity

This IE may be included to assign or unassign a new TMSI to a UE during a combined TA/LA update.

8.2.26.8 EMM cause

This IE shall be included if the combined tracking area updating procedure was successful for EPS services only.

8.2.26.9 T3402 value

This IE may be included to indicate a value for timer T3402.

If this IE is not included, the UE shall use the default value.

8.2.26.10 T3423 value

This IE may be included to indicate a value for timer T3423.

If this IE is not included, the UE shall use the default value.

8.2.26.11 Equivalent PLMNs

This IE may be included in order to assign a new equivalent PLMNs list to a UE.

8.2.27 Tracking area update complete

This message shall be sent by the UE to the network in response to a tracking area update accept message if a GUTI has been changed. See table 8.2.27.1.

Message type: TRACKING AREA UPDATE COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.27.1: TRACKING AREA UPDATE COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Tracking area update complete message identity	Message type 9.8	M	V	1

8.2.28 Tracking area update reject

This message is sent by the network to the UE in order to reject the tracking area updating procedure. See table 8.2.28.1.

Message type: TRACKING AREA UPDATE REJECT

Significance: dual

Direction: network to UE

Table 8.2.28.1: TRACKING AREA UPDATE REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Tracking area update reject message identity	Message type 9.8	M	V	1
	EMM cause	EMM cause 9.9.3.9	M	V	1

8.2.29 Tracking area update request

8.2.29.1 Message definition

The purposes of sending the tracking area update request by the UE to the network are described in subclause 5.5.3.1. See table 8.2.29.1.

Message type: TRACKING AREA UPDATE REQUEST

Significance: dual

Direction: UE to network

Table 8.2.29.1: TRACKING AREA UPDATE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Tracking area update request message identity	Message type 9.8	M	V	1
	EPS update type	EPS update type 9.9.3.14	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2
	Old GUTI	EPS mobile identity 9.9.3.12	M	LV	12
	NAS key set identifier$_{ASME}$	NAS key set identifier 9.9.3.21	M	V	1/2
	NAS key set identifier$_{SGSN}$	NAS key set identifier 9.9.3.21	M	V	1/2
19	Old P-TMSI signature	P-TMSI signature 9.9.3.26	O	TV	4
50	Additional GUTI	EPS mobile identity 9.9.3.12	O	TLV	13
55	Nonce$_{UE}$	Nonce 9.9.3.25	O	TV	5
58	UE network capability	UE network capability 9.9.3.34	O	TLV	4-15
52	Last visited registered TAI	Tracking area identity 9.9.3.32	O	TV	6
5C	DRX parameter	DRX parameter 9.9.3.8	O	TV	3
A-	UE radio capability information update needed	UE radio capability information update needed 9.9.3.35	O	TV	1
57	EPS bearer context status	EPS bearer context status 9.9.2.1	O	TLV	4
31	MS network capability	MS network capability 9.9.3.20	O	TLV	4-10
13	Old location area identification	Location area identification 9.9.2.2	O	TV	6
9-	TMSI status	TMSI status 9.9.3.31	O	TV	1
11	Mobile station classmark 2	Mobile station classmark 2 9.9.2.4	O	TLV	5
20	Mobile station classmark 3	Mobile station classmark 3 9.9.2.5	O	TLV	2-34
40	Supported Codecs	Supported Codec List 9.9.2.8	O	TLV	5-n

8.2.29.2 Old P-TMSI signature

This IE is included if the UE holds a valid P-TMSI signature.

8.2.29.3 Additional GUTI

The UE shall include this IE if it holds a valid GUTI, the TIN indicates "P-TMSI" and the UE holds a valid P-TMSI and RAI.

8.2.29.4 Nonce$_{UE}$

This IE is included if the UE performs an A/Gb mode or Iu mode to S1 mode inter-system change in idle mode.

8.2.29.5 UE network capability

The UE shall include this IE, unless the UE performs a periodic tracking area updating procedure.

8.2.29.6 Last visited registered TAI

This IE shall be included if the UE holds a valid last visited registered TAI.

8.2.29.7 DRX parameter

This IE is included by the UE if it wants to indicate UE specific DRX parameters to the network.

8.2.29.8 UE radio capability information update needed

The UE shall include this IE if the UE radio capability information in the network needs to be updated.

8.2.29.9 EPS bearer context status

This IE shall be included if the UE wants to indicate the EPS bearer contexts that are active within the UE.

8.2.29.10 MS network capability

A UE supporting A/Gb mode or Iu mode shall include this IE, unless the UE performs a periodic tracking area updating procedure.

8.2.29.11 Old location area identification

The UE shall include this IE during a combined tracking area updating procedure if it has a valid location area identification.

8.2.29.12 TMSI status

The UE shall include this IE during a combined tracking area updating procedure if it has no valid TMSI available.

8.2.29.13 Mobile station classmark 2

This IE shall be included if the UE supports SRVCC to GERAN or UTRAN (see 3GPP TS 23.216 [8]).

8.2.29.14 Mobile station classmark 3

This IE shall be included if the UE supports SRVCC to GERAN.

8.2.29.15 Supported Codecs

This IE shall be included if the UE supports SRVCC to GERAN or UTRAN to indicate its supported speech codecs for CS speech calls.

8.2.30 Uplink NAS Transport

This message is sent by the UE to the network in order to carry an SMS message in encapsulated format. See table 8.2.30.1.

Message type: UPLINK NAS TRANSPORT

Significance: dual

Direction: UE to network

Table 8.2.30.1: UPLINK NAS TRANSPORT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	Security header type	Security header type 9.3.1	M	V	1/2
	Uplink NAS transport message identity	Message type 9.8	M	V	1
	NAS message container	NAS message container 9.9.3.22	M	LV	3-252

8.3 EPS session management messages

Editor's note: The layout of the message header, apart from the protocol discriminator, is FFS.

Editor's note: The detailed encoding of the information elements in all message is FFS. It is assumed that existing information elements in other specifications, e.g. 3GPP TS 24.008, 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.

8.3.1 Activate dedicated EPS bearer context accept

8.3.1.1 Message definition

This message is sent by the UE to the network to acknowledge activation of a dedicated EPS bearer context associated with the same PDN address(es) and APN as an already active EPS bearer context. See table 8.3.1.1.

Message type: ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT

Significance: dual

Direction: UE to network

Table 8.3.1.1: ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Activate dedicated EPS bearer context accept message identity	Message type 9.8	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.1.2 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.2 Activate dedicated EPS bearer context reject

8.3.2.1 Message definition

This message is sent by UE to the network to reject activation of a dedicated EPS bearer context. See table 8.3.2.1.

Message type: ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT

Significance: dual

Direction: UE to network

Table 8.3.2.1: ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Activate dedicated EPS bearer context reject message identity	Message type 9.8	M	V	1
	ESM cause	ESM cause 9.9.4.4	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.2.2 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.3 Activate dedicated EPS bearer context request

8.3.3.1 Message definition

This message is sent by the network to the UE to request activation of a dedicated EPS bearer context associated with the same PDN address(es) and APN as an already active default EPS bearer context. See table 8.3.3.1.

Message type: ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST

Significance: dual

Direction: network to UE

Table 8.3.3.1: ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Activate dedicated EPS bearer context request message identity	Message type 9.8	M	V	1
	Linked EPS bearer identity	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2
	EPS QoS	EPS quality of service 9.9.4.3	M	LV	2-10
	TFT	Traffic flow template 9.9.4.16	M	LV	2-256
5D	Transaction identifier	Transaction identifier 9.9.4.17	O	TLV	3-4
30	Negotiated QoS	Quality of service 9.9.4.12	O	TLV	14-18
32	Negotiated LLC SAPI	LLC service access point identifier 9.9.4.7	O	TV	2
8-	Radio priority	Radio priority 9.9.4.13	O	TV	1
34	Packet flow Identifier	Packet flow Identifier 9.9.4.8	O	TLV	3
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

Editor's note: The inclusion of the Negotiated LLC SAPI is FFS.

8.3.3.2 Transaction identifier

If the UE supports A/Gb mode or Iu mode or both, the network may include this IE

8.3.3.3 Negotiated QoS

If the UE supports A/Gb mode or Iu mode or both, the network may include the corresponding pre-Rel-8 QoS parameter values of a PDP context.

8.3.3.4 Negotiated LLC SAPI

If the UE supports A/Gb mode, the network may include this IE.

8.3.3.5 Radio priority

If the UE supports A/Gb mode, the network may include this IE.

8.3.3.6 Packet flow identifier

If the UE supports A/Gb mode, the network may include this IE. If the UE indicated in the UE Network Capability it does not support BSS packet flow procedures, then the MME shall not include this IE.

8.3.3.7 Protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.4 Activate default EPS bearer context accept

8.3.4.1 Message definition

This message is sent by the UE to the network to acknowledge activation of a default EPS bearer context. See table 8.3.4.1.

Message type: ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT

Significance: dual

Direction: UE to network

Table 8.3.4.1: ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Activate default EPS bearer context accept message identity	Message type 9.8	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.4.2 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.5 Activate default EPS bearer context reject

8.3.5.1 Message definition

This message is sent by UE to the network to reject activation of a default EPS bearer context. See table 8.3.5.1.

Message type: ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT

Significance: dual

Direction: UE to network

Table 8.3.5.1: ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Activate default EPS bearer context reject message identity	Message type 9.8	M	V	1
	ESM cause	ESM cause 9.9.4.4	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.5.2 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.6 Activate default EPS bearer context request

8.3.6.1 Message definition

This message is sent by the network to the UE to request activation of a default EPS bearer context. See table 8.3.6.1.

Message type: ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST

Significance: dual

Direction: network to UE

Table 8.3.6.1: ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Activate default EPS bearer context request message identity	Message type 9.8	M	V	1
	EPS QoS	EPS quality of service 9.9.4.3	M	LV	2-10
	Access point name	Access point name 9.9.4.1	M	LV	2-101
59	PDN address	PDN address 9.9.4.9	O	TLV	7-15
5D	Transaction identifier	Transaction identifier 9.9.4.17	O	TLV	3-4
30	Negotiated QoS	Quality of service 9.9.4.12	O	TLV	14-18
32	Negotiated LLC SAPI	LLC service access point identifier 9.9.4.7	O	TV	2
8-	Radio priority	Radio priority 9.9.4.13	O	TV	1
34	Packet flow Identifier	Packet flow Identifier 9.9.4.8	O	TLV	3
5E	APN-AMBR	APN aggregate maximum bit rate 9.9.4.2	O	TLV	4-8
58	ESM cause	ESM cause 9.9.4.4	O	TV	2
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

Editor's note: The inclusion of the Negotiated LLC SAPI is FFS.

8.3.6.2 PDN address

If the IP addresses of the UE are allocated during the default EPS bearer context activation procedure, this IE shall be included by the network to assign an IPv4 address or an IPv6 interface identifier or both to the UE.

8.3.6.3 Transaction identifier

If the UE supports A/Gb mode or Iu mode or both, the network may include this IE

8.3.6.4 Negotiated QoS

If the UE supports A/Gb mode or Iu mode or both, the network may include the corresponding pre-Rel-8 QoS parameter values of a PDP context.

8.3.6.5 Negotiated LLC SAPI

If the UE supports A/Gb mode, the network may include this IE.

8.3.6.6 Radio priority

If the UE supports A/Gb mode, the network may include this IE.

8.3.6.7 Packet flow identifier

If the UE supports A/Gb mode, the network may include this IE. If the UE indicated in the UE Network Capability it does not support BSS packet flow procedures, then the MME shall not include this IE.

8.3.6.8 APN-AMBR

This IE is included in the message when the network wishes to transmit the APN-AMBR to the UE for possible uplink policy enforcement.

8.3.6.9 ESM cause

The network shall include this IE, if the network allocated a PDN address of a PDN type which is different from the PDN type requested by the UE.

8.3.6.10 Protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.7 Bearer resource modification reject

8.3.7.1 Message definition

This message is sent by the network to the UE to reject the modification of a dedicated bearer resource. See table 8.3.7.1.

Message type: BEARER RESOURCE MODIFICATION REJECT

Significance: dual

Direction: network to UE

Table 8.3.7.1: BEARER RESOURCE MODIFICATION REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource modification reject message identity	Message type 9.8	M	V	1
	ESM cause	ESM cause 9.9.4.4	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.7.2 Protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.8 Bearer resource modification request

8.3.8.1 Message definition

This message is sent by the UE to the network to request the modification of a dedicated bearer resource. See table 8.3.8.1.

Message type: BEARER RESOURCE MODIFICATION REQUEST

Significance: dual

Direction: UE to network

Table 8.3.8.1: BEARER RESOURCE MODIFICATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Bearer resource modification request message identity	Message type 9.8	M	V	1
	Linked EPS bearer identity	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
5B	Required traffic flow QoS	EPS quality of service 9.9.4.3	O	TLV	3-11
58	ESM cause	ESM cause 9.9.4.4	O	TV	2
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.8.2 Required traffic flow QoS

This IE is included in the message when the UE requests a change of QoS for the indicated traffic flows.

8.3.8.3 ESM cause

This IE is included in the message when the UE requests the release of a dedicated bearer resource.

8.3.8.4 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.9 Deactivate EPS bearer context accept

8.3.9.1 Message definition

This message is sent by the UE to acknowledge deactivation of the EPS bearer context requested in the corresponding Deactivate EPS bearer context request message. See table 8.3.9.1.

Message type: DEACTIVATE EPS BEARER CONTEXT ACCEPT

Significance: dual

Direction: UE to network

Table 8.3.9.1: DEACTIVATE EPS BEARER CONTEXT ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Deactivate EPS bearer context accept message identity	Message type 9.8	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.9.2 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.10 Deactivate EPS bearer context request

8.3.10.1 Message definition

This message is sent by the network to request deactivation of an active EPS bearer context. See table 8.3.10.1.

Message type: DEACTIVATE EPS BEARER CONTEXT REQUEST

Significance: dual

Direction: network to UE

Table 8.3.10.1: DEACTIVATE EPS BEARER CONTEXT REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Deactivate EPS bearer context request message identity	Message type 9.8	M	V	1
	ESM cause	ESM cause 9.9.4.4	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.10.2 Protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.11 ESM information request

This message is sent by the network to the UE to request the UE to provide ESM information, i.e. protocol configuration options or APN or both. See table 8.3.11.1.

Message type: ESM INFORMATION REQUEST

Significance: dual

Direction: network to UE

Table 8.3.11.1: ESM INFORMATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	ESM information request message identity	Message type 9.8	M	V	1

8.3.12 ESM information response

8.3.12.1 Message definition

This message is sent by the UE to the network in response to an ESM INFORMATION REQUEST message and provides the requested ESM information. See table 8.3.12.1.

Message type: ESM INFORMATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.3.12.1: ESM INFORMATION RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	ESM information response message identity	Message type 9.8	M	V	1
28	Access point name	Access point name 9.9.4.1	O	TLV	3-102
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.12.2 Access point name

This IE is included in the message when the UE wishes to request network connectivity as defined by a certain access point name during the attach procedure.

8.3.12.3 Protocol configuration options

This IE is included in the message when, during the attach procedure, the UE wishes to transmit security protected (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.13 ESM status

This message is sent by the network or the UE to pass information on the status of the indicated EPS bearer context and report certain error conditions (e.g. as listed in clause 7). See table 8.3.13.1.

Message type: ESM STATUS

Significance: dual

Direction: both

Table 8.3.13.1: ESM STATUS message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	ESM status message identity	Message type 9.8	M	V	1
	ESM cause	ESM cause 9.9.4.4	M	V	1

8.3.14 Modify EPS bearer context accept

8.3.14.1 Message definition

This message is sent by the UE to the network to acknowledge the modification of an active EPS bearer context. See table 8.3.14.1.

Message type: MODIFY EPS BEARER CONTEXT ACCEPT

Significance: dual

Direction: UE to network

Table 8.3.14.1: MODIFY EPS BEARER CONTEXT ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Modify EPS bearer context accept message identity	Message type 9.8	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.14.2 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.15 Modify EPS bearer context reject

8.3.15.1 Message definition

This message is sent by the UE or the network to reject a modification of an active EPS bearer context. See table 8.3.15.1.

Message type: MODIFY EPS BEARER CONTEXT REJECT

Significance: dual

Direction: UE to network

Table 8.3.15.1: MODIFY EPS BEARER CONTEXT REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Modify EPS bearer context reject message identity	Message type 9.8	M	V	1
	ESM cause	ESM cause 9.9.4.4	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.15.2 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.16 Modify EPS bearer context request

8.3.16.1 Message definition

This message is sent by the network to the UE to request modification of an active EPS bearer context. See table 8.3.16.1.

