ETSI TS 124 301 V9.11.0 (2013-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
Non-Access-Stratum (NAS)
protocol for Evolved Packet System (EPS);
Stage 3
(3GPP TS 24.301 version 9.11.0 Release 9)

Reference
RTS/TSGC-0124301v9b0

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2013.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

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://ipr.etsi.org).

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

Intellectual Property Rights 2
Foreword 2
Foreword 15
1 Scope 16
2 References 16
3 Definitions and abbreviations 18
3.1 Definitions 18
3.2 Abbreviations 21
4 General 22
4.1 Overview 22
4.2 Linkage between the protocols for EPS mobility management and EPS session management 22
4.3 UE mode of operation 23
4.3.1 General 23
4.3.2 Change of UE mode of operation 23
4.3.2.1 General 23
4.3.2.2 Change of UE's usage setting 25
4.3.2.3 Change of voice domain preference for E-UTRAN 26
4.3.2.4 Change of IMS registration status 27
4.3.2.5 Change of configuration regarding the use of SMS. 28
4.4 NAS security 29
4.4.1 General 29
4.4.2 Handling of EPS security contexts 29
4.4.2.1 General 29
4.4.2.2 Establishment of a mapped EPS security context during intersystem handover 30
4.4.2.3 Establishment of secure exchange of NAS messages 31
4.4.2.4 Change of security keys 32
4.4.3 Handling of NAS COUNT and NAS sequence number 32
4.4.3.1 General 32
4.4.3.2 Replay protection 33
4.4.3.3 Integrity protection and verification 33
4.4.3.4 Ciphering and deciphering 33
4.4.3.5 NAS COUNT wrap around 33
4.4.4 Integrity protection of NAS signalling messages 34
4.4.4.1 General 34
4.4.4.2 Integrity checking of NAS signalling messages in the UE 34
4.4.4.3 Integrity checking of NAS signalling messages in the MME 35
4.4.5 Ciphering of NAS signalling messages 36
4.5 Disabling and re-enabling of UE's E-UTRA capability 37
5 Elementary procedures for EPS mobility management 37
5.1 Overview 37
5.1.1 General 37
5.1.2 Types of EMM procedures 37
5.1.3 EMM sublayer states 38
5.1.3.1 General 38
5.1.3.2 EMM sublayer states in the UE 39
5.1.3.2.1 General 39
5.1.3.2.2 Main states 39
5.1.3.2.2.1 EMM-NULL 39
5.1.3.2.2.2 EMM-DEREGISTERED 39
5.1.3.2.2.3 EMM-REGISTERED-INITIATED 39
5.1.3.2.2.4 EMM-REGISTERED 39
5.1.3.2.2.5 EMM-DEREGISTERED-INITIATED 39
5.1.3.2.2.6 EMM-TRACKING-AREA-UPDATING-INITIATED 39

5.1.3.2.2.7 EMM-SERVICE-REQUEST-INITIATED 39
5.1.3.2.3 Substates of state EMM-DEREGISTERED 40
5.1.3.2.3.1 General 40
5.1.3.2.3.2 EMM-DEREGISTERED.NORMAL-SERVICE 40
5.1.3.2.3.3 EMM-DEREGISTERED.LIMITED-SERVICE 40
5.1.3.2.3.4 EMM-DEREGISTERED.ATTEMPTING-TO-ATTACH 40
5.1.3.2.3.5 EMM-DEREGISTERED.PLMN-SEARCH 41
5.1.3.2.3.6 EMM-DEREGISTERED.NO-IMSI 41
5.1.3.2.3.7 EMM-DEREGISTERED.ATTACH-NEEDED 41
5.1.3.2.3.8 EMM-DEREGISTERED.NO-CELL-AVAILABLE 41
5.1.3.2.4 Substates of state EMM-REGISTERED 41
5.1.3.2.4.1 General 41
5.1.3.2.4.2 EMM-REGISTERED.NORMAL-SERVICE 41
5.1.3.2.4.3 EMM-REGISTERED.ATTEMPTING-TO-UPDATE 41
5.1.3.2.4.4 EMM-REGISTERED.LIMITED-SERVICE 41
5.1.3.2.4.5 EMM-REGISTERED.PLMN-SEARCH 41
5.1.3.2.4.6 EMM-REGISTERED.UPDATE-NEEDED 41
5.1.3.2.4.7 EMM-REGISTERED.NO-CELL-AVAILABLE 41
5.1.3.2.4.8 EMM-REGISTERED.ATTEMPTING-TO-UPDATE-MM 42
5.1.3.2.4.9 EMM-REGISTERED.IMSI-DETACH-INITIATED 42
5.1.3.3 EPS update status 42
5.1.3.4 EMM sublayer states in the MME 42
5.1.3.4.1 EMM-DEREGISTERED 42
5.1.3.4.2 EMM-COMMON-PROCEDURE-INITIATED 42
5.1.3.4.3 EMM-REGISTERED 42
5.1.3.4.4 EMM-DEREGISTERED-INITIATED 42
5.1.4 Coordination between EMM and GMM 43
5.1.5 Coordination between EMM and MM 43
5.2 Behaviour of the UE in state EMM-DEREGISTERED and state EMM-REGISTERED 44
5.2.1 General 44
5.2.2 UE behaviour in state EMM-DEREGISTERED 44
5.2.2.1 General 44
5.2.2.2 Primary substate selection 44
5.2.2.2.1 Selection of the substate after power on 44
5.2.2.3 Detailed description of UE behaviour in state EMM-DEREGISTERED 44
5.2.2.3.1 NORMAL-SERVICE 44
5.2.2.3.2 LIMITED-SERVICE 45
5.2.2.3.3 ATTEMPTING-TO-ATTACH 45
5.2.2.3.4 PLMN-SEARCH 45
5.2.2.3.5 NO-IMSI 45
5.2.2.3.6 ATTACH-NEEDED 45
5.2.2.3.7 NO-CELL-AVAILABLE 45
5.2.2.4 Substate when back to state EMM-DEREGISTERED from another EMM state 45
5.2.3 UE behaviour in state EMM-REGISTERED 46
5.2.3.1 General 46
5.2.3.2 Detailed description of UE behaviour in state EMM-REGISTERED 46
5.2.3.2.1 NORMAL-SERVICE 46
5.2.3.2.2 ATTEMPTING-TO-UPDATE 46
5.2.3.2.3 LIMITED-SERVICE 46
5.2.3.2.4 PLMN-SEARCH 46
5.2.3.2.5 UPDATE-NEEDED 47
5.2.3.2.6 NO-CELL-AVAILABLE 47
5.2.3.2.7 ATTEMPTING-TO-UPDATE-MM 47
5.2.3.2.8 IMSI-DETACH-INITIATED 47
5.3 General on elementary EMM procedures 47
5.3.1 EMM modes and NAS signalling connection 47
5.3.1.1 Establishment of the NAS signalling connection 47
5.3.1.2 Release of the NAS signalling connection 48
5.3.2 Lists of forbidden tracking areas 48
5.3.3 List of forbidden PLMNs for attach in S101 mode 49
5.3.4 Equivalent PLMNs list 49
5.3.5 Handling of the periodic tracking area update timer and mobile reachable timer (S1 mode only) 49

5.3.6 Handling of timer T3402 50
5.3.7 Handling of the Local Emergency Numbers List 50
5.3.8 Abnormal cases in the UE 51
5.4 EMM common procedures 51
5.4.1 GUTI reallocation procedure 51
5.4.1.1 General 51
5.4.1.2 GUTI reallocation initiation by the network 51
5.4.1.3 GUTI reallocation completion by the UE 52
5.4.1.4 GUTI reallocation completion by the network 52
5.4.1.5 Abnormal cases in the UE 52
5.4.1.6 Abnormal cases on the network side 52
5.4.2 Authentication procedure 53
5.4.2.1 General 53
5.4.2.2 Authentication initiation by the network 54
5.4.2.3 Authentication response by the UE 54
5.4.2.4 Authentication completion by the network 55
5.4.2.5 Authentication not accepted by the network 55
5.4.2.6 Authentication not accepted by the UE 56
5.4.2.7 Abnormal cases 56
5.4.3 Security mode control procedure 60
5.4.3.1 General 60
5.4.3.2 NAS security mode control initiation by the network 60
5.4.3.3 NAS security mode command accepted by the UE 62
5.4.3.4 NAS security mode control completion by the network 63
5.4.3.5 NAS security mode command not accepted by the UE 63
5.4.3.6 Abnormal cases in the UE 63
5.4.3.7 Abnormal cases on the network side 64
5.4.4 Identification procedure 64
5.4.4.1 General 64
5.4.4.2 Identification initiation by the network 65
5.4.4.3 Identification response by the UE 65
5.4.4.4 Identification completion by the network 65
5.4.4.5 Abnormal cases in the UE 65
5.4.4.6 Abnormal cases on the network side 65
5.4.5 EMM information procedure 66
5.4.5.1 General 66
5.4.5.2 EMM information procedure initiation by the network 66
5.4.5.3 EMM information procedure in the UE 67
5.4.5.4 Abnormal cases on the network side 67
5.5 EMM specific procedures 67
5.5.1 Attach procedure 67
5.5.1.1 General 67
5.5.1.2 Attach procedure for EPS services 68
5.5.1.2.1 General 68
5.5.1.2.2 Attach procedure initiation 68
5.5.1.2.3 EMM common procedure initiation 69
5.5.1.2.4 Attach accepted by the network 70
5.5.1.2.5 Attach not accepted by the network 71
5.5.1.2.5A Attach for emergency bearer services not accepted by the network 74
5.5.1.2.5B Attach for initiating a PDN connection for emergency bearer services not accepted by the network 74
5.5.1.2.6 Abnormal cases in the UE 74
5.5.1.2.7 Abnormal cases on the network side 76
5.5.1.3 Combined attach procedure for EPS services and non-EPS services (S1 mode only) 77
5.5.1.3.1 General 77
5.5.1.3.2 Combined attach procedure initiation 77
5.5.1.3.3 EMM common procedure initiation 77
5.5.1.3.4 Combined attach accepted by the network 78
5.5.1.3.4.1 General 78
5.5.1.3.4.2 Combined attach successful 78
5.5.1.3.4.3 Combined attach successful for EPS services only 79
5.5.1.3.5 Combined attach not accepted by the network 80

5.5.1.3.6 Abnormal cases in the UE 82
5.5.1.3.7 Abnormal cases on the network side 83
5.5.2 Detach procedure 83
5.5.2.1 General 83
5.5.2.2 UE initiated detach procedure 84
5.5.2.2.1 UE initiated detach procedure initiation 84
5.5.2.2.2 UE initiated detach procedure completion for EPS services only 85
5.5.2.2.3 UE initiated combined detach procedure completion 85
5.5.2.2.4 Abnormal cases in the UE 85
5.5.2.2.5 Abnormal cases on the network side 87
5.5.2.3 Network initiated detach procedure 87
5.5.2.3.1 Network initiated detach procedure initiation 87
5.5.2.3.2 Network initiated detach procedure completion by the UE 87
5.5.2.3.3 Network initiated detach procedure completion by the network 91
5.5.2.3.4 Abnormal cases in the UE 91
5.5.2.3.5 Abnormal cases on the network side 91
5.5.3 Tracking area updating procedure (S1 mode only) 92
5.5.3.1 General 92
5.5.3.2 Normal and periodic tracking area updating procedure 93
5.5.3.2.1 General 93
5.5.3.2.2 Normal and periodic tracking area updating procedure initiation 94
5.5.3.2.3 EMM common procedure initiation 96
5.5.3.2.4 Normal and periodic tracking area updating procedure accepted by the network 96
5.5.3.2.5 Normal and periodic tracking area updating procedure not accepted by the network 99
5.5.3.2.5A Tracking area updating procedure for initiating a PDN connection for emergency bearer services not accepted by the network 102
5.5.3.2.6 Abnormal cases in the UE 102
5.5.3.2.7 Abnormal cases on the network side 104
5.5.3.3 Combined tracking area updating procedure 105
5.5.3.3.1 General 105
5.5.3.3.2 Combined tracking area updating procedure initiation 105
5.5.3.3.3 EMM common procedure initiation 106
5.5.3.3.4 Combined tracking area updating procedure accepted by the network 106
5.5.3.3.4.1 General 106
5.5.3.3.4.2 Combined tracking area updating successful 106
5.5.3.3.4.3 Combined tracking area updating successful for EPS services only 107
5.5.3.3.5 Combined tracking area updating procedure not accepted by the network 108
5.5.3.3.6 Abnormal cases in the UE 111
5.5.3.3.7 Abnormal cases on the network side 112
5.6 EMM connection management procedures (S1 mode only) 112
5.6.1 Service request procedure 112
5.6.1.1 General 112
5.6.1.2 Service request procedure initiation 114
5.6.1.3 EMM common procedure initiation 115
5.6.1.4 Service request procedure accepted by the network 115
5.6.1.5 Service request procedure not accepted by the network 116
5.6.1.5A Service request procedure for initiating a PDN connection for emergency bearer services not accepted by the network 119
5.6.1.6 Abnormal cases in the UE 119
5.6.1.7 Abnormal cases on the network side 121
5.6.2 Paging procedure 122
5.6.2.1 General 122
5.6.2.2 Paging for EPS services 122
5.6.2.2.1 Paging for EPS services through E-UTRAN using S-TMSI 122
5.6.2.2.2 Paging for EPS services through E-UTRAN using IMSI 122
5.6.2.3 Paging for CS fallback to A/Gb or Iu mode 123
5.6.2.3.1 General 123
5.6.2.3.2 Abnormal cases in the UE 124
5.6.2.4 Paging for SMS 124
5.6.3 Transport of NAS messages procedure 124
5.6.3.1 General 124
5.6.3.2 UE initiated transport of NAS messages 124

5.6.3.3 Network initiated transport of NAS messages 124
5.6.3.4 Abnormal cases in the UE 124
5.6.3.5 Abnormal cases on the network side 125
5.6.4 Generic transport of NAS messages procedure 125
5.6.4.1 General 125
5.6.4.2 UE initiated generic transport of NAS messages 125
5.6.4.3 Network initiated transport of NAS messages 125
5.6.4.4 Abnormal cases in the UE 125
5.6.4.5 Abnormal cases on the network side 125
5.7 Reception of an EMM STATUS message by an EMM entity 126

6 Elementary procedures for EPS session management 126
6.1 Overview 126
6.1.1 General 126
6.1.2 Types of ESM procedures 127
6.1.3 ESM sublayer states 127
6.1.3.1 General 127
6.1.3.2 ESM sublayer states in the UE 128
6.1.3.2.1 BEARER CONTEXT INACTIVE 128
6.1.3.2.2 BEARER CONTEXT ACTIVE 128
6.1.3.2.3 PROCEDURE TRANSACTION INACTIVE 128
6.1.3.2.4 PROCEDURE TRANSACTION PENDING 128
6.1.3.3 ESM sublayer states in the MME 128
6.1.3.3.1 BEARER CONTEXT INACTIVE 128
6.1.3.3.2 BEARER CONTEXT ACTIVE PENDING 128
6.1.3.3.3 BEARER CONTEXT ACTIVE 129
6.1.3.3.4 BEARER CONTEXT INACTIVE PENDING 129
6.1.3.3.5 BEARER CONTEXT MODIFY PENDING 129
6.1.3.3.6 PROCEDURE TRANSACTION INACTIVE 129
6.1.3.3.7 PROCEDURE TRANSACTION PENDING 129
6.1.4 Coordination between ESM and SM 130
6.1.5 Coordination between ESM and EMM for supporting ISR 130
6.2 IP address allocation 131
6.2.1 General 131
6.2.2 IP address allocation via NAS signalling 131
6.3 General on elementary ESM procedures 132
6.3.1 Services provided by lower layers 132
6.3.2 Principles of address handling for ESM procedures 132
6.3.3 Abnormal cases in the UE 133
6.3.4 Abnormal cases in the network 134
6.4 Network initiated ESM procedures 134
6.4.1 Default EPS bearer context activation procedure 134
6.4.1.1 General 134
6.4.1.2 Default EPS bearer context activation initiated by the network 134
6.4.1.3 Default EPS bearer context activation accepted by the UE 135
6.4.1.4 Default EPS bearer context activation not accepted by the UE 135
6.4.1.5 Abnormal cases in the UE 136
6.4.1.6 Abnormal cases on the network side 136
6.4.2 Dedicated EPS bearer context activation procedure 136
6.4.2.1 General 136
6.4.2.2 Dedicated EPS bearer context activation initiated by the network 136
6.4.2.3 Dedicated EPS bearer context activation accepted by the UE 137
6.4.2.4 Dedicated EPS bearer context activation not accepted by the UE 137
6.4.2.5 Abnormal cases in the UE 138
6.4.2.6 Abnormal cases on the network side 139
6.4.3 EPS bearer context modification procedure 139
6.4.3.1 General 139
6.4.3.2 EPS bearer context modification initiated by the network 139
6.4.3.3 EPS bearer context modification accepted by the UE 140
6.4.3.4 EPS bearer context modification not accepted by the UE 140
6.4.3.5 Abnormal cases in the UE 142
6.4.3.6 Abnormal cases on the network side 142

6.4.4 EPS bearer context deactivation procedure....143
6.4.4.1 General....143
6.4.4.2 EPS bearer context deactivation initiated by the network....143
6.4.4.3 EPS bearer context deactivation accepted by the UE....144
6.4.4.4 Abnormal cases in the UE....144
6.4.4.5 Abnormal cases on the network side....145
6.4.4.6 Local EPS bearer context deactivation without ESM signalling....145
6.5 UE requested ESM procedures....146
6.5.1 UE requested PDN connectivity procedure....146
6.5.1.1 General....146
6.5.1.2 UE requested PDN connectivity procedure initiation....146
6.5.1.3 UE requested PDN connectivity procedure accepted by the network....147
6.5.1.4 UE requested PDN connectivity procedure not accepted by the network....148
6.5.1.5 Abnormal cases in the UE....148
6.5.1.6 Abnormal cases on the network side....149
6.5.2 UE requested PDN disconnect procedure....149
6.5.2.1 General....149
6.5.2.2 UE requested PDN disconnection procedure initiation....149
6.5.2.3 UE requested PDN disconnection procedure accepted by the network....150
6.5.2.4 UE requested PDN disconnection procedure not accepted by the network....150
6.5.2.5 Abnormal cases in the UE....150
6.5.2.6 Abnormal cases on the network side....151
6.5.3 UE requested bearer resource allocation procedure....151
6.5.3.1 General....151
6.5.3.2 UE requested bearer resource allocation procedure initiation....151
6.5.3.3 UE requested bearer resource allocation procedure accepted by the network....152
6.5.3.4 UE requested bearer resource allocation procedure not accepted by the network....152
6.5.3.5 Abnormal cases in the UE....154
6.5.3.6 Abnormal cases on the network side....154
6.5.4 UE requested bearer resource modification procedure....154
6.5.4.1 General....154
6.5.4.2 UE requested bearer resource modification procedure initiation....155
6.5.4.3 UE requested bearer resource modification procedure accepted by the network....155
6.5.4.4 UE requested bearer resource modification procedure not accepted by the network....156
6.5.4.5 Abnormal cases in the UE....158
6.5.4.6 Abnormal cases on the network side....159
6.6 Miscellaneous procedures....159
6.6.1 Exchange of protocol configuration options....159
6.6.1.1 General....159
6.6.1.2 ESM information request procedure....159
6.6.1.2.1 General....159
6.6.1.2.2 ESM information request initiated by the network....159
6.6.1.2.3 ESM information request completion by the UE....160
6.6.1.2.4 ESM information request completion by the network....160
6.6.1.2.5 Abnormal cases in the UE....160
6.6.1.2.6 Abnormal cases on the network side....160
6.6.1.3 Exchange of protocol configuration options in other messages....160
6.6.2 Notification procedure....161
6.6.2.1 General....161
6.6.2.2 Notification procedure initiation by the network....161
6.6.2.3 Notification procedure in the UE....161
6.6.2.4 Abnormal cases on the network side....161
6.7 Reception of an ESM STATUS message by an ESM entity....161

7 Handling of unknown, unforeseen, and erroneous protocol data....162
7.1 General....162
7.2 Message too short....163
7.3 Unknown or unforeseen procedure transaction identity or EPS bearer identity....163
7.3.1 Procedure transaction identity....163
7.3.2 EPS bearer identity....164
7.4 Unknown or unforeseen message type....166
7.5 Non-semantical mandatory information element errors....166

7.5.1 Common procedures 166
7.5.2 EPS mobility management 166
7.5.3 EPS session management 167
7.6 Unknown and unforeseen IEs in the non-imperative message part 167
7.6.1 IEIs unknown in the message 167
7.6.2 Out of sequence IEs 167
7.6.3 Repeated IEs 167
7.7 Non-imperative message part errors 168
7.7.1 Syntactically incorrect optional IEs 168
7.7.2 Conditional IE errors 168
7.8 Messages with semantically incorrect contents 168

8 Message functional definitions and contents 168
8.1 Overview 168
8.2 EPS mobility management messages 169
8.2.1 Attach accept 169
8.2.1.1 Message definition 169
8.2.1.2 GUTI 170
8.2.1.3 Location area identification 170
8.2.1.4 MS identity 170
8.2.1.5 EMM cause 170
8.2.1.6 T3402 value 170
8.2.1.7 T3423 value 171
8.2.1.8 Equivalent PLMNs 171
8.2.1.9 Emergency number list 171
8.2.1.10 EPS network feature support 171
8.2.1.11 Additional update result 171
8.2.2 Attach complete 171
8.2.3 Attach reject 171
8.2.3.1 Message definition 171
8.2.3.2 ESM message container 172
8.2.4 Attach request 172
8.2.4.1 Message definition 172
8.2.4.2 Old P-TMSI signature 173
8.2.4.3 Additional GUTI 173
8.2.4.4 Last visited registered TAI 173
8.2.4.5 DRX parameter 173
8.2.4.6 MS network capability 174
8.2.4.7 Old location area identification 174
8.2.4.8 TMSI status 174
8.2.4.9 Mobile station classmark 2 174
8.2.4.10 Mobile station classmark 3 174
8.2.4.11 Supported Codecs 174
8.2.4.12 Additional update type 174
8.2.4.13 Voice domain preference and UE's usage setting 174
8.2.5 Authentication failure 174
8.2.5.1 Message definition 174
8.2.5.2 Authentication failure parameter 175
8.2.6 Authentication reject 175
8.2.7 Authentication request 175
8.2.8 Authentication response 176
8.2.9 CS service notification 176
8.2.9.1 Message definition 176
8.2.9.2 CLI 177
8.2.9.3 SS Code 177
8.2.9.4 LCS indicator 177
8.2.9.5 LCS client identity 177
8.2.10 Detach accept 177
8.2.10.1 Detach accept (UE originating detach) 177
8.2.10.2 Detach accept (UE terminated detach) 178
8.2.11 Detach request 178
8.2.11.1 Detach request (UE originating detach) 178

8.2.11.2 Detach request (UE terminated detach) 179
8.2.11.2.1 Message definition 179
8.2.11.2.2 EMM cause 179
8.2.12 Downlink NAS Transport 179
8.2.13 EMM information 179
8.2.13.1 Message definition 179
8.2.13.2 Full name for network 180
8.2.13.3 Short name for network 180
8.2.13.4 Local time zone 180
8.2.13.5 Universal time and local time zone 180
8.2.13.6 Network daylight saving time 181
8.2.14 EMM status 181
8.2.15 Extended service request 181
8.2.15.1 Message definition 181
8.2.15.2 CSFB response 182
8.2.15.3 EPS bearer context status 182
8.2.16 GUTI reallocation command 182
8.2.16.1 Message definition 182
8.2.16.2 TAI list 182
8.2.17 GUTI reallocation complete 182
8.2.18 Identity request 183
8.2.19 Identity response 183
8.2.20 Security mode command 183
8.2.20.1 Message definition 183
8.2.20.2 IMEISV request 184
8.2.20.3 Replayed $nonce_{UE}$ 184
8.2.20.4 $Nonce_{MME}$ 184
8.2.21 Security mode complete 184
8.2.21.1 Message definition 184
8.2.21.2 IMEISV 185
8.2.22 Security mode reject 185
8.2.23 Security protected NAS message 185
8.2.24 Service reject 185
8.2.24.1 Message definition 185
8.2.24.2 T3442 value 186
8.2.25 Service request 186
8.2.26 Tracking area update accept 186
8.2.26.1 Message definition 186
8.2.26.2 T3412 value 187
8.2.26.3 GUTI 187
8.2.26.4 TAI list 187
8.2.26.5 EPS bearer context status 187
8.2.26.6 Location area identification 188
8.2.26.7 MS identity 188
8.2.26.8 EMM cause 188
8.2.26.9 T3402 value 188
8.2.26.10 T3423 value 188
8.2.26.11 Equivalent PLMNs 188
8.2.26.12 Emergency number list 188
8.2.26.13 EPS network feature support 188
8.2.26.14 Additional EPS result 188
8.2.27 Tracking area update complete 188
8.2.28 Tracking area update reject 189
8.2.29 Tracking area update request 189
8.2.29.1 Message definition 189
8.2.29.2 Non-current native NAS key set identifier 190
8.2.29.3 GPRS ciphering key sequence number 191
8.2.29.4 Old P-TMSI signature 191
8.2.29.5 Additional GUTI 191
8.2.29.6 $Nonce_{UE}$ 191
8.2.29.7 UE network capability 191
8.2.29.8 Last visited registered TAI 191

8.2.29.9 DRX parameter 191
8.2.29.10 UE radio capability information update needed 191
8.2.29.11 EPS bearer context status 191
8.2.29.12 MS network capability 191
8.2.29.13 Old location area identification 191
8.2.29.14 TMSI status 191
8.2.29.15 Mobile station classmark 2 191
8.2.29.16 Mobile station classmark 3 192
8.2.29.17 Supported Codecs 192
8.2.29.18 Additional update type 192
8.2.29.19 Voice domain preference and UE's usage setting 192
8.2.30 Uplink NAS Transport 192
8.2.31 Downlink generic NAS transport 192
8.2.31.1 Message definition 192
8.2.31.2 Additional information 193
8.2.32 Uplink generic NAS transport 193
8.2.32.1 Message definition 193
8.2.32.2 Additional information 193
8.3 EPS session management messages 194
8.3.1 Activate dedicated EPS bearer context accept 194
8.3.1.1 Message definition 194
8.3.1.2 Protocol configuration options 194
8.3.2 Activate dedicated EPS bearer context reject 194
8.3.2.1 Message definition 194
8.3.2.2 Protocol configuration options 195
8.3.3 Activate dedicated EPS bearer context request 195
8.3.3.1 Message definition 195
8.3.3.2 Transaction identifier 196
8.3.3.3 Negotiated QoS 196
8.3.3.4 Negotiated LLC SAPI 196
8.3.3.5 Radio priority 196
8.3.3.6 Packet flow identifier 196
8.3.3.7 Protocol configuration options 196
8.3.4 Activate default EPS bearer context accept 197
8.3.4.1 Message definition 197
8.3.4.2 Protocol configuration options 197
8.3.5 Activate default EPS bearer context reject 197
8.3.5.1 Message definition 197
8.3.5.2 Protocol configuration options 198
8.3.6 Activate default EPS bearer context request 198
8.3.6.1 Message definition 198
8.3.6.2 Transaction identifier 198
8.3.6.3 Negotiated QoS 198
8.3.6.4 Negotiated LLC SAPI 199
8.3.6.5 Radio priority 199
8.3.6.6 Packet flow identifier 199
8.3.6.7 APN-AMBR 199
8.3.6.8 ESM cause 199
8.3.6.9 Protocol configuration options 199
8.3.7 Bearer resource allocation reject 199
8.3.7.1 Message definition 199
8.3.7.2 Protocol configuration options 199
8.3.8 Bearer resource allocation request 200
8.3.8.1 Message definition 200
8.3.8.2 Protocol configuration options 200
8.3.9 Bearer resource modification reject 200
8.3.9.1 Message definition 200
8.3.9.2 Protocol configuration options 201
8.3.10 Bearer resource modification request 201
8.3.10.1 Message definition 201
8.3.10.2 Required traffic flow QoS 201
8.3.10.3 ESM cause 202

8.3.10.4 Protocol configuration options 202
8.3.11 Deactivate EPS bearer context accept 202
8.3.11.1 Message definition 202
8.3.11.2 Protocol configuration options 202
8.3.12 Deactivate EPS bearer context request 202
8.3.12.1 Message definition 202
8.3.12.2 Protocol configuration options 203
8.3.13 ESM information request 203
8.3.14 ESM information response 203
8.3.14.1 Message definition 203
8.3.14.2 Access point name 204
8.3.14.3 Protocol configuration options 204
8.3.15 ESM status 204
8.3.16 Modify EPS bearer context accept 204
8.3.16.1 Message definition 204
8.3.16.2 Protocol configuration options 205
8.3.17 Modify EPS bearer context reject 205
8.3.17.1 Message definition 205
8.3.17.2 Protocol configuration options 205
8.3.18 Modify EPS bearer context request 206
8.3.18.1 Message definition 206
8.3.18.2 New EPS QoS 206
8.3.18.3 TFT 206
8.3.18.4 New QoS 206
8.3.18.5 Negotiated LLC SAPI 206
8.3.18.6 Radio priority 207
8.3.18.7 Packet flow identifier 207
8.3.18.8 APN-AMBR 207
8.3.18.9 Protocol configuration options 207
8.3.18A Notification 207
8.3.19 PDN connectivity reject 207
8.3.19.1 Message definition 207
8.3.19.2 Protocol configuration options 208
8.3.20 PDN connectivity request 208
8.3.20.1 Message definition 208
8.3.20.2 ESM information transfer flag 208
8.3.20.3 Access point name 209
8.3.20.4 Protocol configuration options 209
8.3.21 PDN disconnect reject 209
8.3.21.1 Message definition 209
8.3.21.2 Protocol configuration options 209
8.3.22 PDN disconnect request 209
8.3.22.1 Message definition 209
8.3.22.2 Protocol configuration options 210

9 General message format and information elements coding 210
9.1 Overview 210
9.2 Protocol discriminator 211
9.3 Security header type and EPS bearer identity 211
9.3.1 Security header type 211
9.3.2 EPS bearer identity 212
9.4 Procedure transaction identity 212
9.5 Message authentication code 212
9.6 Sequence number 212
9.7 NAS message 212
9.8 Message type 213
9.9 Other information elements 214
9.9.1 General 214
9.9.2 Common information elements 215
9.9.2.0 Additional information 215
9.9.2.1 EPS bearer context status 215
9.9.2.2 Location area identification 216

9.9.2.3 Mobile identity 216
9.9.2.4 Mobile station classmark 2 216
9.9.2.5 Mobile station classmark 3 216
9.9.2.6 NAS security parameters from E-UTRA 216
9.9.2.7 NAS security parameters to E-UTRA 216
9.9.2.8 PLMN list 217
9.9.2.9 Spare half octet 217
9.9.2.10 Supported codec list 217
9.9.3 EPS Mobility Management (EMM) information elements 217
9.9.3.0A Additional update result 217
9.9.3.0B Additional update type 218
9.9.3.1 Authentication failure parameter 218
9.9.3.2 Authentication parameter AUTN 218
9.9.3.3 Authentication parameter RAND 219
9.9.3.4 Authentication response parameter 219
9.9.3.4A Ciphering key sequence number 219
9.9.3.5 CSFB response 219
9.9.3.6 Daylight saving time 220
9.9.3.7 Detach type 220
9.9.3.8 DRX parameter 221
9.9.3.9 EMM cause 221
9.9.3.10 EPS attach result 222
9.9.3.11 EPS attach type 223
9.9.3.12 EPS mobile identity 223
9.9.3.12A EPS network feature support 225
9.9.3.13 EPS update result 226
9.9.3.14 EPS update type 227
9.9.3.15 ESM message container 227
9.9.3.16 GPRS timer 228
9.9.3.17 Identity type 2 228
9.9.3.18 IMEISV request 228
9.9.3.19 KSI and sequence number 228
9.9.3.20 MS network capability 229
9.9.3.21 NAS key set identifier 229
9.9.3.22 NAS message container 229
9.9.3.23 NAS security algorithms 230
9.9.3.24 Network name 231
9.9.3.25 Nonce 231
9.9.3.25A Paging identity 231
9.9.3.26 P-TMSI signature 232
9.9.3.27 Service type 232
9.9.3.28 Short MAC 232
9.9.3.29 Time zone 233
9.9.3.30 Time zone and time 233
9.9.3.31 TMSI status 233
9.9.3.32 Tracking area identity 233
9.9.3.33 Tracking area identity list 234
9.9.3.34 UE network capability 238
9.9.3.35 UE radio capability information update needed 241
9.9.3.36 UE security capability 241
9.9.3.37 Emergency Number List 245
9.9.3.38 CLI 245
9.9.3.39 SS Code 246
9.9.3.40 LCS indicator 246
9.9.3.41 LCS client identity 246
9.9.3.42 Generic message container type 247
9.9.3.43 Generic message container 247
9.9.3.44 Voice domain preference and UE's usage setting 248
9.9.4 EPS Session Management (ESM) information elements 248
9.9.4.1 Access point name 248
9.9.4.2 APN aggregate maximum bit rate 248
9.9.4.3 EPS quality of service 250

9.9.4.4 ESM cause....253
9.9.4.5 ESM information transfer flag....254
9.9.4.6 Linked EPS bearer identity....255
9.9.4.7 LLC service access point identifier....255
9.9.4.7A Notification indicator....256
9.9.4.8 Packet flow identifier....256
9.9.4.9 PDN address....256
9.9.4.10 PDN type....257
9.9.4.11 Protocol configuration options....258
9.9.4.12 Quality of service....258
9.9.4.13 Radio priority....258
9.9.4.14 Request type....258
9.9.4.15 Traffic flow aggregate description....258
9.9.4.16 Traffic flow template....258
9.9.4.17 Transaction identifier....259

10 List of system parameters....259
10.1 General....259
10.2 Timers of EPS mobility management....260
10.3 Timers of EPS session management....264

Annex A (informative): Cause values for EPS mobility management....266

A.1 Causes related to UE identification....266

A.2 Cause related to subscription options....266

A.3 Causes related to PLMN specific network failures and congestion/authentication failures....267

A.4 Causes related to nature of request....268

A.5 Causes related to invalid messages....268

Annex B (informative): Cause values for EPS session management....269

B.1 Causes related to nature of request....269

B.2 Protocol errors (e.g., unknown message) class....271

Annex C (normative): Storage of EMM information....273

Annex D (normative): Establishment cause (S1 mode only)....274

D.1 Mapping of NAS procedure to RRC establishment cause (S1 mode only)....274

Annex E (informative): Change history....276

History....284

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]).

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

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".

[1A] 3GPP TS 22.011: "Service accessibility".

[1B] 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS)".

[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".

[8A] 3GPP TS 23.221: "Architectural requirements".

[8B] 3GPP TS 23.251: "Network Sharing; Architecture and Functional Description".

[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".

[13A] 3GPP TS 24.011: "Point-to-Point Short Message Service (SMS) support on mobile radio interface".

[13B] 3GPP TS 24.167: "3GPP IMS Management Object (MO); Stage 3".

[13C] 3GPP TS 24.171: "NAS Signalling for Control Plane LCS in Evolved Packet System (EPS)".

[13D] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); 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".

[15A] 3GPP TS 25.304: "User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode".

[15B] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

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

[16A] 3GPP TS 29.212: "Policy and Charging Control over Gx reference point".

[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".

[22A] 3GPP TS 36.355: "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP)".

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

[23A] 3GPP TS 45.008: "Radio Access Network; Radio subsystem link control".

[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].

1x CS fallback capable UE: A UE that uses a CS infrastructure for a voice call and other CS-domain services by falling back to cdma2000® 1x access network if the UE is served by E-UTRAN when a CS service is requested.

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].

Attached for emergency bearer services: A UE is attached for emergency bearer services if it has only a PDN connection for emergency bearer services established.

CS fallback capable UE: A UE that uses a CS infrastructure for a voice call and other CS-domain services by falling back to A/Gb or Iu mode if the UE is served by E-UTRAN when a CS service is requested.

CSG cell: A CSG cell in which only members of the CSG can get normal service. Depending on local regulation, the CSG cell can provide emergency bearer services also to subscribers who are not member of the CSG. Definition derived from 3GPP TS 23.401 [10].

CSG ID: A CSG ID is a unique identifier within the scope of one PLMN defined in 3GPP TS 23.003 [2] which identifies a Closed Subscriber Group (CSG) in the PLMN associated with a cell or group of cells to which access is restricted to members of the CSG.

CSG selection: A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs. Definition derived from 3GPP TS 23.122 [6].

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 gets established with every new PDN connection. Its context remains established throughout the lifetime of that PDN connection. A default EPS bearer is a non-GBR bearer. Definition derived from 3GPP TS 23.401 [10].

Emergency EPS bearer context: a default EPS bearer context which was activated with request type "emergency", or any dedicated EPS bearer context associated to this default EPS bearer context.

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].

EPS security context: In the present specification, EPS security context is used as a synonym for EPS NAS security context specified in 3GPP TS 33.401 [19].

EPS services: Within the context of this specification, EPS services is used as a synonym for GPRS services in 3GPP TS 24.008 [13].

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].

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.

Kilobit: 1000 bits.

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].

Megabit: 1,000,000 bits.

Message header: a standard L3 message header as defined in 3GPP TS 24.007 [12].

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

NAS signalling connection: is a peer to peer S1 mode connection between UE and MME. A NAS signalling connection consists of the concatenation of an RRC connection via the "LTE-Uu" interface and an S1AP connection via the S1 interface. 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.

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

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.

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-emergency EPS bearer context: any EPS bearer context which is not an emergency EPS bearer context.

Non-EPS services: services provided by CS domain. Within the context of this specification, non-EPS services is used as a synonym for non-GPRS services in 3GPP TS 24.008 [13]. A UE which camps on E-UTRAN can attach to both EPS services and non-EPS services.

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).

PDN connection for emergency bearer services: a PDN connection for which the default EPS bearer context or default PDP context was activated with request type "emergency".

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.

Registered PLMN: The PLMN on which the UE is registered. The identity of the registered PLMN is provided to the UE within the GUTI.

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].

"SMS only": A subset of non-EPS services which includes only Short Message Service. A UE camping on E-UTRAN can attach to both EPS services and "SMS only".

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.

Traffic flow aggregate: A temporary aggregate of packet filters that are included in a UE requested bearer resource allocation procedure or 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 allocation procedure or UE requested bearer resource modification procedure is completed.

UE's availability for voice calls in the IMS: the indication of this availability or non-availability is provided by the upper layers of the UE as specified in 3GPP TS 24.229 [13D] in the annex relevant to the IP-Connectivity Access Network in use. If availability is indicated, the UE uses the IM CN Subsystem and can terminate or originate requests for SIP sessions including an audio component with codecs suited for voice.

UE's usage setting: This is a UE setting that indicates whether the UE has preference for voice services over data services or vice-versa. If a UE has preference for voice services, then the UE's usage setting is "voice centric". If a UE has preference for data services, then the UE's usage setting is "data centric". A UE whose setting is "data centric" may still require access to voice services. A UE whose setting is "voice centric" may still require access to data services. This definition is derived from 3GPP TS 23.221 [8A] and it applies to voice capable UEs.

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

MME pool area
PDN connection

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

CS fallback
SMS over SGs

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

A/Gb mode
Access domain selection
Default PDP context
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:

Current EPS security context
Full native EPS security context
K_{ASME}
K'_{ASME}
Mapped security context
Native EPS security context
Non-current EPS security context
Partial native EPS 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
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
IP-CAN	IP-Connectivity Access Network
ISR	Idle mode Signalling Reduction
kbps	Kilobits per second
KSI	Key Set Identifier
M-TMSI	M-Temporary Mobile Subscriber Identity
Mbps	Megabits per second
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
RRC	Radio Resource Control
S-TMSI	S-Temporary Mobile Subscriber Identity

S101-AP	S101 Application Protocol
S1AP	S1 Application Protocol
SAE	System Architecture Evolution
TA	Tracking Area
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

The non-access stratum (NAS) described in the present document forms the highest stratum of the control plane between UE and MME at the radio interface (reference point "LTE-Uu"; see 3GPP TS 23.401 [10]).

Main functions of the protocols that are part of the NAS are:

- the support of mobility of the user equipment (UE); and
- the support of session management procedures to establish and maintain IP connectivity between the UE and a packet data network gateway (PDN GW).

NAS security is an additional function of the NAS providing services to the NAS protocols, e.g. integrity protection and ciphering of NAS signalling messages.

For the support of the above functions, the following procedures are supplied within this specification:

- elementary procedures for EPS mobility management in clause 5; and
- elementary procedures for EPS session management in clause 6.

Complete NAS transactions consist of specific sequences of elementary procedures. Examples of such specific sequences can be found in 3GPP TS 23.401 [10].

The NAS for EPS follows the protocol architecture model for layer 3 as described in 3GPP TS 24.007 [12]; however, due to the objective of EPS to provide the subscriber with a "ready-to-use" IP connectivity and an "always-on" experience, there is a linkage between mobility management and session management procedures during the attach procedure (see subclause 4.2).

Signalling procedures for the control of NAS security are described as part of the EPS mobility management in clause 5. In addition to that, principles for the handing of EPS security contexts and for the activation of ciphering and integrity protection, when a NAS signalling connection is established, are provided in subclause 4.4.

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, the default EPS bearer context activation procedure, and the dedicated EPS bearer context activation procedure in parallel. The UE and network shall complete the combined default EPS bearer context activation procedure and the attach procedure before the dedicated EPS bearer context activation procedure is completed. 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 procedures also fail.

Except for the attach procedure and the service request procedure, during EMM procedures the MME shall suspend the transmission of ESM messages. During the service request procedure the MME may suspend the transmission of ESM messages.

Except for the attach procedure, during EMM procedures the UE shall suspend the transmission of ESM messages.

4.3 UE mode of operation

4.3.1 General

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

- PS mode 1 of operation: the UE registers only to EPS services, and UE's usage setting is "voice centric";
- PS mode 2 of operation: the UE registers only to EPS services, and UE's usage setting is "data centric";
- CS/PS mode 1 of operation: the UE registers to both EPS and non-EPS services, and UE's usage setting is "voice centric"; and
- CS/PS mode 2 of operation: the UE registers to both EPS and non-EPS services, and UE's usage setting is "data centric".

A UE configured to use CS fallback, shall operate in CS/PS mode 1 or CS/PS mode 2. Such UE may also be configured to use IMS, in which case the voice domain preference for E-UTRAN as defined in 3GPP TS 24.167 [13B] shall be used for the selection of the domain for originating voice communication services.

A UE configured to use SMS over SGs, but not configured to use CS fallback, shall operate in CS/PS mode 1 or CS/PS mode 2.

The behaviour of the UE in CS/PS mode 1 of operation, upon failure to access the CS domain or upon reception of a "CS fallback not preferred" or "SMS only" indication, will depend on the availability of voice over IMS. In the present document, "IMS voice not available" refers to one of the following conditions:

- the UE is not configured to use IMS;
- the UE is not configured to use IMS voice, i.e. when the voice domain preference for E-UTRAN, as defined in 3GPP TS 24.167 [13B], indicates that voice communication services are allowed to be invoked only over the CS domain;
- the UE is configured to use IMS voice, but the network indicates in the ATTACH ACCEPT message or the TRACKING AREA UPDATE ACCEPT message that IMS voice over PS sessions are not supported; or
- the UE is configured to use IMS voice, the network indicates in the ATTACH ACCEPT message or the TRACKING AREA UPDATE ACCEPT message that IMS voice over PS sessions are supported, but the upper layers indicate that the UE is not available for voice calls in the IMS.

Other conditions may exist but these are implementation specific.

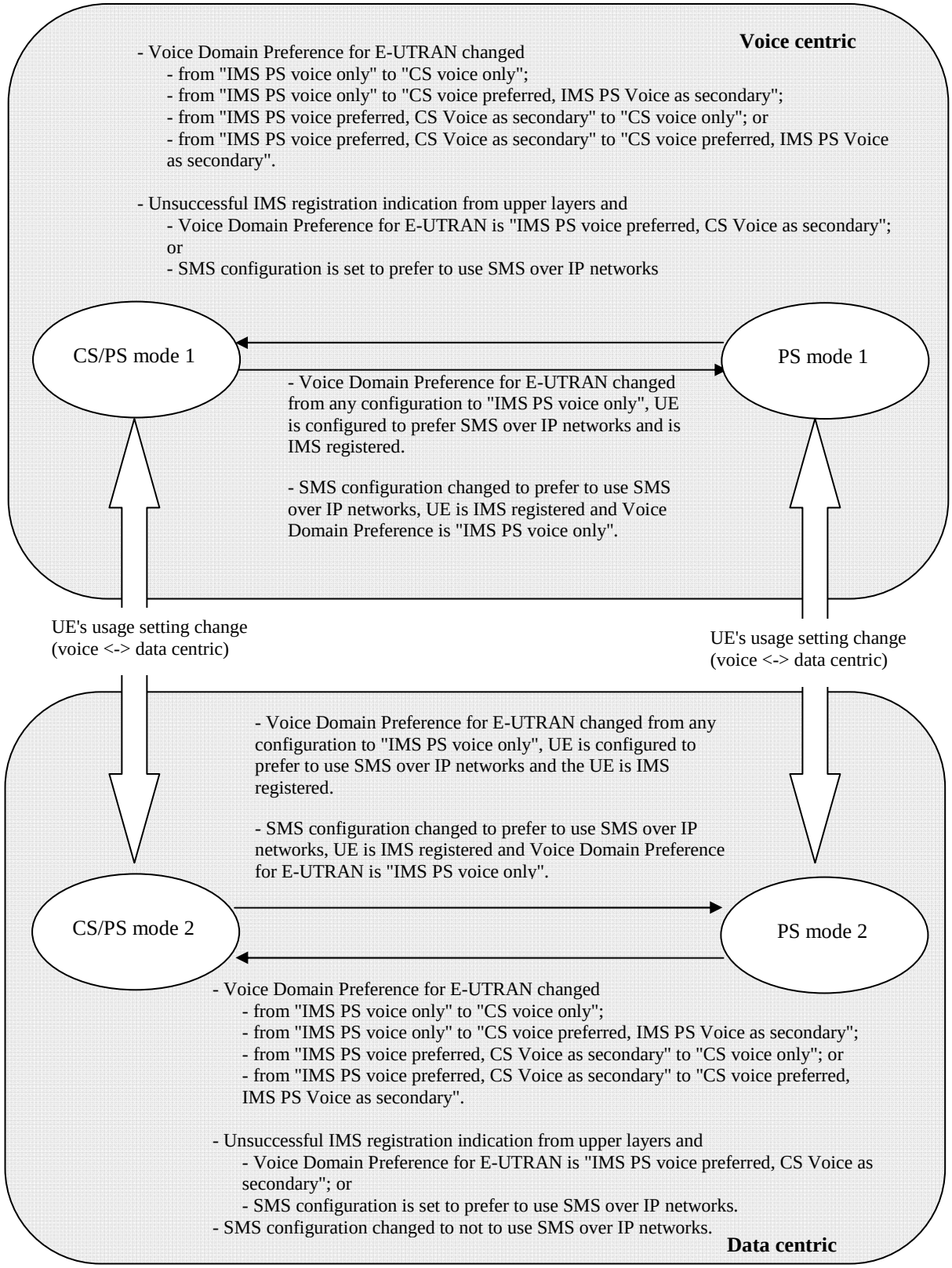
4.3.2 Change of UE mode of operation

4.3.2.1 General

The UE mode of operation can change as a result of e.g.:

- a change of UE's usage setting for a CS voice capable UE;
- a change of voice domain preference for E-UTRAN as defined in 3GPP TS 24.167 [13B] for a CS voice capable UE;
- a change in the UE's availability for voice calls in the IMS; or
- a change in UE configuration regarding the use of SMS as defined in 3GPP TS 24.167 [13B].

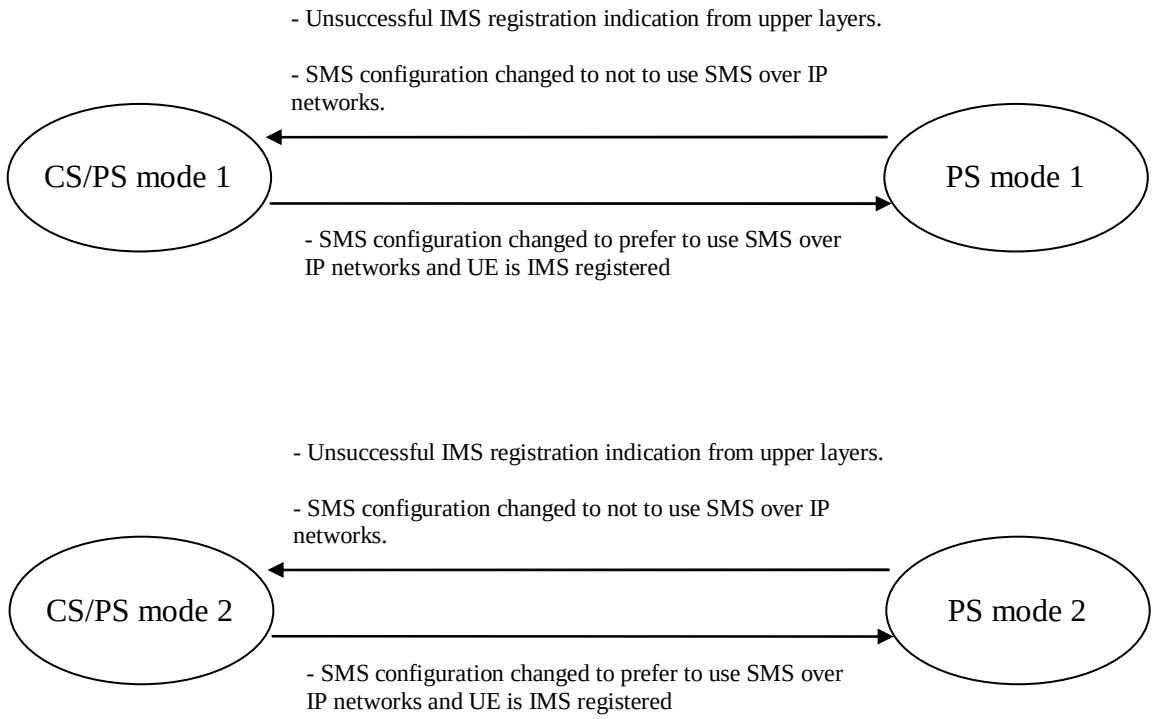
Figure 4.3.2.1.1 and figure 4.3.2.1.2 illustrate the transitions between different UE mode of operations when UE's usage settings, voice domain preference for E-UTRAN or configuration regarding SMS changes.



NOTE 1: The UE may transit from CS/PS mode 1 to PS mode 1 or from CS/PS mode 2 to PS mode 2 if "CS domain not available" is received. After the transition to PS mode 1 or PS mode 2 due to "CS domain not available", the UE can transit back to CS/PS mode 1 or CS/PS mode 2, e.g. due to change of PLMN which is not in the list of the equivalent PLMNs.

NOTE 2: Not all possible transitions are shown in this figure.

Figure 4.3.2.1.1: Change of UE mode of operation for a CS voice capable UE



NOTE: Not all possible transitions are shown in this figure.

Figure 4.3.2.1.2: Change of UE mode of operation for a UE with no CS voice capability

4.3.2.2 Change of UE's usage setting

Whenever the UE's usage setting changes, the UE dependent on its mode of operation shall execute procedures according to table 4.3.2.2.1 and table 4.3.2.2.2:

a) The UE is operating in PS mode 1 or PS mode 2

Table 4.3.2.2.1: Change of UE's usage setting for a UE in PS mode 1 or PS mode 2

UE's usage setting change	Procedure to execute
From data centric to voice centric and "IMS voice not available"	Disable E-UTRAN capabilities if voice domain selection results in a selection to a different RAT, or combined tracking area update with IMSI attach if voice domain selection results in attempt to stay in E-UTRAN.
From voice centric to data centric and E-UTRAN is disabled	Re-enable E-UTRAN capabilities

b) The UE is operating in CS/PS mode 1 or CS/PS mode 2

Table 4.3.2.2.2: Change of UE's usage setting for a UE in CS/PS mode 1 or CS/PS mode 2

UE's usage setting change	Procedure to execute
From data centric to voice centric, CS fallback is not available and "IMS voice not available" (NOTE 1)	Disable E-UTRAN capabilities
From data centric to voice centric, "IMS voice not available" and the UE received a "CS fallback not preferred" or "SMS only" indication during the last successful combined attach or combined tracking area updating procedure	Disable E-UTRAN capabilities
From voice centric to data centric and E-UTRAN is disabled	Re-enable E-UTRAN capabilities
NOTE: "CS fallback is not available" includes EMM causes #16, #17, #18 and #22	

4.3.2.3 Change of voice domain preference for E-UTRAN

Whenever the voice domain preference for E-UTRAN changes, the UE dependent on its mode of operation shall execute procedures according to table 4.3.2.3.1 and table 4.3.2.3.2:

a) The UE is operating in PS mode 1 or PS mode 2

Table 4.3.2.3.1: Change of voice domain preference for E-UTRAN for a UE in PS mode 1 or PS mode 2

Voice domain preference for E-UTRAN change	Procedure to execute
From "IMS PS voice only" to "CS voice only" or "CS voice preferred, IMS PS Voice as secondary"	Transit from PS mode 1 to CS/PS mode 1 or from PS mode 2 to CS/PS mode 2. Combined tracking area update with IMSI attach
From "IMS PS voice preferred, CS Voice as secondary" to "CS voice only" or "CS voice preferred, IMS PS Voice as secondary"	Transit from PS mode 1 to CS/PS mode 1 or from PS mode 2 to CS/PS mode 2. Combined tracking area update with IMSI attach

b) The UE is operating in CS/PS mode 1 or CS/PS mode 2

Table 4.3.2.3.2: Change of voice domain preference for E-UTRAN for a UE in CS/PS mode 1 or CS/PS mode 2

Voice domain preference for E-UTRAN change	Procedure to execute
From any configuration to "IMS PS voice only", UE is configured to prefer SMS over IP networks and the UE is available for voice calls in the IMS.	May detach for non-EPS services

4.3.2.4 Change of IMS registration status

Whenever the upper layers indicate a change of IMS registration status, the UE dependent on its mode of operation shall execute procedures according to table 4.3.2.4.1 and table 4.3.2.4.2:

a) The UE is operating in PS mode 1

Table 4.3.2.4.1: Change of IMS registration status for a UE in PS mode 1

Change of IMS registration status	Procedure to execute
UE is not available for voice calls in the IMS indication from upper layers and voice domain preference for E-UTRAN is "IMS PS voice preferred, CS Voice as secondary"	Transit to CS/PS mode 1. Combined tracking area update with IMSI attach
UE is not available for voice calls in the IMS indication from upper layers, SMS configuration is set to prefer to use SMS over IP networks, and voice domain preference for E-UTRAN is "IMS PS voice only"	Disable E-UTRAN capabilities
UE is not available for voice calls in the IMS indication from upper layers, SMS configuration is set to prefer to use SMS over IP networks, and UE is not CS voice capable	May disable E-UTRAN capabilities

b) The UE is operating in PS mode 2

Table 4.3.2.4.2: Change of IMS registrtion status for a UE in PS mode 2

Change of IMS registration status	Procedure to execute
UE is not available for voice calls in the IMS indication from upper layers and voice domain preference for E-UTRAN is "IMS PS voice preferred, CS Voice as secondary"	Transit to CS/PS mode 2. Combined tracking area update with IMSI attach
Unsuccessful IMS registration indication from upper layers, SMS configuration is set to prefer to use SMS over IP networks, and voice domain preference for E-UTRAN is "IMS PS voice only"	Transit to CS/PS mode 2. Combined tracking area update with "SMS only"
Unsuccessful IMS registration indication from upper layers, SMS configuration is set to prefer to use SMS over IP networks, and UE is not CS voice capable	Transit to CS/PS mode 2. Combined tracking area update with "SMS only"

4.3.2.5 Change of configuration regarding the use of SMS.

Whenever the UE's configuration on use of SMS changes, the UE dependent on its mode of operation shall execute procedures according to table 4.3.2.5.1 and table 4.3.2.5.2:

a) The UE is operating in PS mode 1 or PS mode 2

Table 4.3.2.5.1: Change of configuration regarding the use of SMS in PS mode 1 or PS mode 2

SMS configuration change	Procedure to execute
Change to not to use SMS over IP networks	Transit from PS mode 1 to CS/PS mode 1 or from PS mode 2 to CS/PS mode 2. Combined tracking area update with IMSI attach, (with or without "SMS only")

b) The UE is operating in CS/PS mode 1 or CS/PS mode 2

Table 4.3.2.5.2: Change of configuration regarding the use of SMS in CS/PS mode 1 or CS/PS mode 2

SMS configuration change	Procedure to execute
Change to "SMS service is preferred to be invoked over IP networks", the UE is IMS registered, and UE has no CS voice capability	May detach for non-EPS services
Change to "SMS service is preferred to be invoked over IP networks", UE is IMS registered, and the voice domain preference for E-UTRAN is "IMS PS voice only"	May detach for 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", EEA0.

4.4.2 Handling of EPS security contexts

4.4.2.1 General

The security parameters for authentication, integrity protection and ciphering are tied together in an EPS security context and identified by a key set identifier for E-UTRAN (eKSI). The relationship between the security parameters is defined in 3GPP TS 33.401 [19].

Before security can be activated, the MME and the UE need to establish an EPS security context. Usually, the EPS security context is created as the result of an EPS 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 taken into use by the UE and the MME, when the MME initiates a security mode control procedure or during the inter-system handover procedure from A/Gb mode to S1 mode or Iu mode to S1 mode. The EPS security context which has been taken into use by the network most recently is called current EPS security context. This current EPS security context can be of type native or mapped, i.e. originating from a native EPS security context or mapped EPS security context.

The key set identifier eKSI is assigned by the MME either during the EPS authentication procedure or, for the mapped EPS security context, during the inter-system handover procedure. The eKSI consists of a value and a type of security context parameter indicating whether an EPS security context is a native EPS security context or a mapped EPS security context. When the EPS security context is a native EPS security context, the eKSI has the value of KSI_{ASME}, and when the current EPS security context is of type mapped, the eKSI has the value of KSI_{SGSN}.

The eKSI indicates the EPS security context which can be taken into use to establish the secure exchange of NAS messages at the next establishment of a NAS signalling connection without executing a new EPS authentication procedure (see subclause 4.4.2.3).To this purpose the initial NAS messages (ATTACH REQUEST, TRACKING AREA UPDATE REQUEST, DETACH REQUEST, SERVICE REQUEST and EXTENDED SERVICE REQUEST) and the SECURITY MODE COMMAND message contain an eKSI in the NAS key set identifier IE or the value part of eKSI in the KSI and sequence number IE indicating the current EPS security context used to integrity protect the NAS message.

In the present document, when the UE is required to delete an eKSI, the UE shall set the eKSI to the value "no key is available" and consider also the associated keys K_{ASME} or K'_{ASME}, EPS NAS ciphering key and EPS NAS integrity key invalid (i.e. the EPS security context associated with the eKSI 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).

The UE and the MME need to be able to maintain two EPS security contexts simultaneously, i.e. a current EPS security context and a non-current EPS security context, since:

- after an EPS re-authentication, the UE and the MME can have both a current EPS security context and a non-current EPS security context which has not yet been taken into use (i.e. a partial native EPS security context); 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, which is the current EPS security context, and a non-current native EPS security context that was created during a previous access in S1 mode or S101 mode.

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 EPS (re-)authentication, which creates a new partial native EPS security context, the MME and the UE shall delete the non-current EPS security context, if any.

- When a partial native EPS security context is taken into use through a security mode control procedure, the MME and the UE shall delete the previously current EPS security context.

- When the MME and the UE create an EPS security context using null integrity and null ciphering algorithm during an attach procedure for emergency bearer services, or a tracking area updating procedure for a UE that has a PDN connection for emergency bearer services (see subclause 5.4.3.2), the MME and the UE shall delete the previous current EPS security context.

- When a new mapped EPS security context or EPS security context created using null integrity and null ciphering algorithm is taken into use during the inter-system handover from A/Gb mode to S1 mode or Iu mode to S1 mode, the MME and the UE shall not delete the previously current native EPS security context, if any. Instead, the previously current native EPS security context shall become a non-current native EPS security context, and the MME and the UE shall delete any partial native EPS security context.

  If no previously current native EPS security context exists, the MME and the UE shall not delete the partial native EPS security context, if any.

- 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 current mapped EPS security context.

- When a non-current full native EPS security context is taken into use by a security mode control procedure, then the MME and the UE shall delete the previously current mapped EPS security context.

- When the UE or the MME moves from EMM-REGISTERED to EMM-DEREGISTERED state, if the current EPS security context is a mapped EPS security context and a non-current full native EPS security context exists, then the non-current EPS security context shall become the current EPS security context. Furthermore, the UE and the MME shall delete any mapped EPS security context or partial native EPS security context.

The UE shall mark the EPS security context on the USIM or in the non-volatile memory as invalid when the UE initiates an attach procedure as described in subclause 5.5.1 or when the UE leaves state EMM-DEREGISTERED for any other state except EMM-NULL.

The UE shall store the current native EPS security context as specified in annex C and mark it as valid only when the UE enters state EMM-DEREGISTERED from any other state except EMM-NULL or when the UE aborts the attach procedure without having left EMM-DEREGISTERED.

4.4.2.2 Establishment of a mapped EPS security context during intersystem handover

In order for the UE to derive a mapped EPS security context for an inter-system change from A/Gb mode or Iu mode to S1 mode in EMM-CONNECTED mode, the MME shall generate a KSI_{SGSN}, create a $nonce_{MME}$ and generate the K'_{ASME} using the created $nonce_{MME}$ as indicated in 3GPP TS 33.401 [19]. The MME shall include the selected NAS algorithms, $nonce_{MME}$ and generated KSI_{SGSN} (associated with the K'_{ASME}) in the NAS security transparent container for handover to E-UTRAN. The MME shall derive the EPS NAS keys from K'_{ASME}.

When the UE receives the command to perform handover to E-UTRAN, the UE shall derive $K'_{ASME,}$ as indicated in 3GPP TS 33.401 [19], using the $nonce_{MME}$ received in the NAS security transparent container. Furthermore, the UE shall associate the derived K'_{ASME} with the received KSI_{SGSN} and derive the EPS NAS keys from K'_{ASME}.

When the UE has a PDN connection for emergency bearer services and has no current UMTS security context, the MME shall set EIA0 and EEA0 as the selected NAS security algorithms in the NAS security transparent container for handover to E-UTRAN. The MME shall create a locally generated K'_{ASME}. The MME shall set the KSI value of the

associated security context to "000" and the type of security context flag to "mapped security context" in the NAS security transparent container for handover to E-UTRAN.

When the UE receives the command to perform handover to E-UTRAN and has a PDN connection for emergency bearer services, if EIA0 and EEA0 as the selected NAS security algorithms are included in the NAS security transparent container for handover to E-UTRAN, the UE shall create a locally generated K'_{ASME}. The UE shall set the KSI value of the associated security context to the KSI value received.

If the inter-system change from A/Gb mode or Iu mode to S1 mode in EMM-CONNECTED mode is not completed successfully, the MME and the UE shall delete the new mapped EPS security context.

4.4.2.3 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, all NAS messages exchanged between the UE and the MME are sent integrity protected using the current EPS security algorithms, and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the MME are sent ciphered using the current EPS security algorithms.

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, all NAS messages exchanged between the UE and the MME are sent integrity protected using the mapped EPS security context, and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the MME are sent 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 3 below, the UE shall transmit the initial NAS message integrity protected with the current EPS security context, but unciphered. The UE shall include the eKSI indicating the current EPS security context value in the initial NAS message. 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, all NAS messages exchanged between the UE and the MME are sent integrity protected and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the MME are sent ciphered; or

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

2) If the initial NAS message was a SERVICE REQUEST message or EXTENDED SERVICE REQUEST message, secure exchange of NAS messages is triggered by the indication from the lower layers that the user plane radio bearers are successfully set up. After successful completion of the procedure, all NAS messages exchanged between the UE and the MME are sent integrity protected and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the MME are sent ciphered.

3) If the UE has no current EPS security context and performs 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, the UE shall send the TRACKING AREA UPDATE REQUEST message without integrity protection and encryption. The UE shall include a nonce and a GPRS ciphering key sequence number for creation of a mapped EPS security context. The

MME creates a fresh mapped EPS security context and takes this context into use by initiating a security mode control procedure and this context becomes the current EPS security context in both the UE and the MME. This re-establishes the secure exchange of NAS messages.

4.4.2.4 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 SECURITY MODE COMMAND 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 the current EPS security context or take the non-current native EPS security context, if any, into use, 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

Each EPS NAS security context shall be associated with 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 shall be constructed as a NAS sequence number (8 least significant bits) concatenated with a NAS overflow counter (16 most significant bits).

When NAS COUNT is input to NAS ciphering or NAS integrity algorithms it shall be considered to be a 32-bit entity which shall be constructed by padding the 24-bit internal representation with 8 zeros in the most significant bits.

The value of the uplink NAS COUNT that is stored or read out of the USIM or non-volatile memory as described in annex C, is the value that shall be used in the next NAS message.

The value of the downlink NAS COUNT that is stored or read out of the USIM or non-volatile memory as described in annex C, is the largest downlink NAS COUNT used in a successfully integrity checked NAS message.

The NAS sequence number part of the NAS COUNT shall be exchanged between the UE and the MME as part of the NAS signalling. After each new or retransmitted outbound security protected NAS message, the sender shall increase the NAS COUNT number by one. Specifically, on the sender side, the NAS sequence number shall be increased by one, and if the result is zero (due to wrap around), the NAS overflow counter shall also be incremented by one (see subclause 4.4.3.5). The receiving side shall estimate the NAS COUNT used by the sending side. Specifically, if the estimated NAS sequence number wraps around, the NAS overflow counter shall be incremented by one.

After the derivation of a NAS token due to an inter-system change from S1mode to A/Gb mode or Iu mode in idle mode as specified in 3GPP TS 24.008 [13], the UE shall increase the uplink NAS COUNT by one.

When the MME receives a NAS token via SGSN during an idle mode inter-system change from S1 mode to A/Gb mode or Iu mode, the MME shall check the NAS token as specified in 3GPP TS 33.401 [19], subclause 9.1.1, and update its uplink NAS COUNT with the uplink NAS COUNT value used for the successful check of the NAS token.

During the handover from UTRAN/GERAN to E-UTRAN, when a mapped EPS security context is derived and taken into use, the MME shall set both the uplink and downlink NAS COUNT counters of this EPS security context to zero. The UE shall set both the uplink and downlink NAS COUNT counters to zero.

During the handover from E-UTRAN to UTRAN/GERAN the MME signals the current downlink NAS COUNT value in a NAS security transparent container (see subclause 9.9.2.6).

During handover to or from E-UTRAN, the MME shall increment downlink NAS COUNT by one after it has created a NAS security transparent container (see subclause 9.9.2.6 and 9.9.2.7).

NOTE: During the handover from UTRAN/GERAN to E-UTRAN, the NAS security transparent container (see subclause 9.9.2.7) is treated as an implicit SECURITY MODE COMMAND message for the UE and the MME, and therefore the MME regards the sending of the NAS security transparent container as the sending of an initial SECURITY MODE COMMAND message in order to derive and take into use a mapped EPS security context for the purpose of the NAS COUNT handling.

In some NAS messages only 5 of the 8 NAS sequence number bits are transmitted. When this is the case, the receiver shall estimate the remaining 3 most significant bits of the sequence number.

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.

Replay protection is not applicable when EIA0 is used.

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 (or estimated from the 5 bits of the NAS sequence number received in the message) and an estimate for the NAS overflow counter as defined in subclause 4.4.3.1 to form the NAS COUNT input to the integrity verification algorithm.

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. The integrity protection of the SERVICE REQUEST message is defined in subclause 9.9.3.28. In addition to the data that is to be integrity protected, the constant BEARER ID, DIRECTION bit, NAS COUNT and NAS integrity key are input to the integrity protection algorithm. These parameters are described in 3GPP TS 33.401 [19].

After successful integrity protection validation, the receiver shall update its corresponding locally stored NAS COUNT with the value of the estimated NAS COUNT for this NAS message.

Integrity verification is not applicable when EIA0 is used.

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 (or estimated from the 5 bits of the NAS sequence number received in the message) and an estimate for the NAS overflow counter as defined in subclause 4.4.3.1 to form the NAS COUNT input to the deciphering algorithm.

The input parameters to the NAS ciphering algorithm are the constant BEARER ID, DIRECTION bit, NAS COUNT, NAS encryption key and the length of the key stream to be generated by the encryption algorithm.

4.4.3.5 NAS COUNT wrap around

If, when increasing the NAS COUNT as specified above, the MME detects that either its downlink NAS COUNT or the UE's uplink NAS COUNT is "close" to wrap around, (close to 2^{24}), the MME shall take the following actions:

- If there is no non-current native EPS security context with sufficiently low NAS COUNT values, 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;

- Otherwise, the MME can activate a non-current native EPS security context with sufficiently low NAS COUNT values or initiate a new AKA procedure as specified above.

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 eKSI indicating the current EPS security context.

When the EIA0 is used as the NAS integrity algorithm, the UE and the MME shall allow NAS COUNT wrap around. If NAS COUNT wrap around occurs, the following requirements apply:

- the UE and the MME shall continue to use the current security context;
- the MME shall not initiate the EPS AKA procedure;
- the MME shall not release the NAS signalling connection; and
- the UE shall not perform a local release of the NAS signalling connection.

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.

The use of "null integrity protection algorithm" EIA0 (see subclause 9.9.3.23) in the current security context is only allowed for an unauthenticated UE. For setting the security header type in outbound NAS messages, the UE and the MME shall apply the same rules irrespective of whether the "null integrity protection algorithm" or any other integrity protection algorithm is indicated in the security context.

If the "null integrity protection algorithm" EIA0 has been selected as a integrity protection algorithm, the receiver shall regard the NAS messages with the security header indicating integrity protection as integrity protected.

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 network has established secure exchange of NAS messages for the NAS signalling connection:

- EMM messages:
  - IDENTITY REQUEST (if requested identification parameter is IMSI);
  - AUTHENTICATION REQUEST;
  - AUTHENTICATION REJECT;
  - ATTACH REJECT (if the EMM cause is not #25);
  - DETACH ACCEPT (for non switch off);
  - TRACKING AREA UPDATE REJECT (if the EMM cause is not #25);
  - SERVICE REJECT (if the EMM cause is not #25).

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.

All ESM messages are integrity protected.

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. The processing of the SECURITY MODE COMMAND message that has not successfully passed the integrity check is specified in subclause 5.4.3.5. 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 current 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.

All ESM messages are integrity protected except a PDN CONNECTIVITY REQUEST message if it is sent piggybacked in ATTACH REQUEST message and NAS security is not activated.

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 processed 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 and it is not an attach request for emergency bearer services, the MME shall authenticate the subscriber before processing the attach request any further. For the case when the attach procedure is for emergency bearer services see subclause 5.5.1.2.3 and subclause 5.4.2.5.

If a TRACKING AREA UPDATE REQUEST message fails the integrity check and the UE provided a $nonce_{UE}$, GPRS ciphering key sequence number , P-TMSI and RAI in the TRACKING AREA UPDATE REQUEST message, the MME shall initiate a security mode control procedure to take a new mapped EPS security context into use; otherwise if the UE has only a PDN connection for non-emergency bearer services established, the MME shall initiate an authentication procedure. For the case when the UE has a PDN connection for emergency bearer services see subclause 5.5.1.2.3 and subclause 5.4.2.5.

If a SERVICE REQUEST or EXTENDED SERVICE REQUEST message fails the integrity check, the MME shall reject the request with EMM cause #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 subject to MME configuration. When operation of the network without ciphering is configured, the MME shall indicate the use of "null ciphering algorithm" EEA0 (see subclause 9.9.3.23) in the current security context for all UEs. For setting the security header type in outbound NAS messages, the UE and the MME shall apply the same rules irrespective of whether the "null ciphering algorithm" or any other ciphering algorithm is indicated in the security context.

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

The UE shall send the ATTACH REQUEST message always unciphered.

The UE shall send the TRACKING AREA UPDATE REQUEST message always 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, unless explicitly defined, 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 4.4.2.3. 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.

Once the encryption of NAS messages has been started between the MME and the UE, the receiver shall discard the unciphered NAS messages which shall have been ciphered according to the rules described in this specification.

If the "null ciphering algorithm" EEA0 has been selected as a ciphering algorithm, the NAS messages with the security header indicating ciphering are regarded as ciphered.

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

4.5 Disabling and re-enabling of UE's E-UTRA capability

When the UE supporting the A/Gb and/or Iu mode together with the S1 mode needs to stay in A/Gb or Iu mode, in order to prevent unwanted handover or cell reselection from UTRAN/GERAN to E-UTRAN, the UE shall disable the E-UTRA capability.

- The UE shall not set the E-UTRA support bits of the MS Radio Access capability IE (see 3GPP TS 24.008 [13], subclause 10.5.5.12a), the E-UTRA support bits of Mobile Station Classmark 3 IE (see 3GPP TS 24.008 [13], subclause 10.5.1.7) and the ISR support bit of the MS network capability IE (see 3GPP TS 24.008 [13], subclause 10.5.5.12) in the ATTACH REQUEST message and the ROUTING AREA UPDATE REQUEST message after it selects GERAN or UTRAN; and
- the UE NAS layer shall indicate the access stratum layer(s) of disabling of the E-UTRA capability.

NOTE: The UE can only disable the E-UTRAN capabilities when in EMM-IDLE mode.

The UE shall enable the E-UTRA capability again in the following cases:

- the UE mode of operation changes from CS/PS mode 1 of operation to CS/PS mode 2 of operation;
- the UE mode of operation changes from PS mode 1 of operation to PS mode 2 of operation;
- the UE powers off and powers on again; or
- for the PLMN selection purpose.

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.

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]).

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/or non-EPS services, and to establish an EMM context and a default bearer:

- attach and combined attach.

Initiated by the UE and used to attach the IMSI or IMEI for emergency bearer services, and to establish an EMM context and a default bearer to a PDN that provides emergency bearer services:

- attach.

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

- detach and combined detach.

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

- normal tracking area updating and combined 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;
- generic transport of NAS messages.

The transport of NAS messages procedure and the generic transport of NAS messages procedure cannot be initiated while an EMM specific procedure or a service request 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.

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 or combined 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 or combined 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 or combined tracking area updatingprocedure 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).

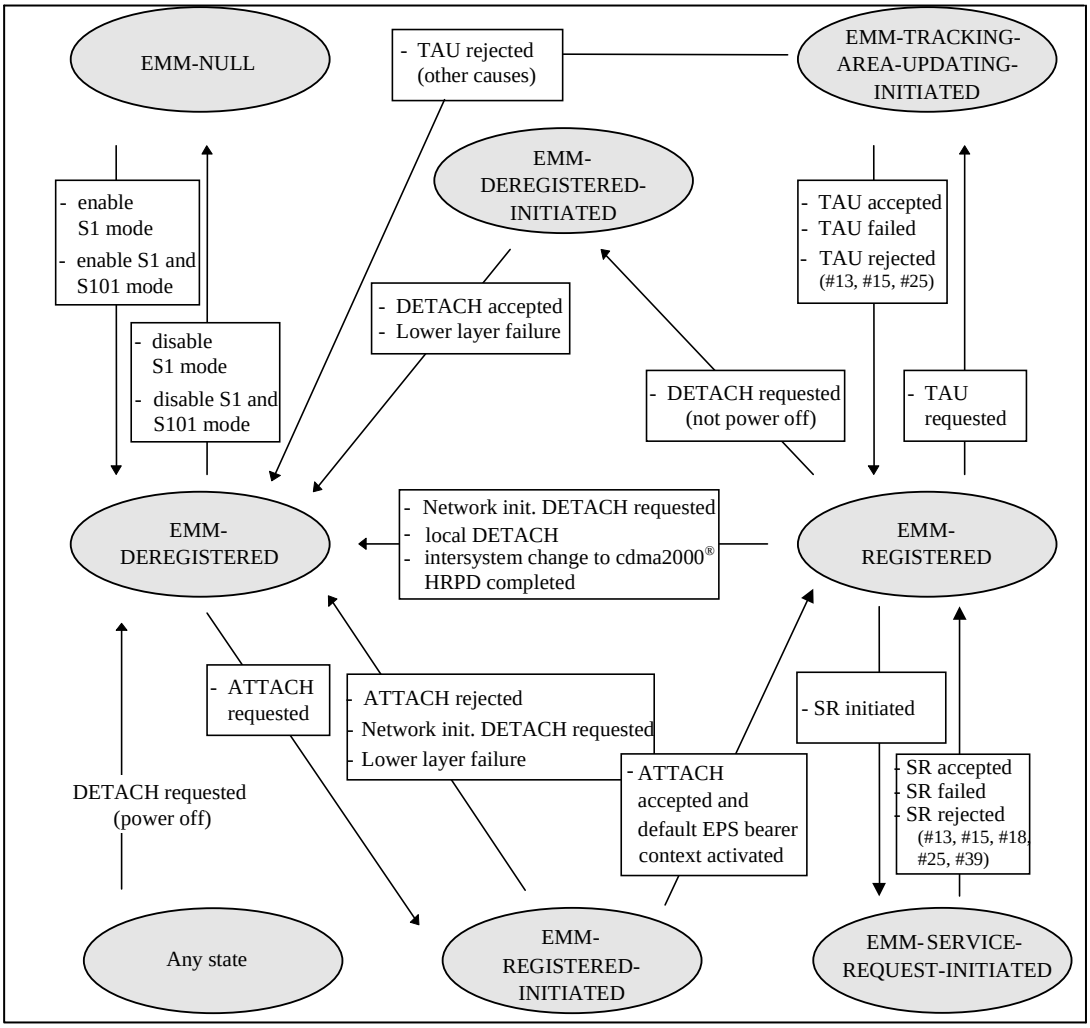


Figure 5.1.3.2.7.1: EMM main states in the UE

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 it is known that a selected cell is unable to provide normal service (e.g. the selected cell is in a forbidden PLMN, is in a forbidden tracking area or the selected cell is a CSG cell whose CSG ID and associated PLMN identity are not included in the UE's Allowed CSG list or in the UE's Operator 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 enters 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 or combined tracking area updating procedure failed due to a missing response from the network. No EMM procedure except the tracking area updating or combined tracking area updating procedure 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 or combined 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 or combined tracking area updating or service request as a response to paging 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 or combined attach, network initiated detach, authentication, tracking area update or combined tracking area update, service request or paging for EPS services using IMSI procedure.

EU1: UPDATED

The last attach or tracking area updating attempt was successful.

EU2: NOT UPDATED

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

EU3: ROAMING NOT ALLOWED

The last attach, service request 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).

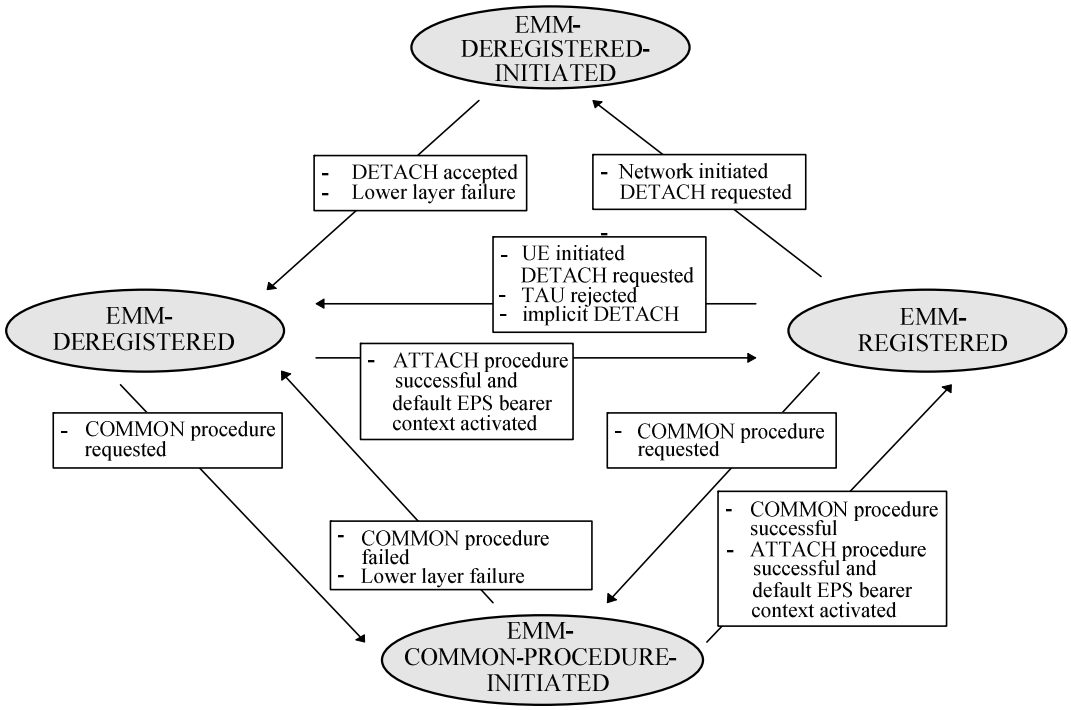


Figure 5.1.3.4.4.1: EMM main states in the MME

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 or combined 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 or combined 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 or combined routing area updating and tracking area updating or combined 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 shall use the combined EPS/IMSI attach procedure in order to attach to both EPS and non-EPS services.

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 service request procedure is rejected by the MME (see subclause 5.6.1);
- the UE deactivates all EPS bearer contexts locally (see subclause 6.4.4.6);
- the UE is switched on; or
- when an inter-system change from S1 mode to non-3GPP access is completed and the non-3GPP access network provides PDN connectivity to the same EPC.

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 initiate an attach or combined attach procedure.

5.2.2.3.2 LIMITED-SERVICE

The UE shall initiate an attach or combined attach procedure when entering a cell which provides normal service.

The UE may initiate attach for emergency bearer services.

5.2.2.3.3 ATTEMPTING-TO-ATTACH

The UE shall:

- initiate an attach or combined attach procedure on the expiry of timers T3411 or T3402;
- initiate an attach or combined attach procedure when the UE enters a new cell in a different tracking area, and the tracking area of the new cell is not in the list of forbidden tracking areas; and
- initiate an attach procedure upon request of the upper layers to establish a PDN connection for emergency bearer services.

5.2.2.3.4 PLMN-SEARCH

The UE shall perform PLMN selection. If a new PLMN is selected, the UE shall reset the attach attempt counter and initiate the attach or combined attach procedure (see subclause 5.5.1).

5.2.2.3.5 NO-IMSI

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

The UE may initiate attach for emergency bearer services.

5.2.2.3.6 ATTACH-NEEDED

The UE shall initiate the attach or combined 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 and the PLMN identity of the target cell provided with this indication is not in one of forbidden PLMN lists, the UE shall enter substate NORMAL-SERVICE.

NOTE: It is assumed that the UE can determine the PLMN identity of networks supporting cdma2000® HRPD access from the information broadcast over the radio interface. For the purpose of S101 mode to S1 mode handover, the UE can use the PLMN identity of the visited cdma2000® HRPD network also as PLMN identity of the target cell.

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 or combined 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 initiate normal and combined tracking area updating (see subclause 5.5.3);
- shall perform periodic tracking area updating (see subclause 5.5.3) except when attached for emergency bearer services (see subclause 5.3.5); and
- shall respond to paging.

5.2.3.2.2 ATTEMPTING-TO-UPDATE

The UE:

- shall not send any user data;
- shall initiate tracking area updating on the expiry of timers T3411 or T3402;
- shall initiate 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; and
- shall initiate a tracking area updating procedure upon request of the upper layers to establish a PDN connection for emergency bearer services.

5.2.3.2.3 LIMITED-SERVICE

The UE:

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

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 reset the tracking area updating attempt counter and initiate the tracking area updating or combined tracking area updating procedure (see subclause 5.5.3).

5.2.3.2.5 UPDATE-NEEDED

The UE:

- shall not send any user data;
- shall not send signalling information unless as a response 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 initiate combined 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.

5.2.3.2.8 IMSI-DETACH-INITIATED

The UE:

- shall be able to receive and transmit user data and signalling information; and
- shall initiate combined tracking area updating procedure (see subclause 5.5.3.3).

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 RRC connection. In this request to the lower layer the NAS shall provide to the lower layer the RRC establishment cause and the call type as specified in annex D of this specification.

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]) according to the following rules:

- 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 or combined 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. Instead,

  a) if the TIN indicates "GUTI" or "RAT-related TMSI", or the TIN is not available, and the UE holds a valid GUTI, the UE NAS shall provide the lower layers with the MME identifier part of the valid GUTI; or

  b) if the TIN indicates "P-TMSI" and the UE holds a valid P-TMSI and RAI, the UE NAS shall provide the lower layers with the MME identifier part of the mapped GUTI, which is generated from the P-TMSI and RAI.

The UE NAS also provides the lower layers with the identity of the selected PLMN (see 3GPP TS 36.331 [22]). In a shared network, the UE shall choose one of the PLMN identities as specified in 3GPP TS 23.122 [6].

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 and the tracking area updating or combined tracking area updating procedure has been initiated in EMM-IDLE mode.

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 UICC containing the

USIM is removed, and periodically (with a period in the range 12 to 24 hours). One or more tracking areas is removed from the list of "forbidden tracking areas for roaming" in the UE, as well as the list of "forbidden tracking areas for regional provision of service" if, after a subsequent procedure e.g. attach procedure, tracking area updating procedure and GUTI reallocation procedure, one or more tracking areas in the lists is received from the network. If the UE has only one PDN connection established which is for emergency bearer services, the tracking areas shall not be removed from these lists if one or more tracking areas in the lists are received from the network.

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 #12 "tracking area not allowed", #13 "roaming not allowed in this tracking area", or #15 "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 List of forbidden PLMNs for attach in S101 mode

A UE supporting S101 mode shall store a list of "forbidden PLMNs for attach in S101 mode". The UE shall erase this list when the UE is switched off or when the USIM is removed.

In S101 mode, the UE shall add to the "forbidden PLMNs for attach in S101 mode" list the PLMN identity provided with the indication from the lower layers to prepare for an S101 mode to S1 mode handover whenever an ATTACH REJECT message is received with the EMM cause #11 "PLMN not allowed", #13 "roaming not allowed in this tracking area", #12 "tracking area not allowed", or #15 "no suitable cells in tracking area".

The maximum number of possible entries in the "forbidden PLMNs for attach in S101 mode" list is implementation dependent, but the list shall accommodate at least one PLMN identity. When the list is full and a new PLMN identity has to be inserted, the UE shall delete the oldest PLMN identity.