Message type: MODIFY EPS BEARER CONTEXT REQUEST

Significance: dual

Direction: network to UE

Table 8.3.16.1: MODIFY EPS BEARER CONTEXT REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	Modify EPS bearer context request message identity	Message type 9.8	M	V	1
5B	New EPS QoS	EPS quality of service 9.9.4.3	O	TLV	3-11
36	TFT	Traffic flow template 9.9.4.16	O	TLV	3-257
30	New QoS	Quality of service 9.9.4.12	O	TLV	14-18
32	Negotiated LLC SAPI	LLC service access point identifier 9.9.4.7	O	TV	2
8-	Radio priority	Radio priority 9.9.4.13	O	TV	1
34	Packet flow Identifier	Packet flow Identifier 9.9.4.8	O	TLV	3
5E	APN-AMBR	APN aggregate maximum bit rate 9.9.4.2	O	TLV	4-8
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

Editor's note: The inclusion of the Negotiated LLC SAPI is FFS.

8.3.16.2 New EPS QoS

When the QoS of the EPS bearer context is modified, the network shall include the modified EPS QoS assigned to the EPS bearer context.

8.3.16.3 TFT

This IE provides the UE with packet filters.

8.3.16.4 New QoS

If the UE supports A/Gb mode or Iu mode or both, the network may include the corresponding pre-Rel-8 QoS parameter values of a PDP context.

8.3.16.5 Negotiated LLC SAPI

If the UE supports A/Gb mode, the network may include this IE.

8.3.16.6 Radio priority

If the UE supports A/Gb mode, the network may include this IE.

8.3.16.7 Packet flow identifier

If the UE supports A/Gb mode, the network may include this IE. If the UE indicated in the UE Network Capability it does not support BSS packet flow procedures, then the MME shall not include this IE.

8.3.16.8 APN-AMBR

This IE is included when the APN-AMBR has been changed by the network.

8.3.16.9 Protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.17 PDN connectivity reject

8.3.17.1 Message definition

This message is sent by the network to the UE to reject establishment of a PDN connection. See table 8.3.17.1.

Message type: PDN CONNECTIVITY REJECT

Significance: dual

Direction: network to UE

Table 8.3.17.1: PDN CONNECTIVITY REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	PDN connectivity reject message identity	Message type 9.8	M	V	1
	ESM cause	ESM cause 9.9.4.4	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.17.2 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.18 PDN connectivity request

8.3.18.1 Message definition

This message is sent by the UE to the network to initiate establishment of a PDN connection. See table 8.3.18.1.

Message type: PDN CONNECTIVITY REQUEST

Significance: dual

Direction: UE to network

Table 8.3.18.1: PDN CONNECTIVITY REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	PDN connectivity request message identity	Message type 9.8	M	V	1
	Request type	Request type 9.9.4.14	M	V	1/2
	PDN type	PDN type 9.9.4.10	M	V	1/2
D-	ESM information transfer flag	ESM information transfer flag 9.9.4.5	O	TV	1
28	Access point name	Access point name 9.9.4.1	O	TLV	3-102
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.18.2 ESM information transfer flag

The UE shall include this IE in the PDN CONNECTIVITY REQUEST message sent during the attach procedure if the UE has protocol configuration options that need to be transferred security protected or wishes to provide an access point name for the PDN connection to be established during the attach procedure.

8.3.18.3 Access point name

This IE is included in the message when the UE wishes to request network connectivity as defined by a certain access point name. This IE shall not be included when the PDN CONNECTIVITY REQUEST message is included in an ATTACH REQUEST message.

8.3.18.4 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.19 PDN disconnect reject

8.3.19.1 Message definition

This message is sent by the network to the UE to reject release of a PDN connection. See table 8.3.19.1.

Message type: PDN DISCONNECT REJECT

Significance: dual

Direction: network to UE

Table 8.3.19.1: PDN DISCONNECT REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	PDN disconnect reject message identity	Message type 9.8	M	V	1
	ESM cause	ESM cause 9.9.4.4	M	V	1
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.19.2 Protocol configuration options

This IE is included in the message when the network wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.20 PDN disconnect request

8.3.20.1 Message definition

This message is sent by the UE to the network to initiate release of a PDN connection. See table 8.3.20.1.

Message type: PDN DISCONNECT REQUEST

Significance: dual

Direction: UE to network

Table 8.3.20.1: PDN DISCONNECT REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 9.2	M	V	1/2
	EPS bearer identity	EPS bearer identity 9.3.2	M	V	1/2
	Procedure transaction identity	Procedure transaction identity 9.4	M	V	1
	PDN disconnect request message identity	Message type 9.8	M	V	1
	Linked EPS bearer identity	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.7	M	V	1/2
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.20.2 Protocol configuration options

This IE is included in the message when the UE wishes to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

9 General message format and information elements coding

9.1 Overview

Within the protocols defined in the present document, every message, except the SERVICE REQUEST message, is a standard L3 message as defined in 3GPP TS 24.007 [12]. This means that the message consists of the following parts:

1) if the message is a plain NAS message:
   a) protocol discriminator;
   b) EPS bearer identity or security header type;
   c) procedure transaction identity;
   d) message type;
   e) other information elements, as required.
2) if the message is a security protected NAS message:
   a) protocol discriminator;
   b) security header type;
   c) message authentication code;
   d) sequence number;
   e) plain NAS message, as defined in item 1.

The organization of a plain NAS message is illustrated in the example shown in figure 9.1.1.

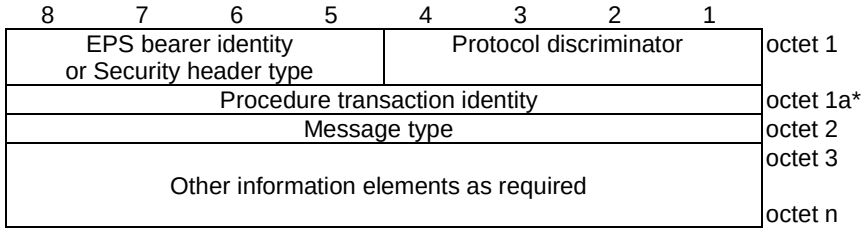

Figure 9.1.1: General message organization example for a plain NAS message

The organization of a security protected NAS message is illustrated in the example shown in figure 9.1.2.

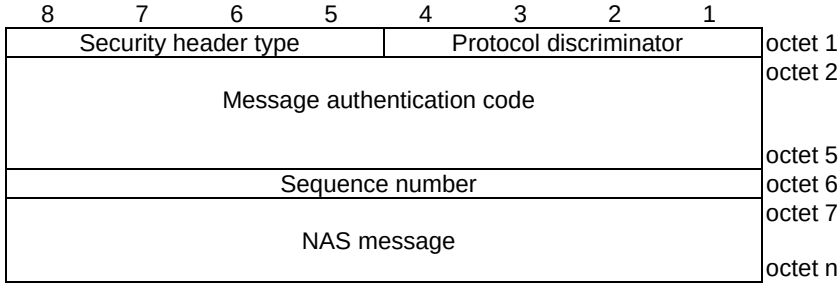

Figure 9.1.2: General message organization example for a security protected NAS message

The EPS bearer identity and the procedure transaction identity are only used in messages with protocol discriminator EPS session management. Octet 1a with the procedure transaction identity shall only be included in these messages.

Unless specified otherwise in the message descriptions of clause 8, 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.

9.2 Protocol discriminator

The Protocol Discriminator (PD) and its use are defined in 3GPP TS 24.007 [12].

9.3 Security header type and EPS bearer identity

9.3.1 Security header type

Bits 5 to 8 of the first octet of every EPS Mobility Management (EMM) message contain the Security header type IE. This IE includes control information related to the security protection of a NAS message. The total size of the Security header type IE is 4 bits.

The Security header type IE can take the values shown in table 9.3.1.

Table 9.3.1: Security header type

Security header type (octet 1)				
8	**7**	**6**	**5**	
0	0	0	0	Plain NAS message, not security protected
				Security protected NAS message:
0	0	0	1	Integrity protected
0	0	1	0	Integrity protected and ciphered
0	0	1	1	Integrity protected with new EPS security context (NOTE 1)
0	1	0	0	Integrity protected and ciphered with new EPS security context (NOTE 2)
				Non-standard L3 message:
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". (NOTE 3)
1	1	1	1	
All other values are reserved.				

NOTE 1: This codepoint may be used only for a SECURITY MODE COMMAND message.
NOTE 2: This codepoint may be used only for a SECURITY MODE COMPLETE message.
NOTE 3: When bits 7 and 8 are set to '11', bits 5 and 6 can be used for future extensions of the SERVICE REQUEST message.

An EMM message received with the security header type encoded as 0000 shall be treated as not security protected, plain NAS message. A protocol entity sending a not security protected EMM message shall send the message as plain NAS message and encode the security header type as 0000.

9.3.2 EPS bearer identity

Bits 5 to 8 of the first octet of every EPS Session Management (ESM) message contain the EPS bearer identity. The EPS bearer identity and its use to identify a message flow are defined in 3GPP TS 24.007 [12].

9.4 Procedure transaction identity

Bits 1 to 8 of the second octet (octet 1a) of every EPS Session Management (ESM) message contain the procedure transaction identity. The procedure transaction identity and its use are defined in 3GPP TS 24.007 [12].

9.5 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 [19], and the integrity protection shall include octet 6 to n of the SECURITY PROTECTED NAS MESSAGE, i.e. the Sequence Number IE and the NAS message IE. In addition to the data that is to be integrity protected, the constant BEARER ID, DIRECTION bit and COUNT are input to the MAC algorithm. The BEARER ID is defined in TS 33.401 [19], the DIRECTION bit is 1 for uplink and 0 for downlink and the 32-bit COUNT is constructed as a padding octet (0x00) followed by the 16-bit overflow counter followed by the 8-bit sequence number for the NAS message. The MAC IE shall be included in the security protected NAS message if a valid NAS security context exists and security functions are started.

Editor's note: The detailed description of the input of the integrity protection algorithm will be moved to a different part of this specification.

9.6 Sequence number

This IE includes the NAS message sequence number (SN).

Editor's note: The usage of the sequence number is FFS.

9.7 NAS message

This IE includes a complete plain NAS message as specified in subclause 8.2 and 8.3. The SECURITY PROTECTED NAS MESSAGE and the SERVICE REQUEST message are not plain NAS messages and shall not be included in this IE.

9.8 Message type

The message type IE and its use are defined in 3GPP TS 24.007 [12]. Tables 9.8.1 and 9.8.2 define the value part of the message type IE used in the EPS mobility management protocol and EPS session management protocol.

Table 9.8.1: Message types for EPS mobility management

Bits 8	7	6	5	4	3	2	1	
0	1	-	-	-	-	-	-	EPS 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	Extended 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
0	1	1	0	0	0	1	0	Downlink NAS transport
0	1	1	0	0	0	1	1	Uplink NAS transport

Table 9.8.2: Message types for EPS session management

Bits 8	7	6	5	4	3	2	1	
1	1	-	-	-	-	-	-	EPS session management messages
1	1	0	0	0	0	0	1	Activate default EPS bearer context request
1	1	0	0	0	0	1	0	Activate default EPS bearer context accept
1	1	0	0	0	0	1	1	Activate default EPS bearer context reject
1	1	0	0	0	1	0	1	Activate dedicated EPS bearer context request
1	1	0	0	0	1	1	0	Activate dedicated EPS bearer context accept
1	1	0	0	0	1	1	1	Activate dedicated EPS bearer context reject
1	1	0	0	1	0	0	1	Modify EPS bearer context request
1	1	0	0	1	0	1	0	Modify EPS bearer context accept
1	1	0	0	1	0	1	1	Modify EPS bearer context reject
1	1	0	0	1	1	0	1	Deactivate EPS bearer context request
1	1	0	0	1	1	1	0	Deactivate EPS bearer context accept
1	1	0	1	0	0	0	0	PDN connectivity request
1	1	0	1	0	0	0	1	PDN connectivity reject
1	1	0	1	0	0	1	0	PDN disconnect request
1	1	0	1	0	0	1	1	PDN disconnect reject
1	1	0	1	0	1	0	0	Bearer resource modification request
1	1	0	1	0	1	0	1	Bearer resource modification reject
1	1	0	1	1	0	0	1	ESM information request
1	1	0	1	1	0	1	0	ESM information response
1	1	1	0	1	0	0	0	ESM status

9.9 Other information elements

9.9.1 General

The different formats (V, LV, T, TV, TLV, TLV-E) and the five categories of information elements (type 1, 2, 3, 4 and 6) are defined in 3GPP TS 24.007 [12].

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 [12]).

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 9.9.2.

The information elements of the EMM or ESM protocols can be defined by reference to an appropriate specification, e.g., "see subclause 10.5.6.3 in 3GPP TS 24.008 [13]".

9.9.2 Common information elements

9.9.2.1 EPS bearer context status

The purpose of the EPS bearer context status information element is to indicate the state of each EPS bearer context that can be identified by an EPS bearer identity.

The EPS bearer context status information element is coded as shown in figure 9.9.2.1.1 and table 9.9.2.1.1.

The EPS bearer context status information element is a type 4 information element with 4 octets length.

8	7	6	5	4	3	2	1	
EPS bearer context status IEI								octet 1
Length of EPS bearer context status contents								octet 2
EBI (7)	EBI (6)	EBI (5)	EBI (4)	EBI (3)	EBI (2)	EBI (1)	EBI (0)	octet 3
EBI (15)	EBI (14)	EBI (13)	EBI (12)	EBI (11)	EBI (10)	EBI (9)	EBI (8)	octet 4

Figure 9.9.2.1.1: EPS bearer context status information element

Table 9.9.2.1.1: EPS bearer context status information element

EBI(x) shall be coded as follows:

EBI(0) - EBI(4):
Bits 0 to 4 of octet 3 are spare and shall be coded as zero.

EBI(5) – EBI(15):
0 indicates that the ESM state of the corresponding EPS bearer context is BEARER CONTEXT-INACTIVE.
1 indicates that the ESM state of the corresponding EPS bearer context is BEARER CONTEXT-ACTIVE.

9.9.2.2 Location area identification

See subclause 10.5.1.3 in 3GPP TS 24.008 [13].

9.9.2.3 Mobile identity

See subclause 10.5.1.4 in 3GPP TS 24.008 [13].

9.9.2.4 Mobile station classmark 2

See subclause 10.5.1.6 in 3GPP TS 24.008 [13].

9.9.2.5 Mobile station classmark 3

See subclause 10.5.1.7 in 3GPP TS 24.008 [13].

9.9.2.6 PLMN list

See subclause 10.5.1.13 in 3GPP TS 24.008 [13].

9.9.2.7 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.

9.9.2.8 Supported codec list

See subclause 10.5.4.32 in 3GPP TS 24.008 [13].

9.9.3 EPS Mobility Management (EMM) information elements

9.9.3.1 Authentication failure parameter

See subclause 10.5.3.2.2 in 3GPP TS 24.008 [13].

9.9.3.2 Authentication parameter AUTN

See subclause 10.5.3.1.1 in 3GPP TS 24.008 [13].

9.9.3.3 Authentication parameter RAND

See subclause 10.5.3.1 in 3GPP TS 24.008 [13].

9.9.3.4 Authentication response parameter

The purpose of the Authentication response parameter information element is to provide the network with the authentication response calculated in the USIM.

The Authentication response parameter information element is coded as shown in figure 9.9.3.4.1 and table 9.9.3.4.1.

The Authentication response parameter is a type 4 information element with a minimum length of 6 octets and a maximum length of 18 octets.

In an EPS authentication challenge, the response calculated in the USIM (RES) is minimum 4 octets and may be up to 16 octets in length.

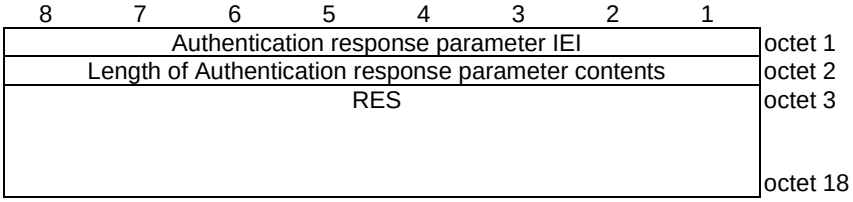

Figure 9.9.3.4.1: Authentication response parameter information element

Table 9.9.3.4.1: Authentication response parameter information element

RES value (octet 3 to 18) This contains the RES.

9.9.3.5 CSFB response

The purpose of the CSFB response information element is to indicate whether the UE accepts or rejects a paging for CS fallback.

The CSFB response information element is coded as shown in figure 9.9.3.5.1 and table 9.9.3.5.1.

The CSFB response is a type 1 information element.

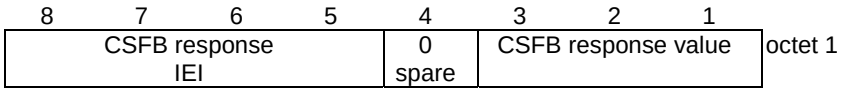

Figure 9.9.3.5.1: CSFB response information element

Table 9.9.3.5.1: CSFB response information element

CSFB response value (octet 1)			
Bits			
3	**2**	**1**	
0	0	0	CS fallback rejected by the UE
0	0	1	CS fallback accepted by the UE
All other values are reserved.			

9.9.3.6 Daylight saving time

See subclause 10.5.3.12 in 3GPP TS 24.008 [13].