5.3.4 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 combined attach or tracking area updating or combined 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 or when the UE attached for emergency bearer services enters the state EMM-DEREGISTERED. The maximum number of possible entries in the stored list is 16.

5.3.5 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.

If the timer T3412 received by the UE in an ATTACH ACCEPT or TRACKING AREA UPDATE ACCEPT contains an indication that the timer is deactivated or the timer value is zero, then the timer T3412 is deactivated and the UE shall not perform periodic tracking area updating procedure.

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.

If the UE is attached for emergency bearer services, and timer T3412 expires, the UE shall not initiate a periodic tracking area updating procedure, but shall locally detach from the network.

When a UE is not attached for emergency bearer services, and 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 not attached for emergency bearer services, and 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 set its TIN to "P-TMSI".

If the E-UTRAN Deactivate ISR timer T3423 expires the UE shall memorize that it has to initiate a tracking area updating procedure when it returns to state EMM-REGISTERED.NORMAL-SERVICE.

If the UE is attached to both EPS and non-EPS services, and if timer T3412 expires or timer T3423 expires when the UE is in EMM-REGISTERED.NO-CELL-AVAILABLE state, then the UE shall initiate the combined tracking area updating procedure indicating "combined TA/LA updating with IMSI attach" when the UE returns to EMM-REGISTERED.NORMAL-SERVICE state.

The network supervises the periodic tracking area updating procedure of the UE by means of the mobile reachable timer.

If the UE is not attached for emergency bearer services, the mobile reachable timer shall be longer than T3412.In this case, 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.

If the UE is attached for emergency bearer services, the MME shall set the mobile reachable timer with a value equal toT3412. When the mobile reachable timer expires, the MME shall locally detach the UE.

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.

Upon expiry of the mobile reachable timer the network shall start the implicit detach timer. The value of the implicit detach timer is network dependent. If ISR is activated, the default value of 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.

5.3.6 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.

5.3.7 Handling of the Local Emergency Numbers List

The Local Emergency Numbers List contains additional emergency numbers used by the serving network. The list can be downloaded by the network to the UE at successful registration and subsequent registration updates. There is only one Local Emergency Numbers List in the UE, and it can be updated with EMM procedures if the UE is in S1 mode and with GMM and MM procedures if the the UE is in A/Gb or Iu mode.

The UE shall use the stored Local Emergency Numbers List received from the network in addition to the emergency numbers stored on the USIM or user equipment to detect that the number dialled is an emergency number.

NOTE: The user equipment may use the emergency numbers list to assist the end user in determining whether the dialled number is intended for an emergency service or for another destination, e.g. a local directory service. The possible interactions with the end user are implementation specific.

The network may send a Local Emergency Numbers List in the ATTACH ACCEPT or in the TRACKING AREA UPDATE ACCEPT messages, by including the Emergency Number List IE. The user equipment shall store the Local Emergency Numbers List, as provided by the network, except that any emergency number that is already stored in the USIM shall be removed from the Local Emergency Numbers List before it is stored by the user equipment. If there are no emergency numbers stored on the USIM, then before storing the received Local Emergency Numbers List, the user equipment shall remove from the Local Emergency Numbers List any emergency number stored permanently in the user equipment for use in this case (see 3GPP TS 22.101 [8]). The Local Emergency Numbers List stored in the user equipment shall be replaced on each receipt of a new Emergency Number List IE.

The emergency number(s) received in the Emergency Number List IE are valid only in networks with the same MCC as in the cell on which this IE is received. If no Local Emergency Numbers List is contained in the ATTACH ACCEPT or in the TRACKING AREA UPDATE ACCEPT message, then the stored Local Emergency Numbers List in the user equipment shall be kept, except if the user equipment has successfully registered to a PLMN with an MCC different from that of the last registered PLMN.

The Local Emergency Numbers List shall be deleted at switch off and removal of the USIM. The user equipment shall be able to store up to ten local emergency numbers received from the network.

5.3.8 Abnormal cases in the UE

The following abnormal case can be identified:

a) EMM uplink message transmission failure indication by lower layers

When it is specified in the relevant procedure that it is up to the UE implementation to rerun the ongoing procedure that triggered that procedure, the 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.

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.

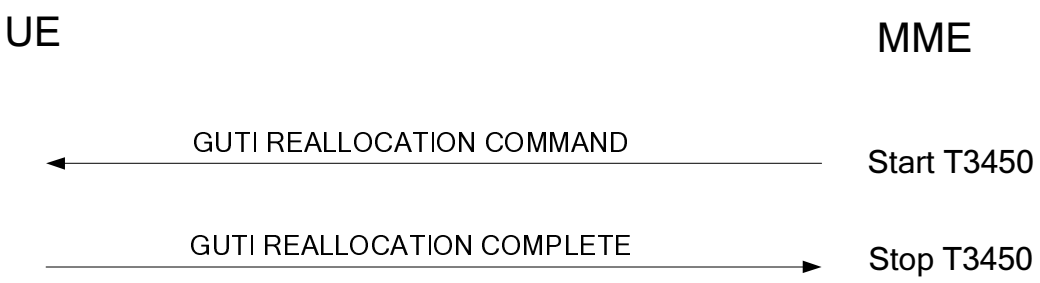


Figure 5.4.1.2.1: GUTI reallocation procedure

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. If no response is received to the paging attempts, the network may use the IMSI for paging for an implementation dependent number of paging attempts;

NOTE: Paging with IMSI causes the UE to re-attach as described in subclause 5.6.2.2.2.

- 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 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 an EXTENDED SERVICE REQUEST message before the ongoing GUTI reallocation procedure has been completed, the network shall progress both procedures.

g) Lower layer indication of non-delivered NAS PDU due to handover

If the GUTI REALLOCATION COMMAND message could not be delivered due to an intra MME handover and the target TA is included in the TAI list, then upon successful completion of the intra MME handover the MME shall retransmit the GUTI REALLOCATION COMMAND message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the GUTI REALLOCATION COMMAND message.

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 proceed with an EPS authentication challenge only if a USIM is present.

A partial native EPS security context is established in the UE and the network when an EPS authentication is successfully performed. During a successful EPS authentication procedure, the CK and IK are computed by the USIM. CK and IK are then used by the ME 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 in the volatile memory of the ME while attached to the network, 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. For restrictions applicable after handover or inter-system handover to S1 mode see subclause 5.5.3.2.3.

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]).

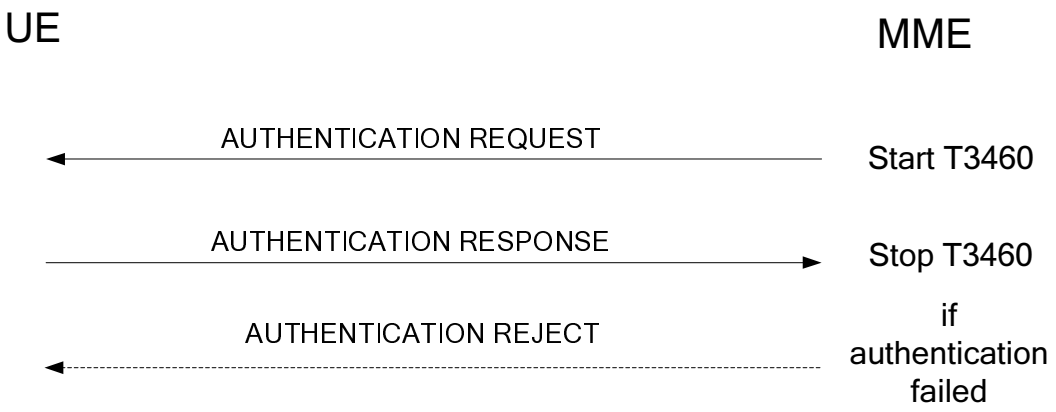


Figure 5.4.2.2.1: Authentication procedure

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 UE shall determine the PLMN identity to be used for the calculation of the new K_{ASME} from the authentication challenge data according to the following rules:

a) When the UE moves from EMM-IDLE mode to EMM-CONNECTED mode, until the first handover, the UE shall use the PLMN identity of the selected PLMN; and

b) After handover or inter-system handover to S1-mode,

- if the target cell is not a shared network cell, the UE shall use the PLMN identity received as part of the broadcast system information;
- if the target cell is a shared network cell and the UE has a valid GUTI, the UE shall use the PLMN identity that is part of the GUTI; and
- if the target cell is a shared network cell and the UE has a valid P-TMSI and RAI, but not a valid GUTI, the UE shall use the PLMN identity that is part of the RAI.

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 in the volatile memory of the ME.

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

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 of the ME. 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 ME 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 ME or the stored RAND is different from the new received value in the AUTHENTICATION REQUEST message, the ME 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 ME shall be deleted and timer T3416, if running, shall be stopped:

- upon receipt of a
  - SECURITY MODE COMMAND,
  - SERVICE REJECT,
  - TRACKING AREA UPDATE 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

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]).

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

Upon receipt of an AUTHENTICATION FAILURE message, the network stops the timer T3460. In the case where the EMM cause #21 "synch failure" is received, the core network may renegotiate with the HSS/AuC and provide the UE with new authentication parameters.

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 A/Gb 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 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 authentication and ciphering procedure is not accepted by the network.

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.

Depending on local requirements or operator preference for emergency bearer services, if the UE has a PDN connection for emergency bearer services established or is establishing a PDN connection for emergency bearer services, the MME need not follow the procedures specified for the authentication failure in the present subclause. The MME may continue a current EMM specific procedure or PDN connectivity request procedure. Upon completion of the authentication procedure, if not initiated as part of another procedure, or upon completion of the EMM procedure or PDN connectivity request procedure, the MME shall deactivate all non-emergency EPS bearers, if any, by initiating an EPS bearer context deactivation procedure. The network shall consider the UE to be attached for emergency bearer services only.

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 three 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 #20 "MAC failure". The UE shall then follow the procedure described in subclause 5.4.2.7, item c.

b) Non-EPS authentication unacceptable:

   If the UE finds that the "separation bit" in the AMF field of AUTN supplied by the core network is 0, the UE shall send an AUTHENTICATION FAILURE message to the network, with the EMM cause #26 "non-EPS authentication unacceptable" (see subclause 6.1.1 in 3GPP TS 33.401 [19]). The UE shall then follow the procedure described in subclause 5.4.2.7, item d.

c) 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 #21 "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 e.

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.

If the UE has a PDN connection for emergency bearer services established or is establishing such a PDN connection, additional UE requirements are specified in subclause 5.4.2.7, under "for items c, d, e".

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 message 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 #20 "MAC failure"):

The UE shall send an AUTHENTICATION FAILURE message, with EMM cause #20 "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 #20 "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 #20 "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, the UE shall follow the procedure specified in this subclause, item c, starting again from the beginning, or if the message contains a UMTS authentication challenge, the UE shall follow the procedure specified in item d. If the SQN is invalid, the UE shall proceed as specified in item e.

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 #20 "MAC failure" the timer T3418 expires;

- the UE detects any combination of the authentication failures: EMM causes #20 "MAC failure" and #21 "synch failure", 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 f.

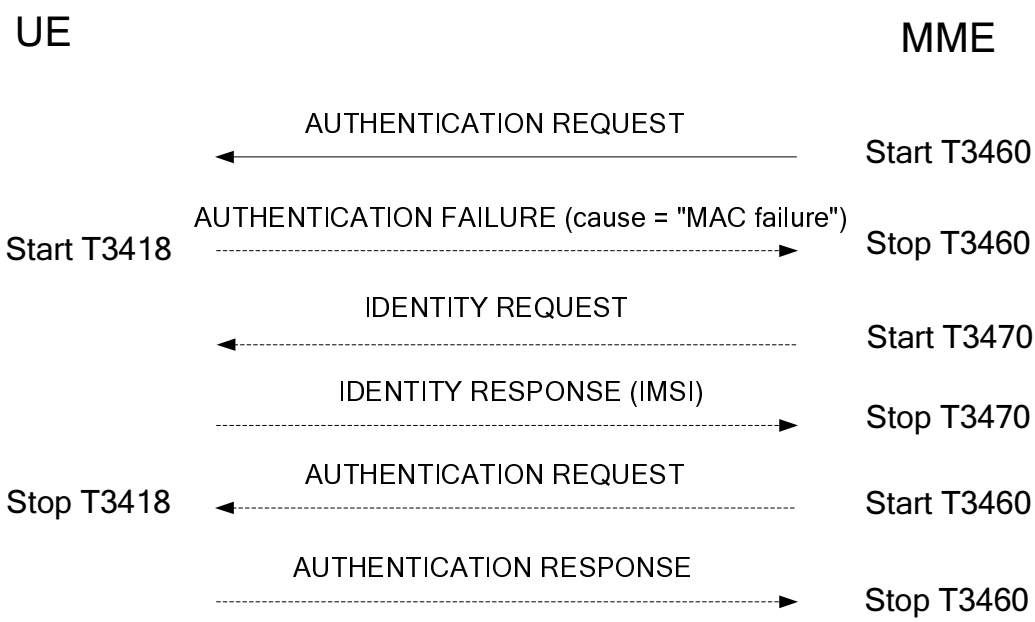


Figure 5.4.2.7.1: Authentication failure procedure (EMM cause #20 "MAC failure" or #26 "non-EPS authentication unacceptable")

d) Authentication failure (EMM cause #26 "non-EPS authentication unacceptable"):

The UE shall send an AUTHENTICATION FAILURE message, with EMM cause #26 "non-EPS authentication unacceptable", to the network and start the 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 #26 "non-EPS authentication unacceptable", 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 2: Upon receipt of an AUTHENTICATION FAILURE message from the UE with EMM cause #26 "non-EPS authentication unacceptable", 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 GUTI/IMSI mapping in the network was correct, the network terminates the authentication procedure (see subclause 5.4.2.5).

e) Authentication failure (EMM cause #21 "synch failure"):

The UE shall send an AUTHENTICATION FAILURE message, with EMM cause #21 "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 #21 "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 3: Upon receipt of two consecutive AUTHENTICATION FAILURE messages from the UE with EMM cause #21 "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, the UE shall follow the procedure specified in item c or if the message contains a UMTS authentication challenge, the UE shall proceed as specified in item d; if the SQN is invalid, the UE shall follow the procedure specified in this subclause, item e, starting again from the beginning.

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

- the timer T3420 expires;
- the UE detects any combination of the authentication failures: EMM cause #20 "MAC failure", #21 "synch failure", or #26 "non-EPS authentication unacceptable", 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.

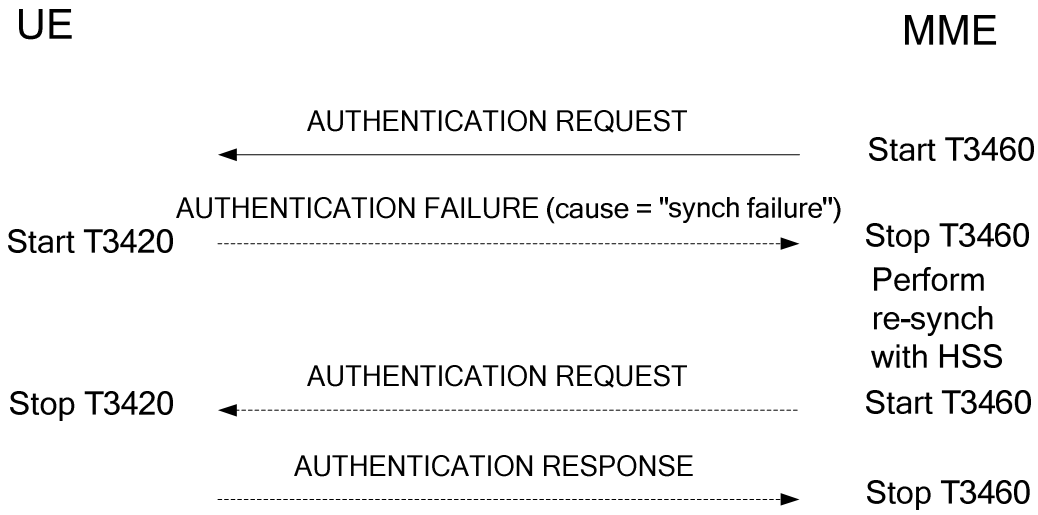


Figure 5.4.2.7.2: Authentication failure procedure (EMM cause #21 "synch failure")

f) 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 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.

g) 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.

h) 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.

i) 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.

j) Lower layers indication of non-delivered NAS PDU due to handover

If the AUTHENTICATION REQUEST message could not be delivered due to an intra MME handover and the target TA is included in the TAI list, then upon successful completion of the intra MME handover the MME shall retransmit the AUTHENTICATION REQUEST message. If a failure of handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the AUTHENTICATION REQUEST message.

For items c, d, and e:

Depending on local requirements or operator preference for emergency bearer services, if the UE has a PDN connection for emergency bearer services established or is establishing a PDN connection for emergency bearer services, the MME need not follow the procedures specified for the authentication failure specified in the present subclause. The MME may respond to the AUTHENTICATION FAILURE message by initiating the security mode control procedure selecting the "null integrity protection algorithm" EIA0, null ciphering algorithm or may abort the authentication procedure and continue using the current security context, if any. The MME shall deactivate all non-emergency EPS bearer contexts, if any, by initiating an EPS bearer context deactivation procedure. If there is an ongoing PDN connectivity procedure, the MME shall deactivate all non-emergency EPS bearer contexts upon completion of the PDN connectivity procedure. The network shall consider the UE to be attached for emergency bearer services only.

If a UE has a PDN connection for emergency bearer services established or is establishing a PDN connection for emergency bearer services and sends an AUTHENTICATION FAILURE message to the MME with the EMM cause appropriate for these cases (#20, #21, or #26, respectively) and receives the SECURITY MODE COMMAND message before the timeout of timer T3418 or T3420, the UE shall deem that the network has passed the authentication check successfully, stop timer T3418 or T3420, respectively, and execute the security mode control procedure.

If a UE has a PDN connection for emergency bearer services established or is establishing a PDN connection for emergency bearer services when timer T3418 or T3420 expires, the UE shall not deem that the network has failed the authentication check and not behave as described in item f. Instead the UE shall continue using the current security context, if any, deactivate all non-emergency EPS bearer contexts, if any, by initiating UE requested PDN disconnect procedure. If there is an ongoing PDN connectivity procedure, the UE shall deactivate all non-emergency EPS bearer contexts upon completion of the PDN connectivity procedure. The UE shall consider itself to be attached for emergency bearer services only.

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 EPS NAS keys and EPS security algorithms.

Furthermore, the network may also initiate a SECURITY MODE COMMAND in order to change the NAS security algorithms for a current EPS security context already in use.

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 reset the downlink NAS COUNT counter and use it to integrity protect the initial SECURITY MODE COMMAND message if the security mode control procedure is initiated:

- to take into use the EPS security context created after a successful execution of the EPS authentication procedure;

- upon receipt of TRACKING AREA UPDATE REQUEST message including a GPRS ciphering key sequence number IE, if the MME wishes to create a mapped EPS security context (i.e. the type of security context flag is set to "mapped security context" in the NAS key set identifier IE included in the SECURITY MODE COMMAND message).

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} or mapped K'_{ASME} indicated by the eKSI included in the message. The MME shall set the security header type of the message to "integrity protected with new EPS security context".

The MME shall create a locally generated K_{ASME} and send the SECURITY MODE COMMAND message including a KSI value in the NAS key set identifier IE set to "000" and EIA0 and EEA0 as the selected NAS security algorithms when the security mode control procedure is initiated:

- during an attach procedure for emergency bearer services if no shared EPS security context is available;

- during a tracking area updating procedure for a UE that has a PDN connection for emergency bearer services if no shared EPS security context is available; or

- after a failed authentication procedure for a UE that has a PDN connection for emergency bearer services if continued usage of a shared security context is not possible.

The UE shall process a SECURITY MODE COMMAND message including a KSI value in the NAS key set identifier IE set to "000" and EIA0 and EEA0 as the selected NAS security algorithms and, if accepted, create a locally generated K_{ASME} when the security mode control procedure is initiated:

- during an attach procedure for emergency bearer services;

- during a tracking area updating procedure when the UE has a PDN connection for emergency bearer services; or

- after an authentication procedure when the UE has a PDN connection for emergency bearer services.

NOTE 1: The process for creation of the locally generated K_{ASME} by the MME and the UE is implementation dependent.

Upon receipt of a TRACKING AREA UPDATE REQUEST message including a GPRS ciphering key sequence number IE, if the MME does not have the valid current EPS security context indicated by the UE, the MME shall either:

- indicate the use of the new mapped EPS security context to the UE by setting the type of security context flag in the NAS key set identifier IE to "mapped security context" and the KSI value related to the security context of the source system; or

- set the KSI value "000" in the NAS key set identifier IE if the MME sets EIA0 and EEA0 as the selected NAS security algorithms if the UE has a PDN connection for emergency bearer services.

While having a current mapped EPS security context with the UE, if the MME wants to take the native EPS security context into use, the MME shall include the eKSI that indicates the native EPS security context in the SECURITY MODE COMMAND 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 (eKSI).

The MME shall include both the $nonce_{MME}$ and the $nonce_{UE}$ when creating a mapped EPS security context during inter-system change from A/Gb mode to S1 mode or Iu mode to S1 mode in EMM-IDLE mode.

The MME may initiate a SECURITY MODE COMMAND in order to change the NAS security algorithms for a current EPS security context already in use. The MME re-derives the NAS keys from K_{ASME} with the new NAS algorithm identities as input and provides the new NAS algorithm identities within the SECURITY MODE COMMAND message.

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

NOTE 2: 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.

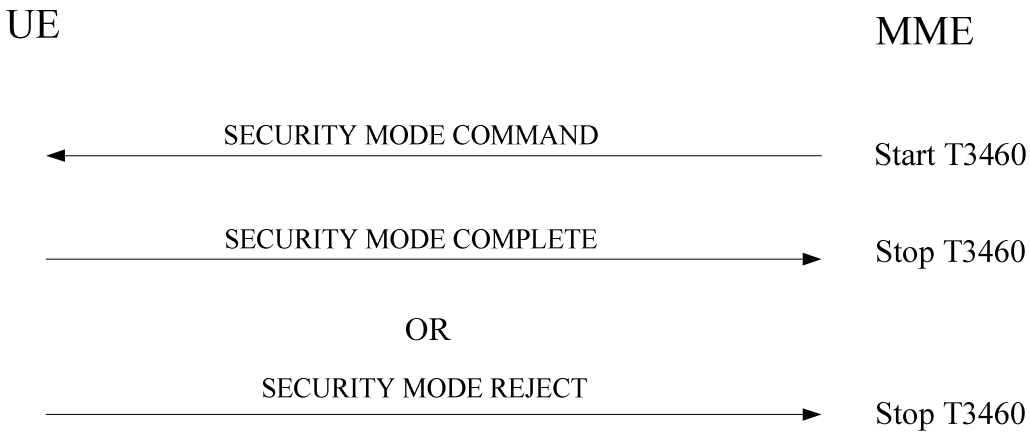


Figure 5.4.3.2.1: Security mode control procedure

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 replayed 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. However, the UE is not required to perform the checking of the received $nonce_{UE}$ if the UE does not want to re-generate the K'_{ASME} (i.e. the SECURITY MODE COMMAND message is to derive and take into use a mapped EPS security context and the eKSI matches the current EPS security context, if it is a mapped EPS security context). When the UE has a PDN connection for emergency bearer services established or the UE is establishing a PDN connection for emergency bearer services, the UE is not required to locally re-generate the K_{ASME} (i.e. the SECURITY MODE COMMAND message is used to derive and take into use a native EPS security context where the KSI value "000" is included in the NAS key set identifier IE and the EIA0 and EEA0 are included as the selected NAS security algorithms).

The UE shall accept a SECURITY MODE COMMAND message indicating the "null integrity protection algorithm" EIA0 as the selected NAS integrity algorithm only if the message is received for a UE that has a PDN connection for emergency bearer services established or a UE that is establishing a PDN connection for emergency bearer services.

If the type of security context flag included in the SECURITY MODE COMMAND message is set to "native security context" and if the KSI matches a valid non-current native EPS security context held in the UE while the UE has a mapped EPS security context as the current EPS security context, the UE shall take the non-current native EPS security context into use which then becomes the current native EPS security context and delete the mapped EPS security context.

If the SECURITY MODE COMMAND message can be accepted, the UE shall take the EPS security context indicated in the message into use. The UE shall in addition reset the uplink NAS COUNT counter if:

- the SECURITY MODE COMMAND message is received in order to take an EPS security context into use created after a successful execution of the EPS authentication procedure;

- the SECURITY MODE COMMAND message received includes the type of security context flag set to "mapped security context" in the NAS key set identifier IE the eKSI does not match the current EPS security context, if it is a mapped EPS security context.

If the SECURITY MODE COMMAND message can be accepted and a new EPS security context is taken into use and SECURITY MODE COMMAND message does not indicate the "null integrity protection algorithm" EIA0 as the selected NAS integrity algorithm, the UE shall:

- if the SECURITY MODE COMMAND message has been successfully integrity checked using an estimated downlink NAS COUNT equal 0, then the UE shall set the downlink NAS COUNT of this new EPS security context to 0;

- otherwise the UE shall set the downlink NAS COUNT of this new EPS security context to the downlink NAS COUNT that has been used for the successful integrity checking of the SECURITY MODE COMMAND message.

If the SECURITY MODE COMMAND message can be accepted, the UE shall send a SECURITY MODE COMPLETE message integrity protected with the selected NAS integrity algorithm and the EPS NAS integrity key based on the K_{ASME} or mapped K'_{ASME} if the type of security context flag is set to "mapped security context" indicated by the eKSI. When the SECURITY MODE COMMAND message includes the type of security context flag set to "mapped security context" in the NAS key set identifier IE, the $nonce_{MME}$ and the $nonce_{UE}$, then the UE shall either:

- generate K'_{ASME} from both the $nonce_{MME}$ and the $nonce_{UE}$ as indicated in 3GPP TS 33.401 [19];or
- check whether the SECURITY MODE COMMAND message indicates the eKSI of the current EPS security context, if it is a mapped EPS security context, in order not to re-generate the K'_{ASME}.

Furthermore, if the SECURITY MODE COMMAND message can be accepted, the UE shall cipher the SECURITY MODE COMPLETE message with the selected NAS ciphering algorithm and the EPS NAS ciphering key based on the K_{ASME} or mapped K'_{ASME} indicated by the eKSI. The UE shall set the security header type of the message to "integrity protected and ciphered with new EPS security context".

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. 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.

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.

Both the UE and the MME shall apply the EPS security context in use before the initiation of the security mode control procedure, if any, to protect the SECURITY MODE REJECT message and any other subsequent messages according to the rules in subclauses 4.4.4 and 4.4.5.

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 message 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.

NOTE: If the SECURITY MODE COMMAND message was sent to create a mapped EPS security context during inter-system change from A/Gb mode to S1 mode or Iu mode to S1 mode, then the network does not generate new values for the $nonce_{MME}$ and the $nonce_{UE}$, but includes the same values in the SECURITY MODE COMMAND message (see the subclause 7.2.4.4 in 3GPP TS 33.401 [19]).

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

e) Lower layers indication of non-delivered NAS PDU due to handover

If the SECURITY MODE COMMAND message could not be delivered due to an intra MME handover and the target TA is included in the TAI list, then upon successful completion of the intra MME handover the MME shall retransmit the SECURITY MODE COMMAND message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the SECURITY MODE COMMAND message.

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].

For mobile device supporting both 3GPP access and cdma2000® access a single IMEI is used to identify the device as specified in 3GPP TS 22.278 [1B].

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.

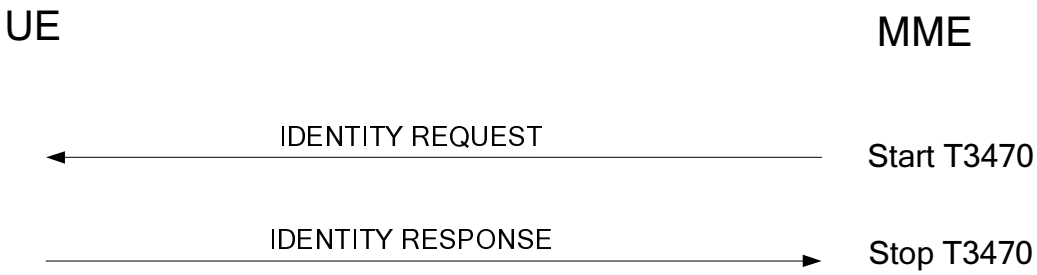


Figure 5.4.4.2.1: Identification procedure

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.

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 attach procedure

If the network receives an ATTACH REQUEST message before the ongoing identification procedure has been completed and no 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 attach procedure.

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

If the network receives an ATTACH REQUEST message before the ongoing identification procedure has been completed and an 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 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 detach procedure

Detach containing cause "switch off" within the Detach type IE:

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 detach procedure.

Detach containing other causes than "switch off" within the Detach type IE:

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 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 an EXTENDED SERVICE REQUEST message before the ongoing identification procedure has been completed, the network shall progress both procedures.

h) Lower layers indication of non-delivered NAS PDU due to handover

If the IDENTITY REQUEST message could not be delivered due to an intra MME handover and the target TA is included in the TAI list, then upon successful completion of the intra MME handover the MME shall retransmit the IDENTITY REQUEST message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the IDENTITY REQUEST message.

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 EMM cause #97 "message type non-existent or not implemented".

5.4.5.4 Abnormal cases on the network side

The following abnormal case can be identified:

a) Lower layers indication of non-delivered NAS PDU due to handover

If the EMM INFORMATION message could not be delivered due to an intra MME handover and the target TA is included in the TAI list, then upon successful completion of the intra MME handover the MME shall retransmit the EMM INFORMATION message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the EMM INFORMATION message.

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 three purposes:

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

If the MME does not support an attach for emergency bearer services, the MME shall reject any request to attach with an attach type set to "EPS emergency attach".

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 EMM cause #11 "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 with the EMM cause

#14 "EPS services not allowed in this PLMN" is received by the UE, the chosen PLMN identity shall be stored in the "forbidden PLMNs for GPRS service". Whenever an ATTACH REJECT message is received by the UE with the EMM cause #12 "tracking area not allowed", #13 "roaming not allowed in this tracking area", or #15 "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 attach procedure is completed for EPS services only with cause #2, #16, #17, #18 or #22;
- an attach or combined attach procedure is rejected with cause #11, #12, #13, #14, #15 or #25; or
- a network initiated detach procedure is completed with cause #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 attach procedure,for normal service the UE shall indicate "EPS attach" in the EPS attach type IE.

When the UE initiates the attach procedure for emergency bearer services, the UE shall indicate "EPS emergency 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.

If the UE supports neither A/Gb mode nor Iu mode, the UE shall handle the EPS mobile identity IE in the ATTACH REQUEST message as follows:

- 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.

If the UE supports A/Gb mode or Iu mode, the UE shall handle the EPS mobile identity 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 EPS mobile identity IE. If a P-TMSI signature is associated with the P-TMSI, the UE shall include it in the Old P-TMSI signature IE. Additionally, if the UE holds a valid GUTI, the UE shall indicate the GUTI in the Additional GUTI IE.

NOTE: The mapping of the P-TMSI and the RAI to the GUTI is specified in 3GPP TS 23.003 [2].

- If the TIN indicates "GUTI" or "RAT-related TMSI" and the UE holds a valid GUTI, the UE shall indicate the GUTI in the EPS mobile identity IE.
- If the TIN is deleted and

- the UE holds a valid GUTI, the UE shall indicate the GUTI in the EPS mobile identity IE; or
- otherwise, if the UE holds a valid P-TMSI and RAI, the UE shall map the P-TMSI and RAI into the EPS mobile identity IE. If a P-TMSI signature is associated with the P-TMSI, the UE shall include it in the Old P-TMSI signature IE.

- Otherwise the UE shall include the IMSI in the EPS mobile identity IE.

If the UE is attaching for emergency bearer services and does not hold a valid GUTI, P-TMSI or IMSI as described above, the IMEI shall be included in the EPS mobile identity IE.

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.

If UE supports A/Gb mode or Iu mode or if the UE wants to indicate its UE specific DRX parameter to the network, the UE shall include the UE specific DRX parameter in the DRX parameter IE in the ATTACH REQUEST message.

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.

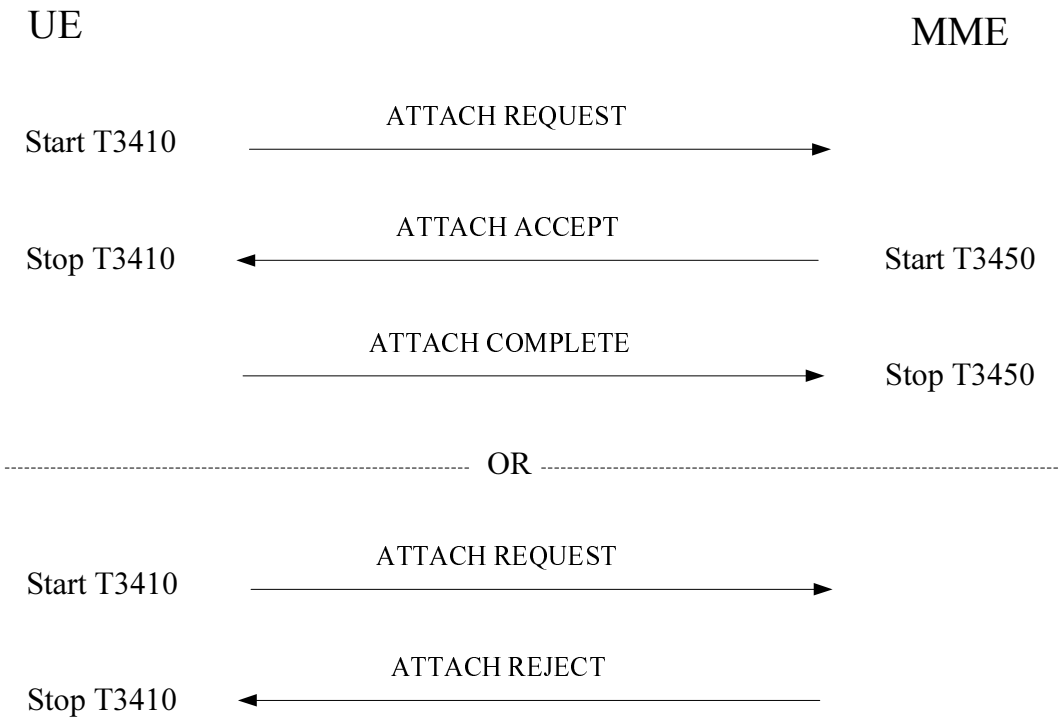


Figure 5.5.1.2.2.1: Attach procedure and combined attach procedure

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).

During an attach for emergency bearer services, the MME may choose to skip the authentication procedure even if no EPS security context is available and proceed directly to the execution of the security mode control procedure as specified in subclause 5.4.3.

5.5.1.2.4 Attach accepted by the network

During an attach for emergency bearer services, if not restricted by local regulations, the MME shall not check for mobility and access restrictions, regional restrictions, subscription restrictions, or perform CSG access control when processing the ATTACH REQUEST message.

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.

If the UE specific DRX parameter was included in the DRX Parameter IE in the ATTACH REQUEST message, the MME shall replace any stored UE specific DRX parameter with the received parameter and use it for the downlink transfer of signalling and user data.

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 IMEI, 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. The MME indicates the selected core network operator PLMN identity to the UE in the GUTI (see 3GPP TS 23.251 [8B]).

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, and if the attach procedure is not for emergency bearer services, the UE shall remove 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.

The network informs the UE about the support of specific features, such as IMS voice over PS session, location services (EPC-LCS, CS-LCS) or emergency bearer services, in the EPS network feature support information element. In a UE with IMS voice over PS capability, the IMS voice over PS session indicator and the emergency bearer services indicator shall be provided to the upper layers. The upper layers take the IMS voice over PS session indicator into account as specified in 3GPP TS 23.221 [8A], subclause 7.2a, when selecting the access domain for voice sessions or calls. When initiating an emergency call, the upper layers also take the emergency bearer services indicator into account for the access domain selection. In a UE with LCS capability, location services indicators (EPC-LCS, CS-LCS) shall be provided to the upper layers. When MO-LR procedure is triggered by the UE's application, those indicators are taken into account as specified in 3GPP TS 24.171 [13C].

If the UE has initiated the attach procedure due to manual CSG selection and receives an ATTACH ACCEPT message; and the UE sent the ATTACH REQUEST message in a CSG cell, the UE shall check if the CSG ID and associated PLMN identity of the cell are contained in the Allowed CSG list. If not, the UE shall add that CSG ID and associated PLMN identity to the Allowed CSG list and the UE may add the HNB Name (if provided by lower layers) to the Allowed CSG list if the HNB Name is present in neither the Operator CSG list nor 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.

When the UE receives any ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST messages during the attach procedure, the UE shall forward the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message(s) to the ESM sublayer. The UE shall send a response to the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message(s) after successful completion of the attach procedure.

If the attach procedure was initiated in S101 mode, the lower layers are informed about the successful completion of the procedure.

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, an ESM procedure failure, or operator determined barring is applied on default EPS bearer context activation during attach procedure, 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 eKSI. 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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 eKSI. Additionally, the UE shall delete the list of equivalent PLMNs and reset the attach attempt counter, and enter state EMM-DEREGISTERED.PLMN-SEARCH.

In S1 mode, the UE shall store the PLMN identity in the "forbidden PLMN list" and enter state EMM-DEREGISTERED.PLMN-SEARCH. The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

In S101 mode, the UE shall store the PLMN identity provided with the indication from the lower layers to prepare for an S101 mode to S1 mode handover in the list of "forbidden PLMNs for attach in S101 mode" and enter the state EMM-DEREGISTERED.NO-CELL-AVAILABLE.

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 the GMM cause with the same 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 eKSI. Additionally, the UE shall reset the attach attempt counter.

In S1 mode, the UE shall store the current TAI in the list of "forbidden tracking areas for regional provision of service" and enter the state EMM-DEREGISTERED.LIMITED-SERVICE.

In S101 mode, the UE shall store the PLMN identity provided with the indication from the lower layers to prepare for an S101 mode to S1 mode handover in the list of "forbidden PLMNs for attach in S101 mode" and enter the state EMM-DEREGISTERED.NO-CELL-AVAILABLE.

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 the GMM cause with the same 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 eKSI. The UE shall delete the list of equivalent PLMNs and reset the attach attempt counter.

In S1 mode, the UE shall store the current TAI in the list of "forbidden tracking areas for roaming". Additionally, the UE shall enter the state EMM-DEREGISTERED.LIMITED-SERVICE or optionally EMM-DEREGISTERED.PLMN-SEARCH. The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

In S101 mode, the UE shall store the PLMN identity provided with the indication from the lower layers to prepare for an S101 mode to S1 mode handover in the list of "forbidden PLMNs for attach in S101 mode" and enter the state EMM-DEREGISTERED.NO-CELL-AVAILABLE.

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 the GMM cause with the same 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 eKSI.

In S1 mode, the UE shall store the PLMN identity in the "forbidden PLMNs for GPRS service" list. Additionally, the UE shall enter state EMM-DEREGISTERED.PLMN-SEARCH. The UE shall perform a PLMN selection according to 3GPP TS 23.122 [6].

In S101 mode, the UE shall store the PLMN identity provided with the indication from the lower layers to prepare for an S101 mode to S1 mode handover in the list of "forbidden PLMNs for attach in S101 mode" and enter the state EMM-DEREGISTERED.NO-CELL-AVAILABLE.

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 the GMM cause with the same 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 eKSI. Additionally, the UE shall reset the attach attempt counter.

In S1 mode, the UE shall store the current TAI in the list of "forbidden tracking areas for roaming" and enter the state EMM-DEREGISTERED.LIMITED-SERVICE. 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].

In S101 mode, the UE shall store the PLMN identity provided with the indication from the lower layers to prepare for an S101 mode to S1 mode handover in the list of "forbidden PLMNs for attach in S101 mode" and enter the state EMM-DEREGISTERED.NO-CELL-AVAILABLE.

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 the GMM cause with the same value.

#25 (Not authorized for this CSG);

EMM cause #25 is only applicable when received from a CSG cell. EMM cause #25 received from a non-CSG cell is considered as an abnormal case and the behaviour of the UE is specified in subclause 5.5.1.2.6.

If the ATTACH REJECT message with EMM cause #25 was received without integrity protection, then the UE shall discard the message.

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.

If the CSG ID and associated PLMN identity of the cell where the UE has sent the ATTACH REQUEST message is contained in the Allowed CSG list, the UE shall remove the entry corresponding to this CSG ID and associated PLMN identity from the Allowed CSG list.

If the CSG ID and associated PLMN identity of the cell where the UE has sent the ATTACH REQUEST message are contained in the Operator CSG list, the UE shall apply the procedures defined in 3GPP TS 23.122 [6] subclause 3.1A.

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 the GMM cause with the same value.

Other values are considered as abnormal cases. The behaviour of the UE in those cases is specified in subclause 5.5.1.2.6.

5.5.1.2.5A Attach for emergency bearer services not accepted by the network

If the attach request for emergency bearer services cannot be accepted by the network, the MME shall send an ATTACH REJECT message to the UE including EMM cause #5 "IMEI not accepted" or one of the EMM cause values as described in subclause 5.5.1.2.5.

NOTE: If EMM cause #11 is sent to a UE of a roaming subscriber attaching for emergency bearer services and the UE is in automatic network selection mode, it cannot obtain normal service provided by this PLMN.

Upon receiving the ATTACH REJECT message including EMM cause #5, the UE shall enter the state EMM-DEREGISTERED.NO-IMSI.

Upon receiving the ATTACH REJECT message including one of the other EMM cause values, the UE shall perform the actions as described in subclause 5.5.1.2.5 with the following addition: upon request from upper layers a CS voice capable UE may establish the emergency call using the CS domain.

In a shared network, upon receiving the ATTACH REJECT message, the UE shall perform the actions as described in subclause 5.5.1.2.5 with the following additions:

a) upon request from upper layers a CS voice capable UE may attempt the emergency call using the CS domain; or

b) a UE may try the attach for emergency bearer services to another PLMN in the shared network.

If options a) and b) above are either not applicable or one or both of them have failed a UE may attempt the emergency call using other implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [13D] that can result in the emergency call being attempted to another IP-CAN.

5.5.1.2.5B Attach for initiating a PDN connection for emergency bearer services not accepted by the network

If the network cannot accept attach request for initiating a PDN connection for emergency bearer services with attach type not set to "EPS emergency attach", the UE shall perform the procedures as described in subclause 5.5.1.2.5. Then if the UE is in the same selected PLMN where the last attach request was attempted, the UE shall:

a) inform the upper layers. This could result in the UE attempting a CS emergency call (if not already attempted in the CS domain) or other implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [13D] that can result in the emergency call being attempted to another IP-CAN; or

b) attempt EPS attach for emergency bearer services.

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 EMM cause values than those treated in subclause 5.5.1.2.5

Upon reception of the EMM cause #19, "ESM failure", the UE may set the attach attempt counter to 5. Upon reception of the EMM causes #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 indication from lower layers

The UE shall restart the attach procedure.

i) Transmission failure of ATTACH COMPLETE message indication from lower layers

If the current TAI is not in the TAI list, the UE shall restart the attach procedure.

If the current TAI is still in the TAI list, it is up to the UE implementation how to re-run the ongoing procedure. The EMM sublayer notifies the ESM sublayer that the ESM message in the ESM message container IE of the ATTACH COMPLETE has failed to be transmitted.

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. Further UE behaviour is implementation specific.

k) Indication from the lower layers that an S101 mode to S1 mode handover has been cancelled (S101 mode only)

The UE shall abort the attach procedure and enter state EMM-DEREGISTERED.NO-CELL-AVAILABLE.

For the cases b, c, and d 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, the network shall locally abort the attach procedure, enter state EMM-DEREGISTERED and shall not resend the message ATTACH ACCEPT. If a new GUTI was assigned to the UE in the attach procedure, the MME shall consider both the old and the new GUTI as valid until the old GUTI can be considered as invalid by the network or the EMM context which has been marked as detached in the network is released.

   If the old GUTI was allocated by an MME other than the current MME, the current MME does not need to retain the old GUTI. If the old GUTI is used by the UE in a subsequent attach message, the network may use the identification procedure to request the UE's IMSI.

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 and the MME enters state EMM-DEREGISTERED. If a new GUTI was allocated in the ATTACH ACCEPT message, the network shall consider both the old and the new GUTI as valid until the old GUTI can be considered as invalid by the network. If the old GUTI was allocated by an MME other than the current MME, the current MME does not need to retain the old GUTI. or the EMM context which has been marked as detached in the network is released.

   If the old GUTI is used by the UE in a subsequent attach message, 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 in the attach procedure shall be considered as valid and the tracking area updating procedure shall be rejected with the EMM cause #10 "implicitly detached" as described in subclause 5.5.3.2.5.

5.5.1.3 Combined attach procedure for EPS services and non-EPS services (S1 mode only)

5.5.1.3.1 General

The combined 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, or both EPS services and "SMS only".

The combined attach procedure is also used by a UE in CS/PS mode 1 or CS/PS mode 2 of operation to attach for EPS services if it is already IMSI attached for non-EPS services.

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

The combined 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.

If the UE initiates a combined attach procedure for EPS services and "SMS only", the UE shall indicate "SMS only" in the Additional update type IE.

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, the following different cases can be distinguished:

1) The EPS attach result IE value indicates "combined EPS/IMSI attach": attach for EPS and non-EPS services, or for EPS services and "SMS only" 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 or "SMS only" 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 or "SMS only" 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 as described in subclause 5.4.1.4, and enter state EMM-COMMON-PROCEDURE-INITIATED. If the MME does not indicate "SMS only" in the ATTACH ACCEPT message, subject to operator policies the MME should allocate a TAI list that does not span more than one location area.

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 an IMSI, the UE is not allocated any TMSI, and shall delete any TMSI accordingly. If the message contains a TMSI, the UE shall use this TMSI as the new temporary identity. The UE shall delete its old TMSI and shall store the new TMSI. If neither a TMSI nor an IMSI has been included by the network in the ATTACH ACCEPT message, the old TMSI, if any available, shall be kept.

If the UE requested "SMS only" in the Additional update type IE, the network shall indicate "SMS only" in the Additional update result IE.

If the ATTACH ACCEPT message includes the Additional update result IE with value "SMS only" or "CS Fallback not preferred", a UE operating in CS/PS mode 1 with "IMS voice not available" shall attempt to select GERAN or UTRAN radio access technology rather than E-UTRAN for the selected PLMN or equivalent PLMN. The UE shall disable the E-UTRA capability (see subclause 4.5). If the UE is in the EMM-CONNECTED mode, the UE shall locally release the established NAS signalling connection and enter the EMM-IDLE mode before selecting GERAN or UTRAN radio access technology.

If the ATTACH ACCEPT message includes the Additional update result IE with value "SMS only", a UE operating in CS/PS mode 2 shall not attempt to use CS fallback for mobile originating services.

If the ATTACH ACCEPT message includes the Additional update result IE with value "CS Fallback not preferred", this indicates to a UE operating in CS/PS mode 2 that it is attached for EPS and non-EPS services and that it can use CS fallback.

If the LAI contained in the ATTACH ACCEPT message is a member of the list of "forbidden location areas for regional provision of service" or the list of "forbidden location areas for roaming" then such entry shall be deleted.

If the PLMN ID for the CS domain which is provided as part of the LAI contained in the ATTACH ACCEPT message differs from the PLMN ID provided as part of the GUTI, the MME shall include the "Equivalent PLMNs" IE in the ATTACH ACCEPT message and include the PLMN ID for the CS domain in this IE.

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

Apart from the actions on the tracking area updating attempt counter, 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 and shall reset the tracking area updating attempt counter. 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:

- a UE operating in CS/PS mode 2 of operation 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 with "IMS voice not available" shall attempt to select GERAN or UTRAN radio access technology and proceed with appropriate MM or GMM specific procedures. The UE shall disable the E-UTRA capability (see subclause 4.5). If the UE is in the EMM-CONNECTED mode, the UE shall locally release the established NAS signalling connection and enter the EMM-IDLE mode before selecting GERAN or UTRAN radio access technology.

NOTE 1: It is up to the UE implementation when to enable E-UTRAN radio access technology selection.

#18 (CS domain not available)

The UE shall stop timer T3410 if still running, shall reset the tracking area updating attempt counter, 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 with "IMS voice not available" shall attempt to select GERAN or UTRAN radio access technology rather than E-UTRAN for the selected PLMN or equivalent PLMN. The UE shall disable the E-UTRA capability (see subclause 4.5). If the UE is in the EMM-CONNECTED mode, the UE shall locally release the established NAS signalling connection and enter the EMM-IDLE mode before selecting GERAN or UTRAN radio access technology.

A UE in CS/PS mode 2 of operation may provide a notification to the user or the upper layers that the CS domain is not available.

The UE shall not attempt combined attach or combined tracking area update procedure with current PLMN until switching off the UE or the UICC containing the USIM is removed.

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 eKSI.

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 the GMM cause with the same 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 eKSI. 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.

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 IMSI attached for non-EPS services is still IMSI 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.

NOTE: Some interaction is required with the access stratum to disable E-UTRAN cell reselection.

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 the GMM cause with the same 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 eKSI, 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same value.

#25 (Not authorized for this CSG);

EMM cause #25 is only applicable when received from a CSG cell. EMM cause #25 received from a non-CSG cell is considered as an abnormal case and the behaviour of the UE is specified in subclause 5.5.1.3.6.

If the ATTACH REJECT message with EMM cause #25 was received without integrity protection, then the UE shall discard the message.

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.

If the CSG ID and associated PLMN identity of the cell where the UE has sent the ATTACH REQUEST message are contained in the Allowed CSG list, the UE shall remove the entry corresponding to this CSG ID and associated PLMN identity from the Allowed CSG list.

If the CSG ID and associated PLMN identity of the cell where the UE has sent the ATTACH REQUEST message is contained in the Operator CSG list, the UE shall apply the procedures defined in 3GPP TS 23.122 [6] subclause 3.1A.

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 the GMM cause with the same 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 UE requested the combined attach for EPS services and "SMS only" and the ATTACH ACCEPT message indicates a combined attach successful for EPS and non-EPS services, the UE shall behave as if the combined attach was successful for EPS services and "SMS only".

NOTE: In this case the UE can ignore the Paging with CN domain indicator set to "CS", as specified in subclause 5.6.2.3.2.

- if the combined attach was successful for EPS services only and the ATTACH ACCEPT message contained an EMM 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 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.

NOTE: It is up to the UE implementation when to enable E-UTRAN radio access technology selection.

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;

- by the network to inform the UE that it is detached for EPS services or non-EPS services or both; and

- by the network to disconnect the UE from the last PDN to which it is connected.

NOTE: After a successful completion of an inter-system change of the UE from S1 mode to non-3GPP access, if the non-3GPP network provides PDN connectivity to the same EPC, the MME performs a local detach of the UE.

The detach procedure also applies to the UE which is IMSI attached for "SMS only".

The detach procedure with appropriate detach type shall be invoked by the UE if the UE is switched off, the USIM card is removed from the UE or the EPS capability of the UE is disabled or the UE wishes to detach for non-EPS services.

After the completion of application for which the emergency services were invoked, in order to regain normal services, a UE attached for emergency bearer services may perform a detach procedure, followed by a subsequent re-attach, if the UE moves to a new cell that provides normal service.

If a detach is requested by the HSS for a UE that has bearers for emergency services, the MME shall not send a DETACH REQUEST message to the UE, and shall follow the procedures in subclause 6.4.4.1 for a UE that has bearers for emergency services.

If the detach procedure for EPS services 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.

Upon successful completion of the detach procedure, if the UE and the MME enter the EMM-DEREGISTERED state, the UE and the MME shall delete any mapped EPS security context or partial native EPS security context.

If the UE supports A/Gb mode or Iu mode, the UE shall store the TIN in the non-volatile memory in the ME, as described in annex C, for a subsequent attach procedure.

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 UE has a mapped EPS security context as the current EPS security context, the UE shall set the type of security context flag to "mapped security context". Otherwise, the UE shall set the type of security context flag to "native security context".

If the UE has a valid GUTI, the UE shall populate the EPS mobile identity IE with the valid GUTI. If the UE does not have a valid GUTI, the UE shall populate the EPS mobile identity IE with its IMSI.

If the UE does not have a valid GUTI and it does not have a valid IMSI, then the UE shall populate the EPS mobile identity IE with its IMEI.

NOTE: During the attach for emergency service when the UE (with no USIM or invalid USIM) is in EMM-REGISTERED-INITIATED STATE, the UE has neither a valid GUTI nor a valid IMSI.

If the detach is not due to switch off and the UE is in the state EMM-REGISTERED or EMM-REGISTERED-INITIATED, 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 the last DETACH REQUEST message is sent, the UE shall proceed as follows:

- if the current EPS security context is a native EPS security context, then the UE shall store the current EPS security context as specified in annex C and mark it as valid;

- else if the current EPS security context is a mapped EPS security context and a non-current full native EPS security context exists, then the UE shall store the non-current EPS security context as specified in annex C and mark it as valid, and finally the UE shall delete any mapped EPS security context or partial native EPS security context.

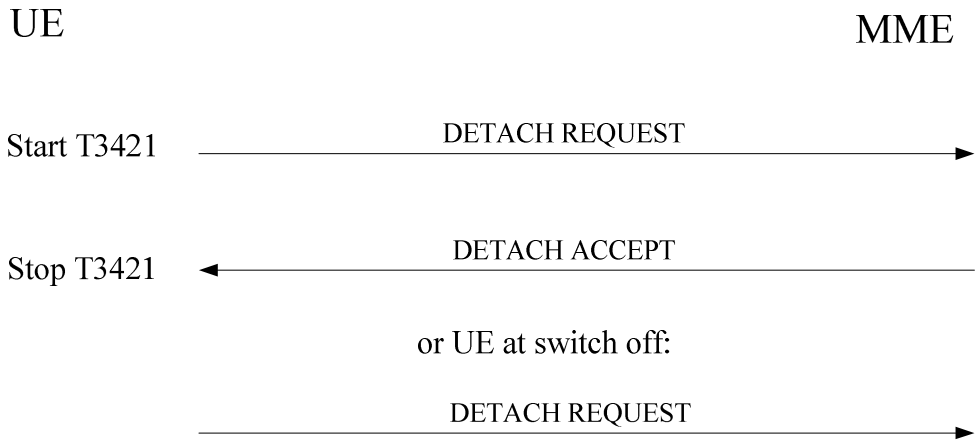


Figure 5.5.2.2.1.1: UE initiated detach procedure

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 and store the current EPS security context, 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 current EPS security context if it is a mapped EPS security context.

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 network.

The UE in PS mode of operation shall enter the EMM-DEREGISTERED state.

The UE in CS/PS mode 1 or CS/PS mode 2 of operation shall set the update status to U2 NOT UPDATED, disable E-UTRAN and select GERAN or UTRAN access technology and enter the EMM-NULL state.

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 signalling procedure shall not be started. The UE stays in the current serving cell and applies the normal cell reselection process. The detach signalling 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 treat the message as specified in subclause 5.5.2.3.2 and 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.

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 or in the Operator 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 valid for the UE, and the detach procedure is not due to "switch off", the network shall proceed as follows:

- if the detach type is "IMSI detach" and the UE has a PDN connection for emergency bearer services active, the MME shall send a DETACH ACCEPT message and deactivate all non-emergency EPS bearers, if any, by initiating an EPS bearer context deactivation procedure;

- otherwise, the network shall initiate the detach procedure. The MME shall send a DETACH REQUEST message including the EMM cause #25,"not authorized for this CSG", to indicate to the UE to remove the entry corresponding to this CSG ID and associated PLMN identity of the cell where the UE has sent the DETACH REQUEST message from the Allowed CSG list.

b) Lower layers indication of non-delivered NAS PDU due to handover

If the DETACH ACCEPT message could not be delivered due to an intra MME handover and the target TA is included in the TAI list, then upon successful completion of the intra MME handover the MME shall retransmit the DETACH ACCEPT message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the DETACH ACCEPT message.

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 either a DETACH REQUEST message to the UE (see example in figure 5.5.2.3.1) or EMM messages (e.g. SERVICE REJECT or TRACKING AREA UPDATE reject) with EMM cause #10 "implicitly detached". The network may include an EMM cause IE to specify the reason for the detach request. The network shall start timer T3422. In case of detach with Detach type IE indicating "re-attach required" or "re-attach not required" and the EMM cause value is not #2 "IMSI unknown in HSS", or in case of EMM message with EMM cause #10 "implicitly detached", the MME shall store the current EPS security context. Otherwise, the current EPS security context is deleted if it is a mapped EPS security context. If the detach type IE indicates "re-attach required" or "re-attach not required" and the EMM cause value is not #2 "IMSI unknown in HSS", the network shall deactivate the EPS bearer context(s) for the UE locally and enter state EMM-DEREGISTERED-INITIATED.

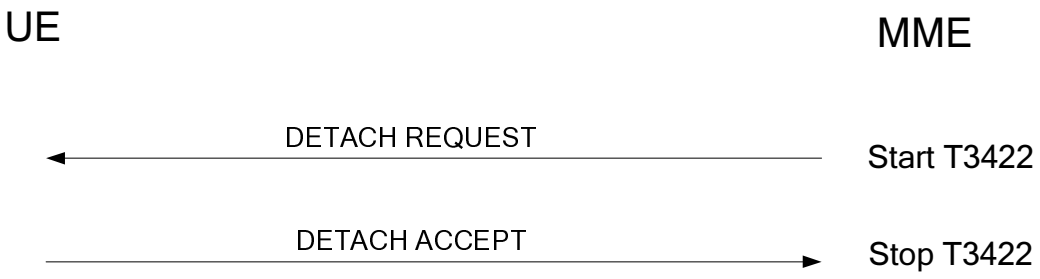


Figure 5.5.2.3.1: Network initiated detach procedure

5.5.2.3.2 Network initiated detach procedure completion by the UE

When receiving the DETACH REQUEST message and the detach type 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. Furthermore, the UE shall, after the completion of the detach procedure, and the existing NAS signalling connection has been released, initiate an attach or combined attach procedure.

NOTE 1: When detach type indicates "re-attach required", user interaction is necessary in some cases when the UE cannot re-activate the EPS bearer(s) automatically.

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 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 UE is attached for EPS and non-EPS services, then the UE shall set the update status to U2 NOT UPDATED if:

- the Detach type IE indicates "re-attach required"; or
- the Detach type IE indicates "re-attach not required" and no EMM cause IE is included.

When receiving the DETACH REQUEST message and the detach type 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 indicates "IMSI detach" or "re-attach required", then the UE shall ignore the EMM cause IE if received.

If the detach type 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 the GMM cause with the same 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 the GMM cause with the same 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 2: 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 the GMM cause with the same 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 is still IMSI attached for non-EPS services in the network. The UE operating in CS/PS mode 1 or CS/PS mode 2 of operation shall set the update status to U2 NOT UPDATED, 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 the GMM cause with the same 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 the GMM cause with the same 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 the GMM cause with the same value and with detach type set to "re-attach not required". If the UE is IMSI 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 the GMM cause with the same 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 the GMM cause with the same value and with detach type set to "re-attach not required". If the UE is IMSI 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 the GMM cause with the same 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 and shall set the update status to U2 NOT UPDATED.

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 the GMM cause with the same 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 the GMM cause with the same value and with detach type set to "re-attach not required". If the UE is IMSI 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 the GMM cause with the same 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.

If the cell where the UE has received the DETACH REQUEST message is a CSG cell and the CSG ID and associated PLMN identity of the cell are contained in the Allowed CSG list, the UE shall remove the entry corresponding to this CSG ID and associated PLMN identity from the Allowed CSG list.

If the cell where the UE has received the DETACH REQUEST message is a CSG cell and the CSG ID and associated PLMN identity of the cell are contained in the Operator CSG list, the UE shall apply the procedures defined in 3GPP TS 23.122 [6] subclause 3.1A.

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 GMM cause with the same value and with detach type set to "re-attach not required". If the UE is IMSI 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 the GMM cause with the same value and with detach type set to "re-attach not required".

Other EMM 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 stop timer T3422 upon receipt of the DETACH ACCEPT message. If the Detach type IE indicates "re-attach required" or "re-attach not required", the network shall enter state EMM-DEREGISTERED. If the Detach type IE indicates "IMSI detach", the network shall not change the current EMM state.

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 EMM 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 set the GPRS update status to GU2 NOT UPDATED and shall delete the GMM parameters 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. If the detach type is "re-attach required" or "re-attach not required", the network shall change to state EMM-DEREGISTERED. If the detach type is "IMSI detach", the network shall not change the current EMM state.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.

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 not required" with EMM cause other than #2 "IMSI unknown in HSS" or indicates "re-attach 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 "re-attach not required" with EMM cause #2 "IMSI unknown in HSS" or 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 (e.g. the DETACH REQUEST message is pending to be sent to the UE) and the DETACH REQUEST contains detach type "re-attach not required" with EMM cause #2 "IMSI unknown in HSS" or detach type "IMSI detach", the network shall progress both procedures. If the DETACH REQUEST message contains detach type "re-attach not required" with EMM cause other than #2 "IMSI unknown in HSS" or detach type "re-attach required", the network shall ignore the SERVICE REQUEST message and shall progress with the detach procedure.

g) Lower layers indication of non-delivered NAS PDU due to handover

If the DETACH REQUEST message could not be delivered due to an intra MME handover and the target TA is included in the TAI list, then upon successful completion of the intra MME handover the MME shall retransmit the DETACH REQUEST message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the DETACH 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;
- combined tracking area updating to update the registration of the actual tracking area for a UE in CS/PS mode 1 or CS/PS mode 2 of operation;
- periodic tracking area updating to periodically notify the availability of the UE to the network;
- IMSI attach for non-EPS services when the UE is attached for EPS services. This procedure is used by a UE in CS/PS mode 1 or CS/PS mode 2 of operation;

- in various cases of inter-system change from Iu mode to S1 mode or from A/Gb mode to S1 mode (for details see subclauses 5.5.3.2.2 and subclause 5.5.3.3.2);
- S101 mode to S1 mode inter-system change;
- MME load balancing;
- to update certain UE specific parameters in the network (for details see subclauses 5.5.3.2.2 and subclause 5.5.3.3.2);
- recovery from certain error cases (for details see subclauses 5.5.3.2.2 and subclause 5.5.3.3.2);
- to indicate that the UE enters S1 mode after CS fallback or 1xCS fallback;
- to indicate to the network that the UE has selected a CSG cell whose CSG identity and associated PLMN identity are not included in the UE's Allowed CSG list or in the UE's Operator CSG list; and
- to indicate to the network that the UE's availability for voice calls in the IMS has changed to "available".

While a UE has a PDN connection for emergency bearer services, the UE shall not perform manual CSG selection.

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 UPDATE REJECT message with the EMM cause #11 "PLMN not allowed" is received by the UE, the chosen PLMN identity shall be stored in the "forbidden PLMN list". Whenever a TRACKING AREA UPDATE REJECT message with the EMM cause #14 "EPS services not allowed in this PLMN" is received by the UE, the chosen PLMN identity shall be stored in the "forbidden PLMNs for GPRS service". Whenever a TRACKING AREA UPDATE REJECT message is received by the UE with the EMM cause #12 "tracking area not allowed", #13 "roaming not allowed in this tracking area", or #15 "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:

- an attach 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 EMM cause #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 or EMM-REGISTERED.ATTEMPTING-TO-UPDATE-MM, 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 5.3.5.

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 enters EMM-REGISTERED.NORMAL-SERVICE 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 in EMM-REGISTERED.NO-CELL-AVAILABLE, and then returns to EMM-REGISTERED.NORMAL-SERVICE;

g) when the UE changes the UE network capability information or the MS network capability information or both;

h) when the UE changes the UE specific DRX parameter;

i) when the UE receives an indication of "RRC Connection failure" from the lower layers and has no signalling or user uplink data pending (i.e when the lower layer requests NAS signalling connection recovery);

j) when the UE enters S1 mode after 1xCS fallback;

k) when due to manual CSG selection the UE has selected a CSG cell whose CSG identity and associated PLMN identity are not included in the UE's Allowed CSG list or in the UE's Operator CSG list;

l) when the UE reselects an E-UTRAN cell while it was in GPRS READY state or PMM-CONNECTED mode;

m) when the UE supports SRVCC to GERAN or UTRAN and changes the mobile station classmark 2 or the supported codecs, or the UE supports SRVCC to GERAN and changes the mobile station classmark 3;

n) when the UE changes the radio capability for GERAN or cdma2000® or both;

o) when the UE's usage setting or the voice domain preference for E-UTRAN change in the UE;

p) when the UE activates mobility management for IMS voice termination as specified in 3GPP TS 24.008 [13], annex P.2, and the TIN indicates "RAT-related TMSI"; or

q) when the UE performs an intersystem change from A/Gb mode to S1 mode and the TIN indicates "RAT-related TMSI", but the UE is required to perform tracking area updating for IMS voice termination as specified in 3GPP TS 24.008 [13], annex P.4.

For all cases except case b, the UE shall set the EPS update type IE to "TA updating". For case b, the UE shall set the EPS update type IE to "periodic updating".

For case n, the UE shall include a UE radio capability information update needed IE in the TRACKING AREA UPDATE REQUEST message.

For case l, if the UE was in PMM-CONNECTED mode and the TIN indicates "RAT-related TMSI", the UE shall set the TIN to "P-TMSI" before initiating the tracking area updating procedure.

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 while in S1 mode, the UE shall use the current EPS NAS integrity key to integrity protect the TRACKING AREA UPDATE REQUEST message.

In order to indicate its UE specific DRX parameter while in E-UTRAN coverage, the UE shall send the TRACKING AREA UPDATE REQUEST message containing the UE specific DRX parameter in the DRX parameter IE to the network, with the exception of the case if the UE had indicated its DRX parameter (3GPP TS 24.008 [13]) to the

network while in GERAN or UTRAN coverage. In this case, when the UE enters E-UTRAN coverage and initiates a tracking area updating procedure, the UE shall not include the UE specific DRX parameter in the DRX parameter IE in the TRACKING AREA UPDATE REQUEST message.

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 5.5.3.2.2.1). If timer T3402 is currently running, the UE shall stop timer T3402. If timer T3411 is currently running, the UE shall stop timer T3411. If timer T3442 is currently running, the UE shall stop timer T3442.

If the UE supports neither A/Gb mode nor Iu mode, the UE shall include a valid GUTI in the Old GUTI IE in the TRACKING AREA UPDATE REQUEST message.

If the UE supports A/Gb mode or Iu mode, the UE shall handle the Old GUTI IE 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. If a P-TMSI signature is associated with the P-TMSI, the UE shall include it in the Old P-TMSI signature IE. Additionally, if the UE holds a valid GUTI, the UE shall indicate the GUTI in the Additional GUTI IE.

NOTE 2: The mapping of the P-TMSI and RAI to the GUTI is specified in 3GPP TS 23.003 [2].

- 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.

In the TRACKING AREA UPDATE REQUEST message the UE shall set the value of the EPS update type IE to "periodic updating", if the procedure initiated due to expiry of T3412; otherwise, the UE shall set the value to "TA updating". If a UE 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 a current EPS security context, the UE shall include the eKSI (either KSI_{ASME} or KSI_{SGSN}) in the NAS Key Set Identifier IE in the TRACKING AREA UPDATE REQUEST message. Otherwise, the UE shall set the NAS Key Set Identifier IE to the value "no key is available". If the UE has a current EPS security context, the UE shall integrity protect the TRACKING AREA UPDATE REQUEST message with the current EPS security context. Otherwise the UE shall not integrity protect the TRACKING AREA UPDATE REQUEST message.

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 and the TIN is set to "P-TMSI", the UE shall include the GPRS ciphering key sequence number applicable for A/Gb mode or Iu mode and a $nonce_{UE}$ in the TRACKING AREA UPDATE REQUEST message.

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 derive the EPS NAS keys from the mapped K'_{ASME} using the selected NAS algorithms, $nonce_{MME}$ and KSI_{SGSN} (to be associated with the mapped K'_{ASME}) provided by lower layers as indicated in 3GPP TS 33.401 [19]. The UE shall reset both the uplink and downlink NAS COUNT counters of the mapped EPS security context which shall be taken into use. If the UE has a non-current native EPS security context, the UE shall include the KSI_{ASME} in the Non-current native NAS key set identifier IE and its associated GUTI, as specified above, either in the Old GUTI IE or in the Additional GUTI IE of the TRACKING AREA UPDATE REQUEST message. The UE shall set the TSC flag in the Non-current native NAS key set identifier IE to "native security context".

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.

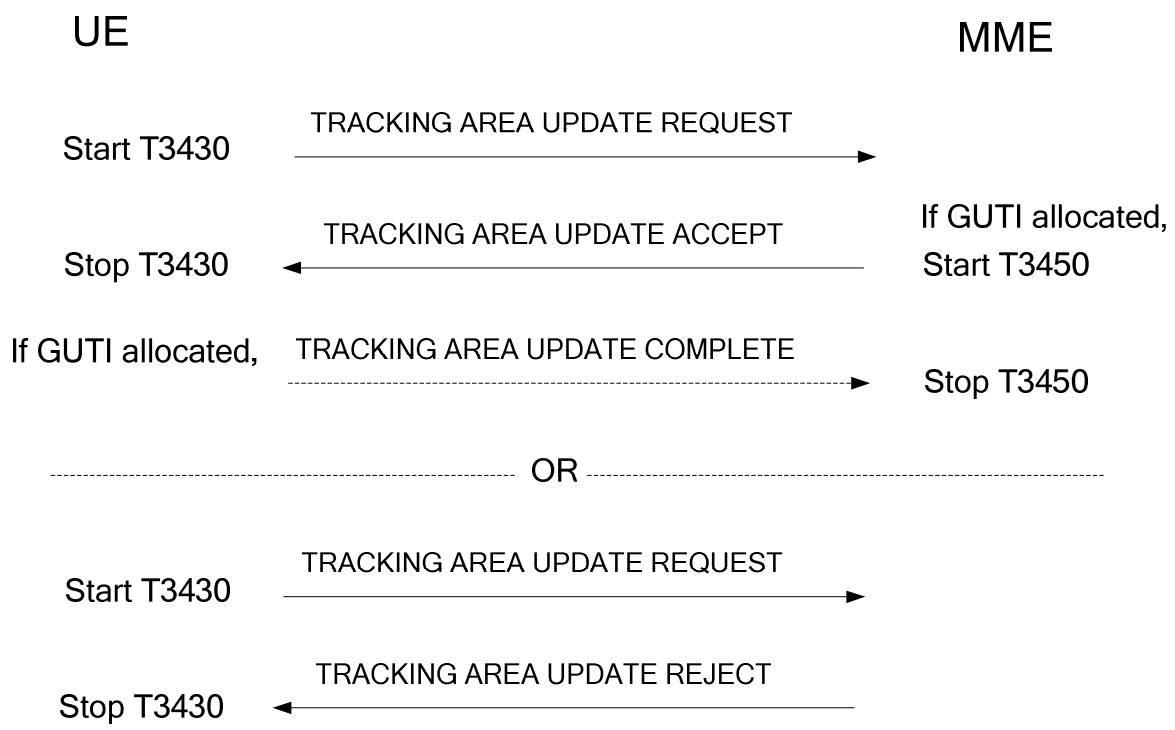


Figure 5.5.3.2.2.1: Tracking area updating procedure

5.5.3.2.3 EMM common procedure initiation

During the tracking area updating procedure, the MME may initiate EMM common procedures, e.g. the EMM authentication and security mode control procedures.

The MME may be configured to skip the authentication procedure even if no EPS security context is available and proceed directly to the execution of the security mode control procedure as specified in subclause 5.4.3, during a tracking area updating procedure for a UE that has only a PDN connection for emergency bearer services.

The MME shall not initiate an EMM authentication procedure before completion of the tracking area updating procedure, if the following conditions apply:

a) the UE initiated the tracking area updating procedure after handover or inter-system handover to S1 mode;

b) the target cell is a shared network cell; and

- the UE has provided its GUTI in the Old GUTI IE or the Additional GUTI IE in the TRACKING AREA UPDATE REQUEST message, and the PLMN identity included in the GUTI is different from the selected PLMN identity of the target cell; or

- the UE has mapped the P-TMSI and RAI into the Old GUTI IE and not included an Additional GUTI IE in the TRACKING AREA UPDATE REQUEST message, and the PLMN identity included in the RAI is different from the selected PLMN identity of the target cell.

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.

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 1: 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 the UE specific DRX parameter was included in the DRX Parameter IE in the TRACKING AREA UPDATE REQUEST message, the network shall replace any stored UE specific DRX parameter with the received parameter and use it for the downlink transfer of signalling and user data.

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. If a default EPS bearer context is marked as inactive in the EPS bearer context status IE included in the TRACKING AREA UPDATE REQUEST message, and this default bearer is not associated with the last PDN of the user in the MME, 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.

If the EPS bearer context status IE is included in the TRACKING AREA UPDATE REQUEST, 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.

If the EPS update type IE included in the TRACKING AREA UPDATE REQUEST message indicates "periodic updating", and the UE was previously successfully attached for EPS and non-EPS services, subject to operator policies the MME should allocate a TAI list that does not span more than one location area.

Also during the tracking area updating procedure without "active" flag, if the MME has deactivated EPS bearer context(s) locally for any reason, the MME shall inform the UE of the deactivated EPS bearer context(s) by including the EPS bearer context status IE in the TRACKING AREA UPDATE ACCEPT message.

If due to regional subscription restrictions or access restrictions the UE is not allowed to access the TA, but it has a PDN connection for emergency bearer services established, the MME may accept the TRACKING AREA UPDATE REQUEST message and deactivate all non-emergency EPS bearer contexts by initiating an EPS bearer context deactivation procedure when the TAU is initiated in EMM-CONNECTED mode. When the TAU is initiated in EMM-IDLE mode, the MME locally deactivates all non-emergency EPS bearer contexts and informs the UE via the EPS bearer context status IE in the TRACKING AREA UPDATE ACCEPT message. The MME shall not deactivate the emergency EPS bearer contexts. The network shall consider the UE to be attached for emergency bearer services only and shall indicate in the EPS update result IE in the TRACKING AREA UPDATE ACCEPT message that ISR is not activated.

For a shared network, the TAIs included in the TAI list can contain different PLMN identities. The MME indicates the selected core network operator PLMN identity to the UE in the GUTI (see 3GPP TS 23.251 [8B]).

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 the UE had initiated the tracking area updating procedure in EMM-IDLE mode to perform an inter-system change from A/Gb mode or Iu mode to S1 mode and the $nonce_{UE}$ was included in the TRACKING AREA UPDATE REQUEST message, the UE shall delete the $nonce_{UE}$ upon receipt of the TRACKING AREA UPDATE ACCEPT message.

If the UE had initiated the tracking area updating proceduredue to a change in UE network capability or change in DRX parameters or both, the UE shall locally deactivate ISR by setting TIN value to "GUTI".

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

are active in the UE, but are indicated by the MME as being inactive. If a default EPS bearer context is marked as inactive in the EPS bearer context status IE included in the TRACKING AREA UPDATE ACCEPT message, and this default bearer is not associated with the last PDN in the UE, the UE 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 MME. If only the PDN connection for emergency bearer services remains established, the UE shall consider itself attached for emergency bearer services only.

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, and if there is no PDN connection for emergency bearer services established, the UE shall remove from the list any PLMN code that is already in the list of forbidden PLMNs. If there is a PDN connection for emergency bearer services established, the UE shall remove from the list of equivalent PLMNs any PLMN code present in the list of forbidden PLMNs when the PDN connection for emergency bearer services is released. 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 UE is attached for emergency bearer services, the network shall indicate in the EPS update result IE in the TRACKING AREA UPDATE ACCEPT message that ISR is not activated. If the TRACKING AREA UPDATE ACCEPT message contains:

i) no indication that ISR is activated, the UE shall 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".

The network informs the UE about the support of specific features, such as IMS voice over PS session, location services (EPC-LCS, CS-LCS) or emergency bearer services, in the EPS network feature support information element. In a UE with IMS voice over PS capability, the IMS voice over PS session indicator and the emergency bearer services indicator shall be provided to the upper layers. The upper layers take the IMS voice over PS session indicator into account as specified in 3GPP TS 23.221 [8A], subclause 7.2a, when selecting the access domain for voice sessions or calls. When initiating an emergency call, the upper layers also take the emergency bearer services indicator into account for the access domain selection. In a UE with LCS capability, location services indicators (EPC-LCS, CS-LCS) shall be provided to the upper layers. When MO-LR procedure is triggered by the UE's application, those indicators are taken into account as specified in 3GPP TS 24.171 [13C].

The UE shall deactivate ISR by setting the TIN to "GUTI" if the UE is required to perform routing area updating for IMS voice termination as specified in 3GPP TS 24.008 [13], annex P.5.

If the UE has initiated the tracking area updating procedure due to manual CSG selection and receives a TRACKING AREA UPDATE ACCEPT message, and the UE sent the TRACKING AREA UPDATE REQUEST message in a CSG cell, the UE shall check if the CSG ID and associated PLMN identity of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message are contained in the Allowed CSG list. If not, the UE shall add that CSD ID and associated PLMN identity to the Allowed CSG list and the UE may add the HNB Name (if provided by lower layers) to the Allowed CSG list if the HNB Name is present in neither the Operator CSG list nor 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.

For inter-system change from A/Gb mode to S1 mode or Iu mode to S1 mode in EMM-IDLE mode, if the UE has included an eKSI in the NAS Key Set Identifier IE indicating a current EPS security context in the TRACKING AREA UPDATE REQUEST message by which the TRACKING AREA UPDATE REQUEST message is integrity protected, the MME shall take one of the following actions:

- if the MME retrieves the current EPS security context as indicated by the eKSI and GUTI sent by the UE, the MME shall integrity check the TRACKING AREA UPDATE REQUEST message using the current EPS security context and integrity protect the TRACKING AREA UPDATE ACCEPT message using the current EPS security context; or

- if the MME cannot retrieve the current EPS security context as indicated by the eKSI and GUTI sent by the UE, and if the UE has included a valid GPRS ciphering key sequence number, the MME shall create a new mapped EPS security context as specified in 3GPP TS 33.401 [19], and then perform a security mode control procedure to indicate the use of the new mapped EPS security context to the UE (see subclause 5.4.3.2).

NOTE 2: This does not preclude the option for the MME to perform an EPS authentication procedure and create a new native EPS security context.

For inter-system change from A/Gb mode to S1 mode or Iu mode to S1 mode in EMM-IDLE mode, if the UE has not included a valid eKSI in the NAS Key Set Identifier IE and has included a valid GPRS ciphering key sequence number in the TRACKING AREA UPDATE REQUEST message, the MME shall create a new mapped EPS security context as specified in 3GPP TS 33.401 [19], and then perform a security mode control procedure to indicate the use of the new mapped EPS security context to the UE (see subclause 5.4.3.2).

NOTE 3: This does not preclude the option for the MME to perform an EPS authentication procedure and create a new native EPS security context.

For inter-system change from A/Gb mode to S1 mode or Iu mode to S1 mode in EMM-CONNECTED mode, the MME shall integrity check TRACKING AREA UPDATE REQUEST message using the current K'_{ASME} as derived when triggering the handover to E-UTRAN (see subclause 4.4.2.1). The MME shall verify the received UE security capabilities in the TRACKING AREA UPDATE REQUEST message. The MME shall then take one of the following actions:

- if the TRACKING AREA UPDATE REQUEST does not contain a valid KSI_{ASME} in the Non-current native NAS key set identifier IE, the MME shall remove the non-current native EPS security context, if any, for any GUTI for this UE. The MME shall then integrity protect and cipher the TRACKING AREA UPDATE ACCEPT message using the security context based on K'_{ASME} and take the mapped EPS security context into use; or

- if the TRACKING AREA UPDATE REQUEST contains a valid KSI_{ASME} in the Non-current native NAS key set identifier IE, the MME may initiate a security mode control procedure to take the corresponding native EPS security context into use.

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 eKSI. 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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 eKSI. The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.

If the rejected request was not for initiating a PDN connection for emergency bearer services, the UE shall subsequently, automatically initiate the attach procedure.

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 the GMM cause with the same value.

#10 (Implicitly detached);

The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.NORMAL-SERVICE. The UE shall delete any mapped EPS security context or partial native EPS security context. If the rejected request was not for initiating a PDN connection for emergency bearer services, the UE shall then perform a new attach procedure.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM state as specified in 3GPP TS 24.008 [13] for the case when the normal routing area updating procedure is rejected with the GMM cause with the same 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, TAI list and eKSI. 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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].

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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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 the GMM cause with the same value.

#25 (Not authorized for this CSG);

EMM cause #25 is only applicable when received from a CSG cell. EMM cause #25 received from a non-CSG cell is considered as an abnormal case and the behaviour of the UE is specified in subclause 5.5.3.2.6.

If the TRACKING AREA UPDATE REJECT message with EMM cause #25 was received without integrity protection, then the UE shall discard the message.

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.

If the CSG ID and associated PLMN identity of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message are contained in the Allowed CSG list, the UE shall remove the entry corresponding to this CSG ID and associated PLMN identity from the Allowed CSG list.

If the CSG ID and associated PLMN identity of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message are contained in the Operator CSG list, the UE shall apply the procedures defined in 3GPP TS 23.122 [6] subclause 3.1A.

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 the GMM cause with the same 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.

5.5.3.2.5A Tracking area updating procedure for initiating a PDN connection for emergency bearer services not accepted by the network

If the tracking area updating request for initiating a PDN connection for emergency bearer services cannot be accepted by the network, the UE shall perform the procedures as described in subclause 5.5.3.2.5. Then if the UE is in the same selected PLMN where the last tracking area updating request was attempted, the UE shall:

a) inform the upper layers. This could result in the UE attempting a CS emergency call (if not already attempted in the CS domain) or other implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [13D] that can result in the emergency call being attempted to another IP-CAN; or

b) detach locally, if not detached already, attempt EPS attach for emergency bearer services.

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 EMM causes #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 EPS update status to EU2 NOT UPDATED.

f) Tracking area updating and detach procedure collision

If the UE receives a DETACH REQUEST message with detach type "re-attach not required" with EMM cause other than #2 "IMSI unknown in HSS" or detach type "re-attach required" before the tracking area updating procedure has been completed, the tracking area updating procedure shall be aborted and the detach procedure shall be progressed.

If the UE receives a DETACH REQUEST message with detach type "re-attach not required" with EMM cause #2 "IMSI unknown in HSS" or detach type "IMSI detach" before the tracking area updating procedure has been completed, the DETACH REQUEST message shall be ignored and tracking area updating 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 EPS 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 EPS 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.

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.

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 EPS update status is equal to EU1 UPDATED:

- the UE shall keep the EPS 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 EPS update status is different to EU1 UPDATED:

- the UE shall start timer T3411, shall set the EPS 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 and the GPRS update status is different from GU1 UPDATED.

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

- the UE shall start timer T3402, shall set the EPS 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.

f) Lower layers indication of non-delivered NAS PDU due to handover

   If the TRACKING AREA UPDATE ACCEPT message or TRACKING AREA UPDATE REJECT message could not be delivered due to handover then the MME shall retransmit the TRACKING AREA UPDATE ACCEPT message or TRACKING AREA UPDATE REJECT message if the failure of handover procedure is reported by the lower layer and the S1 signalling connection exists.

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

The UE operating in CS/PS mode 1 or CS/PS mode 2, in state EMM-REGISTERED, shall initiate the combined tracking area updating procedure:

a) when the UE that is attached for both EPS and non-EPS services 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 UE that is attached for EPS services wants to perform an attach for non-EPS services. In this case the EPS update type IE shall be set to "combined TA/LA updating with IMSI attach";

c) when the UE performs an intersystem change from A/Gb mode to S1 mode and the EPS services were previously suspended in A/Gb mode;

d) when the UE performs an intersystem change from A/Gb or Iu mode to S1 mode, and the UE previously either performed a location area update procedure or a combined routing area update procedure in A/Gb or Iu mode, or moved to A/Gb or Iu mode from S1 mode through an SRVCC handover, in order to re-establish the SGs association. In this case the EPS update type IE shall be set to "combined TA/LA updating with IMSI attach";

e) when the UE enters EMM-REGISTERED.NORMAL-SERVICE and the UE's TIN indicates "P-TMSI";

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

g) when the UE deactivated EPS bearer context(s) locally while in EMM-REGISTERED.NO-CELL-AVAILABLE, and then returns to EMM-REGISTERED.NORMAL-SERVICE;

h) when the UE changes the UE network capability information or the MS network capability information or both;

i) when the UE changes the UE specific DRX parameter;

j) when the UE receives an indication of "RRC Connection failure" from the lower layers and has no signalling or user uplink data pending (i.e when the lower layer requests NAS signalling connection recovery);

k) when due to manual CSG selection the UE has selected a CSG cell whose CSG identity and associated PLMN identity are not included in the UE's Allowed CSG list or in the UE's Operator CSG list;

l) when the UE reselects an E-UTRAN cell while it was in GPRS READY state or PMM-CONNECTED mode;

m) when the UE supports SRVCC to GERAN or UTRAN and changes the mobile station classmark 2 or the supported codecs, or the UE supports SRVCC to GERAN and changes the mobile station classmark 3;

n) when the UE changes the radio capability for GERAN or cdma2000® or both;

o) when the UE's usage setting or the voice domain preference for E-UTRAN change in the UE;

p) when the UE activates mobility management for IMS voice termination as specified in 3GPP TS 24.008 [13], annex P.2, and the TIN indicates "RAT-related TMSI"; or

q) when the UE performs an intersystem change from A/Gb mode to S1 mode and the TIN indicates "RAT-related TMSI", but the UE is required to perform tracking area updating for IMS voice termination as specified in 3GPP TS 24.008 [13], annex P.4.

For case n, the UE shall include a UE radio capability information update needed IE in the TRACKING AREA UPDATE REQUEST message.

For case l, if the UE was in PMM-CONNECTED mode and the TIN indicates "RAT-related TMSI", the UE shall set the TIN to "P-TMSI" before initiating the combined tracking area updating procedure.

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.

If the UE initiates the combined tracking area updating procedure for EPS services and "SMS only", the UE shall indicate "SMS only" in the Additional update Type IE.

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

During the combined tracking area updating procedure, the MME may initiate EMM common procedures, e.g. the EMM authentication and security mode control procedures. For restrictions applicable after handover or inter-system handover to S1 mode see subclause 5.5.3.2.3.

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, the following different cases can be distinguished:

1) The EPS update result IE value indicates "combined TA/LA updated": Tracking and location area updating is successful for EPS and non-EPS services, or for EPS services and "SMS only";

2) The EPS update result IE value indicates "TA updated": Tracking area updating is successful, but location area updating for non-EPS services or "SMS only" 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. If the MME does not indicate "SMS only" in the TRACKING AREA UPDATE ACCEPT message, subject to operator policies the MME should allocate a TAI list that does not span more than one location area.