9.9.3.7 Detach type

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

The Detach type information element is coded as shown in figure 9.9.3.7.1 and table 9.9.3.7.1.

The Detach type is a type 1 information element.

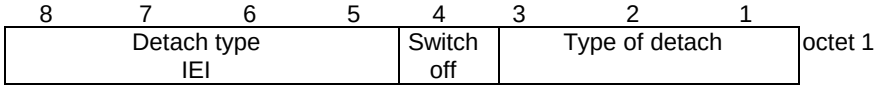

Figure 9.9.3.7.1: Detach type information element

Table 9.9.3.7.1: Detach type information element

Type of detach (octet 1)

In the UE to network direction:
Bits

3	**2**	**1**	
0	0	1	EPS detach
0	1	0	IMSI detach
0	1	1	combined EPS/IMSI detach

All other values are interpreted as "combined EPS/IMSI detach" in this version of the protocol.

In the network to UE direction:
Bits

3	**2**	**1**	
0	0	1	re-attach required
0	1	0	re-attach not required
0	1	1	IMSI detach

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

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.

9.9.3.8 DRX parameter

See subclause 10.5.5.6 in 3GPP TS 24.008 [13].

9.9.3.9 EMM cause

The purpose of the EMM cause information element is to indicate the reason why an EMM request from the UE is rejected by the network.

The EMM cause information element is coded as shown in figure 9.9.3.9.1 and table 9.9.3.9.1.

The EMM cause is a type 3 information element with 2 octets length.

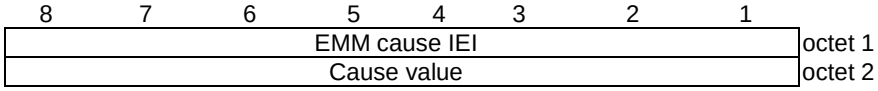

Figure 9.9.3.9.1: EMM cause information element

Table 9.9.3.9.1: EMM cause information element

Cause value (octet 2)

Bits

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	1	0	IMSI unknown in HSS
0	0	0	0	0	0	1	1	Illegal UE
0	0	0	0	0	1	1	0	Illegal ME
0	0	0	0	0	1	1	1	EPS services not allowed
0	0	0	0	1	0	0	0	EPS services and non-EPS services not allowed
0	0	0	0	1	0	0	1	UE identity cannot be derived by the network
0	0	0	0	1	0	1	0	Implicitly detached
0	0	0	0	1	0	1	1	PLMN not allowed
0	0	0	0	1	1	0	0	Tracking Area not allowed
0	0	0	0	1	1	0	1	Roaming not allowed in this tracking area
0	0	0	0	1	1	1	0	EPS services not allowed in this PLMN
0	0	0	0	1	1	1	1	No Suitable Cells In tracking area
0	0	0	1	0	0	0	0	MSC temporarily not reachable
0	0	0	1	0	0	0	1	Network failure
0	0	0	1	0	0	1	0	CS domain not available
0	0	0	1	0	0	1	1	ESM failure
0	0	0	1	0	1	0	0	MAC failure
0	0	0	1	0	1	0	1	Synch failure
0	0	0	1	0	1	1	0	Congestion
0	0	0	1	0	1	1	1	UE security capabilities mismatch
0	0	0	1	1	0	0	0	Security mode rejected, unspecified
0	0	0	1	1	0	0	1	Not authorized for this CSG
0	0	1	0	0	1	1	0	CS fallback call establishment not allowed
0	0	1	0	0	1	1	1	CS domain temporarily not available
0	0	1	0	1	0	0	0	No EPS bearer context activated
0	1	0	1	1	1	1	1	Semantically incorrect message
0	1	1	0	0	0	0	0	Invalid mandatory information
0	1	1	0	0	0	0	1	Message type non-existent or not implemented
0	1	1	0	0	0	1	0	Message type not compatible with the protocol state
0	1	1	0	0	0	1	1	Information element non-existent or not implemented
0	1	1	0	0	1	0	0	Conditional IE error
0	1	1	0	0	1	0	1	Message not compatible with the protocol state
0	1	1	0	1	1	1	1	Protocol error, unspecified

Any other value received by the mobile station shall be treated as 0110 1111, "Protocol error, unspecified". Any other value received by the network shall be treated as 0110 1111, "Protocol error, unspecified".

9.9.3.10 EPS attach result

The purpose of the EPS attach result information element is to specify the result of an attach procedure.

The EPS attach result information element is coded as shown in figure 9.9.3.10.1 and table 9.9.3.10.1.

The EPS attach result is a type 1 information element.

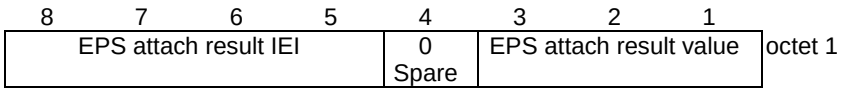

Figure 9.9.3.10.1: EPS attach result information element

Table 9.9.3.10.1: EPS attach result information element

EPS attach result value (octet 1) Bits **3 2 1** 0 0 1 EPS only 0 1 0 combined EPS/IMSI attach All other values are reserved. Bit 4 of octet 1 is spare and shall be coded as zero.

9.9.3.11 EPS attach type

The purpose of the EPS attach type information element is to indicate the type of the requested attach.

The EPS attach type information element is coded as shown in figure 9.9.3.11.1 and table 9.9.3.11.1.

The EPS attach type is a type 1 information element.

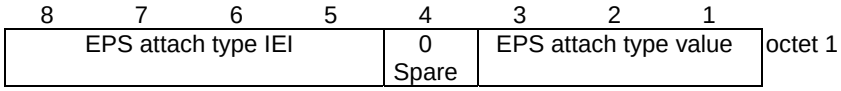

Figure 9.9.3.11.1: EPS attach type information element

Table 9.9.3.11.1: EPS attach type information element

EPS attach type value (octet 1) Bits **3 2 1** 0 0 1 EPS attach 0 1 0 combined EPS/IMSI attach All other values are unused and shall be interpreted as "EPS attach", if received by the network. Bit 4 of octet 1 is spare and shall be coded as zero.

9.9.3.12 EPS mobile identity

The purpose of the EPS mobile identity information element is to provide either the IMSI or the GUTI. If the information element is sent by the UE and the UE has a valid GUTI, the EPS mobile identity is populated with the GUTI value. When the UE does not have a valid GUTI, the UE populates this IE with its IMSI value.

The EPS mobile identity information element is coded as shown in figures 9.9.3.12.1 and 9.9.3.12.2 and table 9.9.3.12.1.

The EPS mobile identity is a type 4 information element with a minimum length of 3 octets and a maximum length of 13 octets.

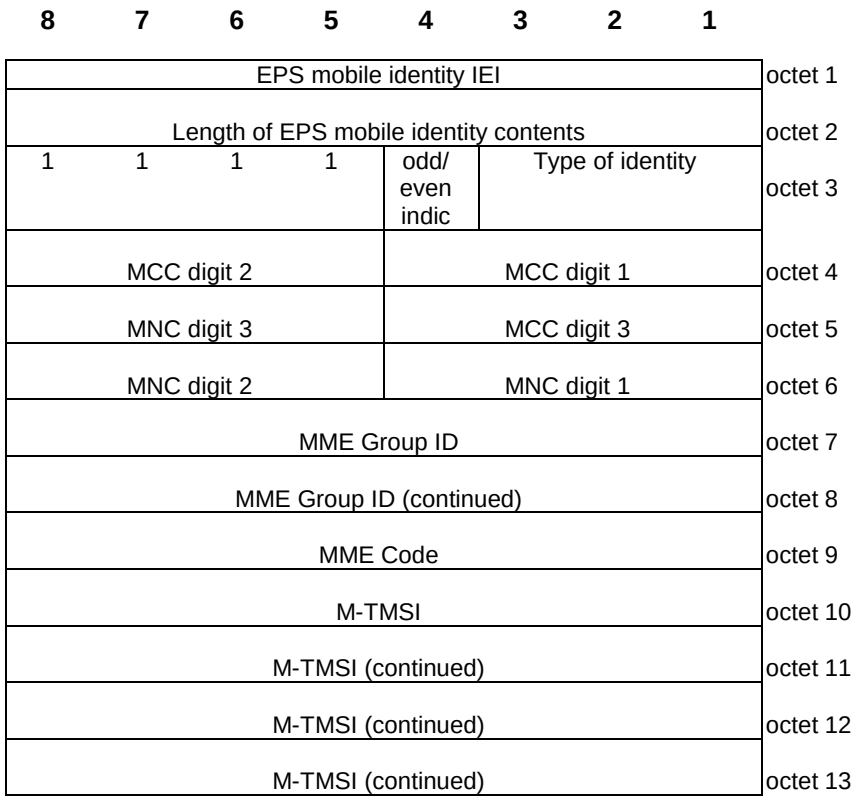

Figure 9.9.3.12.1: EPS mobile identity information element for type of identity "GUTI"

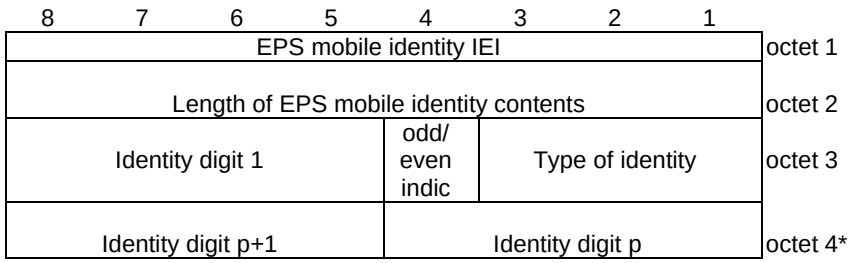

Figure 9.9.3.12.2: EPS mobile identity information element for type of identity "IMSI"

Table 9.9.3.12.1: EPS mobile identity information element

Type of identity (octet 3)
Bits

3	**2**	**1**	
0	0	1	IMSI
1	1	0	GUTI

All other values are reserved.

Odd/even indication (octet 3)
Bit

4	
0	even number of identity digits and also when the GUTI is used
1	odd number of identity digits

Identity digits (octet 4 etc)

For the IMSI, 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 the GUTI, then bits 5 to 8 of octet 3 are coded as "1111", octet 4 through 6 contain the MCC and MNC values as specified below, and bit 8 of octet 7 is the most significant bit and bit 1 of the last octet the least significant bit for the subsequent fields. The required fields for the GUTI are as defined in 3GPP TS 23.003 [2].

MCC, Mobile country code (octet 3, octet 4 bits 1 to 4)

The MCC field is coded as in ITU-T Recommendation E.212 [30], Annex A.

MNC, Mobile network code (octet 4 bits 5 to 8, octet 5)

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 of 3GPP TS 24.008 [13].

9.9.3.13 EPS update result

The purpose of the EPS update result information element is to specify the result of the associated updating procedure.

The EPS update type information element is coded as shown in figure 9.9.3.13.1 and table 9.9.3.13.1.

The EPS update type is a type 1 information element.

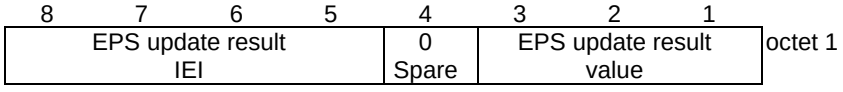

Figure 9.9.3.13.1: EPS update result information element

Table 9.9.3.13.1: EPS update result information element

EPS update result value (octet 1, bit 1 to 3) Bits **3 2 1** 0 0 0 TA updated 0 0 1 combined TA/LA updated 1 0 0 TA updated and ISR activated (NOTE) 1 0 1 combined TA/LA updated and ISR activated (NOTE) All other values are reserved. Bit 4 of octet 1 is spare and shall be coded as zero.
NOTE: Values 'TA updated and ISR activated' and 'combined TA/LA updated and ISR activated' are used only for a UE supporting also A/Gb or Iu mode.

9.9.3.14 EPS update type

The purpose of the EPS update type information element is to specify the area the updating procedure is associated with.

The ESP update type information element is coded as shown in figure 9.9.3.14.1 and table 9.9.3.14.1.

The EPS update type is a type 1 information element.

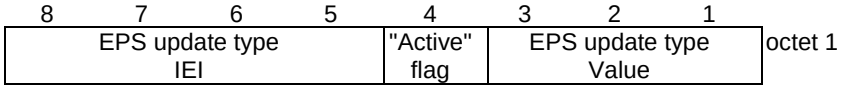

Figure 9.9.3.14.1: EPS update type information element

Table 9.9.3.14.1: EPS update type information element

EPS update type value (octet 1, bit 1 to 3) Bits **3 2 1** 0 0 0 TA updating 0 0 1 Combined TA/LA updating 0 1 0 Combined TA/LA updating with IMSI attach 0 1 1 Periodic updating All other values are reserved. "Active" flag (octet 1, bit 4) Bit **4** 0 No bearer establishment requested 1 Bearer establishment requested

9.9.3.15 ESM message container

The purpose of the ESM message container information element is to enable piggybacked transfer of a single ESM message within an EMM message. The ESM message included in this IE shall be coded as specified in subclause 8.3, i.e. without NAS security header.

The ESM message container information element is coded as shown in figure 9.9.3.15.1 and table 9.9.3.15.1.

The ESM message container is a type 6 information element.

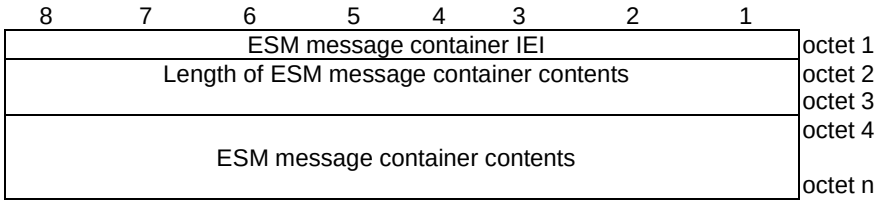

Figure 9.9.3.15.1: ESM message container information element

Table 9.9.3.15.1: ESM message container information element

ESM message container contents (octet 4 to octet n) ; Max value of 65535 octets This IE can contain any ESM PDU as defined in subclause 8.3.

9.9.3.16 GPRS timer

See subclause 10.5.7.3 in 3GPP TS 24.008 [13].

9.9.3.17 Identity type 2

See subclause 10.5.5.9 in 3GPP TS 24.008 [13].

9.9.3.18 IMEISV request

See subclause 10.5.5.10 in 3GPP TS 24.008 [13].

9.9.3.19 KSI and sequence number

The purpose of the KSI and sequence number information element is to provide the network with the key set identifier KSI_{asme} and the 5 least significant bits of the NAS COUNT value applicable for the message including this information element.

The KSI and sequence number information element is coded as shown in figure 9.9.3.19.1 and table 9.9.3.19.1.

The KSI and sequence number is a type 3 information element with a length of 2 octets.

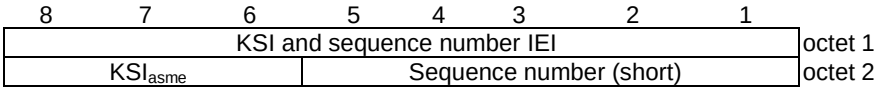

Figure 9.9.3.19.1: KSI and sequence number information element

Table 9.9.3.19.1: KSI and sequence number information element

Sequence number (short) (octet 2, bit 1 to 5) This field contains the 5 least significant bits of the NAS COUNT value applicable when this message is sent. KSI_{asme} (octet 2, bit 6 to 8) This field contains the key sequence number as specified in subclause (FFS).

Editor's note: The reference in the definition of the field KSI_{asme} needs to be added, when the NAS key set identifier IE has been specified.

9.9.3.20 MS network capability

See subclause 10.5.5.12 in 3GPP TS 24.008 [13].

9.9.3.21 NAS key set identifier

The NAS key set identifier is allocated by the network.

The NAS key set identifier information element is coded as shown in figure 9.9.3.21.1 and table 9.9.3.21.1.

The NAS key set identifier is a type 1 information element.

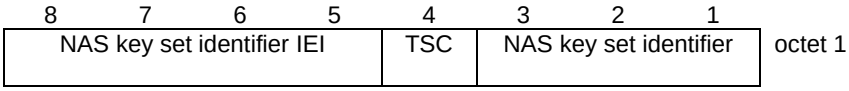

Figure 9.9.3.21.1: NAS key set identifier information element

Table 9.9.3.21.1: NAS key set identifier information element

Type of security context flag (TSC) (octet 1) Bit **4** 0 cached security context 1 mapped security context TSC does not apply for NAS key set identifier value "111". NAS key set identifier (octet 1) Bits **3 2 1** 0 0 0 through possible values for the NAS key set identifier 1 1 0 1 1 1 no key is available

9.9.3.22 NAS message container

Editor's note: The definition of this IE is FFS.

9.9.3.23 NAS security algorithms

The purpose of the NAS security algorithms information element is to indicate the algorithms to be used for ciphering and integrity protection.

The NAS security algorithms information element is coded as shown in figure 9.9.3.23.1 and table 9.9.3.23.1.