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.

If the LAI contained in the TRACKING AREA UPDATE ACCEPT message is a member of the list of "forbidden location areas for regional provision of service" or the list of "forbidden location areas for roaming" then such entry shall be deleted.

If the PLMN ID for the CS domain which is provided as part of the LAI contained in the TRACKING AREA UPDATE ACCEPT message differs from the PLMN ID provided as part of the GUTI, the MME shall include the "Equivalent PLMNs" IE in the TRACKING AREA UPDATE ACCEPT message and include the PLMN ID for the CS domain in this IE.

If the UE requested "SMS only" in the Additional update type IE, the network shall indicate "SMS only" in the Additional update result IE.

If the TRACKING AREA UPDATE ACCEPT message includes the Additional update result IE with value "SMS only" or "CS Fallback not preferred", a UE operating in CS/PS mode 1 with "IMS voice not available" shall attempt to select GERAN or UTRAN radio access technology rather than E-UTRAN for the selected PLMN or equivalent PLMN. The UE shall disable the E-UTRA capability (see subclause 4.5). If the UE is in the EMM-CONNECTED mode, the UE shall locally release the established NAS signalling connection and enter the EMM-IDLE mode before selecting GERAN or UTRAN radio access technology.

If the TRACKING AREA UPDATE ACCEPT message includes the Additional update result IE with value "SMS only", a UE operating in CS/PS mode 2 shall not attempt to use CS fallback for mobile originating services.

If the TRACKING AREA UPDATE ACCEPT message includes the Additional update result IE with value "CS Fallback not preferred", this indicates to a UE operating in CS/PS mode 2 that it is attached for EPS and non-EPS services and that it can use CS fallback.

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

Apart from the actions on the tracking area updating attempt counter, 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 and shall reset the tracking area updating attempt counter. 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 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 again.

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

- a UE operating in CS/PS mode 2 of operation 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 with "IMS voice not available" shall attempt to select GERAN or UTRAN radio access technology and proceed with appropriate MM or GMM specific procedures. The UE shall disable the E-UTRA capability (see subclause 4.5). If the UE is in the EMM-CONNECTED mode, the UE shall locally release the established NAS signalling connection and enter the EMM-IDLE mode before selecting GERAN or UTRAN radio access technology.

NOTE 1: It is up to the UE implementation when to enable E-UTRAN radio access technology selection.

#18 (CS domain not available)

The UE shall stop timer T3430 if still running, shall reset the tracking area updating attempt counter, 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 with "IMS voice not available" shall attempt to select GERAN or UTRAN radio access technology rather than E-UTRAN for the selected PLMN or equivalent PLMN. The UE shall disable the E-UTRA capability (see subclause 4.5). If the UE is in the EMM-CONNECTED mode, the UE shall locally release the established NAS signalling connection and enter the EMM-IDLE mode before selecting GERAN or UTRAN radio access technology.

A UE in CS/PS mode 2 of operation may provide a notification to the user or the upper layers that the CS domain is not available.

The UE shall not attempt combined attach or combined tracking area updating procedure with current PLMN until switching off the UE or the UICC containing the USIM is removed.

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 eKSI.

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 the GMM cause with the same 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 eKSI. 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.

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 set the update status to U2 NOT UPDATED, 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.

NOTE: Some interaction is required with the access stratum to disable E-UTRAN cell reselection.

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 the GMM cause with the same 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 eKSI. The UE shall delete the list of equivalent PLMNs and enter the state EMM-DEREGISTERED.

If the rejected request was not for initiating a PDN connection for emergency bearer services, the UE shall subsequently, automatically initiate the attach procedure.

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 the GMM cause with the same 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 set the update status to U2 NOT UPDATED.

#10 (Implicitly detached);

The UE shall delete the list of equivalent PLMNs and shall enter the state EMM-DEREGISTERED.NORMAL-SERVICE. the UE shall delete any mapped EPS security context or partial native EPS security context. If the rejected request was not for initiating a PDN connection for emergency bearer services, the UE shall then perform a new attach procedure.

If A/Gb mode or Iu mode is supported by the UE, the UE shall in addition handle the GMM state as specified in 3GPP TS 24.008 [13] for the case when the combined routing area updating procedure is rejected with the GMM cause with the same 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 set the update status to U2 NOT UPDATED.

#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 eKSI, 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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 the GMM cause with the same 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 eKSI. 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 operating in CS/PS mode 1 or CS/PS mode 2 of operation is still IMSI attached for non-EPS services and shall set the update status to U2 NOT UPDATED.

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 the GMM cause with the same 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 the GMM cause with the same value.

#25 (Not authorized for this CSG);

EMM cause #25 is only applicable when received from a CSG cell. EMM cause #25 received from a non-CSG cell is considered as an abnormal case and the behaviour of the UE is specified in subclause 5.5.3.3.6.

If the TRACKING AREA UPDATE REJECT message with EMM cause #25 was received without integrity protection, then the UE shall discard the message.

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.

If the CSG ID and associated PLMN identity of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message are contained in the Allowed CSG list, the UE shall remove the entry corresponding to this CSG ID and associated PLMN identity from the Allowed CSG list.

If the CSG ID and associated PLMN identity of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message are contained in the Operator CSG list, the UE shall apply the procedures defined in 3GPP TS 23.122 [6] subclause 3.1A.

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 the GMM cause with the same 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 the attach procedure.

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 UE requested the combined tracking area update for EPS services and "SMS only" and the TRACKING AREA UPDATE ACCEPT message indicates a combined tracking area updating procedure successful for EPS and non-EPS services, the UE shall behave as if the combined tracking area updating procedure was successful for EPS services and "SMS only".

NOTE: In this case the UE can ignore the Paging with CN domain indicator set to "CS", as specified in subclause 5.6.2.3.2.

- if the combined tracking area update was successful for EPS services only and the TRACKING AREA UPDATE ACCEPT message contained an EMM 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 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.

NOTE: It is up to the UE implementation when to enable E-UTRAN radio access technology selection.

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;

- the network has downlink cdma2000® signalling pending; or

- the UE has uplink cdma2000® signalling pending.

The service request procedure is initiated by the UE, however, for the downlink transfer of signalling, cdma2000® 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 in EMM-IDLE mode receives a paging request with CN domain indicator set to "PS" from the network;

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 is configured to use CS fallback and has a mobile originating CS fallback request from the upper layer;

e) the UE in EMM-IDLE mode is configured to use CS fallback and receives a paging request with CN domain indicator set to "CS", or the UE in EMM-CONNECTED mode is configured to use CS fallback and receives a CS SERVICE NOTIFICATION message;

f) the UE in EMM-IDLE or EMM-CONNECTED mode is configured to use 1xCS fallback and has a mobile originating 1xCS fallback request from the upper layer;

g) the UE in EMM-CONNECTED mode is configured to use 1xCS fallback and accepts cdma2000® signalling messages containing a 1xCS paging request received over E-UTRAN;

h) the UE, in EMM-IDLE mode, has uplink cdma2000® signalling pending to be transmitted over E-UTRAN;

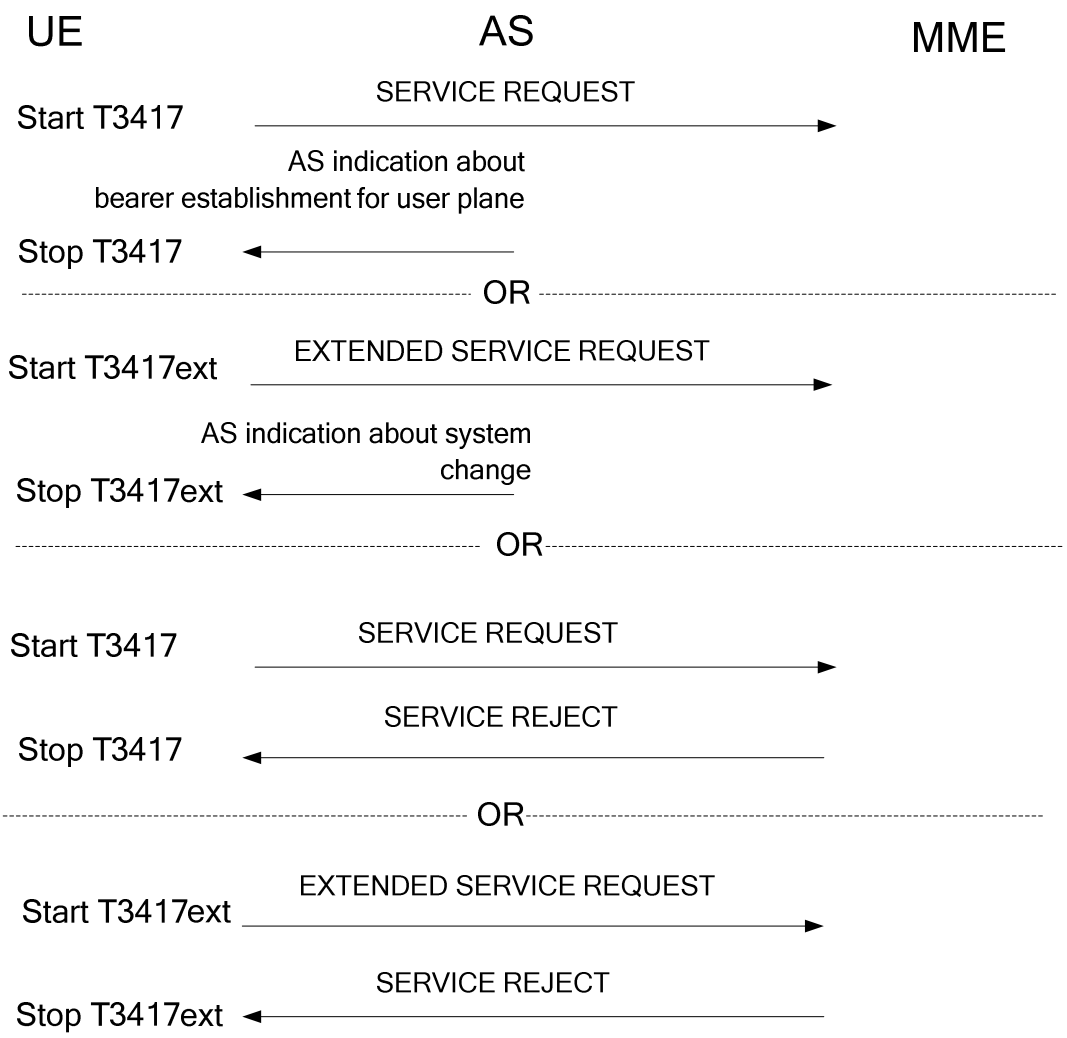
i) the UE, in EMM-IDLE or EMM-CONNECTED mode, is configured to use 1xCS fallback, accepts cdma2000® signalling messages containing a 1xCS paging request received over cdma2000® 1xRTT, and the network supports dual Rx CSFB or provide CS fallback registration parameters (see 3GPP TS 36.331 [22]); or

j) the UE, in EMM-IDLE or EMM-CONNECTED mode, has uplink cdma2000® signalling pending to be transmitted over cdma2000® 1xRTT, and the network supports dual Rx CSFB or provide CS fallback registration parameters (see 3GPP TS 36.331 [22]).

If one of the above criteria to invoke the service request procedure is fulfilled, then the service request procedure may only be initiated by the UE when the following conditions are fulfilled:

- its EPS update status is EU1 UPDATED, and the TAI of the current serving cell is included in the TAI list; and

- no EMM specific procedure is ongoing.



NOTE 1: AS indications (indications from lower layers) are results of procedures triggered by MME in Service Request procedure. Triggered procedures could be e.g. RRC Connection Reconfiguration procedure (see 3GPP TS 36.331 [22]) and inter system PS handover to GERAN or UTRAN procedure as a result of CSFB procedure (see 3GPP TS 23.272 [9]).

NOTE 2: For 1xCS fallback, the UE sends the EXTENDED SERVICE REQUEST message and starts timer T3417. The procedure is considered completed upon receiving indication of system change from AS.

Figure 5.6.1.1.1: Service Request procedure

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.

For case d in subclause 5.6.1.1, the UE shall send an EXTENDED SERVICE REQUEST message, start T3417ext and enter the state EMM-SERVICE-REQUEST-INITIATED.

For case e in subclause 5.6.1.1:

- if the UE is in EMM-IDLE mode, the UE shall send an EXTENDED SERVICE REQUEST message, start T3417ext and enter the state EMM-SERVICE-REQUEST-INITIATED;

- if the UE is in EMM-CONNECTED mode and if the UE accepts the paging, the UE shall send an EXTENDED SERVICE REQUEST message with the CSFB response IE indicating "CS fallback accepted by the UE", start T3417ext and enter the state EMM-SERVICE-REQUEST-INITIATED; or

- if the UE is in EMM-CONNECTED mode and if the UE rejects the paging, the UE shall send an EXTENDED SERVICE REQUEST message with the CSFB response IE indicating "CS fallback rejected by the UE" and enter the state EMM-REGISTERED.NORMAL-SERVICE. The network shall not initiate CS fallback procedures.

For cases f, g, i and j in subclause 5.6.1.1, the UE shall send an EXTENDED SERVICE REQUEST message, start T3417 and enter the state EMM-SERVICE-REQUEST-INITIATED.

5.6.1.3 EMM common procedure initiation

Upon receipt of the SERVICE REQUEST or EXTENDED SERVICE REQUEST message, the MME may initiate the EMM common procedures e.g. the authentication procedure and security mode control procedure.

5.6.1.4 Service request procedure accepted by the network

For cases a, b, c and h 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. The UE shall stop the timer T3417 and enter the state EMM-REGISTERED.

If the service type information element in the EXTENDED SERVICE REQUEST message indicates "mobile terminating CS fallback or 1xCS fallback" and the CSFB response IE indicates "CS fallback accepted by the UE", or if the service type information element in the EXTENDED SERVICE REQUEST message indicates "mobile originating CS fallback or 1xCS fallback" or "mobile originating CS fallback emergency call or 1xCS fallback emergency call", the network initiates CS fallback procedures. If the EPS bearer context status IE is included in the EXTENDED SERVICE REQUEST message, the network shall deactivate all those EPS bearer contexts locally (without peer-to-peer signalling between the network and the UE) which are active on the network side but are indicated by the UE as being inactive.

If the SERVICE REQUEST message was sent in a CSG cell and the CSG subscription has expired or was removed for a UE, but the UE has a PDN connection for emergency bearer services established, the network shall accept the SERVICE REQUEST message and deactivate all non-emergency EPS bearers locally. The emergency EPS bearers shall not be deactivated.

For cases d in subclause 5.6.1.1, and for case e in subclause 5.6.1.1 when the CSFB response was set to "CS fallback accepted by the UE", 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. The UE shall stop the timer T3417ext and enter the state EMM-REGISTERED.NO-CELL-AVAILABLE.

If the service request procedure was initiated in EMM-IDLE mode and an EXTENDED SERVICE REQUEST message was sent in a CSG cell and the CSG subscription has expired or was removed for the UE, the network need not perform CSG access control if the service type information element indicates "mobile originating CS fallback emergency call or 1xCS fallback emergency call".

For cases f, and g in subclause 5.6.1.1, the UE shall treat the indication from the lower layers that the signalling connection is released with the redirection indication to cdma2000® 1x access network or the indication from the lower layers that a change to cdma2000® 1x access network for 1xCS fallback has started (see 3GPP TS 36.331 [22]) as successful completion of the procedure. The UE shall stop the timer T3417 and enter the state EMM-REGISTERED.NO-CELL-AVAILABLE. If the UE receives a cdma2000® signalling message indicating 1xCS fallback rejection by cdma2000® 1x access network, the UE shall abort the service request procedure, stop timer T3417 and enter the state EMM-REGISTERED.NORMAL-SERVICE.

For cases i and j in subclause 5.6.1.1, if the UE receives the indication from the lower layers that the signalling connection is released, the UE shall consider the service request procedure successfully completed, stop timer T3417 and enter the state EMM-REGISTERED.NO-CELL-AVAILABLE.

If the SERVICE REQUEST message was used, the UE shall locally deactivate the EPS bearer contexts that do not have a user plane radio bearer established upon successful completion of the service request procedure.

If the EXTENDED SERVICE REQUEST message was used and radio bearer establishment takes place during the procedure, the UE shall locally deactivate the EPS bearer contexts that do not have a user plane radio bearer established upon receiving a lower layer indication of radio bearer establishment. The UE does not perform local deactivation of EPS bearer contexts upon receiving an indication of inter-system change from lower layers.

If the EXTENDED SERVICE REQUEST message was used and radio bearer establishment does not take place during the procedure, the UE does not perform local deactivation of the EPS bearer context. The UE does not perform local deactivation of EPS bearer contexts upon receiving an indication of inter-system change from lower layers.

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.

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 eKSI. 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 the GMM cause with the same 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 1: 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 eKSI. 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.

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 set the update status to U2 NOT UPDATED, 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.

NOTE 2: Some interaction is required with the access stratum to disable E-UTRAN cell reselection.

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 the GMM cause with the same 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 eKSI. The UE shall enter the state EMM-DEREGISTERED.

If the rejected request was not for initiating a PDN connection for emergency bearer services, the UE shall subsequently, automatically initiate the attach procedure.

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 the GMM cause with the same 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 set the update status to U2 NOT UPDATED.

#10 (Implicitly detached);

The UE shall enter the state EMM-DEREGISTERED.NORMAL-SERVICE. The UE shall delete any mapped EPS security context or partial native EPS security context. If the rejected request was not for initiating a PDN connection for emergency bearer services, the UE shall then perform a new attach procedure.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM state as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with the GMM cause with the same 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 set the update status to U2 NOT UPDATED.

#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 eKSI. 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 the GMM cause with the same 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 eKSI. 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 the GMM cause with the same 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). 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" and 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 and GPRS update status as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with the GMM cause with the same 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" and 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 and GPRS update status as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with the GMM cause with the same value.

#18 (CS domain not available);

If the request was related to CS fallback, the UE shall send an indication to the MM sublayer and shall not attempt CS fallback until combined tracking area updating procedure has been successfully completed. The UE shall enter the state EMM-REGISTERED.NORMAL-SERVICE.

If the UE is in CS/PS mode 1 or CS/PS mode 2 mode of operation, the UE may provide a notification to the user or the upper layers that the CS domain is not available.

If the request was related to 1xCS fallback, the UE shall cancel upper layer actions related to CS fallback and enter the state EMM-REGISTERED.NORMAL-SERVICE.

#25 (Not authorized for this CSG);

EMM cause #25 is only applicable when received from a CSG cell. EMM cause #25 received from a non-CSG cell is considered as an abnormal case and the behaviour of the UE is specified in subclause 5.6.1.6.

If the SERVICE REJECT message with EMM cause #25 was received without integrity protection, then the UE shall discard the message.

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.

If the CSG ID and associated PLMN identity of the cell where the UE has initiated the service request procedure are contained in the Allowed CSG list, the UE shall remove the entry corresponding to this CSG ID and associated PLMN identity from the Allowed CSG list.

If the CSG ID and associated PLMN identity of the cell where the UE has initiated the service request procedure are contained in the Operator CSG list, the UE shall apply the procedures defined in 3GPP TS 23.122 [6] subclause 3.1A.

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 the GMM cause with the same value.

#39 (CS domain temporarily not available);

The UE shall start timer T3442 and 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, except for mobile originating CS fallback for emergency calls, 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.

5.6.1.5A Service request procedure for initiating a PDN connection for emergency bearer services not accepted by the network

If the service request for initiating a PDN connection for emergency bearer services cannot be accepted by the network, the UE shall perform the procedures as described in subclause 5.6.1.5. Then if the UE is in the same selected PLMN where the last service request was attempted, the UE shall:

a) inform the upper layers. This could result in the UE attempting a CS emergency call (if not already attempted in the CS domain) or other implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [13D] that can result in the emergency call being attempted to another IP-CAN; or

b) detach locally, if not detached already, attempt EPS attach for emergency bearer services.

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.

   If the service request was initiated for CS fallback, the UE shall select GERAN or UTRAN radio access technology. The UE then proceeds with appropriate MM and CC specific procedures. The EMM sublayer shall not indicate the abort of the service request procedure to the MM sublayer.

   If the service request was initiated for 1xCS fallback, the UE shall select cdma2000® 1x radio access technology. The UE then proceeds with appropriate cdma2000® 1x CS call processing.

b) Lower layer failure before the service request procedure is completed (see subclause 5.6.1.4) or before SERVICE REJECT message is received

   If the service request was initiated for CS fallback, the UE shall select GERAN or UTRAN radio access technology. The UE then proceeds with appropriate MM and CC specific procedures. The EMM sublayer shall not indicate the abort of the service request procedure to the MM sublayer.

   If the service request was initiated for 1xCS fallback, the UE shall either:

   - select cdma2000® 1x radio access technology and proceed with appropriate cdma2000® 1x CS call processing; or

   - perform cell selection according to 3GPP TS 36.304 [21].

   Otherwise, the UE shall enter state EMM-REGISTERED. The UE shall abort the service request procedure, stop timer T3417 or T3417ext and locally release any resources allocated for the service request procedure.

c) T3417 expired

   The UE shall enter the state EMM-REGISTERED.

   If the UE triggered service request procedure from EMM-IDLE mode, then the EMM sublayer shall abort the procedure and release locally any resources allocated for the service request procedure.

If the UE triggered service request procedure from EMM-CONNECTED mode, the EMM sublayer shall abort the procedure and consider the 1xCS fallback procedure has failed. The UE shall stay in EMM-CONNECTED mode.

d) T3417ext expired

The UE shall enter the state EMM-REGISTERED.If the UE triggered service request procedure from EMM-IDLE mode, then the EMM sublayer shall abort the procedure, indicate to the MM sublayer that the CS fallback procedure has failed and release locally any resources allocated for the service request procedure.

If the UE triggered service request procedure from EMM-CONNECTED mode, the EMM sublayer shall abort the procedure and indicate to the MM sublayer that the CS fallback procedure has failed. The UE shall stay in EMM-CONNECTED mode.

e) SERVICE REJECT received, other EMM cause values than those treated in subclause 5.6.1.5

The procedure shall be aborted and move to EMM-REGISTERED.

If the service request was initiated for CS fallback, the UE shall select GERAN or UTRAN radio access technology. It then proceeds with appropriate MM and CC specific procedures. The EMM sublayer shall not indicate the abort of the service request procedure to the MM sublayer.

If the service request was initiated for 1xCS fallback, the UE shall select cdma2000® 1x radio access technology. The UE then proceeds with appropriate cdma2000® 1x CS call processing.

f) Tracking area updating procedure is triggered

The UE shall abort the service request procedure, stop timer T3417 or T3417ext if running and perform the tracking area updating procedure. The "active" flag shall be set in the TRACKING AREA UPDATE REQUEST message. If the service request was initiated for CS fallback or 1xCS fallback, the UE shall send the EXTENDED SERVICE REQUEST message to the MME by using the existing NAS signalling connection after the completion of the tracking area updating procedure.

g) Switch off

If the UE is in state EMM-SERVICE-REQUEST-INITIATED at switch off, the detach procedure shall be performed.

h) Procedure collision

If the UE receives a DETACH REQUEST message with detach type "re-attach not required" with EMM cause other than #2 "IMSI unknown in HSS" or detach type "re-attach required" from the network in state EMM-SERVICE-REQUEST-INITIATED, the detach procedure shall be progressed and the service request procedure shall be aborted.

Additionally, if the service request was initated for CS fallback or 1xCS fallback, the EMM sublayer shall indicate to the MM sublayer or the cdma2000® upper layers that the CS fallback or 1xCS fallback procedure has failed.

If the Detach type IE in the DETACH REQUEST message indicated "re-attach required", the attach procedure shall be performed.

If the UE receives a DETACH REQUEST message with detach type "re-attach not required" with EMM cause #2 "IMSI unknown in HSS" or detach type "IMSI detach" from the network in state EMM-SERVICE-REQUEST-INITIATED, the UE shall progress both procedures.

i) Transmission failure of SERVICE REQUEST or EXTENDED 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 service request was initiated for CS fallback or 1xCS fallback, the UE shall send the EXTENDED SERVICE REQUEST message to the MME by using the existing NAS signalling connection after the completion of the tracking area updating procedure.

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

j) Transmission failure of SERVICE REQUEST or EXTENDED SERVICE REQUEST message indication without TAI change from lower layers

The UE shall restart the service request procedure.

k) Default or dedicated bearer set up failure

If the lower layers indicate a failure to set up a radio bearer, the UE shall locally deactivate the EPS bearer as described in subclause 6.4.4.6.

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 or the EXTENDED 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 the current EMM 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 procedure. The network may e.g. after a successful EMM authentication procedure execution, abort the service request procedure, delete the EMM context, EPS bearer contexts, if any, and progress the new ATTACH REQUEST.

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 procedure. The network may e.g. after a successful EMM authentication procedure execution, abort the service request procedure and progress the tracking area updating procedure.

f) Default or dedicated bearer set up failure

If the lower layers indicate a failure to set up a radio or S1 bearer, the MME shall locally deactivate the EPS bearer as described in subclause 6.4.4.6.

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 prompt the UE to reattach if necessary as a result of a network failure. If the UE is not attached when it receives a paging for EPS services, the UE shall ignore the paging.

Additionally, the network can use the paging procedure to initiate the mobile terminating CS fallback procedure or SMS.

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 (see example in figure 5.6.2.2.1.1).

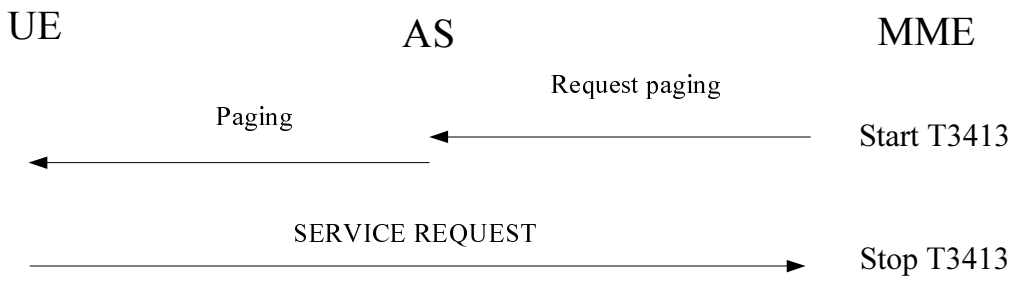


Figure 5.6.2.2.1.1: Paging procedure using S-TMSI

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. The EMM entity may provide the lower layer with a list of CSG IDs, including the CSG IDs of both the expired and the not expired subscriptions. If there is a PDN connection for emergency bearer services established, the EMM entity in the network shall not provide the list of CSG IDs to the lower layer. 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 T3413 for the paging procedure when a response is received from the UE. Upon expiry of T3413, the network may reinitiate paging.

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 (see example in figure 5.6.2.2.2.1).

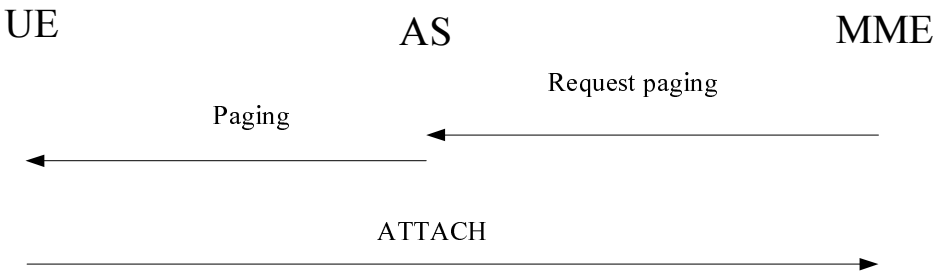


Figure 5.6.2.2.2.1: Paging procedure using IMSI

In S1 mode, to initiate the procedure the EMM entity in the network requests the lower layer to start paging. If the TAI list is not available due to a network failure, the network may perform the paging within all tracking areas served by the MME (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 subclause.

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 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 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.

5.6.2.3 Paging for CS fallback to A/Gb or Iu mode

5.6.2.3.1 General

The network may initiate the paging procedure for CS fallback when the UE is IMSI attached for non-EPS services (see example in figure 5.6.2.3.1).

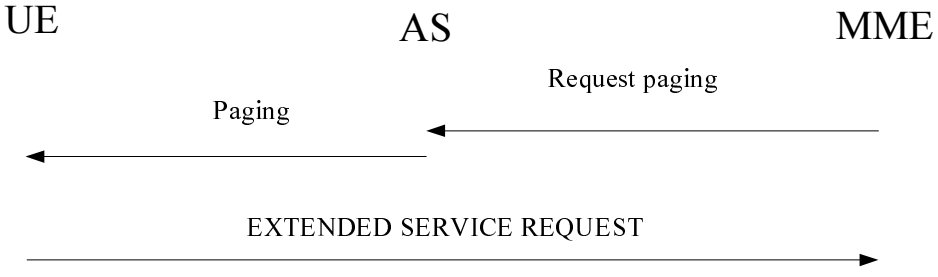


Figure 5.6.2.3.1: Paging procedure for CS fallback to A/Gb or Iu mode

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]). The EMM entity may provide the lower layer with a list of CSG IDs, including the CSG IDs of both the expired and the not expired subscriptions. If there is a PDN connection for emergency bearer services established, the EMM entity in the network shall not provide the list of CSG IDs to the lower layer.The paging message includes a CN domain indicator set to "CS" in order to indicate that this is paging for CS fallback.

NOTE: The timer T3413 is not started in the network when the paging procedure is initiated for CS fallback.

To notify the UE about an incoming mobile terminating CS service excluding SMS over SGs when a NAS signalling connection exists, the EMM entity in the network shall send a CS SERVICE NOTIFICATION message. This message may also include CS service related parameters (e.g. Calling Line Identification, SS or LCS related parameters).

Upon reception of a paging indication, a UE that is IMSI attached for non-EPS services shall respond with an EXTENDED SERVICE REQUEST. If the paging is received in EMM-IDLE mode, the UE shall respond immediately. If the paging is received as NAS CS NOTIFICATION message in EMM-CONNECTED mode, the UE may request upper layers input i.e. to accept or reject CS fallback before responding with an EXTENDED SERVICE REQUEST. The response is indicated in the CSFB response information element in the EXTENDED SERVICE REQUEST message in both EMM-IDLE and EMM-CONNECTED modes.

5.6.2.3.2 Abnormal cases in the UE

A UE that requested "SMS only" in the combined attach procedure or combined tracking area updating procedure may ignore paging indications with the CN domain indicator set to "CS".

5.6.2.4 Paging for SMS

The network shall initiate the paging procedure when it receives an incoming mobile terminating SMS to the UE that is IMSI attached for non-EPS services or for "SMS only", and no NAS signalling connection exists.

To initiate the procedure for SMS when no NAS signalling connection exists, the EMM entity in the network requests the lower layer to start paging (see 3GPP TS 36.413 [23]). The paging message shall include a CN domain indicator set to "PS". The paging procedure is performed according to subclause 5.6.2.2.1. The MME shall not start timer T3413 for this procedure.

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 attached for EPS services and IMSI attached for non-EPS services and is in EMM-CONNECTED mode.

5.6.3.2 UE initiated transport of NAS messages

Upon request from the SMS entity to send an SMS message, the EMM entity in the UE initiates the procedure by sending an UPLINK NAS TRANSPORT message including the SMS message in the NAS message container IE.

5.6.3.3 Network initiated transport of NAS messages

The network initiates the procedure by sending a DOWNLINK NAS TRANSPORT message. When receiving the DOWNLINK NAS TRANSPORT message, the EMM entity in the UE shall forward the contents of the NAS message container IE to the SMS entity.

5.6.3.4 Abnormal cases in the UE

No abnormal cases have been identified.

5.6.3.5 Abnormal cases on the network side

The following abnormal case can be identified:

a) Lower layer indication of non-delivered NAS PDU

If the DOWNLINK NAS TRANSPORT message is not delivered for any reason, the MME shall discard the message.

5.6.4 Generic transport of NAS messages procedure

5.6.4.1 General

The purpose of the generic transport of NAS messages procedure is to carry protocol messages from various applications (e.g., an LCS application to send an LPP message or a location service message) 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 attached for EPS services and is in EMM-CONNECTED mode.

5.6.4.2 UE initiated generic transport of NAS messages

Upon request from an application to send a message encapsulated in the generic transport of NAS message, the EMM entity in the UE initiates the procedure by sending an UPLINK GENERIC NAS TRANSPORT message including the corresponding message in the generic message container IE. The application may also request additional information to be included in the UPLINK GENERIC NAS TRANSPORT message in the Additional information IE. The content, coding and intrepretation of this information element are dependent on the particular application.

The UE shall indicate the application protocol using the generic transport in the corresponding generic message container type. When receiving the UPLINK GENERIC NAS TRANSPORT message, the EMM entity in the MME shall provide the contents of the generic message container IE and the generic message container type IE to the corresponding application. If included, the EMM entity in the MME shall also provide the contents of the Additional information IE.

5.6.4.3 Network initiated transport of NAS messages

Upon request from an application to send a message encapsulated in the generic transport of NAS message, the EMM entity in the MME initiates the procedure by sending a DOWNLINK GENERIC NAS TRANSPORT message including the corresponding message in the generic message container IE. The application may also request additional information to be included in the DOWNLINK GENERIC NAS TRANSPORT message in the Additional information IE. The content, coding and intrepretation of this information element are dependent on the particular application.

The MME shall indicate the application protocol using the generic transport in the corresponding generic message container type. When receiving the DOWNLINK GENERIC NAS TRANSPORT message, the EMM entity in the UE shall provide the contents of the generic message container IE and the generic message container type IE to the corresponding application. If included, the EMM entity in the UE shall also provide the contents of the Additional information IE.

5.6.4.4 Abnormal cases in the UE

No abnormal cases have been identified.

5.6.4.5 Abnormal cases on the network side

The following abnormal case can be identified:

a) Lower layer indication of non-delivered NAS PDU

If the DOWNLINK GENERIC NAS TRANSPORT message is not delivered for any reason, the MME shall discard the 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.

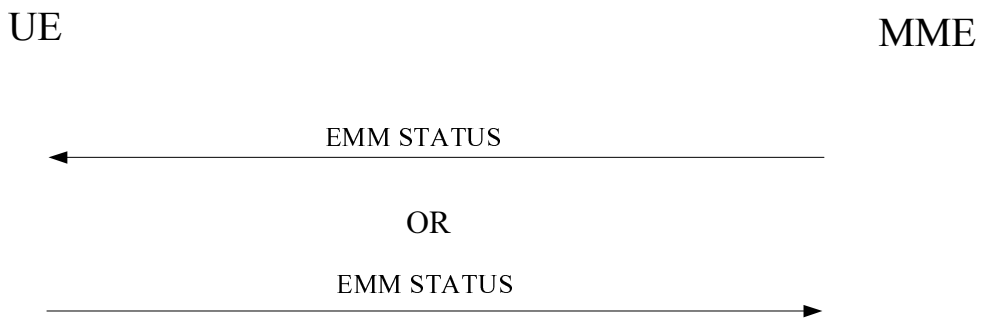


Figure 5.7.1: EMM status procedure

6 Elementary procedures for EPS session management

6.1 Overview

6.1.1 General

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

The main function of the ESM sublayer is to support the EPS bearer context handling in the UE and in the MME.

The ESM comprises procedures for:

- the activation, deactivation and modification of EPS bearer contexts; and
- the request for resources (IP connectivity to a PDN or dedicated bearer resources) by the UE.

Each EPS bearer context represents an EPS bearer between the UE and a PDN. EPS bearer contexts can remain activated even if the radio and S1 bearers constituting the corresponding EPS bearers between UE and MME are temporarily released.

An EPS bearer context can be either a default bearer context or a dedicated bearer context.

A default EPS bearer context is activated when the UE requests a connection to a PDN.

Generally, ESM procedures can be performed only if an EMM context has been established between the UE and the MME, and the secure exchange of NAS messages has been initiated by the MME by use of the EMM procedures described in clause 5. The first default EPS bearer context, however, is activated during the EPS attach procedure (see subclause 4.2). Once the UE is successfully attached, the UE can request the MME to set up connections to additional PDNs. For each additional connection, the MME will activate a separate default EPS bearer context. A default EPS bearer context remains activated throughout the lifetime of the connection to the PDN.

A dedicated EPS bearer context is always linked to a default EPS bearer context and represents additional EPS bearer resources between the UE and the PDN. The network can initiate the activation of dedicated EPS bearer contexts together with the activation of the default EPS bearer context or at any time later, as long as the default EPS bearer context remains activated.

Default and dedicated EPS bearer contexts can be modified. Dedicated EPS bearer contexts can be released without affecting the default EPS bearer context. When the default EPS bearer context is released, then all dedicated EPS bearer contexts linked to it are released, too.

The UE can request the network to allocate, modify or release additional EPS bearer resources. The network decides whether to fulfil a request for additional resources by activating a new dedicated EPS bearer context or modifying an existing dedicated or default EPS bearer context.

6.1.2 Types of ESM procedures

Two types of ESM procedures can be distinguished:

1) Procedures related to EPS bearer contexts:

   These procedures are initiated by the network and are used for the manipulation of EPS bearer contexts:

   - default EPS bearer context activation;
   - dedicated EPS bearer context activation;
   - EPS bearer context modification;
   - EPS bearer context deactivation.

2) Transaction related procedures:

   These procedures are initiated by the UE to request for resources, i.e. a new PDN connection or dedicated bearer resources, or to release these resources:

   - PDN connectivity procedure;
   - PDN disconnect procedure;
   - bearer resource allocation procedure;
   - bearer resource modification procedure.

   When combined with the attach procedure, the PDN connectivity procedure can trigger the network to execute the following transaction related procedure:

   - ESM information request procedure.

A successful transaction related procedure initiated by the UE triggers the network to execute one of the procedures related to EPS bearer contexts. The UE treats the start of the procedure related to the EPS bearer context as completion of the transaction related procedure.

The following ESM procedures can be related to an EPS bearer context or to a procedure transaction:

- ESM status procedure;
- notification procedure.

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.

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.

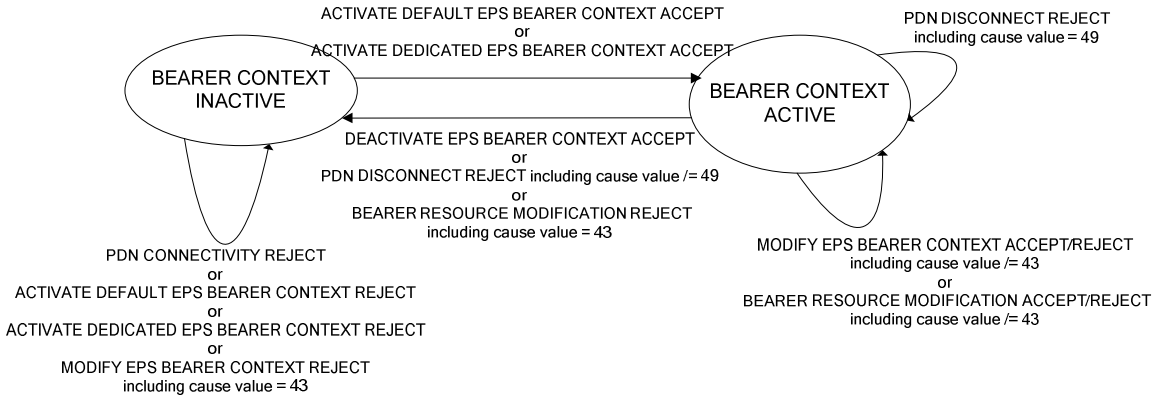


Figure 6.1.3.2.2.1: The ESM sublayer states for EPS bearer context handling in the UE (overview)

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.

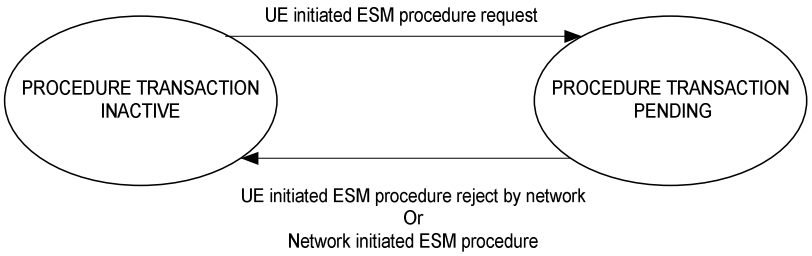


Figure 6.1.3.2.4.1: The procedure transaction states in the UE (overview)

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.

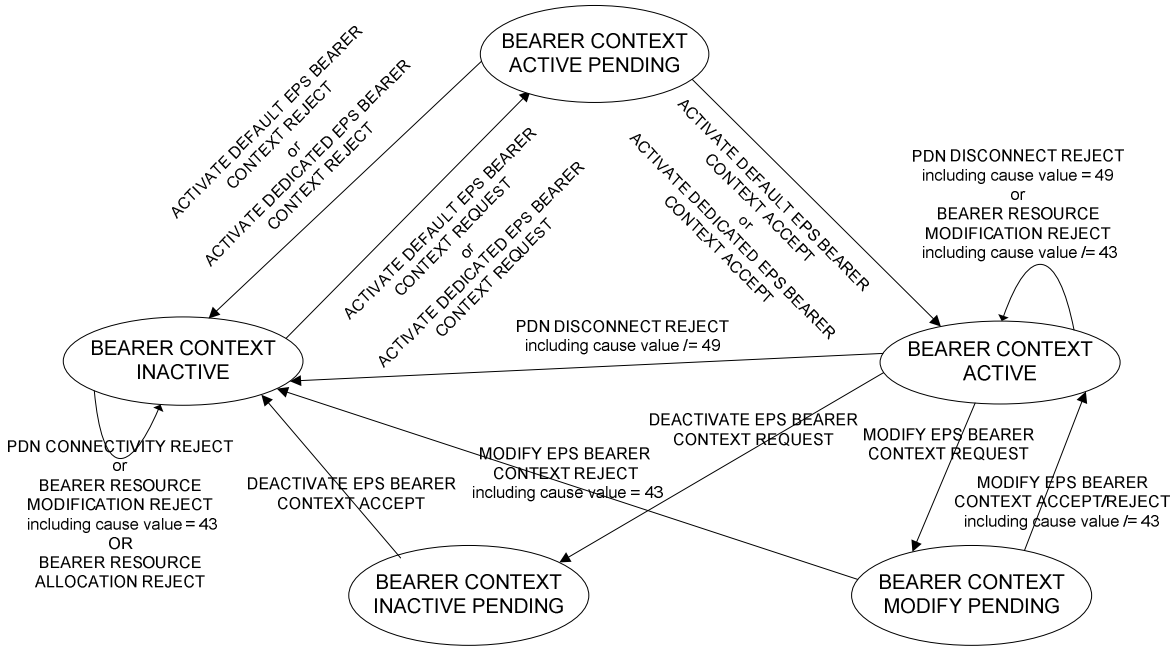


Figure 6.1.3.3.5.1: The ESM sublayer states for EPS bearer context handling in the network (overview)

6.1.3.3.6 PROCEDURE TRANSACTION INACTIVE

No procedure transaction exists.

6.1.3.3.7 PROCEDURE TRANSACTION PENDING

The network has initiated a procedure transaction towards the UE.