The NAS security algorithms is a type 3 information element with a length of 2 octets.

8	7	6	5	4	3	2	1	
NAS security algorithms IEI								octet 1
0 spare	Type of ciphering algorithm			0 spare	Type of integrity protection algorithm			octet 2

Figure 9.9.3.23.1: NAS security algorithms information element

Table 9.9.3.23.1: NAS security algorithms information element

Type of integrity protection algorithm (octet 2, bit 1 to 3)

Bits

3	**2**	**1**	
0	0	0	Reserved
0	0	1	EPS integrity algorithm 128-EIA1
0	1	0	EPS integrity algorithm 128-EIA2
0	1	1	EPS integrity algorithm EIA3
1	0	0	EPS integrity algorithm EIA4
1	0	1	EPS integrity algorithm EIA5
1	1	0	EPS integrity algorithm EIA6
1	1	1	EPS integrity algorithm EIA7

Type of ciphering algorithm (octet 2, bit 5 to 7)

Bits

7	**6**	**5**	
0	0	0	EPS encryption algorithm 128-EEA0 (ciphering not used)
0	0	1	EPS encryption algorithm 128-EEA1
0	1	0	EPS encryption algorithm 128-EEA2
0	1	1	EPS encryption algorithm EEA3
1	0	0	EPS encryption algorithm EEA4
1	0	1	EPS encryption algorithm EEA5
1	1	0	EPS encryption algorithm EEA6
1	1	1	EPS encryption algorithm EEA7

Bit 4 and 8 of octet 2 are spare and shall be coded as zero.

9.9.3.24 Network name

See subclause 10.5.3.5a in 3GPP TS 24.008 [13].

9.9.3.25 Nonce

The purpose of the Nonce information element is to transfer a 32-bit nonce value to support deriving a new mapped EPS security context.

The Nonce information element is coded as shown in figure 9.9.3.25.1 and table 9.9.3.25.1.

The Nonce is a type 3 information element with a length of 5 octets.

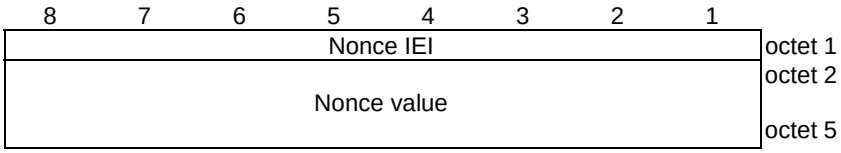

Figure 9.9.3.25.1: Nonce information element

Table 9.9.3.25.1: Nonce information element

Nonce value (octet 2 to 5) This field contains the binary representation of the nonce. Bit 8 of octet 2 represents the most significant bit of the nonce and bit 1 of octet 5 the least significant bit.

9.9.3.26 P-TMSI signature

See subclause 10.5.5.8 in 3GPP TS 24.008 [13].

9.9.3.27 Service type

The purpose of the Service type information element is to specify the purpose of the service request procedure.

The Service type information element is coded as shown in figure 9.9.3.27.1 and table 9.9.3.27.1.

The Service type is a type 1 information element.

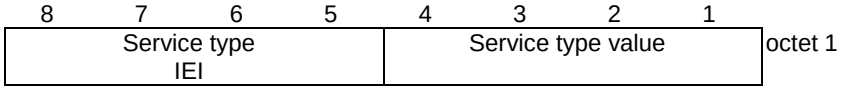

Figure 9.9.3.27.1: Service type information element

Table 9.9.3.27.1: Service type information element

Service type value (octet 1) Service type value Bits **4 3 2 1** 0 0 0 0 mobile originating CS fallback 0 0 0 1 mobile terminating CS fallback 0 0 1 0 mobile originating CS fallback emergency call All other values are reserved.

9.9.3.28 Short MAC

The purpose of the Short MAC information element is to protect the integrity of a SERVICE REQUEST message.

The integrity protection shall include octet 1 and 2 of the SERVICE REQUEST message. For the used algorithm and other input parameters to the algorithm see subclause 9.5. Only the 2 least significant octets of the resulting message authentication code are included in the information element.

The Short MAC information element is coded as shown in figure 9.9.3.28.1 and table 9.9.3.28.1.

The Short MAC is a type 3 information element with a length of 3 octets.

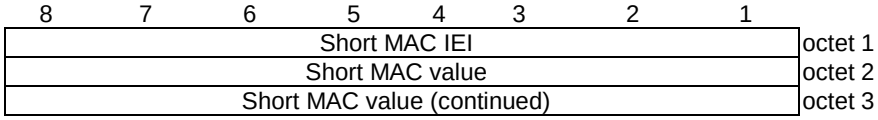

Figure 9.9.3.28.1: Short MAC information element

Table 9.9.3.28.1: Short MAC information element

Short MAC value (octet 2 and 3) This field contains the 2 least significant octets of the message authentication code calculated for the SERVICE REQUEST message. Bit 1 of octet 3 contains the least significant bit, and bit 8 of octet 2 the most significant bit of these 2 octets.

9.9.3.29 Time zone

See subclause 10.5.3.8 in 3GPP TS 24.008 [13].

9.9.3.30 Time zone and time

See subclause 10.5.3.9 in 3GPP TS 24.008 [13].

9.9.3.31 TMSI status

See subclause 10.5.5.4 in 3GPP TS 24.008 [13].

9.9.3.32 Tracking area identity

The purpose of the Tracking area identity information element is to provide an unambiguous identification of tracking areas within the area covered by the 3GPP system.

The Tracking area identity information element is coded as shown in figure 9.9.3.32.1 and table 9.9.3.32.1.

The Tracking area identity is a type 3 information element with a length of 6 octets.

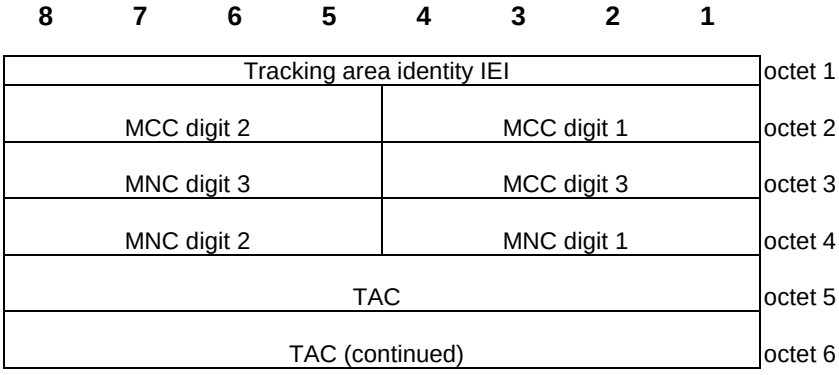

Figure 9.9.3.32.1: Tracking area identity information element

Table 9.9.3.32.1: Tracking area identity information element

MCC, Mobile country code (octet 2 and 3)
The MCC field is coded as in ITU-T Rec. E212, Annex A.

If the TAI is deleted the MCC and MNC shall take the value from the deleted TAI.

In abnormal cases, the MCC stored in the UE can contain elements not in the set {0, 1 ... 9}. In such cases the UE should transmit the stored values using full hexadecimal encoding. When receiving such an MCC, the network shall treat the TAI as deleted.

MNC, Mobile network code (octet 3 bits 5 to 8, octet 4)
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. For PCS 1900 for NA, Federal regulation mandates that a 3-digit MNC shall be used. However a network operator may decide to use only two digits in the MNC in the TAI over the radio interface. In this case, bits 5 to 8 of octet 3 shall be coded as "1111". Mobile equipment shall accept a TAI coded in such a way.

In abnormal cases, the MNC stored in the UE can have:
- digit 1 or 2 not in the set {0, 1 ... 9}, or
- digit 3 not in the set {0, 1 ...9, F} hex.

In such cases the UE shall transmit the stored values using full hexadecimal encoding. When receiving such an MNC, the network shall treat the TAI as deleted.

The same handling shall apply for the network, if a 3-digit MNC is sent by the UE to a network using only a 2-digit MNC.

TAC, Tracking area code (octet 5 and 6)
In the TAC field bit 8 of octet 5 is the most significant bit and bit 1 of octet 6 the least significant bit.
The coding of the tracking area code is the responsibility of each administration except that two values are used to mark the TAC, and hence the TAI, as deleted. Coding using full hexadecimal representation may be used. The tracking area code consists of 2 octets.
If a TAI has to be deleted then all bits of the tracking area code shall be set to one with the exception of the least significant bit which shall be set to zero. If a USIM is inserted in a mobile equipment with the tracking area code containing all zeros, then the mobile equipment shall recognise this TAC as part of a deleted TAI.

Editor's note: It needs to be checked whether there are still operators using only two digits in the MNC in the LAI over the GERAN/UTRAN radio interface, although they should use a three digit MNC. If not, then the above statement: "For PCS 1900 for NA, Federal regulation mandates that a 3-digit MNC shall be used. However … " could be removed.

9.9.3.33 Tracking area identity list

The purpose of the Tracking area identity list information element is to transfer a list of tracking areas from the network to the UE.

The coding of the information element allows combining different types of lists. The lists of type "000" and "001" allow a more compact encoding, when the different TAIs are sharing the PLMN identity.

The Tracking area identity list information element is coded as shown in figure 9.9.3.33.1, figure 9.9.3.33.2, figure 9.9.3.33.3, figure 9.9.3.33.4 and table 9.9.3.33.1.

The Tracking area identity list is a type 4 information element, with a minimum length of 8 octets and a maximum length of 98 octets. The list can contain a maximum of 16 different tracking area identities.

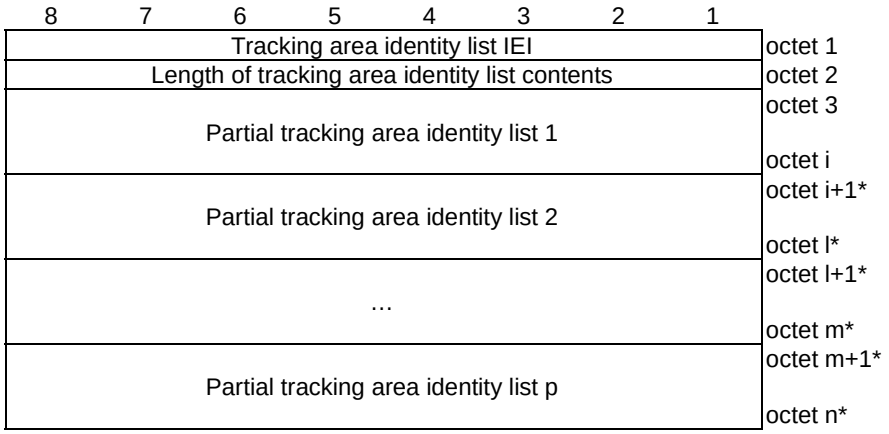

Figure 9.9.3.33.1: Tracking area identity list information element

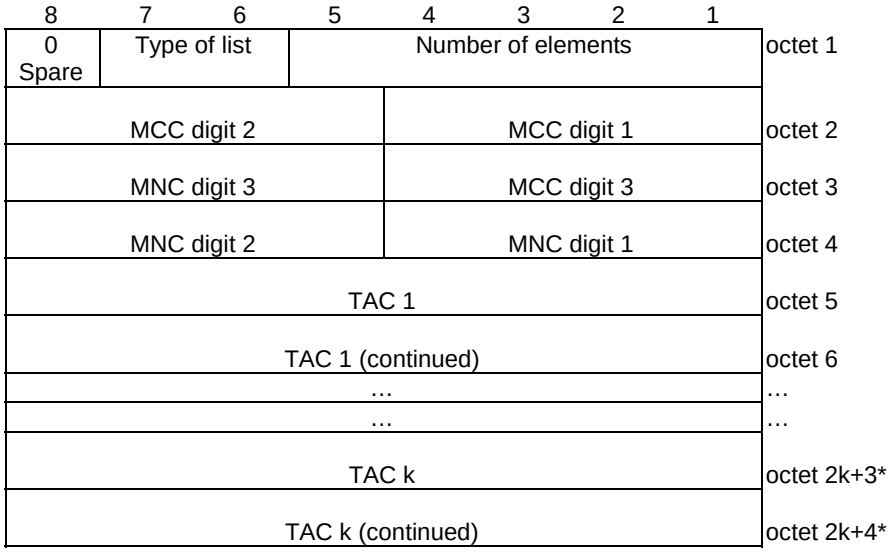

Figure 9.9.3.33.2: Partial tracking area identity list – type of list = "000"

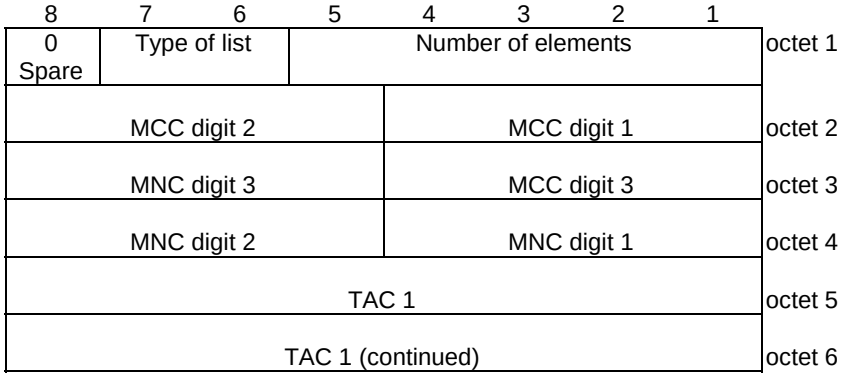

Figure 9.9.3.33.3: Partial tracking area identity list – type of list = "001"

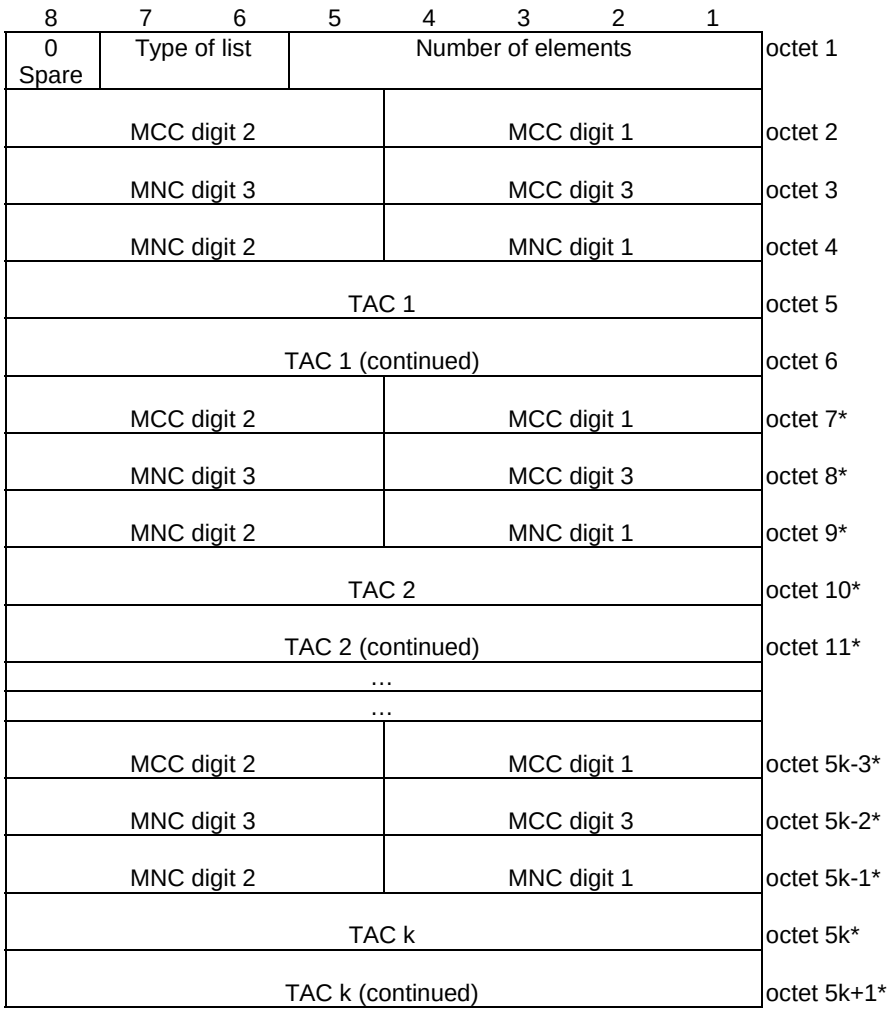

Figure 9.9.3.33.4: Partial tracking area identity list – type of list = "010"

Table 9.9.3.33.1: Tracking area identity list information element

Value part of the Tracking area identity list information element (octet 3 to n)

The value part of the Tracking area identity list information element consists of one or several partial tracking area identity lists. The length of each partial tracking area identity list can be determined from the 'type of list' field and the 'number of elements' field in the first octet of the partial tracking area identity list.
If more than 16 TAIs are included in this information element, the UE shall store the first 16 TAIs and ignore the remaining octets of the information element.