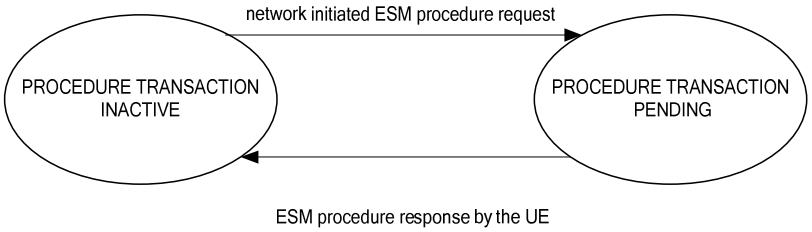


Figure 6.1.3.3.7.1: The procedure transaction states in the network (overview)

6.1.4 Coordination between ESM and SM

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 TI;
- PDN address and APN of the default EPS bearer context to map to PDP address and APN of the default PDP context;
- TFT of the default EPS bearer context, if any, to map to the TFT of the default PDP context;
- TFTs of the dedicated EPS bearer contexts to map to TFTs of the secondary PDP contexts; and
- GERAN/UTRAN parameters as provided by the MME while on E-UTRAN access, i.e. R99 QoS, LLC SAPI, radio priority, packet flow identifier, transaction identifier and BCM (if available).

NOTE: Some networks not supporting mobility from S1 mode to A/Gb mode or Iu mode or both do not provide the UE with the GERAN/UTRAN parameters. However, for this case there is no need for the UE to perform mapping to GERAN/UTRAN parameters (i.e. the PDP contexts cannot be transferred to A/Gb mode or Iu mode).

The MME performs the mapping from EPS to R99 QoS parameters according to 3GPP TS 23.401 [10], annex E.

For inter-system change from S1 mode to A/Gb mode or Iu mode, SM shall not activate the PDP context(s) if SM does not have the following parameters for A/Gb mode from the active EPS bearer context(s): LLC SAPI, radio priority, transaction identifier. SM shall not activate the PDP context(s) if SM does not have the following parameter for Iu mode from the active EPS bearer context(s): transaction identifier.

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;
- NSAPI of the default PDP context to map to linked EPS bearer identity;
- PDP address and APN of the default PDP context to map to PDN address and APN of the default EPS bearer context;
- TFT of the default PDP context, if any, to map to the TFT of the default EPS bearer context; and
- TFTs of the secondary PDP contexts to map to the TFTs of the dedicated EPS bearer contexts.

The MME and the UE perform the mapping from R99 to EPS QoS parameters according to 3GPP TS 23.401 [10], annex E. In particular the MME derives the APN-AMBR for the corresponding PDN connection from the MBR of the R99 subscribed QoS profile and the UE maps the MBR of its default PDP context to the APN-AMBR of the corresponding PDN connection.

6.1.5 Coordination between ESM and EMM for supporting ISR

This subclause applies to a UE with its TIN set as "RAT-related TMSI" for which ISR is activated.

The UE shall change its TIN to "GUTI" to deactivate ISR:

- upon modification of any EPS bearer context which was activated before the ISR is activated in the UE;
- at the time when the UE changes from S1 mode to A/Gb mode or Iu mode, if any EPS bearer context activated after the ISR was activated in the UE exists; or
- upon deactivation of the last non-emergency EPS bearer context in the UE, if the UE has only a PDN connection for emergency bearer services remaining.

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 (the corresponding procedures are specified in 3GPP TS 29.061 [16]):

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 (e.g. the per APN settings specified in 3GPP TS 23.401 [10]) as follows:

a)- A UE, which is IPv6 and IPv4 capable and

- has not been allocated an IP address for this APN, shall set the PDN type IE to IPv4v6.
- has been allocated an IPv4 address for this APN and received the ESM cause #52 "single address bearers only allowed", and is requesting an IPv6 address, shall set the PDN type IE to IPv6.
- has been allocated an IPv6 address for this APN and received the ESM cause #52 "single address bearers only allowed", and is requesting an IPv4 address, shall set the PDN type IE to IPv4.

b) A UE, which is only IPv4 capable, shall set the PDN type IE to IPv4.

c) A UE, which is only IPv6 capable, shall set the PDN type IE to IPv6.

d) 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 should 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.

NOTE: If the MT and TE are separated, the UE might not be able to use ESM cause #52 "single address bearers only allowed" as a trigger for activating a second single-IP-stack EPS bearer context.

- 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.

6.3 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 Principles of address handling for ESM procedures

Transaction related procedures use the procedure transaction identity as address parameter in the ESM message header. When the UE or the network initiates a transaction related procedure, it shall include a valid procedure transaction identity value in the message header and set the EPS bearer identity to "no EPS bearer identity assigned".

If the response message is again a transaction related message, e.g. a PDN CONNECTIVITY REJECT, PDN DISCONNECT REJECT, BEARER RESOURCE ALLOCATION REJECT, BEARER RESOURCE MODIFICATION REJECT or ESM INFORMATION REQUEST message from the network or an ESM INFORMATION RESPONSE message from the UE, the sending entity shall include the procedure transaction identity value received with the request message and set the EPS bearer identity to "no EPS bearer identity assigned" (see examples in figures 6.3.2.1 and 6.3.2.2).

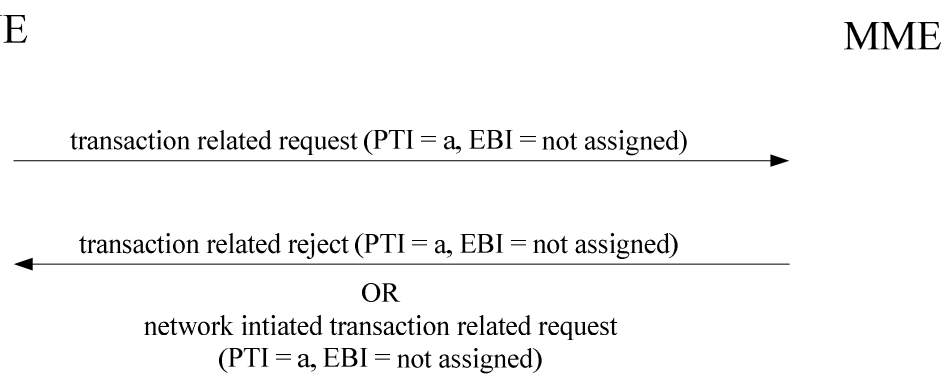


Figure 6.3.2.1: Transaction related procedure initiated by the UE and rejected by the network

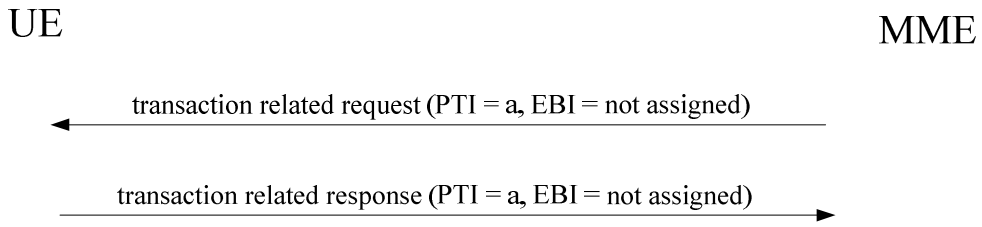


Figure 6.3.2.2: Transaction related procedure initiated by the network

EPS bearer context related procedures use the EPS bearer identity as address parameter in the ESM message header. When the network initiates an EPS bearer context related procedure, it shall include a valid EPS bearer identity value in the message header. The procedure transaction identity value shall be set as follows:

- If the EPS bearer context related procedure was triggered by the receipt of a transaction related request message from the UE, the network shall include the procedure transaction identity value received with the transaction related request message in the message header of the EPS bearer context related request message (see example in figure 6.3.2.3).
- Otherwise, if the procedure was triggered network-internally, the network shall set the procedure transaction identity value in the message header of the EPS bearer context related request message to "no procedure transaction identity assigned" (see example in figure 6.3.2.4).

In the response message of the EPS bearer context related procedure, the UE shall include the EPS bearer identity value received from the network and set the procedure transaction identity value to "no procedure transaction identity assigned".

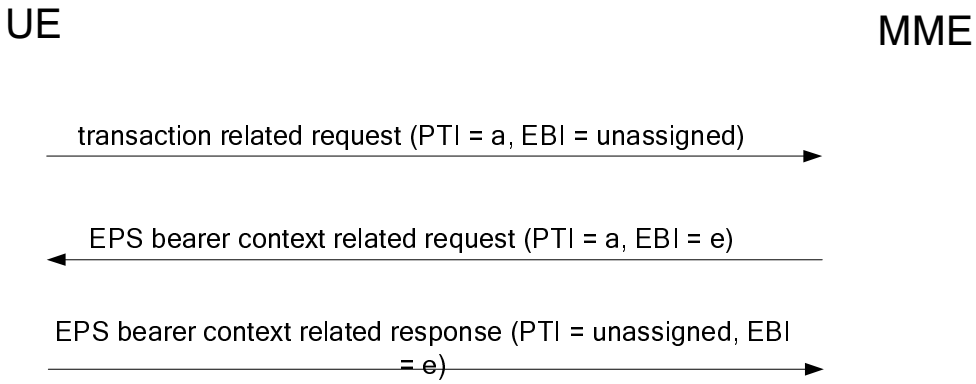


Figure 6.3.2.3: EPS bearer context related procedure triggered by a transaction related request

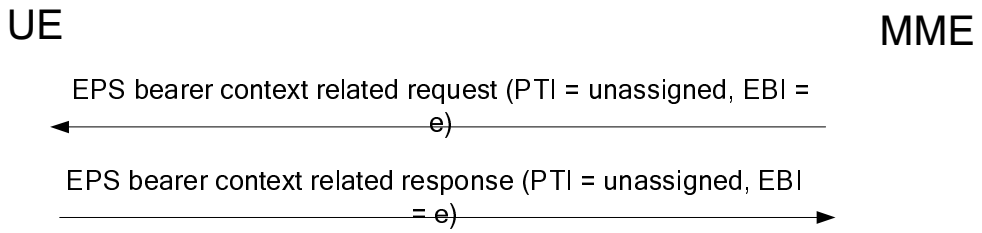


Figure 6.3.2.4: EPS bearer context related procedure triggered network-internally

6.3.3 Abnormal cases in the UE

The following 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 1: 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.

The case a) above does not apply to the ESM INFORMATION RESPONSE message.

NOTE 2: The ESM INFORMATION RESPONSE message can not be subjected to a transmission failure by lower layers due to handover as no handover message can be accepted by the UE prior to reception of the ATTACH ACCEPT message (see 3GPP TS 36.331 [22]).

b) Transmission failure of the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message indication from EMM sublayer when the UE received any ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST messages during the attach procedure

It is up to the UE implementation how the dedicated EPS bearer context activation procedure is re-initiated.

NOTE 3: The ESM procedure can typically be re-initiated using a retransmission mechanism of the ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message or ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message with new sequence number and message authentication code information thus avoiding to restart the whole procedure.

6.3.4 Abnormal cases in the network

The following abnormal case can be identified:

a) Lower layer indication of non-delivered NAS PDU due to handover

If the downlink ESM NAS message could not be delivered due to an intra MME handover and the target TA is included in the TAI list, then upon successful completion of the intra MME handover the MME shall retransmit the ESM message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the downlink ESM NAS message.

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 assigned during the activation procedure. This corresponds to using a match-all packet filter. The network may at anytime after the establishment of this bearer assign a TFT to the default EPS bearer and may subsequently modify the TFT or the packet filters of this default bearer.

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.

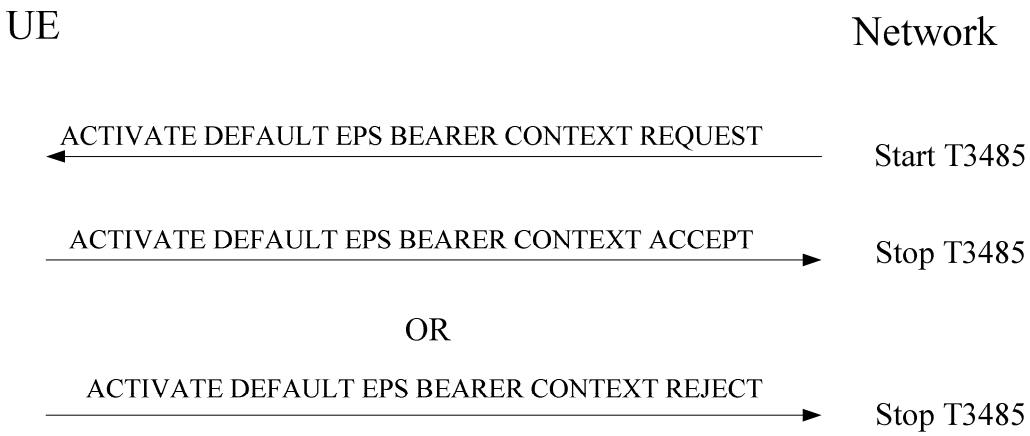


Figure 6.4.1.2.1: Default EPS bearer context activation procedure

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: request rejected, unspecified; or

#95 – 111: protocol errors.

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 EPS bearer context activation procedure is to establish an EPS bearer context with specific QoS and TFT between the UE and the EPC. The dedicated EPS bearer context activation procedure is initiated by the network, but may be requested by the UE by means of the UE requested bearer resource allocation procedure (see subclause 6.5.3) or the UE requested bearer resource modification procedure (see subclause 6.5.4). The dedicated EPS bearer context activation procedure can be part of the attach procedure or be initiated together with the default EPS bearer context activation procedure when the UE initiated stand-alone PDN connectivity procedure. If the attach procedure or the default EPS bearer context activation procedure fails, the UE shall consider that the dedicated EPS bearer activation has implicitly failed. The network may initiate the dedicated EPS bearer context activation procedure together with the completion of the service request procedure.

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. If this procedure was initiated by a UE requested bearer resource allocation procedure or a UE requested bearer resource modification procedure, the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST shall contain the procedure transaction identity (PTI) value received by the MME in the BEARER RESOURCE ALLOCATION REQUEST or BEARER RESOURCE MODIFICATION REQUEST respectively.

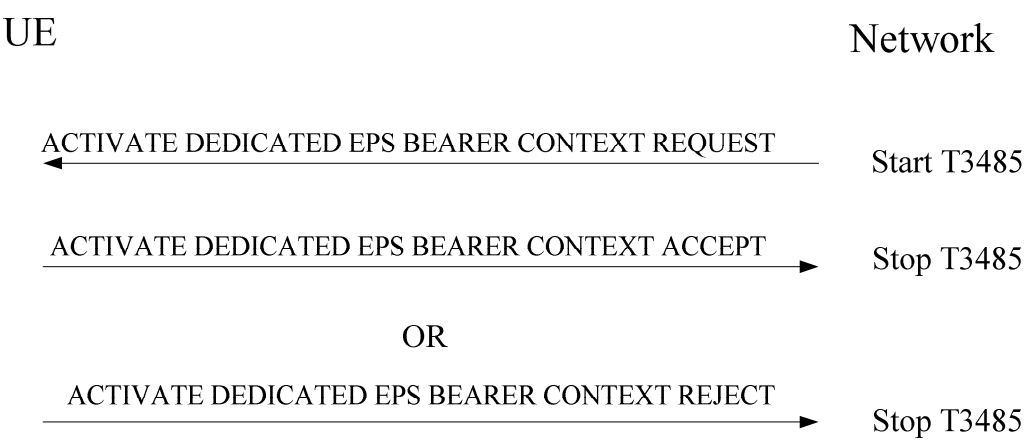


Figure 6.4.2.2.1: Dedicated EPS bearer context activation procedure

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 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 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message contains a PTI value other than "no procedure transaction identity assigned" and "reserved" (see 3GPP TS 24.007 [12]), the UE uses the PTI to identify the UE requested bearer resource allocation procedure or the UE requested bearer resource modification procedure to which the dedicated bearer context activation is related.

If the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message contains a PTI value other than "no procedure transaction identity assigned" and "reserved" (see 3GPP TS 24.007 [12]) and the PTI is associated to a UE requested bearer resource allocation procedure or a UE requested bearer resource modification procedure, the UE shall release the traffic flow aggregate description associated to the PTI value provided.

The UE shall use the received TFT to apply mapping of uplink traffic flows to the radio bearer if the TFT contains packet filters for the uplink direction.

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 an ESM 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 ESM cause values:

#26: insufficient resources;

#31: request rejected, unspecified;

#41: semantic error in the TFT operation;

#42: syntactical error in the TFT operation;

#43: invalid EPS bearer identity;

#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:

a) Semantic errors in TFT operations:

   1) When the *TFT operation* is an operation other than "Create a new TFT"

   The UE shall reject the activation request with ESM cause #41 "semantic error in the TFT operation".

b) Syntactical errors in TFT operations:

   1) When the *TFT operation* = "Create a new TFT" and the packet filter list in the TFT IE is empty.

   2) When there are other types of syntactical errors in the coding of the TFT IE, such as a mismatch between the number of packet filters subfield, and the number of packet filters in the packet filter list.

   The UE shall reject the activation request with ESM cause #42 "syntactical error in the TFT operation".

c) Semantic errors in packet filters:

   When a packet filter consists of conflicting packet filter components which would render the packet filter ineffective, i.e. no IP packet will ever fit this packet filter. How the UE determines a semantic error in a packet filter is outside the scope of the present document.

   The UE shall reject the activation request with ESM cause #44 "semantic errors in packet filter(s)".

d) Syntactical errors in packet filters:

   1) When the *TFT operation* = "Create a new TFT" and two or more packet filters in the resultant TFT would have identical packet filter identifiers.

   2) When the *TFT operation* = "Create a new TFT" and two or more packet filters in all TFTs associated with this PDN connection would have identical packet filter precedence values.

   3) When there are other types of syntactical errors in the coding of packet filters, such as the use of a reserved value for a packet filter component identifier.

   In case 2, if the old packet filters do not belong to the default EPS bearer context, the UE shall not diagnose an error, shall further process the new activation request and, if it was processed successfully, shall delete the old packet filters which have identical filter precedence values. Furthermore, by means of explicit peer-to-peer signalling between the network and the UE, the UE shall perform a UE requested bearer resource modification procedure to deactivate the EPS bearer context(s) for which it has deleted the packet filters.

   In case 2, if one or more old packet filters belong to the default EPS bearer context, the UE shall release the relevant PDN connection. If the relevant PDN connection is the last one that the UE has, the UE shall detach and re-attach to the network.

   In cases 1 and 3 the UE shall reject the activation request with ESM cause #45 "syntactical errors in packet filter(s)".

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. The MME also requests the lower layer to release the radio resources that were established during 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 default 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 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 dedicated EPS bearer context activation.

b) 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.

c) 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 ESM cause #43 "invalid EPS bearer identity".

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 allocation procedure or the UE requested bearer resource modification procedure.

The network may also initiate the EPS bearer context modification procedure to update the APN-AMBR of the UE, for instance after an inter-system handover. See 3GPP TS 23.401 [10] annex E.

The network may initiate the EPS bearer context modification procedure together with the completion of the service request 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.

If this procedure was initiated by a UE requested bearer resource allocation procedure or a UE requested bearer resource modification procedure, the MODIFY EPS BEARER CONTEXT REQUEST shall contain the procedure

transaction identity (PTI) value received by the MME in the BEARER RESOURCE ALLOCATION REQUEST or BEARER RESOURCE MODIFICATION REQUEST respectively.

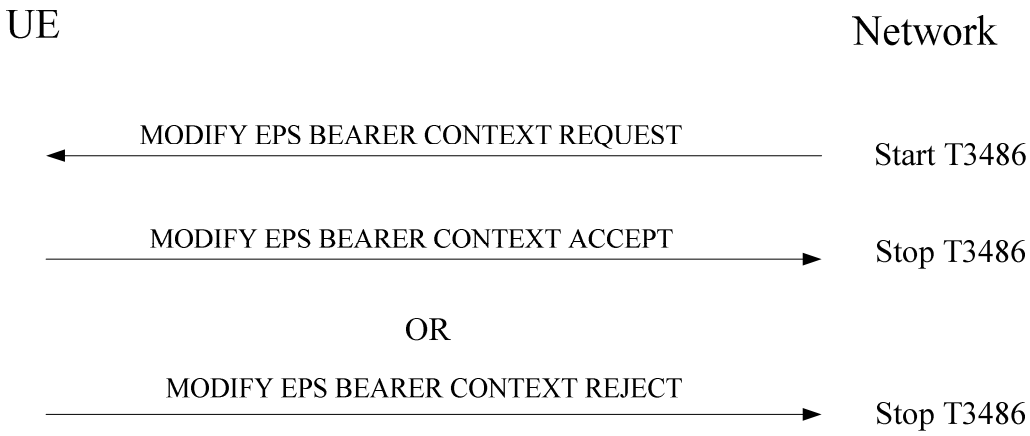


Figure 6.4.3.2.1: EPS bearer context modification procedure

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 TFT before taking it into use and then send a MODIFY EPS BEARER CONTEXT ACCEPT message to the MME.

If the MODIFY EPS BEARER CONTEXT REQUEST message contains a PTI value other than "no procedure transaction identity assigned" and "reserved" (see 3GPP TS 24.007 [12]), the UE uses the PTI to identify the UE requested bearer resource allocation procedure or the UE requested bearer resource modification procedure to which the EPS bearer context modification is related (see subclause 6.5.3 and subclause 6.5.4).

If the MODIFY EPS BEARER CONTEXT REQUEST message contains a PTI value other than "no procedure transaction identity assigned" and "reserved" (see 3GPP TS 24.007 [12]) and the PTI is associated to a UE requested bearer resource allocation procedure or a UE requested bearer resource modification procedure, the UE shall release the traffic flow aggregate description associated to the PTI value provided.

The UE shall use the received TFT to apply mapping of uplink traffic flows to the radio bearer if the TFT contains packet filters for the uplink direction.

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 an ESM 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 ESM cause values:

#26: insufficient resources;

#41: semantic error in the TFT operation;

#42: syntactical error in the TFT operation;

#43: invalid EPS bearer identity;

#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:

a) Semantic errors in TFT operations:

1) *TFT operation* = "Create a new TFT" when there is already an existing TFT for the EPS bearer context.

2) When the *TFT operation* is an operation other than "Create a new TFT" and there is no TFT for the EPS bearer context.

3) *TFT operation* = "Delete packet filters from existing TFT" when it would render the TFT empty.

4) *TFT operation* = "Delete existing TFT" for a dedicated EPS bearer context.

In case 4 the UE shall reject the modification request with ESM cause #41 "semantic error in the TFT operation".

In the other cases the UE shall not diagnose an error and perform the following actions to resolve the inconsistency:

In case 1 the UE shall further process the new activation request and, if it was processed successfully, delete the old TFT.

In case 2 the UE shall:

- process the new request and if the TFT operation is "Delete existing TFT" or "Delete packet filters from existing TFT", and if no error according to items b, c, and d was detected, consider the TFT as successfully deleted;

- process the new request as an activation request, if the TFT operation is "Add packet filters in existing TFT" or "Replace packet filters in existing TFT".

In case 3, if the packet filters belong to a dedicated EPS bearer context, the UE shall process the new deletion request and, if no error according to items b, c, and d was detected, the UE shall reject the modification request with ESM cause #41 "semantic error in the TFT operation".

In case 3, if the packet filters belong to the default EPS bearer context, the UE shall process the new deletion request and if no error according to items b, c, and d was detected then delete the existing TFT, this corresponds to using match-all packet filter for the default EPS bearer context.

b) Syntactical errors in TFT operations:

1) When the *TFT operation* = "Create a new TFT", "Add packet filters in existing TFT", "Replace packet filters in existing TFT" or "Delete packet filters from existing TFT" and the packet filter list in the TFT IE is empty.

2) *TFT operation* = "Delete existing TFT" or "No TFT operation" with a non-empty packet filter list in the TFT IE.

3) *TFT operation* = "Replace packet filters in existing TFT" when the packet filter to be replaced does not exist in the original TFT.

4) *TFT operation* = "Delete packet filters from existing TFT" when the packet filter to be deleted does not exist in the original TFT.

5) *TFT operation* = "Delete packet filters from existing TFT" with a packet filter list also including packet filters in addition to the packet filter identifiers.

6) When there are other types of syntactical errors in the coding of the TFT IE, such as a mismatch between the number of packet filters subfield, and the number of packet filters in the packet filter list.

In case 3 the UE shall not diagnose an error, further process the replace request and, if no error according to items c and d was detected, include the packet filters received to the existing TFT.

In case 4 the UE shall not diagnose an error, further process the deletion request and, if no error according to items c and d was detected, consider the respective packet filter as successfully deleted.

Otherwise the UE shall reject the modification request with ESM cause #42 "syntactical error in the TFT operation".

c) Semantic errors in packet filters:

When a packet filter consists of conflicting packet filter components which would render the packet filter ineffective, i.e. no IP packet will ever fit this packet filter. How the UE determines a semantic error in a packet filter is outside the scope of the present document.

The UE shall reject the modification request with ESM cause #44 "semantic errors in packet filter(s)".

d) Syntactical errors in packet filters:

1) When the *TFT operation* = "Create a new TFT", "Add packet filters to existing TFT", and two or more packet filters in the resultant TFT would have identical packet filter identifiers.

2) When the *TFT operation* = "Create a new TFT", "Add packet filters to existing TFT" or "Replace packet filters in existing TFT", and two or more packet filters among all TFTs associated with this PDN connection would have identical packet filter precedence values.

3) When there are other types of syntactical errors in the coding of packet filters, such as the use of a reserved value for a packet filter component identifier.

In case 1, if two or more packet filters with identical packet filter identifiers are contained in the new request, the UE shall reject the modification request with ESM cause #45 "syntactical errors in packet filter(s)". Otherwise, the UE shall not diagnose an error, further process the new request and, if it was processed successfully, delete the old packet filters which have the identical packet filter identifiers.

In case 2, if the old packet filters do not belong to the default EPS bearer context, the UE shall not diagnose an error, shall further process the new request and, if it was processed successfully, shall delete the old packet filters which have identical filter precedence values. Furthermore, the UE shall perform a UE requested bearer resource modification request procedure to deactivate the dedicated EPS bearer context(s) for which it has deleted the packet filters.

In case 2, if one or more old packet filters belong to the default EPS bearer context, the UE shall release the relevant PDN connection. If the relevant PDN connection is the last one that the UE has, the UE shall detach and re-attach to the network.

Otherwise the UE shall reject the modification request with ESM cause #45 "syntactical errors in packet filter(s)".

Upon receipt of the MODIFY EPS BEARER CONTEXT REJECT message with ESM cause value other than #43 "invalid EPS bearer identity" 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. If the network receives the MODIFY EPS BEARER CONTEXT REJECT message with ESM cause #43 "invalid EPS bearer identity", the MME locally deactivates the EPS bearer context(s) without peer-to-peer ESM signalling.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

Apart from the case described in subclause 6.3.3, no abnormal cases have been identified.

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.

If a UE is receiving emergency bearer services from a CSG cell, and the CSG subscription expires or is removed, the MME shall deactivate all non-emergency EPS bearers if any. The MME shall not deactivate the emergency EPS bearers.

If a detach is requested by the HSS for a UE that has bearers for emergency services, the MME shall send a DEACTIVATE EPS BEARER CONTEXT REQUEST message to the UE for all bearers that are not allocated for emergency services.

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 DEACTIVATE EPS BEARER CONTEXT REQUEST message contains an ESM cause typically indicating one of the following:

#8: operator determined barring;

#36: regular deactivation;

#38: network failure;

#39: reactivation requested; or

#112: APN restriction value incompatible with active EPS bearer context.

If the deactivation is triggered by a UE initiated bearer resource modification procedure or UE requested PDN disconnect procedure, the DEACTIVATE EPS BEARER CONTEXT REQUEST message shall contain the procedure transaction identity (PTI) value received by the MME in the BEARER RESOURCE MODIFICATION REQUEST or PDN DISCONNECT REQUEST respectively.

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.

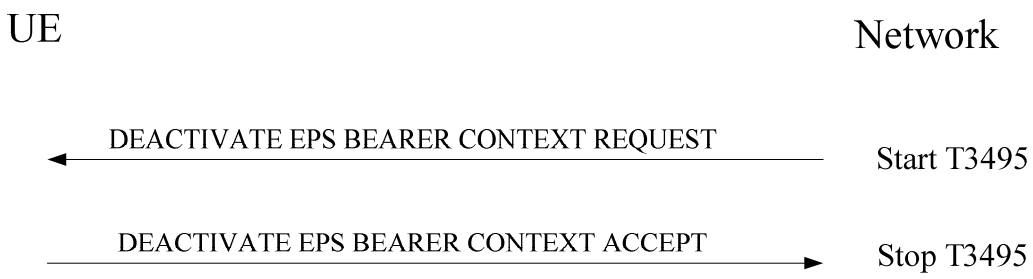


Figure 6.4.4.2.1: EPS bearer context deactivation procedure

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 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 sending the DEACTIVATE EPS BEARER CONTEXT ACCEPT message, the UE shall enter the state BEARER CONTEXT INACTIVE. If due to the EPS bearer context deactivation only the PDN connection for emergency bearer services remains established, the UE shall consider itself attached for emergency bearer services only.

If the DEACTIVATE EPS BEARER CONTEXT REQUEST includes ESM cause #39 "reactivation requested", the UE should reactivate the EPS bearer context, if it was a default EPS bearer context. Additionally, the UE should re-initiate the request(s) for dedicated bearer resources that have been activated on request of the UE and released as a result of this EPS bearer context deactivation procedure.

NOTE 1: User interaction is necessary in some cases when the UE cannot re-activate the EPS bearer context(s) automatically.

NOTE 2: The UE behaviour is not specified for the case where the DEACTIVATE EPS BEARER CONTEXT REQUEST includes ESM cause #39 "reactivation requested" and the deactivated EPS bearer context was a dedicated EPS bearer context.

If the DEACTIVATE EPS BEARER CONTEXT REQUEST message contains a PTI value other than "no procedure transaction identity assigned" and "reserved" (see 3GPP TS 24.007 [12]), the UE uses the PTI to identify the UE requested bearer resource modification procedure or UE requested PDN disconnect procedure to which the EPS bearer context deactivation is related (see subclause 6.5.4).

If the DEACTIVATE EPS BEARER CONTEXT REQUEST message contains a PTI value other than "no procedure transaction identity assigned" and "reserved" (see 3GPP TS 24.007 [12]), the UE shall release the traffic flow aggregate description associated to the PTI value provided.

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

Apart from the case described in subclause 6.3.3, no abnormal cases have been identified.

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:

1) 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 (see subclause 5.6.1.4 for details);

2) during the tracking area updating procedure with "active" flag, or without "active" flag but the network established the user plane radio bearers due to downlink pending data, if the E-UTRAN fails to establish the user plane radio bearers due to lower layer failure for one or more but not all EPS bearer contexts indicated active by both UE and network;

NOTE 1: The synchronisation of the EPS bearers indicated in EPS bearer context status information element in TRACKING AREA UPDATE ACCEPT message is not applicable in item 2.

3) during handover, if the target E-UTRAN cannot establish all the user plane radio bearers for the UE; or

4) 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 2: 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 or tracking area updating procedure with "active" flag, 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.

If due to any of the cases described above the UE locally deactivates all EPS bearer contexts, the UE shall perform a local detach, enter state EMM-DEREGISTERED and initiate an attach procedure.

The MME shall deactivate the GBR EPS bearer contexts locally without peer-to-peer ESM signalling, when the E-UTRAN requests the MME to release the S1AP connection due to radio link failure.

NOTE 3: The UE and the MME will synchronize the EPS bearer contexts subsequently during the next service request procedure, tracking area update procedure or routing area update procedure.

If due to any of the cases described above the network locally deactivates all EPS bearer contexts, the MME shall perform a local detach and enter state EMM-DEREGISTERED.

For EPS bearer context deactivation procedure initiated by the network, if no NAS signalling connection exists, the MME locally deactivates the EPS bearer context(s) without peer-to-peer ESM signalling, except when the MME disconnects the UE from the last PDN to which it is connected. In the latter case, the MME initiates a network initiated detach procedure.

If the UE locally deactivates the EPS bearer context(s) of the last PDN connection for non-emergency bearer services and only the PDN connection for emergency bearer services remains established, the UE shall consider itself attached for emergency bearer services only.

If the MME locally deactivates the EPS bearer context(s) of the last PDN connection for non-emergency bearer services and only the PDN connection for emergency bearer services remains established for the UE, the MME shall consider the UE to be attached for emergency bearer services only.

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. The UE requests connectivity to a PDN by sending a PDN CONNECTIVITY REQUEST message to the network. 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 including the PDN CONNECTIVITY REQUEST message 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 by sending the message stand-alone.

If there is already a PDN connection for emergency bearer services established, the UE shall not request an additional PDN connection for emergency bearer services.

A UE attached for emergency bearer services shall not request a PDN connection to any other PDN.

6.5.1.2 UE requested PDN connectivity procedure initiation

When the PDN CONNECTIVITY REQUEST message is sent together with an ATTACH REQUEST message, the UE shall not include the APN.

NOTE 1: If the UE needs to provide protocol configuration options which require ciphering or provide an APN, or both, during the attach procedure, the ESM information transfer flag is included in the PDN CONNECTIVITY REQUEST. The MME then at a later stage in the PDN connectivity procedure initiates the ESM information request procedure in which the UE can provide the MME with protocol configuration options or APN or both.

In order to request connectivity to a PDN using the default APN, the UE includes the Access point name IE in the PDN CONNECTIVITY REQUEST message or, when applicable, in the ESM INFORMATION RESPONSE message, according to the following conditions:

- if use of a PDN using the default APN requires PAP/CHAP, then the UE should include the Access point name IE; and

- in all other conditions, the UE need not include the Access point name IE.

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). If the additional PDN connection is for emergency bearer services, the UE shall not include an APN in the PDN CONNECTIVITY REQUEST message; otherwise the UE shall include the requested APN.

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 request" when the UE is establishing a new PDN connectivity to a PDN in an attach procedure or in a stand-alone PDN connectivity procedure. The UE shall set the request type to "emergency" when the UE is requesting a new PDN connectivity for emergency bearer services. 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.

NOTE 2: For emergency bearer services, the handover from non-3GPP access to E-UTRA is not supported.

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 shall request the IPv6 Home Network Prefix only if the UE has requested the home agent IPv6 address. The requested home agent address(es) and the Home Network Prefix are related to the APN the UE requested connectivity for.

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.

If the UE supports A/Gb mode or Iu mode, the UE shall indicate the support of the network requested bearer control procedures (see 3GPP TS 24.008 [13]) in A/Gb mode or Iu mode in the Protocol configuration options IE.

Protocol configuration options provided in the ESM INFORMATION RESPONSE message replace any protocol configuration options provided in the PDN CONNECTIVITY REQUEST message.

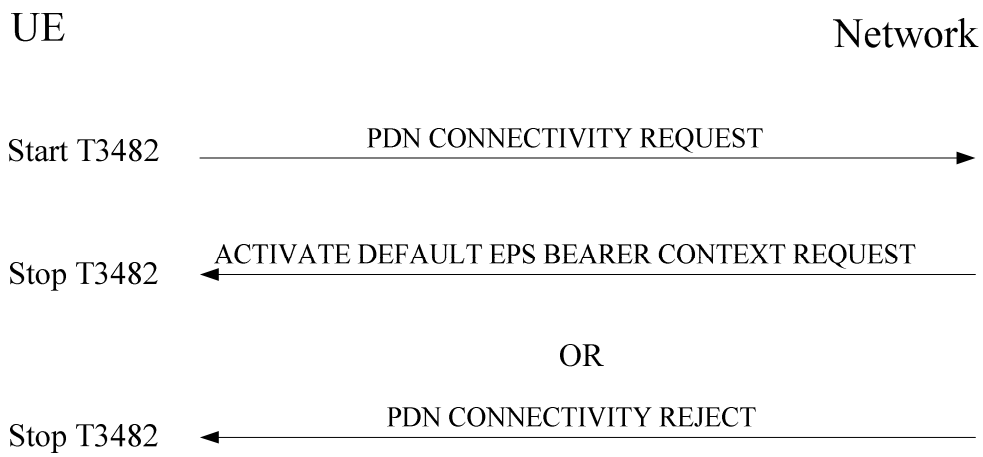


Figure 6.5.1.2.1: UE requested PDN connectivity procedure

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 the ESM information transfer flag is included. If the flag is included the MME waits for completion of the ESM information request procedure before proceeding with the PDN connectivity procedure. The MME then checks if connectivity with the requested PDN can be established. If no requested APN is included in the PDN CONNECTIVITY REQUEST message or the ESM INFORMATION RESPONSE message and the request type is different from "emergency", the MME shall use the default APN as the requested APN. If the request type is "emergency", the MME shall use the APN configured for emergency bearer services or select the statically configured PDN GW for unauthenticated UEs, if applicable.

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), ESM cause #50 "PDN type IPv4 only allowed", #51 "PDN type IPv6 only allowed", or #52 "single address bearers only allowed", respectively, shall be included in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message.

Upon receipt of the message ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message, the UE shall stop timer T3482 and enter the state PROCEDURE TRANSACTION INACTIVE. The UE should ensure that the

procedure transaction identity (PTI) assigned to this procedure is not released immediately. The way to achieve this is implementation dependent. While the PTI value is not released, the UE regards any received ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message with the same PTI value as a network retransmission (see subclause 7.3.1).

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 an ESM 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 ESM cause IE typically indicates one of the following ESM cause values:

#8: operator determined barring;

#26: insufficient resources;

#27: missing or unknown APN;

#28: unknown PDN type;

#29: user authentication failed;

#30: request rejected by Serving GW or PDN GW;

#31: request 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;

#53: ESM information not received;

#54: PDN connection does not exist;

#55: multiple PDN connections for a given APN not allowed;

#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,

If the information elements in the PDN CONNECTIVITY REQUEST message do not differ from the ones received within the previous PDN CONNECTIVITY REQUEST message, and the MME has not received the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message from UE, the network shall resend the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message and continue the previous procedure.

If one or more information elements in the PDN CONNECTIVITY REQUEST message differ from the ones received within the previous PDN CONNECTIVITY REQUEST message, and multiple PDN connections for a given APN are not allowed, the network may deactivate the existing EPS bearer contexts for the PDN connection locally without notification to the UE and proceed with the requested PDN connectivity procedure or may reject this PDN connectivity procedure including the ESM cause #55 "multiple PDN connections for a given APN not allowed", in the PDN CONNECTIVITY REJECT message.

If the network receives a PDN CONNECTIVITY REQUEST message with request type "emergency" and the MME has not received the ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message from UE for the previous PDN connectivity request for emergency bearer services, the network shall resend the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message and continue the previous procedure. If there is already a PDN connection for emergency bearer services existing, the MME shall reject the request with ESM cause #55 "multiple PDN connections for a given APN not allowed" or 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 ESM cause #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 ESM cause #53 "ESM information not received", in the PDN CONNECTIVITY REJECT message.

d) Additional UE initiated PDN connectivity request received from a UE that is attached for emergency bearer services:

The MME shall reject the request with ESM cause #31 "request rejected, unspecified".

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 any 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.

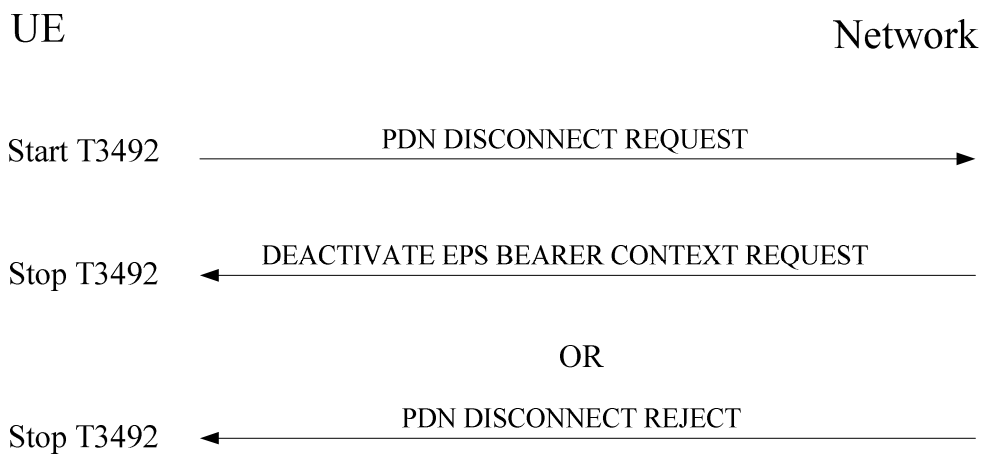


Figure 6.5.2.2.1: UE requested PDN disconnection procedure

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 IE that typically indicates one of the following ESM cause values:

#35: PTI already in use;

#43: invalid EPS bearer identity;

#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 ESM cause #49 "last PDN disconnection not allowed", 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, release the PTI allocated for this invocation 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 that includes the EPS bearer context status IE 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 EPS 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 ESM cause #43 "invalid EPS bearer identity".

6.5.3 UE requested bearer resource allocation procedure

6.5.3.1 General

The purpose of the UE requested bearer resource allocation procedure is for a UE to request an allocation of bearer resources for a traffic flow aggregate. The UE requests a specific QoS demand (QCI) and optionally sends a GBR requirement for a new traffic flow aggregate. If accepted by the network, this procedure invokes a dedicated EPS bearer context activation procedure (see subclause 6.4.2) or an EPS bearer context modification procedure (see subclause 6.4.3).

If there is a PDN connection for emergency bearer services established, the UE shall not request additional bearer resources for this PDN connection.

6.5.3.2 UE requested bearer resource allocation procedure initiation

In order to request the allocation of bearer resources for one traffic flow aggregate, the UE shall send a BEARER RESOURCE ALLOCATION REQUEST message to the MME, start timer T3480 and enter the state PROCEDURE TRANSACTION PENDING (see example in figure 6.5.3.2.1).

The UE shall include the EPS bearer identity of the default EPS bearer associated with the requested bearer resource in the Linked EPS bearer identity IE. The UE shall set the TFT operation code in the Traffic flow aggregate IE to "Create

new TFT". In the Required traffic flow QoS IE, the UE shall indicate a QCI and, if the UE also includes a GBR, the additional GBR required for the traffic flow aggregate.

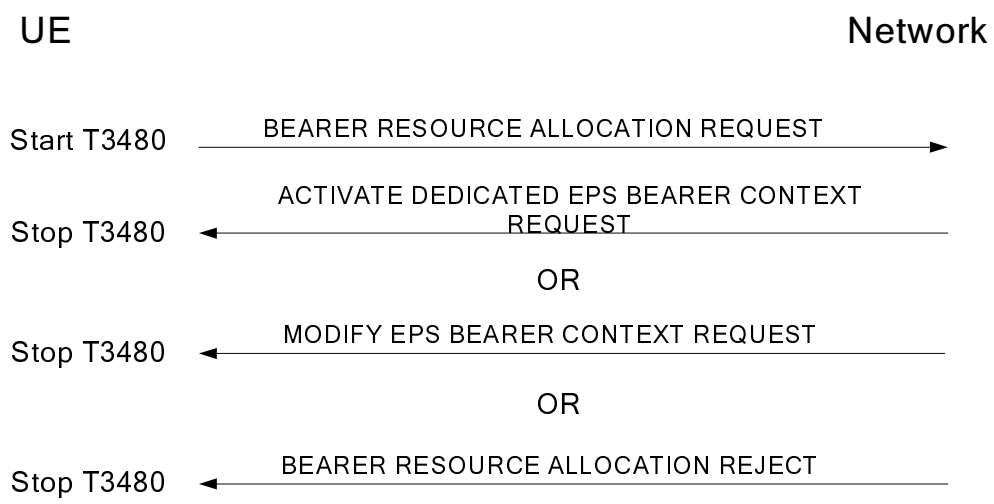


Figure 6.5.3.2.1: UE requested bearer resource allocation procedure

6.5.3.3 UE requested bearer resource allocation procedure accepted by the network

Upon receipt of the BEARER RESOURCE ALLOCATION REQUEST message, the MME checks whether the resources requested by the UE can be established by verifying the EPS 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 allocation requested is accepted by the network, the MME shall initiate either a dedicated EPS bearer context activation procedure or an EPS bearer context modification procedure. Upon receipt of an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST or MODIFY EPS BEARER CONTEXT REQUEST message with a PTI which matches the value used for the BEARER RESOURCE ALLOCATION REQUEST message, the UE shall stop timer T3480 and enter the state PROCEDURE TRANSACTION INACTIVE. The UE should ensure that the procedure transaction identity (PTI) assigned to this procedure is not released immediately. The way to achieve this is implementation dependent. While the PTI value is not released, the UE regards any received ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST or MODIFY EPS BEARER CONTEXT REQUEST message with the same PTI value as a network retransmission (see subclause 7.3.1).