Partial tracking area identity list:

Type of list (octet 1)
Bits

7	**6**	
0	0	list of TACs belonging to one PLMN, with non-consecutive TAC values
0	1	list of TACs belonging to one PLMN, with consecutive TAC values
1	0	list of TAIs belonging to different PLMNs

All other values are reserved.

Number of elements (octet 1)
Bits

5	**4**	**3**	**2**	**1**	
0	0	0	0	0	1 element
0	0	0	0	1	2 elements
0	0	0	1	0	3 elements
		…			
0	1	1	0	1	14 elements
0	1	1	1	0	15 elements
0	1	1	1	1	16 elements

All other values are unused and shall be interpreted as 16, if received by the UE.

Bit 8 of octet 1 is spare and shall be coded as zero.

For type of list = "000" and number of elements = k:

octet 2 to 4 contain the MCC+MNC, and
for j = 1, k:
octet 2j+3 and 2j+4 contain the TAC of the j-th TAI belonging to the partial list,

For type of list = "001" and number of elements = k:

octet 2 to 4 contain the MCC+MNC, and
octet 5 and 6 contain the TAC of the first TAI belonging to the partial list.
The TAC values of the other k-1 TAIs are TAC+1, TAC+2, …, TAC+k-1.

For type of list = "010" and number of elements = k:

for j = 1, k.
octet 5j-3 to 5j-1 contain the MCC+MNC, and
octet 5j and 5j+1 contain the TAC of the j-th TAI belonging to the partial list.

MCC, Mobile country code

The MCC field is coded as in ITU-T Recommendation E.212 [30], Annex A.

MNC, Mobile network code

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, MNC digit 3 shall be coded as "1111".

TAC, Tracking area code

In the TAC field bit 8 of the first octet is the most significant bit and bit 1 of second octet the least significant bit.
The coding of the tracking area code is the responsibility of each administration.
Coding using full hexadecimal representation may be used. The tracking area code consists of 2 octets.

9.9.3.34 UE network capability

The purpose of the UE network capability information element is to provide the network with information concerning aspects of the UE related to EPS or interworking with GPRS. The contents might affect the manner in which the network handles the operation of the UE. The UE network capability information indicates general UE characteristics and it shall therefore, except for fields explicitly indicated, be independent of the frequency band of the channel it is sent on.

The UE network capability information element is coded as shown in figure 9.9.3.34.1 and table 9.9.3.34.1.

The UE network capability is a type 4 information element with a minimum length of 4 octets and a maximum length of 15 octets.

NOTE: The requirements for the support of UMTS security algorithms in the UE are specified in 3GPP TS 33.102 [18], and the requirements for the support of EPS security algorithms in 3GPP TS 33.401 [19].

8	7	6	5	4	3	2	1	
UE network capability IEI								octet 1
Length of UE network capability contents								octet 2
128-EEA0	128-EEA1	128-EEA2	EEA3	EEA4	EEA5	EEA6	EEA7	octet 3
0 spare	128-EIA1	128-EIA2	EIA3	EIA4	EIA5	EIA6	EIA7	octet 4
UEA0	UEA1	UEA2	UEA3	UEA4	UEA5	UEA6	UEA7	octet 5*
UCS2	UIA1	UIA2	UIA3	UIA4	UIA5	UIA6	UIA7	octet 6*
0 spare	0 spare	0 spare	0 spare	0 spare	0 spare	1xSR VCC	ISR	octet 7*
0	0	0	0	0	0	0	0	
Spare								octet 8* -15*

Figure 9.9.3.34.1: UE network capability information element

Table 9.9.3.34.1: UE network capability information element

EPS encryption algorithms supported (octet 3)

EPS encryption algorithm 128-EEA0 supported (octet 3, bit 8)
0 EPS encryption algorithm 128-EEA0 not supported
1 EPS encryption algorithm 128-EEA0 supported

EPS encryption algorithm 128-EEA1 supported (octet 3, bit 7)
0 EPS encryption algorithm 128-EEA1 not supported
1 EPS encryption algorithm 128-EEA1 supported

EPS encryption algorithm 128-EEA2 supported (octet 3, bit 6)
0 EPS encryption algorithm 128-EEA2 not supported
1 EPS encryption algorithm 128-EEA2 supported

EPS encryption algorithm EEA3 supported (octet 3, bit 5)
0 EPS encryption algorithm EEA3 not supported
1 EPS encryption algorithm EEA3 supported

EPS encryption algorithm EEA4 supported (octet 3, bit 4)
0 EPS encryption algorithm EEA4 not supported
1 EPS encryption algorithm EEA4 supported

EPS encryption algorithm EEA5 supported (octet 3, bit 3)
0 EPS encryption algorithm EEA5 not supported
1 EPS encryption algorithm EEA5 supported

EPS encryption algorithm EEA6 supported (octet 3, bit 2)
0 EPS encryption algorithm EEA6 not supported
1 EPS encryption algorithm EEA6 supported

EPS encryption algorithm EEA7 supported (octet 3, bit 1)
0 EPS encryption algorithm EEA7 not supported
1 EPS encryption algorithm EEA7 supported

EPS integrity algorithms supported (octet 4)

Bit 8 of octet 4 is spare and shall be coded as zero.

EPS integrity algorithm 128-EIA1 supported (octet 4, bit 7)
0 EPS integrity algorithm 128-EIA1 not supported
1 EPS integrity algorithm 128-EIA1 supported

EPS integrity algorithm 128-EIA2 supported (octet 4, bit 6)
0 EPS integrity algorithm 128-EIA2 not supported
1 EPS integrity algorithm 128-EIA2 supported

EPS integrity algorithm EIA3 supported (octet 4, bit 5)
0 EPS integrity algorithm EIA3 not supported
1 EPS integrity algorithm EIA3 supported

EPS integrity algorithm EIA4 supported (octet 4, bit 4)
0 EPS integrity algorithm EIA4 not supported
1 EPS integrity algorithm EIA4 supported

EPS integrity algorithm EIA5 supported (octet 4, bit 3)
0 EPS integrity algorithm EIA5 not supported
1 EPS integrity algorithm EIA5 supported

EPS integrity algorithm EIA6 supported (octet 4, bit 2)
0 EPS integrity algorithm EIA6 not supported
1 EPS integrity algorithm EIA6 supported

EPS integrity algorithm EIA7 supported (octet 4, bit 1)
0 EPS integrity algorithm EIA7 not supported
1 EPS integrity algorithm EIA7 supported

UMTS encryption algorithms supported (octet 5)

UMTS encryption algorithm UEA0 supported (octet 5, bit 8)
0 UMTS encryption algorithm UEA0 not supported
1 UMTS encryption algorithm UEA0 supported

UMTS encryption algorithm UEA1 supported (octet 5, bit 7)
0 UMTS encryption algorithm UEA1 not supported
1 UMTS encryption algorithm UEA1 supported

UMTS encryption algorithm UEA2 supported (octet 5, bit 6)
0 UMTS encryption algorithm UEA2 not supported
1 UMTS encryption algorithm UEA2 supported

UMTS encryption algorithm UEA3 supported (octet 5, bit 5)
0 UMTS encryption algorithm UEA3 not supported
1 UMTS encryption algorithm UEA3 supported

UMTS encryption algorithm UEA4 supported (octet 5, bit 4)
0 UMTS encryption algorithm UEA4 not supported
1 UMTS encryption algorithm UEA4 supported

UMTS encryption algorithm UEA5 supported (octet 5, bit 3)
0 UMTS encryption algorithm UEA5 not supported
1 UMTS encryption algorithm UEA5 supported

UMTS encryption algorithm UEA6 supported (octet 5, bit 2)
0 UMTS encryption algorithm UEA6 not supported
1 UMTS encryption algorithm UEA6 supported

UMTS encryption algorithm UEA7 supported (octet 5, bit 1)
0 UMTS encryption algorithm UEA7 not supported
1 UMTS encryption algorithm UEA7 supported

UCS2 support (UCS2) (octet 6, bit 8)
This information field indicates the likely treatment of UCS2 encoded character strings by the UE.

0 The UE has a preference for the default alphabet (defined in 3GPP TS 23.038 [3]) over UCS2 (see ISO/IEC 10646 [29]).
1 The UE has no preference between the use of the default alphabet and the use of UCS2.

UMTS integrity algorithms supported (octet 6)

UMTS integrity algorithm UIA1 supported (octet 6, bit 7)
0 UMTS integrity algorithm UIA1 not supported
1 UMTS integrity algorithm UIA1 supported

UMTS integrity algorithm UIA2 supported (octet 6, bit 6)
0 UMTS integrity algorithm UIA2 not supported
1 UMTS integrity algorithm UIA2 supported

UMTS integrity algorithm UIA3 supported (octet 6, bit 5)
0 UMTS integrity algorithm UIA3 not supported
1 UMTS integrity algorithm UIA3 supported

UMTS integrity algorithm UIA4 supported (octet 6, bit 4)
0 UMTS integrity algorithm UIA4 not supported
1 UMTS integrity algorithm UIA4 supported

UMTS integrity algorithm UIA5 supported (octet 6, bit 3)
0 UMTS integrity algorithm UIA5 not supported
1 UMTS integrity algorithm UIA5 supported

UMTS integrity algorithm UIA6 supported (octet 6, bit 2)
0 UMTS integrity algorithm UIA6 not supported
1 UMTS integrity algorithm UIA6 supported

UMTS integrity algorithm UIA7 supported (octet 6, bit 1) 0 UMTS integrity algorithm UIA7 not supported 1 UMTS integrity algorithm UIA7 supported Bits 8 to 3 of octet 7 are spare and shall be coded as zero. 1xSRVCC capability (octet 7, bit 2) 0 SRVCC from E-UTRAN to 3GPP2 1xCS not supported 1 SRVCC from E-UTRAN to 3GPP2 1xCS supported (see 3GPP TS 23.216 [8]) ISR support (ISR) (octet 7, bit 1) 0 The UE does not support ISR. 1 The UE supports ISR. All other bits in octet 8 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.9.3.35 UE radio capability information update needed

The purpose of the UE radio capability information update needed information element is to indicate whether the MME shall delete the stored UE radio capability information, if any.

The UE radio capability information update needed information element is coded as shown in figure 9.9.3.35.1and table 9.9.3.35.1.

The UE radio capability information update needed is a type 1 information element.

8	7	6	5	4	3	2	1	
UE radio capability information update needed IEI				0	0 spare	0	URC upd	octet 1

Figure 9.9.3.35.1: UE radio capability information update needed information element

Table 9.9.3.35.1: UE radio capability information update needed information element

UE radio capability information update needed flag (URC upd) (octet 1) Bit **1** 0 UE radio capability information update not needed 1 UE radio capability information update needed

9.9.3.36 UE security capability

The UE security capability information element is used by the network to indicate which security algorithms are supported by the UE in S1 mode, Iu mode and Gb mode. Security algorithms supported in S1 mode are supported both for NAS and for AS security. If the UE supports S101 mode, then these security algorithms are also supported for NAS security in S101 mode.

The UE security capability information element is coded as shown in figure 9.9.3.36.1 and table 9.9.3.36.1.

The UE security capability is a type 4 information element with a minimum length of 4 octets and a maximum length of 7 octets.

Octets 5, 6, and 7 are optional. If octet 5 is included, then also octet 6 shall be included and octet 7 may be included.

If a UE did not indicate support of any security algorithm for Gb mode, octet 7 shall not be included. If the UE did not indicate support of any security algorithm for Iu mode and Gb mode, octets 5, 6, and 7 shall not be included.

8	7	6	5	4	3	2	1	
UE security capability IEI								octet 1
Length of UE security capability contents								octet 2
128-EEA0	128-EEA1	128-EEA2	EEA3	EEA4	EEA5	EEA6	EEA7	octet 3
0 spare	128-EIA1	128-EIA2	EIA3	EIA4	EIA5	EIA6	EIA7	octet 4
UEA0	UEA1	UEA2	UEA3	UEA4	UEA5	UEA6	UEA7	octet 5*
0 spare	UIA1	UIA2	UIA3	UIA4	UIA5	UIA6	UIA7	octet 6*
0 spare	GEA1	GEA2	GEA3	GEA4	GEA5	GEA6	GEA7	octet 7*

Figure 9.9.3.36.1: UE security capability information element

Table 9.9.3.36.1: UE security capability information element

EPS encryption algorithms supported (octet 3)

EPS encryption algorithm 128-EEA0 supported (octet 3, bit 8)
0 EPS encryption algorithm 128-EEA0 not supported
1 EPS encryption algorithm 128-EEA0 supported

EPS encryption algorithm 128-EEA1 supported (octet 3, bit 7)
0 EPS encryption algorithm 128-EEA1 not supported
1 EPS encryption algorithm 128-EEA1 supported

EPS encryption algorithm 128-EEA2 supported (octet 3, bit 6)
0 EPS encryption algorithm 128-EEA2 not supported
1 EPS encryption algorithm 128-EEA2 supported

EPS encryption algorithm EEA3 supported (octet 3, bit 5)
0 EPS encryption algorithm EEA3 not supported
1 EPS encryption algorithm EEA3 supported

EPS encryption algorithm EEA4 supported (octet 3, bit 4)
0 EPS encryption algorithm EEA4 not supported
1 EPS encryption algorithm EEA4 supported

EPS encryption algorithm EEA5 supported (octet 3, bit 3)
0 EPS encryption algorithm EEA5 not supported
1 EPS encryption algorithm EEA5 supported

EPS encryption algorithm EEA6 supported (octet 3, bit 2)
0 EPS encryption algorithm EEA6 not supported
1 EPS encryption algorithm EEA6 supported

EPS encryption algorithm EEA7 supported (octet 3, bit 1)
0 EPS encryption algorithm EEA7 not supported
1 EPS encryption algorithm EEA7 supported

EPS integrity algorithms supported (octet 4)

Bit 8 of octet 4 is spare and shall be coded as zero.

EPS integrity algorithm 128-EIA1 supported (octet 4, bit 7)
0 EPS integrity algorithm 128-EIA1 not supported
1 EPS integrity algorithm 128-EIA1 supported

EPS integrity algorithm 128-EIA2 supported (octet 4, bit 6)
0 EPS integrity algorithm 128-EIA2 not supported
1 EPS integrity algorithm 128-EIA2 supported

EPS integrity algorithm EIA3 supported (octet 4, bit 5)
0 EPS integrity algorithm EIA3 not supported
1 EPS integrity algorithm EIA3 supported

EPS integrity algorithm EIA4 supported (octet 4, bit 4)
0 EPS integrity algorithm EIA4 not supported
1 EPS integrity algorithm EIA4 supported

EPS integrity algorithm EIA5 supported (octet 4, bit 3)
0 EPS integrity algorithm EIA5 not supported
1 EPS integrity algorithm EIA5 supported

EPS integrity algorithm EIA6 supported (octet 4, bit 2)
0 EPS integrity algorithm EIA6 not supported
1 EPS integrity algorithm EIA6 supported

EPS integrity algorithm EIA7 supported (octet 4, bit 1)
0 EPS integrity algorithm EIA7 not supported
1 EPS integrity algorithm EIA7 supported

UMTS encryption algorithms supported (octet 5)

UMTS encryption algorithm UEA0 supported (octet 5, bit 8)
0 UMTS encryption algorithm UEA0 not supported
1 UMTS encryption algorithm UEA0 supported

UMTS encryption algorithm UEA1 supported (octet 5, bit 7)
0 UMTS encryption algorithm UEA1 not supported
1 UMTS encryption algorithm UEA1 supported

UMTS encryption algorithm UEA2 supported (octet 5, bit 6)
0 UMTS encryption algorithm UEA2 not supported
1 UMTS encryption algorithm UEA2 supported

UMTS encryption algorithm UEA3 supported (octet 5, bit 5)
0 UMTS encryption algorithm UEA3 not supported
1 UMTS encryption algorithm UEA3 supported

UMTS encryption algorithm UEA4 supported (octet 5, bit 4)
0 UMTS encryption algorithm UEA4 not supported
1 UMTS encryption algorithm UEA4 supported

UMTS encryption algorithm UEA5 supported (octet 5, bit 3)
0 UMTS encryption algorithm UEA5 not supported
1 UMTS encryption algorithm UEA5 supported

UMTS encryption algorithm UEA6 supported (octet 5, bit 2)
0 UMTS encryption algorithm UEA6 not supported
1 UMTS encryption algorithm UEA6 supported

UMTS encryption algorithm UEA7 supported (octet 5, bit 1)
0 UMTS encryption algorithm UEA7 not supported
1 UMTS encryption algorithm UEA7 supported

UMTS integrity algorithms supported (octet 6)

Bit 8 of octet 6 is spare and shall be coded as zero.