If the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message is received, the UE shall verify that the EPS 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. The UE shall then proceed as described in subclause 6.4.2.3 or subclause 6.4.2.4.

If the MODIFY EPS BEARER CONTEXT REQUEST message is received, the UE verifies that the EPS bearer identity given in the EPS bearer identity IE is any of the active EPS bearer contexts. The UE shall then proceed as described in subclause 6.4.3.3 or subclause 6.4.3.4.

6.5.3.4 UE requested bearer resource allocation procedure not accepted by the network

If the bearer resource allocation requested cannot be accepted by the network, the MME shall send a BEARER RESOURCE ALLOCATION REJECT message to the UE. The message shall contain the PTI and an ESM cause value indicating the reason for rejecting the UE requested bearer resource allocation.

The ESM cause value typically indicates one of the following:

#26: insufficient resources;

#30: request rejected by Serving GW or PDN GW;

#31: request 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: invalid EPS bearer identity;

#44: semantic error(s) in packet filter(s);

#45: syntactical error(s) in packet filter(s);

#56: collision with network initiated request;

#59: unsupported QCI value; or

#95 – 111: protocol errors.

If the requested new TFT is not available, then the BEARER RESOURCE ALLOCATION 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 TFT operations:

   1) When the *TFT operation* is an operation other than "Create a new TFT".

   The network shall reject the allocation request with ESM cause #41 "semantic error in the TFT operation".

b) Syntactical errors in TFT operations:

   1) When the *TFT operation* = "Create a new TFT" and the packet filter list in the TFT IE is empty.

   2) When there are other types of syntactical errors in the coding of the TFT IE, such as a mismatch between the number of packet filters subfield, and the number of packet filters in the packet filter list.

   The network shall reject the allocation request with ESM cause #42 "syntactical error in the TFT operation".

c) Semantic errors in packet filters:

   When a packet filter consists of conflicting packet filter components which would render the packet filter ineffective, i.e. no IP packet will ever fit this packet filter. How the network determines a semantic error in a packet filter is outside the scope of the present document.

   The network shall reject the allocation request with ESM cause #44 "semantic errors in packet filter(s)".

d) Syntactical errors in packet filters:

   1) When the *TFT operation* = "Create a new TFT" and two or more packet filters among all TFTs associated with the PDN connection would have identical packet filter precedence values.

   2) When there are other types of syntactical errors in the coding of packet filters, such as the use of a reserved value for a packet filter component identifier.

   In case 1, if the old packet filters do not belong to the default EPS bearer context, the network shall not diagnose an error, shall further process the new request and, if it was processed successfully, shall delete the old packet filters which have identical filter precedence values. Furthermore, the network shall perform an EPS bearer context deactivation request procedure to deactivate the dedicated EPS bearer context(s) for which it has deleted the packet filters.

In case 1, if one or more old packet filters belong to the default EPS bearer context, the network shall release the relevant PDN connection using the EPS bearer context deactivation procedure.If it is the last PDN connection, the network shall detach the UE using detach type "re-attach required".

Otherwise the network shall reject the allocation request with ESM cause #45 "syntactical errors in packet filter(s)".

Upon receipt of a BEARER RESOURCE ALLOCATION REJECT message, the UE shall stop the timer T3480, release the traffic flow aggregate description associated to the PTI value, 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 ALLOCATION 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.

b) Unknown EPS bearer context

Upon receipt of the BEARER RESOURCE ALLOCATION REJECT message including ESM cause #43 "invalid EPS bearer identity", the UE shall deactivate the existing default EPS bearer context locally without peer-to-peer signalling between the UE and the MME.

6.5.3.6 Abnormal cases on the network side

The following abnormal case can be identified:

a) No PDN connection with the linked EPS bearer identity activated:

If the linked EPS bearer identity included in the BEARER RESOURCE ALLOCATION REQUEST message does not belong to the default EPS bearer context of an established PDN connection, the MME shall reply with a BEARER RESOURCE ALLOCATION REJECT message with ESM cause #43 "invalid EPS bearer identity".

b) BEARER RESOURCE ALLOCATION REQUEST message received for a PDN connection established for emergency bearer services:

The MME shall reply with a BEARER RESOURCE ALLOCATION REJECT message with ESM cause #31 "request rejected, unspecified".

6.5.4 UE requested bearer resource modification procedure

6.5.4.1 General

The purpose of the UE requested bearer resource modification procedure is for a UE to request a modification or release of bearer resources for a traffic flow aggregate or modification of a traffic flow aggregate by replacing packet filters or adding packet filters. When requesting a modification of bearer resources for a traffic flow aggregate or a modification of a traffic flow aggregate, the UE can 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).

If there is a PDN connection for emergency bearer services established, the UE shall not request a modification of bearer resources for this PDN connection.

6.5.4.2 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 T3481 and enter the state PROCEDURE TRANSACTION PENDING (see example in figure 6.5.4.2.1).

The UE shall include the EPS bearer identity of the EPS bearer associated with the traffic flow aggregate in the EPS bearer identity for packet filter IE.

To request a change of the GBR without changing the packet filter(s), the UE shall set the TFT operation code in the Traffic flow aggregate IE to "no TFT operation" and include the packet filter identifier(s) to which the change of the GBR applies in the Packet filter identifier parameter in the parameters list. The UE shall indicate the new GBR requested for the EPS bearer context in the Required traffic flow QoS IE.

To request a modification of a traffic flow aggregate, the UE shall set the TFT operation code in the Traffic flow aggregate IE to "Replace packet filters in existing TFT" or "Add packet filters to existing TFT". If the TFT operation code is set to "Add packet filters to existing TFT", the UE shall include in the parameter list one existing packet filter identifier to which the newly added packet filter(s) is linked. If the EPS bearer is a GBR bearer, the UE shall indicate the new GBR requested for the EPS bearer context in the Required traffic flow QoS IE.

To request a release of bearer resources, the UE shall set the TFT operation code in the Traffic flow aggregate IE to "Delete packet filters from existing TFT". If the EPS bearer is a GBR bearer, the UE shall indicate the new GBR requested for the EPS bearer context in the Required traffic flow QoS IE.

If the UE includes the Required traffic flow QoS IE, the UE shall set the QCI to the current QCI value of the EPS bearer context.

If the UE requests the release of bearer resources, the ESM cause value typically indicates one of the following:

#36: regular deactivation.

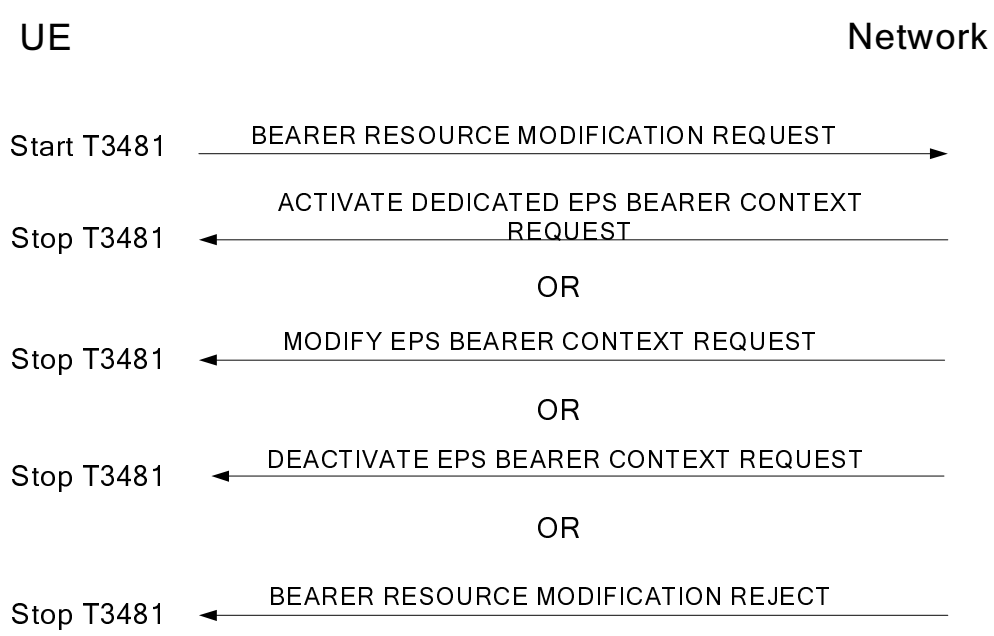


Figure 6.5.4.2.1: UE requested bearer resource modification procedure

6.5.4.3 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 EPS bearer identity given in the EPS bearer identity for packet filter IE.

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 message with a PTI which matches the value used for the BEARER RESOURCE MODIFICATION REQUEST message, the UE shall stop timer T3481 and enter the state PROCEDURE TRANSACTION INACTIVE. The UE should ensure that the procedure transaction identity (PTI) assigned to this procedure is not released immediately. The way to achieve this is implementation dependent. While the PTI value is not released, the UE regards any received ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST or MODIFY EPS BEARER CONTEXT REQUEST message with the same PTI value as a network retransmission (see subclause 7.3.1).

i) If the ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message is received, the UE shall verify that the EPS 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. The UE shall then proceed as described in subclause 6.4.2.3 or subclause 6.4.2.4.

ii) If the MODIFY EPS BEARER CONTEXT REQUEST message is received, the UE verifies that the EPS bearer identity given in the EPS bearer identity IE is any of the active EPS bearer contexts. The UE shall then proceed as described in subclause 6.4.3.3 or subclause 6.4.3.4.

iii) If the DEACTIVATE EPS BEARER CONTEXT REQUEST message is received, the UE verifies that the EPS 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 The UE shall then proceed as described in subclause 6.4.4.3.

In case i, after successful completion of the dedicated EPS bearer context activation procedure, the network may initiate an EPS bearer context modification procedure to delete the packet filters which have packet filter identifiers indicated by the UE in the TFT IE in the BEARER RESOURCE MODIFICATION REQUEST message and for which the network created new packet filters during the dedicated EPS bearer context activation procedure. In this case the MME shall set the procedure transaction identity value in the MODIFY EPS BEARER CONTEXT REQUEST message to "no procedure transaction identity assigned".

6.5.4.4 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 an ESM cause value indicating the reason for rejecting the UE requested bearer resource modification.

The ESM cause value typically indicates one of the following:

#26: insufficient resources;

#30: request rejected by Serving GW or PDN GW;

#31: request 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: invalid EPS bearer identity;

#44: semantic error(s) in packet filter(s);

#45: syntactical error(s) in packet filter(s);

#56: collision with network initiated request;

#59: unsupported QCI value; 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 TFT operations:

1) When the *TFT operation* is an operation other than "Replace packet filters in existing TFT", "Add packet filters to existing TFT", "Delete packet filters from existing TFT" or "No TFT operation".

2) When the *TFT operation* is "Replace packet filters in existing TFT", "Add packet filters to existing TFT" or "Delete packet filters from existing TFT" and there is no TFT for the default EPS bearer context.

3) *TFT operation* = "Delete packet filters from existing TFT" when it would render the TFT empty.

In case 1 the network shall reject the modification request with ESM cause #41 "semantic error in the TFT operation".

In case 2, if the TFT operation is "Delete packet filters from existing TFT", the network shall further process the new request and, if no error according to items b, c, and d was detected, shall perform an EPS bearer context modification procedure including the value of EPS bearer identity for packet filter IE in the EPS bearer identity IE and a TFT IE with *TFT operation* = "Delete existing TFT" in the MODIFY EPS BEARER CONTEXT REQUEST message.

In case 2, if the TFT operation is "Replace packet filters in existing TFT" or "Add packet filters to existing TFT", the network shall process the new request as a request with TFT operation = "Create a new TFT".

In case 3, if the packet filters belong to a dedicated EPS bearer context, the network shall process the new deletion request and, if no error according to items b, c, and d was detected, delete the existing TFT. After successful deletion of the TFT, the network shall perform an EPS bearer context deactivation request procedure to deactivate the dedicated EPS bearer context between the UE and the network.

In case 3, if the packet filters belong to the default EPS bearer context, the network shall process the new deletion request and if no error according to items b, c, and d was detected then perform an EPS bearer context modification procedure to remove the existing TFT of the default EPS bearer context, this corresponds to using match-all packet filter for the default EPS bearer context.

b) Syntactical errors in TFT operations:

1) When the *TFT operation* = "Replace packet filters in existing TFT", "Add packet filters to existing TFT" or "Delete packet filters from existing TFT", and the packet filter list in the TFT IE is empty.

2) *TFT operation* = "No TFT operation" with a non-empty packet filter list in the TFT IE.

3) *TFT operation* = "Replace packet filters in existing TFT" when the packet filter to be replaced does not exist in the original TFT.

4) *TFT operation* = "Delete packet filters from existing TFT" when the packet filter to be deleted does not exist in the original TFT.

5) *TFT operation* = "Delete packet filters from existing TFT" with a packet filter list also including packet filters in addition to the packet filter identifiers.

6) When there are other types of syntactical errors in the coding of the TFT IE, such as a mismatch between the number of packet filters subfield, and the number of packet filters in the packet filter list.

In case 3 the network shall not diagnose an error, shall further process the replace request and, if no error according to items c and d was detected, shall perform an EPS bearer context modification procedure using *TFT operation* = "Add packet filters to existing TFT" to include the packet filters received to the existing TFT.

In case 4 the network shall not diagnose an error, shall further process the deletion request and, if no error according to items c and d was detected, shall perform an EPS bearer context modification procedure including the value of EPS bearer identity for packet filter IE in the EPS bearer identity IE and a TFT IE with *TFT operation* = "Delete packet filters from existing TFT" and the received packet filter identifier(s) in the MODIFY EPS BEARER CONTEXT REQUEST message.

Otherwise the network shall reject the modification request with ESM cause #42 "syntactical error in the TFT operation".

c) Semantic errors in packet filters:

When a packet filter consists of conflicting packet filter components which would render the packet filter ineffective, i.e. no IP packet will ever fit this packet filter. How the network determines a semantic error in a packet filter is outside the scope of the present document.

The network shall reject the modification request with ESM cause #44 "semantic errors in packet filter(s)".

d) Syntactical errors in packet filters:

1) When the *TFT operation* = "Replace packet filters in existing TFT" and two or more packet filters in all TFTs associated with the PDN connection would have identical packet filter precedence values.

2) When there are other types of syntactical errors in the coding of packet filters, such as the use of a reserved value for a packet filter component identifier.

In case 1, if the old packet filters do not belong to the default EPS bearer context, the network shall not diagnose an error, shall further process the new request and, if it was processed successfully, shall delete the old packet filters which have identical filter precedence values. Furthermore, the network shall perform an EPS bearer context deactivation procedure to deactivate the dedicated EPS bearer context(s) for which it has deleted the packet filters.

In case 1, if one or more old packet filters belong to the default EPS bearer context, the network shall release the relevant PDN connection using the EPS bearer context deactivation procedure. If the relevant PDN connection is the last one, the network shall detach the UE using detach type "re-attach required".

Otherwise the network shall reject the modification request with ESM cause #45 "syntactical errors in packet filter(s)".

Upon receipt of a BEARER RESOURCE MODIFICATION REJECT message, the UE shall stop the timer T3481, release the traffic flow aggregate description associated to the PTI value, and enter the state PROCEDURE TRANSACTION INACTIVE. If the ESM cause included in the BEARER RESOURCE MODIFICATION REJECT message is #43 "invalid EPS bearer identity", the UE locally deactivates the EPS bearer context(s) without peer-to-peer ESM signalling.

The further actions to be performed by the UE are implementation dependent as part of upper layers responsibility.

6.5.4.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Expiry of timer T3481:

On the first expiry of the timer T3481, the UE shall resend the BEARER RESOURCE MODIFICATION REQUEST and shall reset and restart timer T3481. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3481, 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 EPS 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 that includes the EPS bearer context status IE to the MME.

b) Unknown EPS bearer context

Upon receipt of the BEARER RESOURCE MODIFICATION REJECT message including ESM cause #43 "invalid EPS bearer identity", the UE shall deactivate the existing EPS bearer context locally without peer-to-peer signalling between the UE and the MME.

c) Collision of a UE requested bearer resource modification procedure and an EPS bearer context deactivation procedure.

When the UE receives a DEACTIVATE EPS BEARER CONTEXT REQUEST message during the bearer resource modification procedure, and the EPS bearer identity indicated in the DEACTIVATE EPS BEARER CONTEXT REQUEST message is a EPS bearer context the UE indicated in the UE requested bearer resource modification procedure, then the UE shall abort the UE requested bearer resource modification procedure and proceed with the EPS bearer context deactivation procedure.

6.5.4.6 Abnormal cases on the network side

a) Unknown EPS bearer context

If the EPS bearer identity provided in the EPS bearer identity for packet filter IE in the BEARER RESOURCE MODIFICATION REQUEST message indicates an EPS bearer identity value and this does not belong to any already activated EPS bearer context, the MME shall reply with a BEARER RESOURCE MODIFICATION REJECT message with ESM cause #43 "invalid EPS bearer identity".

b) BEARER RESOURCE MODIFICATION REQUEST message received for a PDN connection established for emergency bearer services:

The MME shall reply with a BEARER RESOURCE MODIFICATION REJECT message with ESM cause #30 "request rejected by Serving GW or PDN GW".

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 ESM information request procedure by sending a ESM INFORMATION REQUEST message to the UE, starting timer T3489 and entering the state PROCEDURE TRANSACTION PENDING (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.

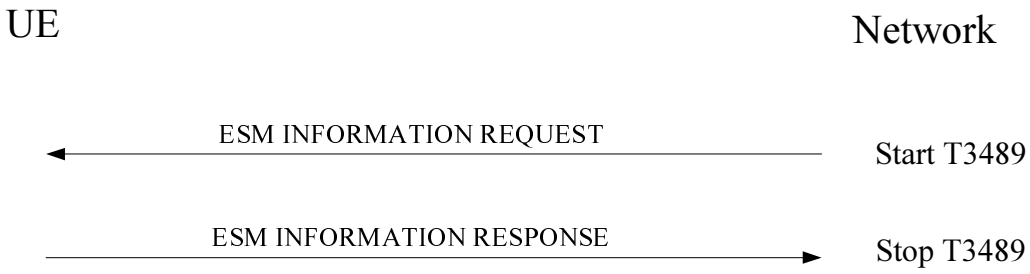


Figure 6.6.1.2.2.1: ESM information request procedure

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 and enter the state PROCEDURE TRANSACTION INACTIVE. A PCO included in the ESM INFORMATION RESPONSE message replaces any PCO that the network previously may have received during the attach procedure execution.

6.6.1.2.5 Abnormal cases in the UE

Apart from the case described in subclause 6.3.3, no abnormal cases have been identified.

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 ESM cause #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, bearer resource allocation 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. In particular, the UE may use this procedure on EPS bearer context activation to perform the MSISDN notification procedure as specified in 3GPP TS 24.008 [13], subclause 6.4.

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, bearer resource allocation 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. In particular, the PDN GW may use this procedure on EPS bearer context activation to perform the MSISDN notification procedure as specified in 3GPP TS 24.008 [13], subclause 6.4.

6.6.2 Notification procedure

6.6.2.1 General

The network can use the notification procedure to inform the UE about events which are relevant for the upper layer which is using an EPS bearer context or has requested a procedure transaction.

If the UE has indicated that it supports the notification procedure, the network may initiate the procedure at any time while a PDN connection exists or a procedure transaction is ongoing.

6.6.2.2 Notification procedure initiation by the network

The network initiates the notification procedure by sending a NOTIFICATION message to the UE (see example in figure 6.6.2.2.1).

Figure 6.6.2.2.1: Notification procedure

6.6.2.3 Notification procedure in the UE

When the UE receives a NOTIFICATION message, the ESM protocol entity in the UE shall provide the notification indicator to the upper layer.

The notification indicator can have the following value:

#1: SRVCC handover cancelled, IMS session re-establishment required.

6.6.2.4 Abnormal cases on the network side

The following abnormal case can be identified:

a) Lower layer indication of non-delivered NAS PDU due to handover

If the NOTIFICATION message could not be delivered due to an intra MME handover, then upon successful completion of the intra MME handover the MME shall retransmit the NOTIFICATION message. If a failure of the handover procedure is reported by the lower layer and the S1 signalling connection exists, the MME shall retransmit the NOTIFICATION message.

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 (see example in figure 6.7.1).

If the ESM entity of the UE receives an ESM STATUS message the UE shall take different actions depending on the received ESM cause value:

#43 (Invalid EPS bearer identity);

The UE shall abort any ongoing ESM procedure related to the received EPS bearer identity, stop any related timer, and deactivate the corresponding EPS bearer context locally (without peer to peer signalling between the UE and the MME).

#81 (Invalid PTI value);

The UE shall abort any ongoing ESM procedure related to the received PTI value and stop any related timer.

#97 (Message type non-existent or not implemented);

The UE shall abort any ongoing ESM procedure related to the PTI or EPS bearer identity and stop any related timer.

On receipt of an ESM STATUS message with any other ESM cause value no state transition and no specific action shall be taken as seen from the radio interface, i.e. local actions are possible.

If the ESM entity of the MME receives an ESM STATUS message the MME shall take different actions depending on the received ESM cause value:

#43 (Invalid EPS bearer identity);

The MME shall abort any ongoing ESM procedure related to the received EPS bearer identity, stop any related timer, and deactivate the corresponding EPS bearer context locally (without peer to peer signalling between the MME and the UE).

#81 (Invalid PTI value);

The MME shall abort any ongoing ESM procedure related to the received PTI value and stop any related timer.

#97 (Message type non-existent or not implemented);

The MME shall abort any ongoing ESM procedure related to the PTI or EPS bearer identity and stop any related timer.

The local actions to be taken by the MME on receipt of an ESM STATUS message with any other ESM cause value are implementation dependent.

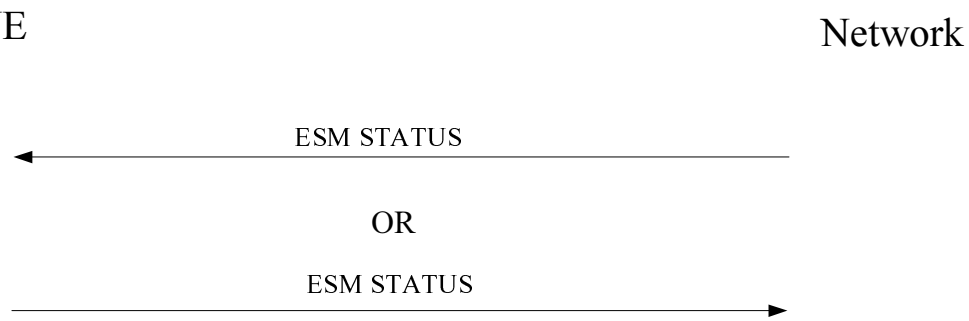


Figure 6.7.1: ESM status procedure

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 ESM cause #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 ESM cause #81 "invalid PTI value".

c) If the network receives a BEARER RESOURCE ALLOCATION REQUEST message with an unassigned or reserved PTI value, the network shall respond with a BEARER RESOURCE ALLOCATION REJECT message including ESM cause #81 "invalid PTI value".

d) 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 ESM cause #81 "invalid PTI value".

e) If the network receives an ESM INFORMATION RESPONSE message which includes an unassigned or reserved PTI value, the network shall ignore the message. If the PTI is an assigned value that does not match the PTI in use for any ongoing transaction related procedure, the network shall respond with an ESM STATUS message including ESM cause #81 "invalid PTI value".

f) If the network receives an ESM message other than those listed in items a through e 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 unassigned or reserved value, or an assigned value that does not match any PTI in use, the UE shall ignore the message.

b) If the UE receives a PDN DISCONNECT REJECT message in which the PTI value is an unassigned or reserved value, or an assigned value that does not match any PTI in use, the UE shall ignore the message.

c) If the UE receives a BEARER RESOURCE ALLOCATION REJECT message in which the PTI value is an unassigned or reserved value, or an assigned value that does not match any PTI in use, the UE shall ignore the message.

d) If the UE receives a BEARER RESOURCE MODIFICATION REJECT message in which the PTI value is an unassigned or reserved value, or an assigned value that does not match any PTI in use, the UE shall ignore the message.

e) If the UE receives an ESM INFORMATION REQUEST message in which the PTI value is an unassigned or reserved value, the UE shall ignore the message. If the PTI 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 respond with an ESM STATUS message including ESM cause #47 "PTI mismatch".

f) If the UE receives a NOTIFICATION message in which the PTI value is an unassigned or reserved value, the UE shall proceed as specified in subclause 7.3.2. If the PTI is an assigned value that does not match any PTI in use, the UE shall respond with an ESM STATUS message including ESM cause #47 "PTI mismatch".

g) 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, if the UE detects that this request is a network retransmission of an already accepted request (see subclause 6.5.1.3) the UE shall respond with an ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT message. Otherwise, the UE shall respond with an ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message including ESM cause #47 "PTI mismatch".

h) If the UE receives an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message which contains a reserved or unassigned PTI value, the UE shall respond with an ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message including ESM cause #81 "invalid PTI value".

i) 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, if the UE detects that this request is a network retransmission of an already accepted request (see subclauses 6.5.3.3 and 6.5.4.3) the UE shall respond with an ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT message. Otherwise, the UE shall respond with an ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message including ESM cause #47 "PTI mismatch".

j) 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 ESM cause #81 "invalid PTI value".

k) 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, if the UE detects that this request is a network retransmission of an already accepted request (see subclauses 6.5.3.3 and 6.5.4.3) the UE shall respond with a MODIFY EPS BEARER CONTEXT ACCEPT message. Otherwise, the UE shall respond with a MODIFY EPS BEARER CONTEXT REJECT message including ESM cause #47 "PTI mismatch".

l) 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 ESM cause #81 "invalid PTI value".

m) If the UE receives a DEACTIVATE EPS BEARER CONTEXT REQUEST message in which the PTI value is a reserved value or an assigned value that does not match any PTI in use, the UE shall ignore the message.

n) If the UE receives an ESM message other than those listed in items a through m with a reserved PTI value or an assigned value that does not match any PTI in use, 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 the header of an ESM message (specified as the header of a standard L3 message, see 3GPP TS 24.007 [12]):

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 ESM cause #43 "invalid EPS bearer identity".

b) If the network receives a PDN DISCONNECT REQUEST message which includes an assigned or reserved EPS bearer identity value, the network shall respond with a PDN DISCONNECT REJECT message including ESM cause #43 "invalid EPS bearer identity".

c) If the network receives a BEARER RESOURCE ALLOCATION REQUEST message which includes an assigned or reserved EPS bearer identity value, the network shall respond with a BEARER RESOURCE ALLOCATION REJECT message including ESM cause #43 "invalid EPS bearer identity".

d) If the network receives a BEARER RESOURCE MODIFICATION REQUEST message which includes an assigned or reserved EPS bearer identity value, the network shall respond with a BEARER RESOURCE MODIFICATION REJECT message including ESM cause #43 "invalid EPS bearer identity".

e) If the network receives an ESM INFORMATION RESPONSE message which includes an assigned or reserved EPS bearer identity value, the network shall ignore the message.

f) If the network receives an ESM message other than those listed in items a through e above in which the message includes a reserved EPS bearer identity value or an assigned value that does not match an existing EPS bearer context, the network shall ignore the message.

The following UE procedures shall apply for handling an unknown, erroneous, or unforeseen EPS bearer identity received in the header of an ESM message:

a) If the UE receives a PDN CONNECTIVITY REJECT message which includes an assigned or reserved EPS bearer identity value, the UE shall ignore the message.

b) If the UE receives a PDN DISCONNECT REJECT message which includes an assigned or reserved EPS bearer identity value, the UE shall ignore the message.

c) If the UE receives a BEARER RESOURCE ALLOCATION REJECT message which includes an assigned or reserved EPS bearer identity value, the UE shall ignore the message.

d) If the UE receives a BEARER RESOURCE MODIFICATION REJECT message which includes an assigned or reserved EPS bearer identity value, the UE shall ignore the message.

e) If the UE receives an ESM INFORMATION REQUEST message which includes an assigned or reserved EPS bearer identity value, the UE shall respond with an ESM STATUS message including ESM cause #43 "invalid EPS bearer identity".

f) If the UE receives a NOTIFICATION message which includes an unassigned or reserved EPS bearer identity value and an unassigned or reserved PTI value, the UE shall respond with an ESM STATUS message including ESM cause #43 "invalid EPS bearer identity".

g) 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 ESM cause #43 "invalid EPS bearer identity".

h) 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 ESM cause #43 "invalid EPS bearer identity".

i) If the UE receives a MODIFY EPS BEARER CONTEXT REQUEST message which includes an unassigned or reserved EPS bearer identity value or an assigned EPS bearer identity value that does not match an existing EPS bearer context, the UE shall respond with a MODIFY EPS BEARER CONTEXT REJECT message including ESM cause #43 "invalid EPS bearer identity".

j) If the UE receives a DEACTIVATE EPS BEARER CONTEXT REQUEST message which includes an unassigned or reserved EPS bearer identity value or an assigned EPS bearer identity value that does not match an existing EPS bearer context, the UE shall respond with a DEACTIVATE EPS BEARER CONTEXT ACCEPT message with the EPS bearer identity set to the received EPS bearer identity.

k) If the UE receives an ESM message other than those listed in items a through j 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 #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 #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 #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, b, c, or d, the UE shall return a status message (EMM STATUS or ESM STATUS depending on the PD) with cause #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 e, f, g or h, 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 #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

The following UE procedures shall apply for handling an error encountered with a mandatory information element in an ESM message:

a) If the message is an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST, an ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message with ESM cause #96 "invalid mandatory information", shall be returned.

b) If the message is an ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST, an ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT message with ESM cause #96 "invalid mandatory information", shall be returned.

c) If the message is a MODIFY EPS BEARER CONTEXT REQUEST, a MODIFY EPS BEARER CONTEXT REJECT message with ESM cause #96 "invalid mandatory information", shall be returned.

d) 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.

The following network procedures shall apply for handling an error encountered with a mandatory information element in an ESM message:

e) If the message is a PDN CONNECTIVITY REQUEST, a PDN CONNECTIVITY REJECT message with ESM cause #96 "invalid mandatory information", shall be returned.

f) If the message is a PDN DISCONNECT REQUEST, a PDN DISCONNECT REJECT message with ESM cause #96 "invalid mandatory information", shall be returned.

g) If the message is a BEARER RESOURCE ALLOCATION REQUEST, a BEARER RESOURCE ALLOCATION REJECT message with ESM cause #96 "invalid mandatory information", shall be returned.

h) If the message is a BEARER RESOURCE MODIFICATION REQUEST, a BEARER RESOURCE MODIFICATION REJECT message with ESM cause #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 #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 #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 #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, LV and LV-E 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, LV-E 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

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 9.9.2.9	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	5-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 9.9.2.8	O	TLV	5-47
34	Emergency number list	Emergency number list 9.9.3.37	O	TLV	5-50
64	EPS network feature support	EPS network feature support 9.9.3.12A	O	TLV	3
F-	Additional update result	Additional update result 9.9.3.0A	O	TV	1

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.

8.2.1.9 Emergency number list

This IE may be sent by the network. If this IE is sent, the contents of this IE indicates a list of emergency numbers valid within the same MCC as in the cell on which this IE is received.

8.2.1.10 EPS network feature support

The network may include this IE to inform the UE of the support of certain features. If this IE is not included then the UE shall interpret this as a receipt of an information element with all bits of the value part coded as zero.

8.2.1.11 Additional update result

The network may include this IE to provide the UE with additional information about the result of a combined attach procedure if the procedure was successful for EPS services and non-EPS services, or for EPS services and "SMS only".

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	5-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	6-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
	EPS mobile identity	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	5-n
19	Old P-TMSI signature	P-TMSI signature 10.5.5.8	O	TV	4
50	Additional GUTI	EPS mobile identity 9.9.3.12	O	TLV	13
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 9.9.2.10	O	TLV	5-n
F-	Additional update type	Additional update type 9.9.3.0B	O	TV	1
5D	Voice domain preference and UE's usage setting	Voice domain preference and UE's usage setting 9.9.3.44	O	TLV	3

8.2.4.2 Old P-TMSI signature

The UE shall include this IE if the UE holds a valid P-TMSI signature, P-TMSI and RAI, and the TIN either indicates "P-TMSI" or is deleted.

8.2.4.3 Additional GUTI

The UE shall include this IE if the TIN indicates "P-TMSI" and the UE holds a valid GUTI, P-TMSI and RAI.

8.2.4.4 Last visited registered TAI

This IE shall be included if the UE holds a valid last visited registered TAI.

8.2.4.5 DRX parameter

This IE is included if UE supports A/Gb mode or Iu mode or if the UE wants to indicate its UE specific DRX parameters to the network.

8.2.4.6 MS network capability

A UE supporting A/Gb mode or Iu mode shall include this IE to indicate its capabilities to the network.

8.2.4.7 Old location area identification

The UE shall include this IE during a combined attach procedure if it has a valid location area identification.

8.2.4.8 TMSI status

The UE shall include this IE during combined attach procedure if it has no valid TMSI available.

8.2.4.9 Mobile station classmark 2

This IE shall be included if the UE supports SRVCC to GERAN or UTRAN (see 3GPP TS 23.216 [8]), or if the UE is performing a combined attach procedure.

8.2.4.10 Mobile station classmark 3

This IE shall be included if the UE supports SRVCC to GERAN.

8.2.4.11 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.

8.2.4.12 Additional update type

The UE shall include this IE if the UE requests "SMS only".

8.2.4.13 Voice domain preference and UE's usage setting

This IE shall be included if the UE supports CS fallback and SMS over SGs, or if the UE is configured to support IMS voice, but does not support 1xCS fallback.

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 #21 "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 9.9.2.9	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 CS service notification

8.2.9.1 Message definition

This message is sent by the network when a paging request with CS call indicator was received via SGs for a UE, and a NAS signalling connection is already established for the UE. See table 8.2.9.1.

Message type: CS SERVICE NOTIFICATION

Significance: dual

Direction: network to UE

Table 8.2.9.1: CS SERVICE NOTIFICATION 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
	CS service notification message identity	Message type 9.8	M	V	1
	Paging identity	Paging identity 9.9.3.25A	M	V	1
60	CLI	CLI 9.9.3.38	O	TLV	3-14
61	SS Code	SS Code 9.9.3.39	O	TV	2
62	LCS indicator	LCS indicator 9.9.3.40	O	TV	2
63	LCS client identity	LCS client identity 9.9.3.41	O	TLV	3-257

8.2.9.2 CLI

The network shall send this IE if it was received via SGs. It contains the identification of the calling line for the mobile terminating call in the CS domain, which triggered the paging via SGs.

8.2.9.3 SS Code

The network shall send this IE if it was received via SGs. It contains information on the supplementary service transaction in the CS domain, which triggered the paging via SGs.

8.2.9.4 LCS indicator

The network shall send this IE if it was received via SGs. It indicates that the paging was triggered by a terminating LCS request in the CS domain.

8.2.9.5 LCS client identity

The network shall send this IE if received via SGs. It contains information related to the requestor of the terminating LCS request in the CS domain.

8.2.10 Detach accept

8.2.10.1 Detach accept (UE originating detach)

This message is sent by the network to indicate that the detach procedure has been completed. See table 8.2.10.1.1.

Message type: DETACH ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.10.1.1: 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

8.2.10.2 Detach accept (UE terminated detach)

This message is sent by the UE to indicate that the detach procedure has been completed. See table 8.2.10.2.1.

Message type: DETACH ACCEPT

Significance: dual

Direction: UE to network

Table 8.2.10.2.1: 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

8.2.11 Detach request

8.2.11.1 Detach request (UE originating detach)

This message is sent by the UE to request the release of an EMM context. See table 8.2.11.1.1.

Message type: DETACH REQUEST

Significance: dual

Direction: UE to network

Table 8.2.11.1.1: 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
	NAS key set identifier	NAS key set identifier 9.9.3.21	M	V	1/2
	EPS mobile identity	EPS mobile identity 9.9.3.12	M	LV	5-12

8.2.11.2 Detach request (UE terminated detach)

8.2.11.2.1 Message definition

This message is sent by the network to request the release of an EMM context. See table 8.2.11.2.1.

Message type: DETACH REQUEST

Significance: dual

Direction: network to UE

Table 8.2.11.2.1: 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 9.9.2.9	M	V	1/2
53	EMM cause	EMM cause 9.9.3.9	O	TV	2

8.2.11.2.2 EMM cause

This information element is included if an EMM cause is provided.

8.2.12 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 8.2.12.1.

Message type: DOWNLINK NAS TRANSPORT

Significance: dual

Direction: network to UE

Table 8.2.12.1: 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

8.2.13 EMM information

8.2.13.1 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 8.2.13.1.

Message type: EMM INFORMATION

Significance: local

Direction: network to UE

Table 8.2.13.1: 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-n
45	Short name for network	Network name 9.9.3.24	O	TLV	3-n
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

8.2.13.2 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.

8.2.13.3 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.

8.2.13.4 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.

8.2.13.5 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.

8.2.13.6 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.

8.2.14 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 8.2.14.1.

Message type: EMM STATUS

Significance: local

Direction: both

Table 8.2.14.1: 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

8.2.15 Extended service request

8.2.15.1 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 8.2.15.1.

Message type: EXTENDED SERVICE REQUEST

Significance: dual

Direction: UE to network

Table 8.2.15.1: 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
57	EPS bearer context status	EPS bearer context status 9.9.2.1	O	TLV	4

8.2.15.2 CSFB response

The UE shall include this IE only if the Service type information element indicates "mobile terminating CS fallback or 1xCS fallback".

8.2.15.3 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.

8.2.16 GUTI reallocation command

8.2.16.1 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 8.2.16.1.

Message type: GUTI REALLOCATION COMMAND

Significance: dual

Direction: network to UE

Table 8.2.16.1: 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

8.2.16.2 TAI list

This IE may be included to assign a TAI list to the UE.

8.2.17 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 8.2.17.1.

Message type: GUTI REALLOCATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.17.1: 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

8.2.18 Identity request

This message is sent by the network to the UE to request the UE to provide the specified identity. See table 8.2.18.1.

Message type: IDENTITY REQUEST

Significance: dual

Direction: network to UE

Table 8.2.18.1: 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 9.9.2.9	M	V	1/2

8.2.19 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 8.2.19.1.

Message type: IDENTITY RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.19.1: 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

8.2.20 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	NAS key set identifier 9.9.3.21	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	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 9.9.2.9	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 9.9.2.8	O	TLV	5-47
34	Emergency number list	Emergency number list 9.9.3.37	O	TLV	5-50
64	EPS network feature support	EPS network feature support 9.9.3.12A	O	TLV	3
F-	Additional update result	Additional update result 9.9.3.0A	O	TV	1

8.2.26.2 T3412 value

The MME shall include this IE during normal and combined tracking area updating procedure, and may include this IE during periodic tracking area updating procedure.

If this IE is not included, the UE shall use the value currently stored, e.g. from a prior ATTACH ACCEPT or TRACKING AREA UPDATE 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.

8.2.26.12 Emergency number list

This IE may be sent by the network. If this IE is sent, the contents of this IE indicates a list of emergency numbers valid within the same MCC as in the cell on which this IE is received.

8.2.26.13 EPS network feature support

The network may include this IE to inform the UE of the support of certain features. If this IE is not included then the UE shall interpret this as a receipt of an information element with all bits of the value part coded as zero.

8.2.26.14 Additional EPS result

The network may include this IE to provide the UE with additional information about the result of a combined tracking area updating procedure if the procedure was successful for EPS services and non-EPS services, or for EPS services and "SMS only".

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 or a new TMSI has been assigned. 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
	NAS key set identifier	NAS key set identifier 9.9.3.21	M	V	1/2
	Old GUTI	EPS mobile identity 9.9.3.12	M	LV	12
B-	Non-current native NAS key set identifier	NAS key set identifier 9.9.3.21	O	TV	1
8-	GPRS ciphering key sequence number	Ciphering key sequence number 9.9.3.4a	O	TV	1
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 9.9.2.10	O	TLV	5-n
F-	Additional update type	Additional update type 9.9.3.0B	O	TV	1
5D	Voice domain preference and UE's usage setting	Voice domain preference and UE's usage setting 9.9.3.44	O	TLV	3

8.2.29.2 Non-current native NAS key set identifier

The UE shall include this IE if the UE has a valid non-current native EPS security context when the UE performs an A/Gb mode or Iu mode to S1 mode inter-system change in EMM-CONNECTED mode and the UE uses a mapped EPS security context to protect the TRACKING AREA UPDATE REQUEST message.

8.2.29.3 GPRS ciphering key sequence number

The UE shall include this IE if the UE performs an A/Gb mode or Iu mode to S1 mode inter-system change in EMM-IDLE mode and the TIN indicates "P-TMSI".

8.2.29.4 Old P-TMSI signature

The UE shall include this IE if the TIN indicates "P-TMSI" and the UE holds a valid P-TMSI signature, P-TMSI and RAI.

8.2.29.5 Additional GUTI

The UE shall include this IE if the TIN indicates "P-TMSI" and the UE holds a valid GUTI, P-TMSI and RAI.

8.2.29.6 $Nonce_{UE}$

This IE is included if the UE performs an A/Gb mode or Iu mode to S1 mode inter-system change in idle mode.

8.2.29.7 UE network capability

The UE shall include this IE, unless the UE performs a periodic tracking area updating procedure.

8.2.29.8 Last visited registered TAI

This IE shall be included if the UE holds a valid last visited registered TAI.

8.2.29.9 DRX parameter

This IE is included by the UE to indicate a change of UE specific DRX parameters to the network.

8.2.29.10 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.

8.2.29.11 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.

8.2.29.12 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.

8.2.29.13 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.

8.2.29.14 TMSI status

The UE shall include this IE during a combined tracking area updating procedure if it has no valid TMSI available.

8.2.29.15 Mobile station classmark 2

This IE shall be included if the UE supports SRVCC to GERAN or UTRAN (see 3GPP TS 23.216 [8]), or if the UE is performing a combined tracking area updating procedure.

8.2.29.16 Mobile station classmark 3

This IE shall be included if the UE supports SRVCC to GERAN.

8.2.29.17 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.

8.2.29.18 Additional update type

The UE shall include this IE if the UE requests "SMS only".

8.2.29.19 Voice domain preference and UE's usage setting

This IE shall be included if the UE supports CS fallback and SMS over SGs, or if the UE is configured to support IMS voice, but does not support 1xCS fallback.

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

8.2.31 Downlink generic NAS transport

8.2.31.1 Message definition

This message is sent by the network to the UE in order to carry an application message in encapsulated format. See table 8.2.31.1.