UMTS integrity algorithm UIA1 supported (octet 6, bit 7)
0 UMTS integrity algorithm UIA1 not supported
1 UMTS integrity algorithm UIA1 supported

UMTS integrity algorithm UIA2 supported (octet 6, bit 6)
0 UMTS integrity algorithm UIA2 not supported
1 UMTS integrity algorithm UIA2 supported

UMTS integrity algorithm UIA3 supported (octet 6, bit 5)
0 UMTS integrity algorithm UIA3 not supported
1 UMTS integrity algorithm UIA3 supported

UMTS integrity algorithm UIA4 supported (octet 6, bit 4)
0 UMTS integrity algorithm UIA4 not supported
1 UMTS integrity algorithm UIA4 supported

UMTS integrity algorithm UIA5 supported (octet 6, bit 3)
0 UMTS integrity algorithm UIA5 not supported
1 UMTS integrity algorithm UIA5 supported

UMTS integrity algorithm UIA6 supported (octet 6, bit 2)
0 UMTS integrity algorithm UIA6 not supported
1 UMTS integrity algorithm UIA6 supported

UMTS integrity algorithm UIA7 supported (octet 6, bit 1)
0 UMTS integrity algorithm UIA7 not supported
1 UMTS integrity algorithm UIA7 supported

GPRS encryption algorithms supported (octet 7)

Bit 8 of octet 7 is spare and shall be coded as zero.

GPRS encryption algorithm GEA1 supported (octet 7, bit 7)
0 GPRS encryption algorithm GEA1 not supported
1 GPRS encryption algorithm GEA1 supported

GPRS encryption algorithm GEA2 supported (octet 7, bit 6)
0 GPRS encryption algorithm GEA2 not supported
1 GPRS encryption algorithm GEA2 supported

GPRS encryption algorithm GEA3 supported (octet 7, bit 5)
0 GPRS encryption algorithm GEA3 not supported
1 GPRS encryption algorithm GEA3 supported

GPRS encryption algorithm GEA4 supported (octet 7, bit 4)
0 GPRS encryption algorithm GEA4 not supported
1 GPRS encryption algorithm GEA4 supported

GPRS encryption algorithm GEA5 supported (octet 7, bit 3)
0 GPRS encryption algorithm GEA5 not supported
1 GPRS encryption algorithm GEA5 supported

GPRS encryption algorithm GEA6 supported (octet 7, bit 2)
0 GPRS encryption algorithm GEA6 not supported
1 GPRS encryption algorithm GEA6 supported

GPRS encryption algorithm GEA7 supported (octet 7, bit 1)
0 GPRS encryption algorithm GEA7 not supported
1 GPRS encryption algorithm GEA7 supported

9.9.4 EPS Session Management (ESM) information elements

9.9.4.1 Access point name

See subclause 10.5.6.1 in 3GPP TS 24.008 [13].

9.9.4.2 APN aggregate maximum bit rate

The purpose of the APN aggregate maximum bit rate information element is to indicate the new APN-AMBR if it is changed by the network.

The APN aggregate maximum bit rate information element is coded as shown in figure 9.9.4.2.1 and table 9.9.4.2.1.

The APN aggregate maximum bit rate is a type 4 information element with a minimum length of 4 octets and a maximum length of 8 octets.

8	7	6	5	4	3	2	1	
APN aggregate maximum bit rate IEI								octet 1
Length of APN aggregate maximum bit rate contents								octet 2
APN-AMBR for downlink								octet 3
APN-AMBR for uplink								octet 4
APN-AMBR for downlink (extended)								octet 5
APN-AMBR for uplink (extended)								octet 6
APN-AMBR for downlink (extended-2)								octet 7
APN-AMBR for uplink (extended-2)								octet 8

Figure 9.9.4.2.1: APN aggregate maximum bit rate information element

Table 9.9.4.2.1: APN aggregate maximum bit rate information element

APN-AMBR for downlink, octet 3

Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 0 Reserved

0 0 0 0 0 0 0 1 The APN-AMBR is binary coded in 8 bits, using a granularity of 1 kbps
to giving a range of values from 1 kbps to 63 kbps in 1 kbps increments.
0 0 1 1 1 1 1 1

0 1 0 0 0 0 0 0 The APN-AMBR is 64 kbps + ((the binary coded value in 8 bits –01000000) * 8 kbps)
to giving a range of values from 64 kbps to 568 kbps in 8 kbps increments.
0 1 1 1 1 1 1 1

1 0 0 0 0 0 0 0 The APN-AMBR is 576 kbps + ((the binary coded value in 8 bits –10000000) * 64 kbps)
to giving a range of values from 576 kbps to 8640 kbps in 64 kbps increments.
1 1 1 1 1 1 1 0

1 1 1 1 1 1 1 1 0kbps

If the network wants to indicate an APN-AMBR for downlink higher than 8640 kbps, it shall set octet 3 to '11111110', i.e. 8640 kbps, and shall encode the value for the APN-AMBR in octet 5.

APN-AMBR for uplink, octet 4

Coding is identical to that of APN-AMBR for downlink.

APN-AMBR for downlink (extended), octet 5

Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 0 Use the value indicated by the APN-AMBR for downlink in octet 3.

For all other values: Ignore the value indicated by the APN-AMBR for downlink in octet 3 and use the following value:
0 0 0 0 0 0 0 1 The APN-AMBR is 8600 kbps + ((the binary coded value in 8 bits) * 100 kbps),
to giving a range of values from 8700 kbps to 16000 kbps in 100 kbps increments.
0 1 0 0 1 0 1 0

0 1 0 0 1 0 1 1 The APN-AMBR is 16 Mbps + ((the binary coded value in 8 bits - 01001010) * 1 Mbps),
to giving a range of values from 17 Mbps to 128 Mbps in 1 Mbps increments.
1 0 1 1 1 0 1 0

1 0 1 1 1 0 1 1 The APN-AMBR is 128 Mbps + ((the binary coded value in 8 bits - 10111010) * 2 Mbps),
to giving a range of values from 130 Mbps to 256 Mbps in 2 Mbps increments.
1 1 1 1 1 0 1 0

APN-AMBR for uplink (extended), octet 6

This field is an extension of the APN-AMBR for uplink in octet 4. The coding is identical to that of the APN-AMBR for downlink (extended).

APN-AMBR for downlink (extended-2), octet 7

Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 0 Use the value indicated by the APN-AMBR for downlink and APN-AMBR for downlink (extended) in octets 3 and 5.

0 0 0 0 0 0 0 1 The APN-AMBR is (the binary coded value in 8 bits) * 256 Mbps + (the value indicated by
to the APN-AMBR for downlink and APN-AMBR for downlink (extended) in octets 3 and 5),
1 1 1 1 1 1 1 0 giving a range of 1kbps to 65280 Mbps with a maximum step size of 2Mbps.

APN-AMBR for uplink (extended-2), octet 8

This field is an extension of the APN-AMBR for uplink and APN-AMBR for uplink (extended) in octets 4 and 6. The coding is identical to that of the APN-AMBR for downlink (extended-2).

9.9.4.3 EPS quality of service

The purpose of the EPS quality of service information element is to specify the QoS parameters for an EPS bearer context.

The EPS quality of service information element is coded as shown in figure 9.9.4.3.1 and table 9.9.4.3.1.

The EPS quality of service is a type 4 information element with a minimum length of 3 octets and a maximum length of 11 octets.

Refer to 3GPP TS 23.203 [7] for a detailed description of the QoS Class Identifier (QCI).

8	7	6	5	4	3	2	1	
EPS quality of service IEI								octet 1
Length of EPS quality of service contents								octet 2
QCI								octet 3
Maximum bit rate for uplink								octet 4
Maximum bit rate for downlink								octet 5
Guaranteed bit rate for uplink								octet 6
Guaranteed bit rate for downlink								octet 7
Maximum bit rate for uplink (extended)								octet 8
Maximum bit rate for downlink (extended)								octet 9
Guaranteed bit rate for uplink (extended)								octet 10
Guaranteed bit rate for downlink (extended)								octet 11

Figure 9.9.4.3.1: EPS quality of service information element

Table 9.9.4.3.1: EPS quality of service information element

Quality of Service Class Identifier (QCI), octet 3 (see 3GPP TS 23.203 [7])
Bits
8 7 6 5 4 3 2 1

In UE to network direction:
0 0 0 0 0 0 0 0 Network selects the QCI

In network to UE direction:
0 0 0 0 0 0 0 0 Reserved

In UE to network direction and in network to UE direction:
0 0 0 0 0 0 0 1 QCI 1
0 0 0 0 0 0 1 0 QCI 2
0 0 0 0 0 0 1 1 QCI 3
0 0 0 0 0 1 0 0 QCI 4
0 0 0 0 0 1 0 1 QCI 5
0 0 0 0 0 1 1 0 QCI 6
0 0 0 0 0 1 1 1 QCI 7
0 0 0 0 1 0 0 0 QCI 8
0 0 0 0 1 0 0 1 QCI 9

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of this protocol.

For all non-GBR QCIs, the maximum and guaranteed bit rates shall be ignored.

Maximum bit rate for uplink, octet 4 (see 3GPP TS 23.107 [5])
Bits
8 7 6 5 4 3 2 1

In UE to network direction:
0 0 0 0 0 0 0 0 Subscribed maximum bit rate for uplink

In network to UE direction:
0 0 0 0 0 0 0 0 Reserved

In UE to network direction and in network to UE direction:
0 0 0 0 0 0 0 1 The maximum bit rate is binary coded in 8 bits, using a granularity of 1 kbps
to giving a range of values from 1 kbps to 63 kbps in 1 kbps increments.
0 0 1 1 1 1 1 1

0 1 0 0 0 0 0 0 The maximum bit rate is 64 kbps + ((the binary coded value in 8 bits – 01000000) * 8 kbps)
to giving a range of values from 64 kbps to 568 kbps in 8 kbps increments.
0 1 1 1 1 1 1 1

1 0 0 0 0 0 0 0 The maximum bit rate is 576 kbps + ((the binary coded value in 8 bits – 10000000) * 64 kbps)
to giving a range of values from 576 kbps to 8640 kbps in 64 kbps increments.
1 1 1 1 1 1 1 0

1 1 1 1 1 1 1 1 0kbps

If the sending entity wants to indicate a maximum bit rate for uplink higher than 8640 kbps, it shall set octet 4 to '11111110', i.e. 8640 kbps, and shall encode the value for the maximum bit rate in octet 8.

Maximum bit rate for downlink, octet 5 (see 3GPP TS 23.107 [5])

Coding is identical to that of maximum bit rate for uplink.

If the sending entity wants to indicate a maximum bit rate for downlink higher than 8640 kbps, it shall set octet 5 to '11111110', i.e. 8640 kbps, and shall encode the value for the maximum bit rate in octet 9.

In this version of the protocol, for messages specified in the present document, the sending entity shall not request 0 kbps for both the maximum bit rate for downlink and the maximum bit rate for uplink at the same time. Any entity receiving a request for 0 kbps in both the maximum bit rate for downlink and the maximum bit rate for uplink shall consider that as a syntactical error (see clause 8 of 3GPP TS 24.008 [13]).

Guaranteed bit rate for uplink, octet 6 (see 3GPP TS 23.107 [5])

Coding is identical to that of maximum bit rate for uplink.

If the sending entity wants to indicate a guaranteed bit rate for uplink higher than 8640 kbps, it shall set octet 6 to '11111110', i.e. 8640 kbps, and shall encode the value for the guaranteed bit rate in octet 10.

Guaranteed bit rate for downlink, octet 7 (see 3GPP TS 23.107 [5])

Coding is identical to that of maximum bit rate for uplink.

If the sending entity wants to indicate a guaranteed bit rate for downlink higher than 8640 kbps, it shall set octet 7 to '11111110', i.e. 8640 kbps, and shall encode the value for the guaranteed bit rate in octet 11.

Maximum bit rate for uplink (extended), octet 8
Bits
8 7 6 5 4 3 2 1

In UE to network direction and in network to UE direction:

0 0 0 0 0 0 0 0	Use the value indicated by the maximum bit rate for uplink in octet 4.
	For all other values: ignore the value indicated by the maximum bit rate for uplink in octet 4 and use the following value:
0 0 0 0 0 0 0 1 to 0 1 0 0 1 0 1 0	The maximum bit rate is 8600 kbps + ((the binary coded value in 8 bits) * 100 kbps), giving a range of values from 8700 kbps to 16000 kbps in 100 kbps increments.
0 1 0 0 1 0 1 1 to 1 0 1 1 1 0 1 0	The maximum bit rate is 16 Mbps + ((the binary coded value in 8 bits - 01001010) * 1 Mbps), giving a range of values from 17 Mbps to 128 Mbps in 1 Mbps increments.
1 0 1 1 1 0 1 1 to 1 1 1 1 1 0 1 0	The maximum bit rate is 128 Mbps + ((the binary coded value in 8 bits - 10111010) * 2 Mbps), giving a range of values from 130 Mbps to 256 Mbps in 2 Mbps increments.

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of the protocol.

Maximum bit rate for downlink (extended), octet 9

This field is an extension of the maximum bit rate for downlink in octet 5. The coding is identical to that of the maximum bit rate for uplink (extended).

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of the protocol.

Guaranteed bit rate for uplink (extended), octet 10
Bits
8 7 6 5 4 3 2 1

In UE to network direction and in network to UE direction:

0 0 0 0 0 0 0 0	Use the value indicated by the guaranteed bit rate for uplink in octet 6.
	For all other values: ignore the value indicated by the guaranteed bit rate for uplink in octet 6 and use the following value:
0 0 0 0 0 0 0 1 to 0 1 0 0 1 0 1 0	The guaranteed bit rate is 8600 kbps + ((the binary coded value in 8 bits) * 100 kbps), giving a range of values from 8700 kbps to 16000 kbps in 100 kbps increments.
0 1 0 0 1 0 1 1 to 1 0 1 1 1 0 1 0	The guaranteed bit rate is 16 Mbps + ((the binary coded value in 8 bits - 01001010) * 1 Mbps), giving a range of values from 17 Mbps to 128 Mbps in 1 Mbps increments.

1 0 1 1 1 0 1 1 to 1 1 1 1 1 0 1 0	The guaranteed bit rate is 128 Mbps + ((the binary coded value in 8 bits - 10111010) * 2 Mbps), giving a range of values from 130 Mbps to 256 Mbps in 2 Mbps increments.

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of the protocol.

Guaranteed bit rate for downlink (extended), octet 11

This field is an extension of the guaranteed bit rate for downlink in octet 7. The coding is identical to that of guaranteed bit rate for uplink (extended).

The network shall map all other values not explicitly defined onto one of the values defined in this version of the protocol. The network shall return a negotiated value which is explicitly defined in this version of the protocol.

9.9.4.4 ESM cause

The purpose of the ESM cause information element is to indicate the reason why a session management request is rejected.

The ESM cause information element is coded as shown in figure 9.9.4.4.1 and table 9.9.4.4.1.

The ESM cause is a type 3 information element with 2 octets length.

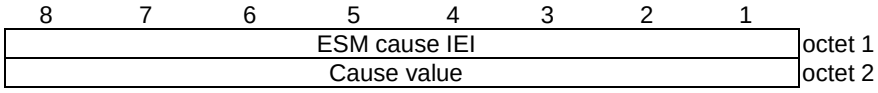

Figure 9.9.4.4.1: ESM cause information element

Table 9.9.4.4.1: ESM cause information element

Cause value (octet 2)

Bits

8	7	6	5	4	3	2	1	
0	0	0	0	1	0	0	0	Operator Determined Barring
0	0	0	1	1	0	1	0	Insufficient resources
0	0	0	1	1	0	1	1	Unknown or missing APN
0	0	0	1	1	1	0	0	Unknown PDN type
0	0	0	1	1	1	0	1	User authentication failed
0	0	0	1	1	1	1	0	Activation rejected by Serving GW or PDN GW
0	0	0	1	1	1	1	1	Activation rejected, unspecified
0	0	1	0	0	0	0	0	Service option not supported
0	0	1	0	0	0	0	1	Requested service option not subscribed
0	0	1	0	0	0	1	0	Service option temporarily out of order
0	0	1	0	0	0	1	1	PTI already in use
0	0	1	0	0	1	0	0	Regular deactivation
0	0	1	0	0	1	0	1	EPS QoS not accepted
0	0	1	0	0	1	1	0	Network failure
0	0	1	0	1	0	0	0	Feature not supported
0	0	1	0	1	0	0	1	Semantic error in the TFT operation
0	0	1	0	1	0	1	0	Syntactical error in the TFT operation
0	0	1	0	1	0	1	1	Unknown EPS bearer context
0	0	1	0	1	1	0	0	Semantic errors in packet filter(s)
0	0	1	0	1	1	0	1	Syntactical errors in packet filter(s)
0	0	1	0	1	1	1	0	EPS bearer context without TFT already activated
0	0	1	1	0	0	0	1	Last PDN disconnection not allowed
0	0	1	1	0	0	1	0	PDN type IPv4 only allowed
0	0	1	1	0	0	1	1	PDN type IPv6 only allowed
0	0	1	1	0	1	0	0	Single address bearers only allowed
0	0	1	1	0	1	0	1	ESM information not received
0	0	1	1	0	1	1	0	PDN connection does not exist
0	1	0	1	0	0	0	1	Invalid PTI value
0	1	0	1	1	1	1	1	Semantically incorrect message
0	1	1	0	0	0	0	0	Invalid mandatory information
0	1	1	0	0	0	0	1	Message type non-existent or not implemented
0	1	1	0	0	0	1	0	Message type not compatible with the protocol state
0	1	1	0	0	0	1	1	Information element non-existent or not implemented
0	1	1	0	0	1	0	0	Conditional IE error
0	1	1	0	0	1	0	1	Message not compatible with the protocol state
0	1	1	0	1	1	1	1	Protocol error, unspecified
0	1	1	1	0	0	0	0	APN restriction value incompatible with active EPS bearer context

Any other value received by the UE shall be treated as 0010 0010, "Service option temporarily out of order". Any other value received by the network shall be treated as 0110 1111, "Protocol error, unspecified".

NOTE: The listed cause values are defined in Annex B.

9.9.4.5 ESM information transfer flag

The purpose of the ESM information transfer flag information element is to indicate whether ESM information, i.e. protocol configuration options or APN or both, is to be transferred security protected.

The ESM information transfer flag information element is coded as shown in figure 9.9.4.5.1 and table 9.9.4.5.1.

The ESM information transfer flag is a type 1 information element.

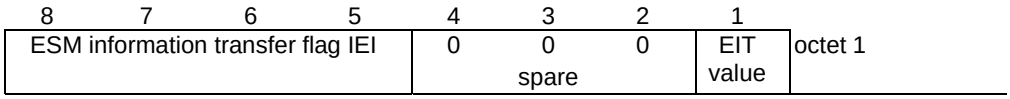

Figure 9.9.4.5.1: Ciphered ESM information transfer flag information element

Table 9.9.4.5.1: Ciphered ESM information transfer flag information element

EIT (ESM information transfer)	
Bit	
1	
0	ESM information transfer not required
1	ESM information transfer required

9.9.4.6 Linked EPS bearer identity

The purpose of the Linked EPS bearer identity IE is to identify the default bearer that is associated with a dedicated EPS bearer.

The Linked EPS bearer identity information element is coded as shown in figure 9.9.4.6.1 and table 9.9.4.6.1.

The Linked EPS bearer identity is a type 1 information element.

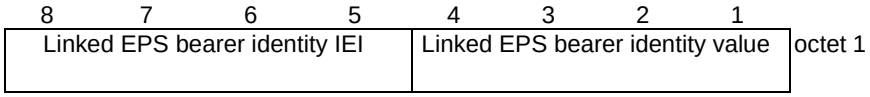

Figure 9.9.4.6.1: Linked EPS bearer identity information element

Table 9.9.4.6.1: Linked EPS bearer identity information element

Linked EPS bearer identity (bits 1-4)				
4	**3**	**2**	**1**	
0	0	0	0	
	to			Reserved
0	1	0	0	
0	1	0	1	EPS bearer identity value 5
0	1	1	0	EPS bearer identity value 6
0	1	1	1	EPS bearer identity value 7
1	0	0	0	EPS bearer identity value 8
1	0	0	1	EPS bearer identity value 9
1	0	1	0	EPS bearer identity value 10
1	0	1	1	EPS bearer identity value 11
1	1	0	0	EPS bearer identity value 12
1	1	0	1	EPS bearer identity value 13
1	1	1	0	EPS bearer identity value 14
1	1	1	1	EPS bearer identity value 15

9.9.4.7 LLC service access point identifier

See subclause 10.5.6.9 in 3GPP TS 24.008 [13].

9.9.4.8 Packet flow identifier

See subclause 10.5.6.11 in 3GPP TS 24.008 [13].

9.9.4.9 PDN address

The purpose of the PDN address information element is to assign an IPv4 address to the UE associated with a packet data network and to provide the UE with an interface identifier to be used to build the IPv6 link local address.

The PDN address information element is coded as shown in figure 9.9.4.9.1 and table 9.9.4.9.1.

The PDN address is a type 4 information element with minimum length of 7 octets and a maximum length of 15 octets.

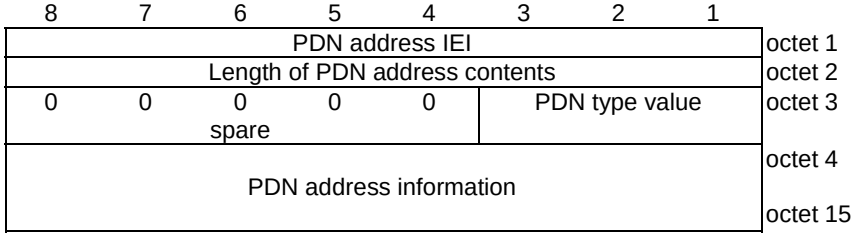

Figure 9.9.4.9.1: PDN address information element

Table 9.9.4.9.1: PDN address information element

PDN type value (octet 3)
Bits

3	**2**	**1**	
0	0	1	IPv4
0	1	0	IPv6
0	1	1	IPv4v6

All other values are reserved.

Bit 4 to 8 of octet 3 are spare and shall be coded as zero.

PDN address information (octet 4 to 15)

If PDN type value indicates IPv4, the PDN address information in octet 4 to octet 7 contains an IPv4 address. Bit 8 of octet 4 represents the most significant bit of the IPv4 address and bit 1 of octet 7 the least significant bit.

If PDN type value indicates IPv6, the PDN address information in octet 4 to octet 11 contains an IPv6 interface identifier. Bit 8 of octet 5 represents the most significant bit of the IPv6 interface identifier and bit 1 of octet 11 the least significant bit.

If PDN type value indicates IPv4v6, the PDN address information in octet 4 to octet 15 contains an IPv6 interface identifier and an IPv4 address. Bit 8 of octet 4 represents the most significant bit of the IPv6 interface identifier and bit 1 of octet 11 the least significant bit. Bit 8 of octet 12 represents the most significant bit of the IPv4 address and bit 1 of octet 15 the least significant bit.

If PDN type value indicates IPv4 or IPv4v6 and DHCPv4 is to be used to allocate the IPv4 address, the IPv4 address shall be coded as 0.0.0.0.

9.9.4.10 PDN type

The purpose of the PDN type information element is to indicate the IP version capability of the IP stack associated with the UE.

The PDN type information element is coded as shown in figure 9.9.4.10.1 and table 9.9.4.10.1.

The PDN type is a type 1 information element.

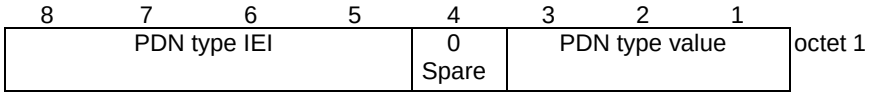

Figure 9.9.4.10.1: PDN type information element

Table 9.9.4.10.1: PDN type information element

PDN type value (octet 1)			
Bits			
3	**2**	**1**	
0	0	1	IPv4
0	1	0	IPv6
0	1	1	IPv4v6
All other values are reserved.			
Bit 4 of octet 1 is spare and shall be coded as zero.			

9.9.4.11 Protocol configuration options

See subclause 10.5.6.3 in 3GPP TS 24.008 [13].

9.9.4.12 Quality of service

See subclause 10.5.6.5 in 3GPP TS 24.008 [13].

9.9.4.13 Radio priority

See subclause 10.5.7.2 in 3GPP TS 24.008 [13].

9.9.4.14 Request type

See subclause 10.5.6.17 in 3GPP TS 24.008 [13].

9.9.4.15 Traffic flow aggregate description

The purpose of the Traffic flow aggregate description information element is to specify the aggregate of packet filters and their related parameters and operations for a dedicated EPS bearer. The traffic flows aggregate description may contain the aggregate of packet filters for the downlink direction, the uplink direction or packet filters that apply for both directions. The packet filters determine the traffic mapping to EPS bearers. The downlink packet filters shall be applied by the network, and the uplink packet filters shall be applied by the UE. A packet filter that applies for both directions shall be applied by the network as a downlink packet filter and by the UE as an uplink filter.

The Traffic flow aggregate description information element is encoded using the same format as the Traffic flow template information element (see subclause 10.5.6.12 in 3GPP TS 24.008 [13]). When sending this IE, the UE shall assign the packet filter identifier values so that they are unique across all packet filters for the PDN connection.

9.9.4.16 Traffic flow template

See subclause 10.5.6.12 in 3GPP TS 24.008 [13].

9.9.4.17 Transaction identifier

The purpose of the Transaction identifier information element is to represent the corresponding PDP context in A/Gb mode or Iu mode which is mapped from the EPS bearer context.

The Transaction identifier information element is coded as the Linked TI information element in 3GPP TS 24.008 [13], subclause 10.5.6.7.

10 List of system parameters

10.1 General

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

10.2 Timers of EPS mobility management

Table 10.2.1: EPS mobility management timers – UE side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T3402	Default 12 min. NOTE 1	EMM-DEREGISTERED EMM-REGISTERED	At attach failure and the attempt counter is equal to 5. At tracking area updating failure and the attempt counter is equal to 5.	ATTACH REQUEST sent TRACKING AREA UPDATE REQUEST sent	Initiation of the attach procedure or TAU procedure
T3410	15s	EMM-REGISTERED-INITIATED	ATTACH REQUEST sent	ATTACH ACCEPT received ATTACH REJECT received	Start T3411 or T3402 as described in subclause 5.5.1.2.6
T3411	10s	EMM-DEREGISTERED. ATTEMPTING-TO-ATTACH EMM-REGISTERED. ATTEMPTING-TO-UPDATE	At attach failure due to lower layer failure, T3410 timeout or attach rejected with other cause values than those treated in subclause 5.5.1.2.5. At tracking area updating failure due to lower layer failure, T3430 timeout or TAU rejected with other cause values than those treated in subclause 5.5.3.2.5.	ATTACH REQUEST sent TRACKING AREA UPDATE REQUEST sent	Retransmission of the ATTACH REQUEST or TRACKING AREA UPDATE REQUEST
T3412	NOTE 2	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
T3416	30s	EMM-REGISTERED-INITIATED EMM-REGISTERED EMM-DEREGISTERED-INITIATED EMM-TRACKING-AREA-UPDATING-INITIATED EMM-SERVICE-REQUEST-INITIATED	RAND and RES stored as a result of a UMTS authentication challenge	SECURITY MODE COMMAND received SERVICE REJECT received TRACKING AREA UPDATE ACCEPT received AUTHENTICATION REJECT received AUTHENTICATION FAILURE sent EMM-DEREGISTERED or EMM-NULL entered	Delete the stored RAND and RES
T3417	5s	EMM-SERVICE-REQUEST-INITIATED	SERVICE REQUEST or EXTENDED SERVICE REQUEST sent	NAS security mode control procedure is completed Bearers have been set up Inter-system change from S1 mode to A/Gb mode or Iu mode is completed SERVICE REJECT received	Abort the procedure

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T3418	20s	EMM-REGISTERED-INITIATED EMM-REGISTERED EMM-TRACKING-AREA-UPDATING-INITIATED EMM-DEREGISTERED-INITIATED EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (cause = "MAC failure") sent	AUTHENTICATION REQUEST received	On first expiry, the UE should consider the network as false
T3420	15s	EMM-REGISTERED-INITIATED EMM-REGISTERED EMM-DEREGISTERED-INITIATED EMM-TRACKING-AREA-UPDATING-INITIATED EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (cause = "synch failure") sent	AUTHENTICATION REQUEST received	On first expiry, the UE should consider the network as false
T3421	15s	EMM-DEREGISTERED-INITIATED	DETACH REQUEST sent	DETACH ACCEPT received	Retransmission of DETACH REQUEST
T3423	NOTE 3	EMM-REGISTERED	T3412 expires while the UE is in EMM-REGISTERED.NO-CELL-AVAILABLE and ISR is activated.	When entering state EMM-DEREGISTERED or when entering EMM-CONNECTED mode.	Deactivate ISR by setting TIN to "P-TMSI"
T3430	15s	EMM-TRACKING-AREA-UPDATING-INITIATED	TRACKING AREA UPDATE REQUEST sent	TRACKING AREA UPDATE ACCEPT received TRACKING AREA UPDATE REJECT received	Start T3411 or T3402 as described in subclause 5.5.3.2.6
T3440	10s	EMM-REGISTERED-INITIATED EMM-TRACKING-AREA-UPDATING-INITIATED EMM-DEREGISTERED-INITIATED EMM-SERVICE-REQUEST-INITIATED EMM-REGISTERED	ATTACH REJECT, DETACH REQUEST, TRACKING AREA UPDATE REJECT with any of the cause values #11, #12, #13, #14 or #15 SERVICE REJECT received with any of the cause values #11, #12, #13 or #15 TRACKING AREA UPDATE ACCEPT received after the UE sent TRACKING AREA UPDATE REQUEST with no "active" flag	Signalling connection released Bearers have been set up	Release the signalling connection and proceed as described in subclause 5.3.1.2
T3442	NOTE 4	EMM-REGISTERED	SERVICE REJECT received with cause value #39	TRACKING AREA UPDATE REQUEST sent	None

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
NOTE 1: The default value of this timer is used if the network does not indicate another value in an EMM signalling procedure.					
NOTE 2: The value of this timer is provided by the network operator during the attach and tracking area updating procedures.					
NOTE 3: The value of this timer may be provided by the network in the ATTACH ACCEPT message and TRACKING AREA UPDATE ACCEPT message. The default value of this timer is identical to the value of T3412.					
NOTE 4: The value of this timer is provided by the network operator when a service request for CS fallback is rejected by the network with EMM cause value #39, "CS domain temporarily not available".					

Table 10.2.2: 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)
T3413	NOTE 2	EMM-REGISTERED	Paging procedure initiated	Paging procedure completed	Network dependent
T3422	6s	EMM-DEREGISTERED-INITIATED	DETACH REQUEST sent	DETACH ACCEPT received	Retransmission of DETACH REQUEST
T3450	6s	EMM-COMMON-PROC-INIT	ATTACH ACCEPT sent TRACKING AREA UPDATE ACCEPT sent with GUTI GUTI REALLOCATION COMMAND sent	ATTACH COMPLETE received TRACKING AREA UPDATE COMPLETE received GUTI REALLOCATION COMPLETE received	Retransmission of the same message type, i.e. ATTACH ACCEPT, TRACKING AREA UPDATE ACCEPT or GUTI REALLOCATION COMMAND
T3460	6s	EMM-COMMON-PROC-INIT	AUTHENTICATION REQUEST sent SECURITY MODE COMMAND sent	AUTHENTICATION RESPONSE received AUTHENTICATION FAILURE received SECURITY MODE COMPLETE received SECURITY MODE REJECT received	Retransmission of the same message type, i.e. AUTHENTICATION REQUEST or SECURITY MODE COMMAND
T3470	6s	EMM-COMMON-PROC-INIT	IDENTITY REQUEST sent	IDENTITY RESPONSE received	Retransmission of IDENTITY REQUEST
Mobile reachable	Default 4 min greater than T3412	All except EMM-DEREGISTERED	Entering EMM-IDLE mode	NAS signalling connection established	Network dependent, but typically paging is halted on 1st expiry
Implicit detach timer	Default 4 min greater than T3423	All except EMM-DEREGISTERED	The mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated	NAS signalling connection established	Implicitly detach the UE on 1st expiry
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.					
NOTE 2: The value of this timer is network dependent.					

10.3 Timers of EPS session management

Table 10.3.1: EPS session management timers – UE side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3480	FFS	PROCEDURE TRANSACTION PENDING	BEARER RESOURCE MODIFICATION REQUEST sent	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or DEACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE MODIFICATION REJECT received	Retransmission of BEARER RESOURCE MODIFICATION REQUEST
T3482	30s	PROCEDURE TRANSACTION PENDING	An additional PDN connection is requested by the UE which is not combined in attach procedure	ACTIVE DEFAULT EPS BEARER CONTEXT REQUEST received or PDN CONNECTIVITY REJECT received	Retransmission of PDN CONNECTIVITY REQUEST
T3492	6s	PROCEDURE TRANSACTION PENDING	PDN DISCONNECT REQUEST sent	DEACTIVATE EPS BEARER CONTEXT REQUEST received or PDN DISCONNECT REJECT received	Retransmission of PDN DISCONNECT REQUEST
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.					

Table 10.3.2: EPS session management timers – network side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3485	FFS	BEARER CONTEXT ACTIVE PENDING	ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST sent ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST sent	ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT received or ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT received or ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT received or ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT received	Retransmission of the same message
T3486	FFS	BEARER CONTEXT MODIFY PENDING	MODIFY EPS BEARER CONTEXT REQUEST sent	MODIFY EPS BEARER CONTEXT ACCEPT received or MODIFY EPS BEARER CONTEXT REJECT received	Retransmission of MODIFY EPS BEARER CONTEXT REQUEST
T3489	4s	FFS	ESM INFORMATION REQUEST sent	ESM INFORMATION RESPONSE received	Retransmission of ESM INFORMATION REQUEST on 1st and 2nd expiry only
T3495	FFS	BEARER CONTEXT INACTIVE PENDING	DEACTIVATE EPS BEARER CONTEXT REQUEST sent	DEACTIVATE EPS BEARER CONTEXT ACCEPT received	Retransmission of DEACTIVATE EPS BEARER CONTEXT REQUEST
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.					

Editor's note: Considerations for defining ESM sublayer procedure transaction states in the MME e.g. for the ESM information procedure (see T3489) are FFS.

Annex A (informative): Cause values for EPS mobility management

A.1 Causes related to UE identification

Cause value #2 – IMSI unknown in HSS

This cause is sent to the UE if the UE is not known (registered) in the HSS. This cause does not affect operation of the EPS service, although is may be used by an EMM procedure.

Cause value #3 – Illegal UE

This cause is sent to the UE when the network refuses service to the UE either because an identity of the UE is not acceptable to the network or because the UE does not pass the authentication check, i.e. the RES received from the UE is different from that generated by the network.

Cause value #6 – Illegal ME

This cause is sent to the UE if the ME used is not acceptable to the network, e.g. blacklisted.

Cause value #9 – UE identity cannot be derived by the network.

This cause is sent to the UE when the network cannot derive the UE's identity from the GUTI/S-TMSI during an inter-MME tracking area update.

Cause value #10 – Implicitly detached

This cause is sent to the UE either if the network has implicitly detached the UE, e.g. some while after the Mobile reachable timer has expired, or if the EMM context data related to the subscription does not exist in the MME e.g. because of a MME restart.

A.2 Cause related to subscription options

Cause value #7 – EPS services not allowed

This cause is sent to the UE when it is not allowed to operate EPS services.

Cause value #8 – EPS services and non-EPS services not allowed

This cause is sent to the UE when it is not allowed to operate either EPS or non-EPS services.

Cause value #11 – PLMN not allowed

This cause is sent to the UE if it requests tracking area updating in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate.

Cause value #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.

NOTE 1: If cause #12 is sent to a roaming subscriber the subscriber is denied service even if other PLMNs are available on which registration was possible.

Cause value #13 – Roaming not allowed in this tracking area

This cause is sent to an 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.

Cause value #14 – EPS services not allowed in this PLMN

This cause is sent to the UE which requests EPS service in a PLMN which does not offer roaming for EPS services to that UE.

NOTE 2: Since only one list of forbidden PLMNs for packet services is maintained in the UE, then the "forbidden PLMNs for GPRS service" is the maintained list and the forbidden PLMNs for EPS service is equivalent to it.

Cause value #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 in the same PLMN.

NOTE 3: Cause #15 and cause #12 differ in the fact that cause #12 does not trigger the UE to search for another allowed tracking area on the same PLMN.

Cause value #25 – Not authorized for this CSG

This cause is sent to the UE if it requests tracking area updating in a CSG cell with CSG ID not belonging to the allowed CSG list where the UE, by subscription, is not allowed to operate, but when it should find another allowed tracking area in the same PLMN.

Cause value #40 – No EPS bearer context activated

This cause is sent to the UE if the UE requests an establishment of the radio access bearers for all active EPS bearer contexts by sending a tracking area update with "active flag" message to the network, but the MME does not have the corresponding active EPS bearer context(s).

A.3 Causes related to PLMN specific network failures and congestion/authentication failures

Cause value #16 – MSC temporarily not reachable

This cause is sent to the UE if it requests a combined EPS attach or tracking area updating in a PLMN where the MSC is temporarily not reachable via the EPS part of the network.

Cause value #17 – Network failure

This cause is sent to the UE if the MME cannot service an UE generated request because of PLMN failures.

Cause value #18 – CS domain not available

This cause is sent to the UE if the MME cannot service an UE generated request because of no availability of CS domain.

Cause value #19 – ESM failure

This cause is sent to the UE when there is a failure in the ESM message contained in the EMM message.

Cause value #20 – MAC failure

This cause is sent to the network if the USIM detects that the MAC in the AUTHENTICATION REQUEST message is not fresh (see 3GPP TS 33.401 [19]).

Cause value #21 – Synch failure

This cause is sent to the network if the USIM detects that the SQN in the AUTHENTICATION REQUEST message is out of range (see 3GPP TS 33.401 [19]).

Cause value #22 – Congestion

This cause is sent to the UE because of congestion in the network (e.g. no channel, facility busy/congested etc.).

Cause value #23 – UE security capabilities mismatch

This cause is sent to the network if the UE detects that one or more security parameter(s) (e.g. the UE security capabilities) do not match the parameter(s) sent back by the network.

Cause value #24 – Security mode rejected, unspecified

This cause is sent to the network if the security mode command is rejected by the UE for unspecified reasons.

Cause value #38 – CS fallback call establishment not allowed

Editor's note: the definition of cause #38 needs to be added.

Cause value #39 – CS domain temporarily not available

Editor's note: the definition of cause #39 needs to be added.

A.4 Causes related to nature of request

NOTE: This subclause has no entries in this version of the specification

A.5 Causes related to invalid messages

Cause value #95 – Semantically incorrect message.

See 3GPP TS 24.008 [13], annex H, subclause H.5.5.

Cause value #96 – Invalid mandatory information.

See 3GPP TS 24.008 [13], annex H, subclause H.6.1.

Cause value #97 – Message type non-existent or not implemented.

See 3GPP TS 24.008 [13], annex H, subclause H.6.2.

Cause value #98 – Message type not compatible with protocol state.

See 3GPP TS 24.008 [13], annex H, subclause H.6.3.

Cause value #99 – Information element non-existent or not implemented.

See 3GPP TS 24.008 [13], annex H, subclause H.6.4.

Cause value #100 – Conditional IE error.

See 3GPP TS 24.008 [13], annex H, subclause H.6.5.

Cause value #101 – Message not compatible with protocol state.

See 3GPP TS 24.008 [13], annex H, subclause H.6.6.

Cause value #111 – Protocol error, unspecified.

See 3GPP TS 24.008 [13], annex H, subclause H.6.8.

Annex B (informative): Cause values for EPS session management

B.1 Causes related to nature of request

Cause value #8 – Operator Determined Barring

This cause is used by the network to indicate that the requested service was rejected by the MME due to Operator Determined Barring.

Cause value #26 – Insufficient resources

This cause is used by the UE or by the network to indicate that the requested service cannot be accepted due to insufficient resources.

Cause value #27 – Unknown or missing access point name

This cause is used by the network to indicate that the requested service was rejected by the external packet data network because the access point name was not included although required or if the access point name could not be resolved.

Cause value #28 – Unknown PDN type

This cause is used by the network to indicate that the requested service was rejected by the external packet data network because the PDN type could not be recognised.

Cause value #29 – User authentication failed

This cause is used by the network to indicate that the requested service was rejected by the external packet data network due to a failed user authentication.

Cause value #30 – Activation rejected by Serving GW or PDN GW

This cause is used by the network to indicate that the requested service was rejected by the Serving GW or PDN GW.

Cause value #31 – Activation rejected, unspecified

This cause is used by the network to indicate that the requested service was rejected due to unspecified reasons.

Cause value #32 – Service option not supported

This cause is used by the network when the UE requests a service which is not supported by the PLMN.

Cause value #33 – Requested service option not subscribed

This cause is sent when the UE requests a service option for which it has no subscription.

Cause value #34 – Service option temporarily out of order

This cause is sent when the network cannot service the request because of temporary outage of one or more functions required for supporting the service.

Cause value #35 – PTI already in use

This cause is used by the network to indicate that the PTI included by the UE is already in use by another active UE requested procedure for this UE.

Cause value #36 – Regular deactivation

This cause is used to indicate a regular UE or network initiated release of EPS bearer resources.

Cause value #37 – EPS QoS not accepted

This cause is used by the network if the new EPS QoS cannot be accepted that was indicated in the UE request.

Cause value #38 – Network failure

This cause is used by the network to indicate that the requested service was rejected due to an error situation in the network.

Cause value #41 – Semantic error in the TFT operation.

This cause is used by the network or the UE to indicate that the requested service was rejected due to a semantic error in the TFT operation included in the request.

Cause value #42 – Syntactical error in the TFT operation.

This cause is used by the network or the UE to indicate that the requested service was rejected due to a syntactical error in the TFT operation included in the request.

Cause value #43 – Unknown EPS bearer context

This cause is used by the network or the UE to indicate that the EPS bearer context identified by the linked EPS bearer identity IE in the request is not active.

Cause value #44 – Semantic errors in packet filter(s)

This cause is used by the network or the UE to indicate that the requested service was rejected due to one or more semantic errors in packet filter(s) of the TFT included in the request.

Cause value #45 – Syntactical error in packet filter(s)

This cause is used by the network or the UE to indicate that the requested service was rejected due to one or more syntactical errors in packet filter(s) of the TFT included in the request.

Cause value #46 – EPS bearer context without TFT already activated

This cause is used by the network or the UE to indicate that it has already activated an EPS bearer context without TFT.

Cause value #49 – Last PDN disconnection not allowed

This cause is used by the network to indicate that the UE requested PDN disconnection procedure on the last remaining PDN connection is not allowed.

Cause value #50 – PDN type IPv4 only allowed

This cause is used by the network to indicate that the requested PDN connectivity is accepted with the restriction that only PDN type IPv4 is allowed.

Cause value #51 – PDN type IPv6 only allowed

This cause is used by the network to indicate that the requested PDN connectivity is accepted with the restriction that only PDN type IPv6 is allowed.

Cause value #52 – single address bearers only allowed

This cause is used by the network to indicate that the requested PDN connectivity is accepted with the restriction that only single IP version bearers are allowed.

Cause value #53 – ESM information not received

This cause is used by the network to indicate that the PDN connectivity procedure was rejected due to the ESM information was not received.

Cause value #54 – PDN connection does not exist

Editor's note: the definition of cause #54 needs to be added.

Cause value #81 – Invalid PTI value

This cause is used by the network or UE to indicate that the PTI provided to it is unassigned or reserved.

Cause value #112 – APN restriction value incompatible with active EPS bearer context.

This cause is used by the network to indicate that the EPS bearer context(s) have an APN restriction value that is not allowed in combination with a currently active EPS bearer context. Restriction values are defined in 3GPP TS 23.060 [4].

B.2 Protocol errors (e.g., unknown message) class

Cause value #95 – Semantically incorrect message

This cause is used to report receipt of a message with semantically incorrect contents.

Cause value #96 – Invalid mandatory information

This cause indicates that the equipment sending this cause has received a message with a non-semantical mandatory IE error.

Cause value #97 – Message type non-existent or not implemented

This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined, or defined but not implemented by the equipment sending this cause.

Cause value #98 – Message type not compatible with protocol state

This cause indicates that the equipment sending this cause has received a message not compatible with the protocol state.

Cause value #99 – Information element non-existent or not implemented

This cause indicates that the equipment sending this cause has received a message which includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the cause. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.

Cause value #100 – Conditional IE error

This cause indicates that the equipment sending this cause has received a message with conditional IE errors.

Cause value #101 – Message not compatible with protocol state

This cause indicates that a message has been received which is incompatible with the protocol state.

Cause value #111 – Protocol error, unspecified

This cause is used to report a protocol error event only when no other cause in the protocol error class applies.

Annex C (normative): Storage of EMM information

The following EMM parameters shall be stored on the USIM if the corresponding file is present:

- GUTI;
- last visited registered TAI;
- EPS update status;
- Allowed CSG list; and
- EPS security context parameters.

The presence and format of corresponding files on the USIM is specified in 3GPP TS 31.102 [17].

If the corresponding file is not present on the USIM, these EMM parameters are stored in a non-volatile memory in the ME together with the IMSI from the USIM. These EMM parameters can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory; else the UE shall delete the EMM parameters.

Annex D (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2008-02					Draft skeleton provided		0.0.0
2008-02	CT1#51 bis				Includes the following contributions agreed by CT1: C1-080690, C1-080743, C1-080769	0.0.0	0.1.0
2008-03	e-mail review				Correction of references that were not updated during the implementation of C1-080769	0.1.0	0.1.1
2008-04	CT1#52				Includes the following contributions agreed by CT1: C1-080943, C1-081020, C1-081037, C1-081057, C1-081058, C1-081268, C1-081269, C1-081272, C1-081273, C1-081278, C1-081280, C1-081289, C1-081290, C1-081291, C1-081292, C1-081296, C1-081301, C1-081302, C1-081387, C1-081407, C1-081409, C1-081417, C1-081418, C1-081436, C1-081437, C1-081438, C1-081439, C1-081440, C1-081442	0.1.1	0.2.0
2008-05	CT1#53				Includes the following contributions agreed by CT1: C1-081650, C1-081651, C1-081878, C1-081886, C1-081887, C1-081888, C1-081889, C1-081890, C1-081971, C1-081972, C1-081973, C1-081974, C1-081975, C1-081978, C1-081979, C1-081988, C1-081989, C1-081990, C1-081991, C1-081992, C1-081993, C1-081994, C1-081996, C1-081997, C1-081998, C1-081999, C1-082000, C1-082062, C1-082095, C1-082097, C1-082099, C1-082100, C1-082101, C1-082111	0.2.0	0.3.0
2008-07	CT1#54				Includes the following contributions agreed by CT1: C1-082125, C1-082126, C1-082282, C1-082415, C1-082432, C1-082485, C1-082487, C1-082510, C1-082572, C1-082573, C1-082574, C1-082577, C1-082578, C1-082579, C1-082580, C1-082586, C1-082588, C1-082589, C1-082633, C1-082634, C1-082635, C1-082636, C1-082701, C1-082702, C1-082703, C1-082705, C1-082719, C1-082720, C1-082722, C1-082723, C1-082724, C1-082725, C1-082726, C1-082727, C1-082728, C1-082729, C1-082791, C1-082794, C1-082795, C1-082797, C1-082802, C1-082807, C1-082811, C1-082816, C1-082819, C1-082820	0.3.0	0.4.0
2008-08	CT1#55				Includes the following contributions agreed by CT1: C1-082981, C1-082995, C1-082997, C1-083013, C1-083030, C1-083031, C1-083032, C1-083056, C1-083131, C1-083139, C1-083140, C1-083146, C1-083151, C1-083168, C1-083442, C1-083445, C1-083450, C1-083452, C1-083453, C1-083454, C1-083456, C1-083457, C1-083461, C1-083462, C1-083463, C1-083465, C1-083468, C1-083471, C1-083472, C1-083473, C1-083474, C1-083476, C1-083477, C1-083517, C1-083522, C1-083580, C1-083581, C1-083582, C1-083583, C1-083584, C1-083588, C1-083591, C1-083592, C1-083593, C1-083597, C1-083598, C1-083599, C1-083605, C1-083606, C1-083607, C1-083609, C1-083616, C1-083619, C1-083629, C1-083630, C1-083635, C1-083636, C1-083638	0.4.0	0.5.0
2008-09	-	-	-	-	Version 1.0.0 created for presentation to TSG CT#41 for information	0.5.0	1.0.0
2008-10	CT1#55 bis				Includes the following contributions agreed by CT1: C1-083788, C1-083789, C1-083948, C1-083949, C1-083953, C1-084002, C1-084012, C1-084104, C1-084143, C1-084144, C1-084146, C1-084308, C1-084310, C1-084316, C1-084329, C1-084332, C1-084333, C1-084335, C1-084337, C1-084338, C1-084340, C1-084341, C1-084343, C1-084344, C1-084346, C1-084348, C1-084349, C1-084351, C1-084352, C1-084353, C1-084355, C1-084357, C1-084358, C1-084359, C1-084360, C1-084362, C1-084381, C1-084475, C1-084478, C1-084479, C1-084480, C1-084484, C1-084490, C1-084491, C1-084492, C1-084499, C1-084551, C1-084554	1.0.0	1.1.0
2008-10	e-mail review				Correction of implementation of C1-084492	1.1.0	1.1.1
2008-10	e-mail review				Correction of implementation of C1-084353	1.1.1	1.1.2
2008-11	CT1#56				Includes the following contributions agreed by CT1: C1-084592, C1-084610, C1-084624, C1-084627, C1-084666, C1-084668, C1-084747, C1-084785, C1-084925, C1-084926,	1.1.2	1.2.0

					C1-084976, C1-084977, C1-085167, C1-085170, C1-085171, C1-085172, C1-085174, C1-085175, C1-085178, C1-085180, C1-085199, C1-085304, C1-085310, C1-085312, C1-085313, C1-085315, C1-085317, C1-085356, C1-085372, C1-085381, C1-085385, C1-085387, C1-085388, C1-085390, C1-085392, C1-085394, C1-085396, C1-085398, C1-085399, C1-085505, C1-085506, C1-085508, C1-085509, C1-085510, C1-085511, C1-085512, C1-085513, C1-085514, C1-085515, C1-085518, C1-085520, C1-085521, C1-085528, C1-085533, C1-085539, C1-085540, C1-085541, C1-085542, C1-085545, C1-085550, C1-085551, C1-085552, C1-085553		
2008-11	review				Correction of implementation of C1-084926, C1-085180	1.2.0	1.2.1
2008-11					Version 2.0.0 created for presentation to TSG CT#42 for approval	1.2.1	2.0.0
2008-12	CT-42				Version 8.0.0 created after approval in CT#42	2.0.0	8.0.0

History

Document history		
V8.0.0	January 2009	Publication