Message type: DOWNLINK GENERIC NAS TRANSPORT

Significance: dual

Direction: network to UE

Table 8.2.31.1: DOWNLINK GENERIC 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 generic NAS transport message identity	Message type 9.8	M	V	1
	Generic message container type	Generic message container type 9.9.3.42	M	V	1
	Generic message container	Generic message container 9.9.3.43	M	LV-E	3-n
65	Additional information	Additional information 9.9.2.0	O	TLV	3-n

8.2.31.2 Additional information

The MME may include this information element if the application wants to send any additional information.

8.2.32 Uplink generic NAS transport

8.2.32.1 Message definition

This message is sent by the UE to the network in order to carry an application protocol message in encapsulated format. See table 8.2.32.1.

Message type: UPLINK GENERIC NAS TRANSPORT

Significance: dual

Direction: UE to network

Table 8.2.32.1: UPLINK GENERIC 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 generic NAS transport message identity	Message type 9.8	M	V	1
	Generic message container type	Generic message container type 9.9.3.42	M	V	1
	Generic message container	Generic message container 9.9.3.43	M	LV-E	3-n
65	Additional information	Additional information 9.9.2.0	O	TLV	3-n

8.2.32.2 Additional information

The UE may include this information element if the application wants to send any additional information.

8.3 EPS session management messages

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 9.9.2.9	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

8.3.3.2 Transaction identifier

If the UE supports A/Gb mode or Iu mode or both, a network supporting mobility from S1 mode to A/Gb mode or Iu mode or both shall include this IE

8.3.3.3 Negotiated QoS

If the UE supports A/Gb mode or Iu mode or both, a network supporting mobility from S1 mode to A/Gb mode or Iu mode or both shall include the corresponding R99 QoS parameter values of a PDP context.

8.3.3.4 Negotiated LLC SAPI

If the UE supports A/Gb mode, a network supporting mobility from S1 mode to A/Gb mode shall include this IE.

8.3.3.5 Radio priority

If the UE supports A/Gb mode, a network supporting mobility from S1 mode to A/Gb mode shall include this IE.

8.3.3.6 Packet flow identifier

If the UE supports A/Gb mode and BSS packet flow procedures, a network supporting mobility from S1 mode to A/Gb mode shall 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
	PDN address	PDN address 9.9.4.9	M	LV	6-14
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

8.3.6.2 Transaction identifier

If the UE supports A/Gb mode or Iu mode or both, a network supporting mobility from S1 mode to A/Gb mode or Iu mode or both shall include this IE.

8.3.6.3 Negotiated QoS

If the UE supports A/Gb mode or Iu mode or both, a network supporting mobility from S1 mode to A/Gb mode or Iu mode or both shall include the corresponding R99 QoS parameter values of a PDP context.

8.3.6.4 Negotiated LLC SAPI

If the UE supports A/Gb mode, a network supporting mobility from S1 mode to A/Gb mode shall include this IE.

8.3.6.5 Radio priority

If the UE supports A/Gb mode, a network supporting mobility from S1 mode to A/Gb mode shall include this IE.

8.3.6.6 Packet flow identifier

If the UE supports A/Gb mode and BSS packet flow procedures, a network supporting mobility from S1 mode to A/Gb mode shall include this IE.

8.3.6.7 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.

8.3.6.8 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.

8.3.6.9 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.

8.3.7 Bearer resource allocation reject

8.3.7.1 Message definition

This message is sent by the network to the UE to reject the allocation of a dedicated bearer resource. See table 8.3.7.1.

Message type: BEARER RESOURCE ALLOCATION REJECT

Significance: dual

Direction: network to UE

Table 8.3.7.1: BEARER RESOURCE ALLOCATION 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 allocation 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 allocation request

8.3.8.1 Message definition

This message is sent by the UE to the network to request the allocation of a dedicated bearer resource. See table 8.3.8.1.

Message type: BEARER RESOURCE ALLOCATION REQUEST

Significance: dual

Direction: UE to network

Table 8.3.8.1: BEARER RESOURCE ALLOCATION 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 allocation 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 9.9.2.9	M	V	1/2
	Traffic flow aggregate	Traffic flow aggregate description 9.9.4.15	M	LV	2-256
	Required traffic flow QoS	EPS quality of service 9.9.4.3	M	LV	2-10
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.8.2 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.

8.3.9 Bearer resource modification reject

8.3.9.1 Message definition

This message is sent by the network to the UE to reject the modification of a dedicated bearer resource. See table 8.3.9.1.

Message type: BEARER RESOURCE MODIFICATION REJECT

Significance: dual

Direction: network to UE

Table 8.3.9.1: 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

8.3.9.2 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.

8.3.10 Bearer resource modification request

8.3.10.1 Message definition

This message is sent by the UE to the network to request the modification of a dedicated bearer resource. See table 8.3.10.1.

Message type: BEARER RESOURCE MODIFICATION REQUEST

Significance: dual

Direction: UE to network

Table 8.3.10.1: 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
	EPS bearer identity for packet filter	Linked EPS bearer identity 9.9.4.6	M	V	1/2
	Spare half octet	Spare half octet 9.9.2.9	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

8.3.10.2 Required traffic flow QoS

This IE is included in the message when the UE requests a change of QoS for the indicated traffic flows.

8.3.10.3 ESM cause

This IE is included in the message when the UE requests the release of a dedicated bearer resource.

8.3.10.4 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.

8.3.11 Deactivate EPS bearer context accept

8.3.11.1 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 8.3.11.1.

Message type: DEACTIVATE EPS BEARER CONTEXT ACCEPT

Significance: dual

Direction: UE to network

Table 8.3.11.1: 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

8.3.11.2 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.

8.3.12 Deactivate EPS bearer context request

8.3.12.1 Message definition

This message is sent by the network to request deactivation of an active EPS bearer context. See table 8.3.12.1.

Message type: DEACTIVATE EPS BEARER CONTEXT REQUEST

Significance: dual

Direction: network to UE

Table 8.3.12.1: 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

8.3.12.2 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.

8.3.13 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 8.3.13.1.

Message type: ESM INFORMATION REQUEST

Significance: dual

Direction: network to UE

Table 8.3.13.1: 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

8.3.14 ESM information response

8.3.14.1 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 8.3.14.1.

Message type: ESM INFORMATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.3.14.1: 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

8.3.14.2 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.

8.3.14.3 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.

8.3.15 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 8.3.15.1.

Message type: ESM STATUS

Significance: dual

Direction: both

Table 8.3.15.1: 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

8.3.16 Modify EPS bearer context accept

8.3.16.1 Message definition

This message is sent by the UE to the network to acknowledge the modification of an active EPS bearer context. See table 8.3.16.1.

Message type: MODIFY EPS BEARER CONTEXT ACCEPT

Significance: dual

Direction: UE to network

Table 8.3.16.1: 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

8.3.16.2 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.

8.3.17 Modify EPS bearer context reject

8.3.17.1 Message definition

This message is sent by the UE or the network to reject a modification of an active EPS bearer context. See table 8.3.17.1.

Message type: MODIFY EPS BEARER CONTEXT REJECT

Significance: dual

Direction: UE to network

Table 8.3.17.1: 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

8.3.17.2 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 Modify EPS bearer context request

8.3.18.1 Message definition

This message is sent by the network to the UE to request modification of an active EPS bearer context. See table 8.3.18.1.

Message type: MODIFY EPS BEARER CONTEXT REQUEST

Significance: dual

Direction: network to UE

Table 8.3.18.1: 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

8.3.18.2 New EPS QoS

When the EPS QoS of the EPS bearer context is modified, the network shall include the modified EPS QoS assigned to the EPS bearer context.

8.3.18.3 TFT

This IE provides the UE with packet filters.

8.3.18.4 New QoS

If the UE supports A/Gb mode or Iu mode or both and when the corresponding R99 QoS of the EPS bearer context is modified, a network supporting mobility from S1 mode to A/Gb mode or Iu mode or both shall include the corresponding R99 QoS parameter values of a PDP context.

8.3.18.5 Negotiated LLC SAPI

If the UE supports A/Gb mode and when the negotiated LLC SAPI is modified, a network supporting mobility from S1 mode to A/Gb mode shall include this IE.

8.3.18.6 Radio priority

If the UE supports A/Gb mode and when the radio priority is modified, a network supporting mobility from S1 mode to A/Gb mode shall include this IE.

8.3.18.7 Packet flow identifier

If the UE supports A/Gb mode and BSS packet flow procedures, a network supporting mobility from S1 mode to A/Gb mode shall include this IE.

8.3.18.8 APN-AMBR

This IE is included when the APN-AMBR has been changed by the network.

8.3.18.9 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.

8.3.18A Notification

This message is sent by the network to inform the UE about events which are relevant for the upper layer using an EPS bearer context or having requested a procedure transaction. See table 8.3.18A.1.

Message type: NOTIFICATION

Significance: local

Direction: network to UE

Table 8.3.18A.1: NOTIFICATION 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
	Notification message identity	Message type 9.8	M	V	1
	Notification indicator	Notification indicator 9.9.4.7A	M	LV	2

8.3.19 PDN connectivity reject

8.3.19.1 Message definition

This message is sent by the network to the UE to reject establishment of a PDN connection. See table 8.3.19.1.

Message type: PDN CONNECTIVITY REJECT

Significance: dual

Direction: network to UE

Table 8.3.19.1: 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

8.3.19.2 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.

8.3.20 PDN connectivity request

8.3.20.1 Message definition

This message is sent by the UE to the network to initiate establishment of a PDN connection. See table 8.3.20.1.

Message type: PDN CONNECTIVITY REQUEST

Significance: dual

Direction: UE to network

Table 8.3.20.1: 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

8.3.20.2 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.

8.3.20.3 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.

8.3.20.4 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.

8.3.21 PDN disconnect reject

8.3.21.1 Message definition

This message is sent by the network to the UE to reject release of a PDN connection. See table 8.3.21.1.

Message type: PDN DISCONNECT REJECT

Significance: dual

Direction: network to UE

Table 8.3.21.1: 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

8.3.21.2 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.

8.3.22 PDN disconnect request

8.3.22.1 Message definition

This message is sent by the UE to the network to initiate release of a PDN connection. See table 8.3.22.1.

Message type: PDN DISCONNECT REQUEST

Significance: dual

Direction: UE to network

Table 8.3.22.1: 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 9.9.2.9	M	V	1/2
27	Protocol configuration options	Protocol configuration options 9.9.4.11	O	TLV	3-253

8.3.22.2 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.

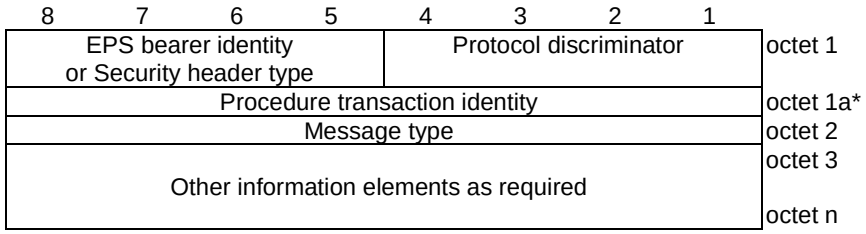


Figure 9.1.1: General message organization example for a plain NAS message

The organization of a security protected NAS message is illustrated in the example shown in figure 9.1.2.

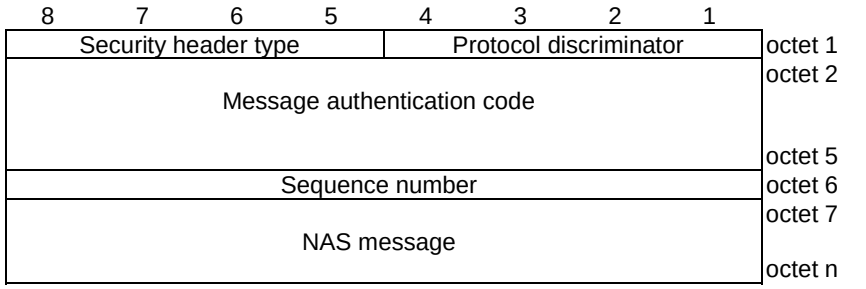


Figure 9.1.2: General message organization example for a security protected NAS message

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]. The protocol discriminator in the header (see 3GPP TS 24.007 [12]) of a security protected NAS message is encoded as "EPS mobility management messages".

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 MAC IE shall be included in the security protected NAS message if a valid NAS security context exists and security functions are started. The usage of MAC is specified in subclause 4.4.3.3.

9.6 Sequence number

This IE includes the NAS message sequence number (SN) which consists of the eight least significant bits of the NAS COUNT for a security protected NAS message The usage of SN is specified in subclause 4.4.3.

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
0	1	1	0	0	1	0	0	CS Service notification
0	1	1	0	1	0	0	0	Downlink generic NAS transport
0	1	1	0	1	0	0	1	Uplink generic 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 allocation request
1	1	0	1	0	1	0	1	Bearer resource allocation reject
1	1	0	1	0	1	1	0	Bearer resource modification request
1	1	0	1	0	1	1	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	0	1	1	0	1	1	Notification
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, LV-E, 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 definitions of information elements which are common for the EMM and ESM protocols or which are used by access stratum 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

9.9.2.0 Additional information

The purpose of the Additional information information element is to provide additional information to upper layers in relation to the generic NAS message transport mechanism.

The Additional information information element is coded as shown in figure 9.9.2.0.1 and table 9.9.2.0.1.

The Additional information is a type 4 information element with a minimum length of 3 octets.

8	7	6	5	4	3	2	1	
Additional information IEI								octet 1
Additional information length								octet 2
Additional information value								octets 3-n

Figure 9.9.2.0.1: Additional information information element

Table 9.9.2.0.1: Additional information information element

Additional information value (octet 3 to octet n) The coding of the additional information value is dependent on the generic message container type.

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 NAS security parameters from E-UTRA

The purpose of the NAS security parameters from E-UTRA information element is to provide the UE with information that enables the UE to create a mapped UMTS security context.

The NAS security parameters from E-UTRA information element is coded as shown in figure 9.9.2.6.1 and table 9.9.2.6.1.

The NAS security parameters from E-UTRA is a type 3 information element with a length of 2 octets.

The value part of the NAS security parameters from E-UTRA information element is included in specific information elements within some RRC messages sent to the UE; see 3GPP TS 36.331 [22]. For these cases the coding of the information element identifier and length information is defined in 3GPP TS 36.331 [22].

8	7	6	5	4	3	2	1	
NAS security parameters to E-UTRA IEI								octet 1
0	0	0	0	DL NAS COUNT value (short)				octet 2
Spare								

Figure 9.9.2.6.1: NAS security parameters from E-UTRA information element

Table 9.9.2.6.1: NAS security parameters from E-UTRA information element

DL NAS COUNT value (short) (octet 2, bit 1 to 4) This field contains the 4 least significant bits of the binary representation of the downlink NAS COUNT value applicable when this information element is sent.

9.9.2.7 NAS security parameters to E-UTRA

The purpose of the NAS security parameters to E-UTRA information element is to provide the UE with parameters that enable the UE to create a mapped EPS security context and take this context into use after inter-system handover to S1 mode.

The NAS security parameters to E-UTRA information element is coded as shown in figure 9.9.2.7.1 and table 9.9.2.7.1.

The NAS security parameters to E-UTRA is a type 3 information element with a length of 7 octets.

The value part of the NAS security parameters to E-UTRA information element is included in specific information elements within some RRC messages sent to the UE; see 3GPP TS 36.331 [22]. For these cases the coding of the information element identifier and length information is defined in 3GPP TS 36.331 [22].

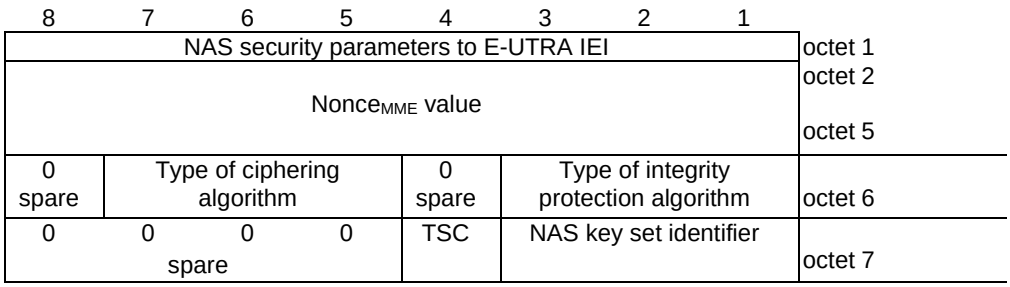


Figure 9.9.2.7.1: NAS security parameters to E-UTRA information element

Table 9.9.2.7.1: NAS security parameters to E-UTRA information element

Nonce$_{MME}$ value (octet 2 to 5) This field is coded as the nonce value in the Nonce information element (see subclause 9.9.3.25). Type of integrity protection algorithm (octet 6, bit 1 to 3) and type of ciphering algorithm (octet 6, bit 5 to 7) These fields are coded as the type of integrity protection algorithm and type of ciphering algorithm in the NAS security algorithms information element (see subclause 9.9.3.23). Bit 4 and 8 of octet 6 are spare and shall be coded as zero. NAS key set identifier (octet 7, bit 1 to 3) and type of security context flag (TSC) (octet 7, bit 4) These fields are coded as the NAS key set identifier and type of security context flag in the NAS key set identifier information element (see subclause 9.9.3.21). Bit 5 to 8 of octet 7 are spare and shall be coded as zero.

9.9.2.8 PLMN list

See subclause 10.5.1.13 in 3GPP TS 24.008 [13].

9.9.2.9 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.

9.9.2.10 Supported codec list

See subclause 10.5.4.32 in 3GPP TS 24.008 [13].

9.9.3 EPS Mobility Management (EMM) information elements

9.9.3.0A Additional update result

The purpose of the Additional update result information element is to provide additional information about the result of a combined attach procedure or a combined tracking area updating procedure.

The Additional update result information element is coded as shown in figure 9.9.3.0A.1 and table 9.9.3.0A.1.

The Additional update result is a type 1 information element.

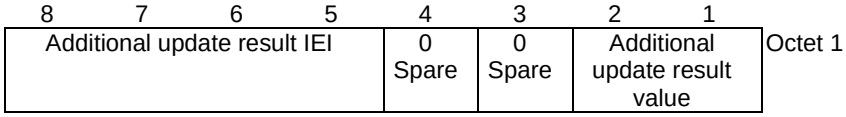


Figure 9.9.3.0A.1: Additional update result information element

Table 9.9.3.0A.1: Additional update result information element

Additional update result value (octet 1) Bits **2 1** 0 0 no additional information 0 1 CS Fallback not preferred 1 0 SMS only 1 1 reserved Bits 4 and 3 of octet 1 are spare and shall all be coded as zero.

9.9.3.0B Additional update type

The purpose of the Additional update type information element is to provide additional information about the type of request for a combined attach or a combined tracking area updating procedure.

The Additional update type information element is coded as shown in figure 9.9.3.0B.1 and table 9.9.3.0B.1.

The Additional update type is a type 1 information element.

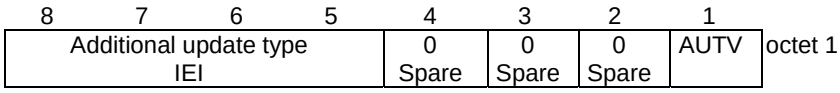


Figure 9.9.3.0B.1: Additional update type information element

Table 9.9.3.0B.1: Additional update type information element

Additional update type value (AUTV) (octet 1) Bit **1** 0 No additional information. If received it shall be interpreted as request for combined attach or combined tracking area updating. 1 SMS only Bits 4 to 2 of octet 1 are spare and shall be all coded as zero.

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.

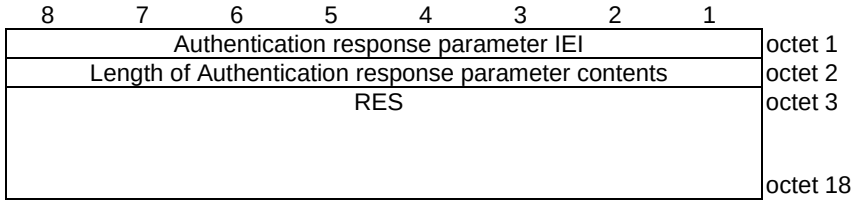


Figure 9.9.3.4.1: Authentication response parameter information element

Table 9.9.3.4.1: Authentication response parameter information element

RES value (octet 3 to 18) This contains the RES.

9.9.3.4A Ciphering key sequence number

See subclause 10.5.1.2 in 3GPP TS 24.008 [13].

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.

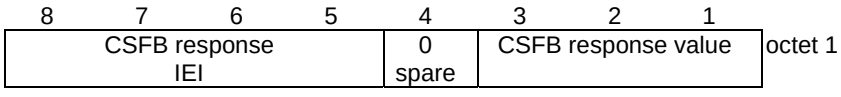


Figure 9.9.3.5.1: CSFB response information element

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.

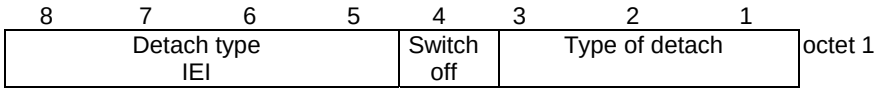


Figure 9.9.3.7.1: Detach type information element

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
1	1	0	reserved
1	1	1	reserved

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
1	1	0	reserved
1	1	1	reserved

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.

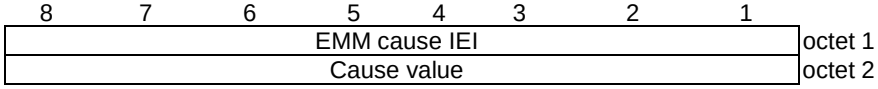


Figure 9.9.3.9.1: EMM cause information element

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	0	1	IMEI not accepted
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	0	1	1	0	1	0	Non-EPS authentication unacceptable
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.

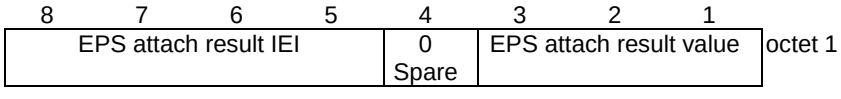


Figure 9.9.3.10.1: EPS attach result information element

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.

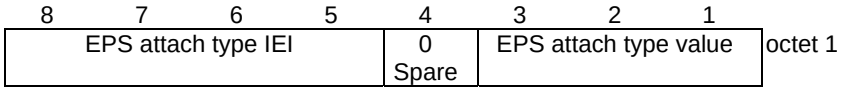


Figure 9.9.3.11.1: EPS attach type information element

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
1	1	0	EPS emergency attach
1	1	1	reserved
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, the GUTI or the IMEI.

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.

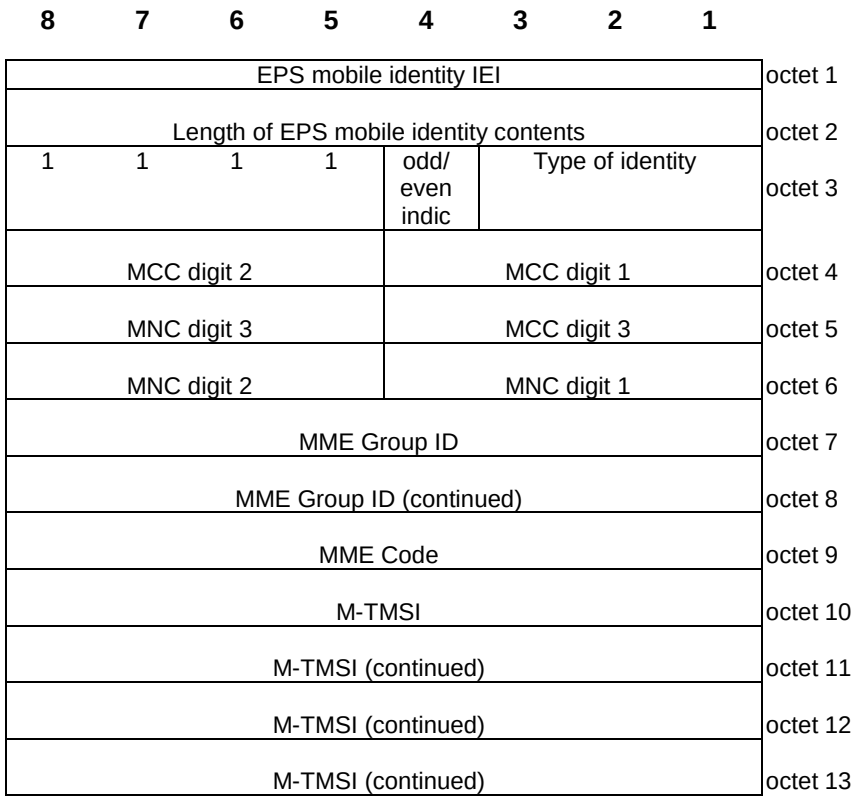


Figure 9.9.3.12.1: EPS mobile identity information element for type of identity "GUTI"

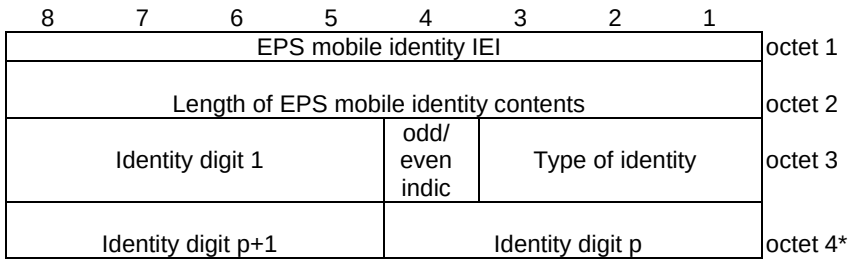


Figure 9.9.3.12.2: EPS mobile identity information element for type of identity "IMSI" or "IMEI"

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
0	1	1	IMEI

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 4, octet 5 bits 1 to 4)

The MCC field is coded as in ITU-T Recommendation E.212 [30], annex A.

MNC, Mobile network code (octet 5 bits 5 to 8, octet 6)

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 5 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].

For the IMEI, this field is coded using BCD coding. The format of the IMEI is described in 3GPP TS 23.003 [2].

9.9.3.12A EPS network feature support

The purpose of the EPS network feature support information element is to indicate whether certain features are supported by the network.

The EPS network feature support information element is coded as shown in figure 9.9.3.12A.1 and table 9.9.3.12A.1.

The EPS network feature support is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
EPS network feature support IEI								octet 1
Length of EPS network feature support contents								octet 2
0	0	0	CS-LCS		EPC-LCS	EMC BS	IMS VoPS	octet 3
Spare								

Figure 9.9.3.12A.1: EPS network feature support information element

Table 9.9.3.12A.1: EPS network feature support information element

IMS voice over PS session indicator (IMS VoPS) (octet 3, bit 1) Bit **1** 0 IMS voice over PS session in S1 mode not supported 1 IMS voice over PS session in S1 mode supported Emergency bearer services indicator (EMC BS) (octet 3, bit 2) Bit **2** 0 emergency bearer services in S1 mode not supported 1 emergency bearer services in S1 mode supported Location services indicator in EPC (EPC-LCS) (octet 3, bit 3) Bit **3** 0 location services via EPC not supported 1 location services via EPC supported Location services indicator in CS (CS-LCS) (octet 3, bit 4 to 5) Bit **5 4** 0 0 no information about support of location services via CS domain is available 0 1 location services via CS domain supported 1 0 location services via CS domain not supported 1 1 reserved Bits 6 to 8 of octet 3 are spare and shall be coded all zero.

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 result information element is coded as shown in figure 9.9.3.13.1 and table 9.9.3.13.1.

The EPS update result is a type 1 information element.

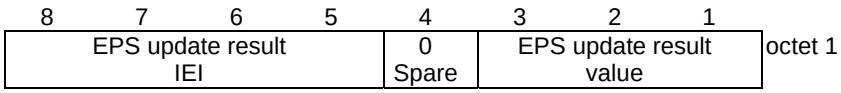


Figure 9.9.3.13.1: EPS update result information element

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.

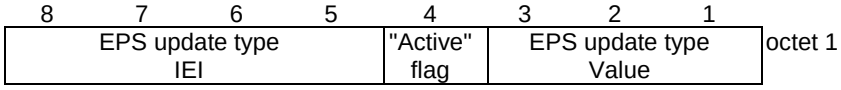


Figure 9.9.3.14.1: EPS update type information element

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 1 0 0 unused; shall be interpreted as "TA updating", if received by the network. 1 0 1 unused; shall be interpreted as "TA updating", if received by the network. 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.

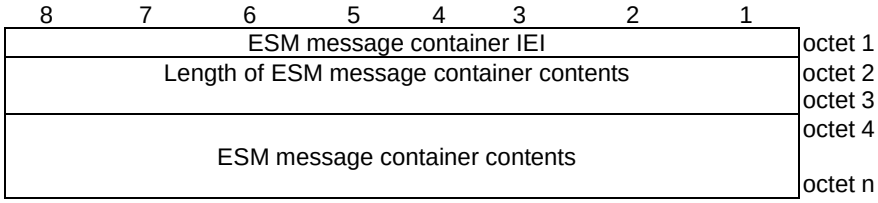


Figure 9.9.3.15.1: ESM message container information element

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) value of the current EPS security context 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.

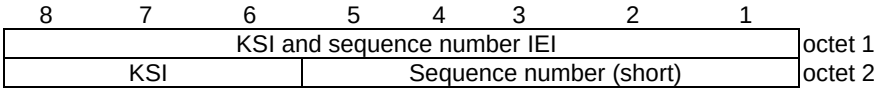


Figure 9.9.3.19.1: KSI and sequence number information element

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 (octet 2, bit 6 to 8) This field contains the key set identifier value, as specified in bit 1 to 3 of octet 1 of the NAS key set identifier information element. (see subclause 9.9.3.21.)

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.

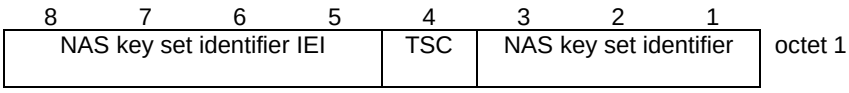


Figure 9.9.3.21.1: NAS key set identifier information element

Table 9.9.3.21.1: NAS key set identifier information element

Type of security context flag (TSC) (octet 1) Bit **4** 0 native security context (for KSI_{ASME}) 1 mapped security context (for KSI_{SGSN}) 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 (UE to network); reserved (network to UE)

9.9.3.22 NAS message container

This information element is used to encapsulate the SMS messages transferred between the UE and the network.The NAS message container information element is coded as shown in figure 9.9.3.22.1 and table 9.9.3.22.1.

The NAS message container is a type 4 information element with a minimum length of 4 octets and a maximum length of 253 octets.

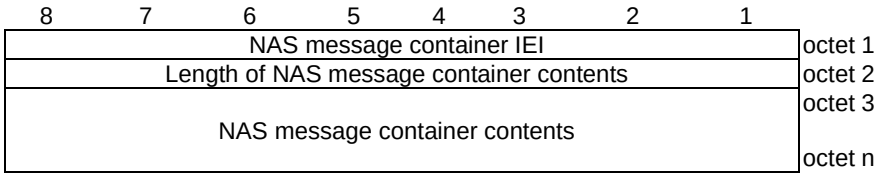


Figure 9.9.3.22.1: NAS message container information element

Table 9.9.3.22.1: NAS message container information element

NAS message container contents (octet 3 to octet n) This IE can contain an SMS message (i.e. CP-DATA, CP-ACK or CP-ERROR) as defined in subclause 7.2 in 3GPP TS 24.011 [13A].

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.

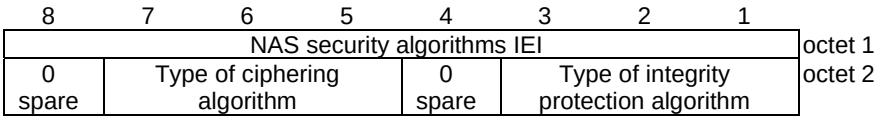


Figure 9.9.3.23.1: NAS security algorithms information element

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 EPS integrity algorithm EIA0 (null integrity protection algorithm) 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 EEA0 (null ciphering algorithm) 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.

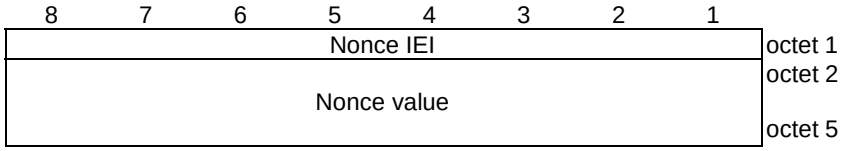


Figure 9.9.3.25.1: Nonce information element

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.

9.9.3.25A Paging identity

The purpose of the Paging identity information element is to indicate the identity used for paging for non-EPS services.

The Paging identity information element is coded as shown in figure 9.9.3.25A.1 and table 9.9.3.25A.1.

The Paging identity is a type 3 information element with 2 octets length.

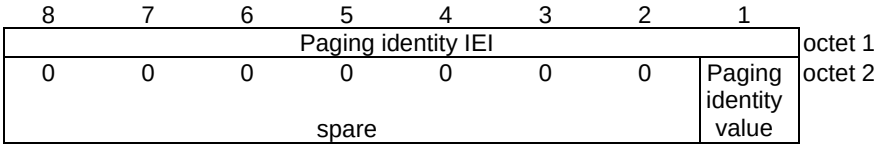


Figure 9.9.3.25A.1: Paging identity information element

Table 9.9.3.25A.1: Paging identity information element

Paging identity value (octet 2) Bit **1** 0 IMSI 1 TMSI

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.

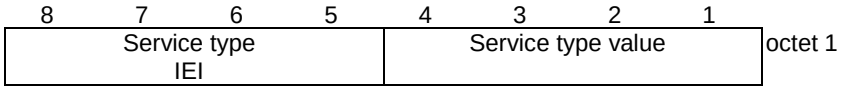


Figure 9.9.3.27.1: Service type information element

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 or 1xCS fallback 0 0 0 1 mobile terminating CS fallback or 1xCS fallback 0 0 1 0 mobile originating CS fallback emergency call or 1xCS 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.

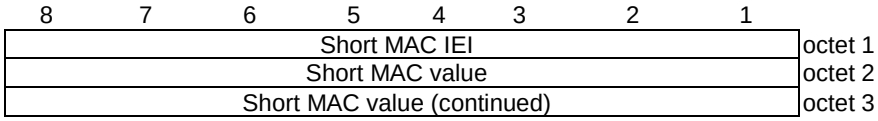


Figure 9.9.3.28.1: Short MAC information element

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.

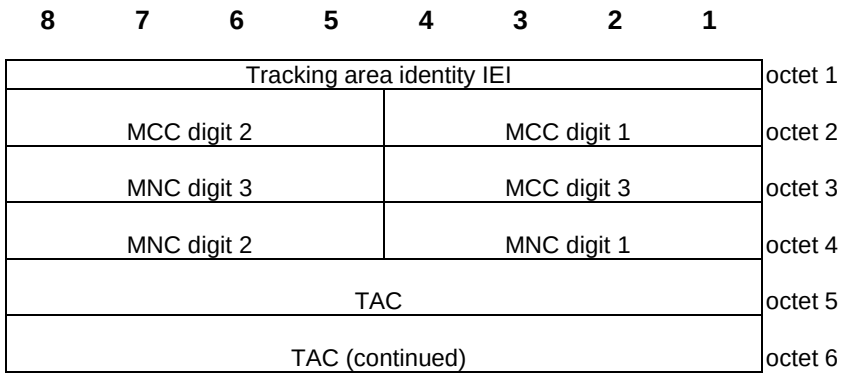


Figure 9.9.3.32.1: Tracking area identity information element

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.

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.

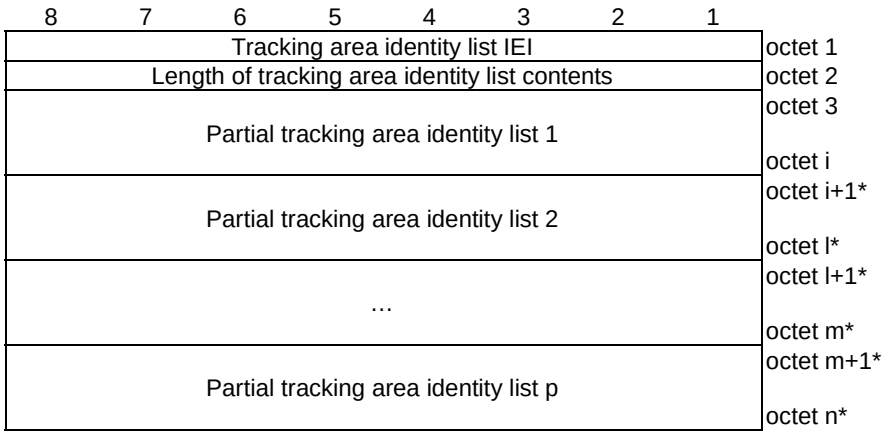


Figure 9.9.3.33.1: Tracking area identity list information element

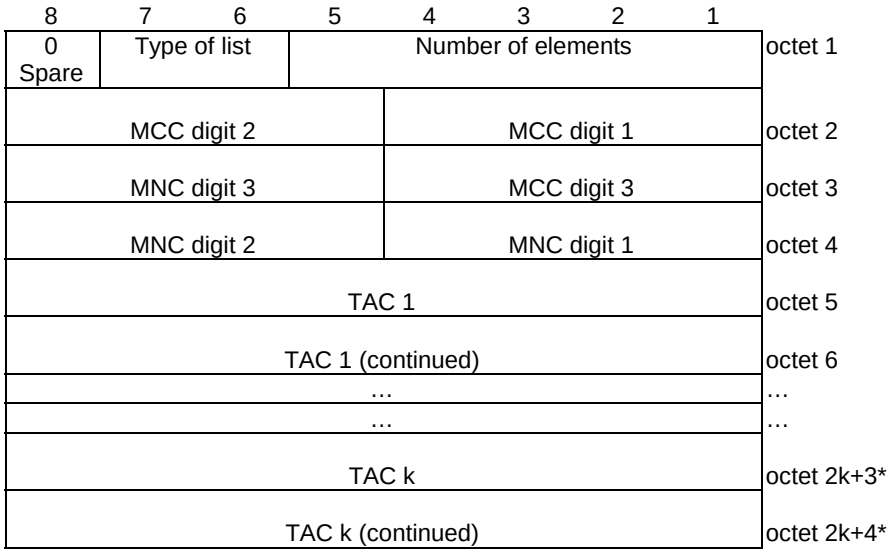


Figure 9.9.3.33.2: Partial tracking area identity list – type of list = "000"

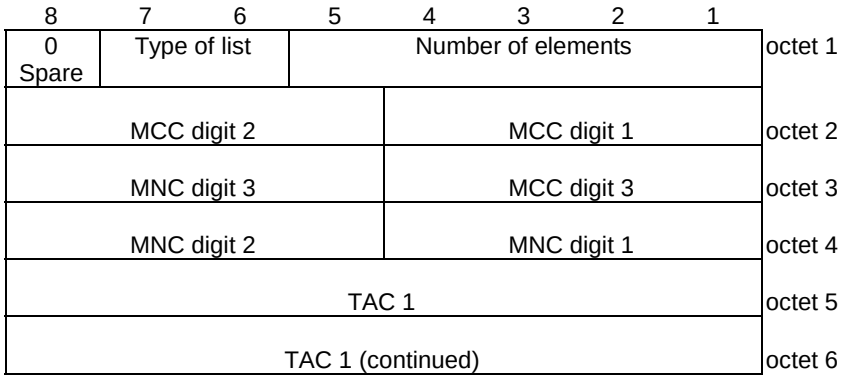


Figure 9.9.3.33.3: Partial tracking area identity list – type of list = "001"

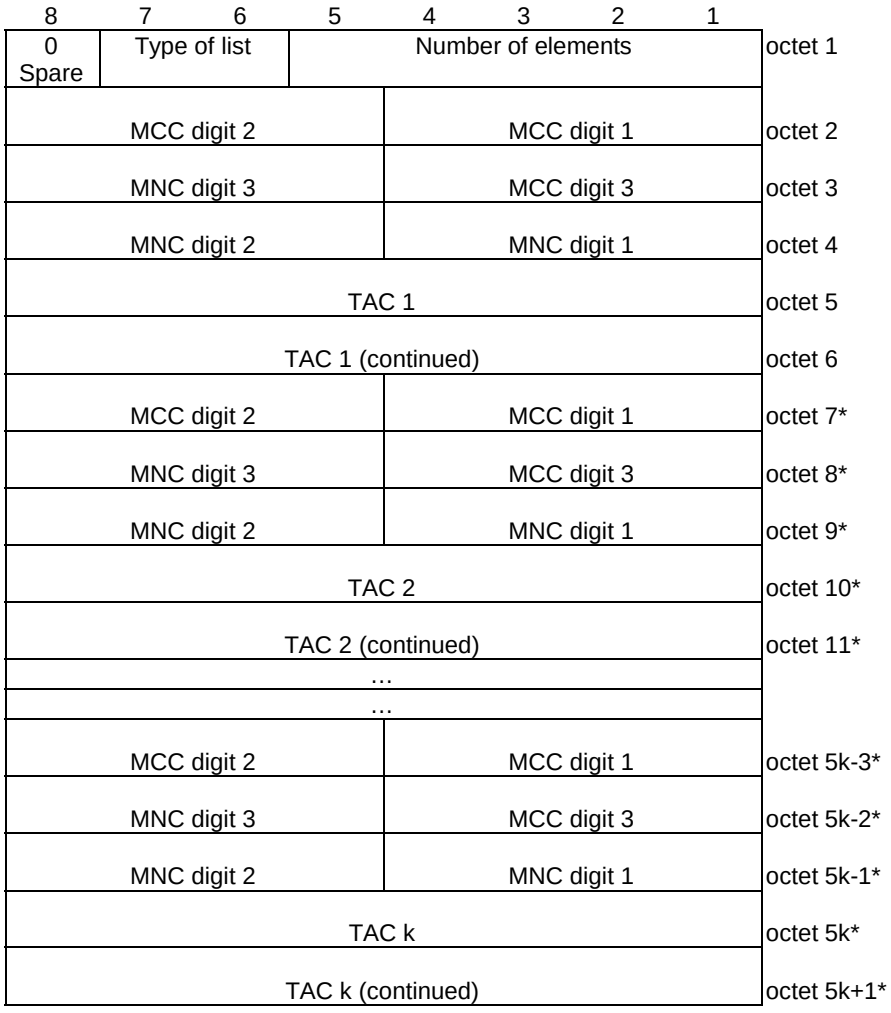


Figure 9.9.3.33.4: Partial tracking area identity list – type of list = "010"

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.
The UE shall store the complete list received. 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
EEA0	128-EEA1	128-EEA2	EEA3	EEA4	EEA5	EEA6	EEA7	octet 3
EIA0	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	LPP	LCS	1xSR VCC	NF	octet 7*
0	0	0	0	0	0	0	0	octet 8* -15*
Spare								

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 EEA0 supported (octet 3, bit 8)
0 EPS encryption algorithm EEA0 not supported
1 EPS encryption algorithm 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)
EPS integrity algorithm EIA0 supported (octet 4, bit 8)
0 EPS integrity algorithm EIA0 not supported
1 EPS integrity algorithm EIA0 supported
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 5 of octet 7 are spare and shall be coded as zero. NF capability (octet 7, bit 1) 0 notification procedure not supported 1 notification procedure supported 1xSRVCC capability (octet 7, bit 2) 0 SRVCC from E-UTRAN to cdma2000® 1x CS not supported 1 SRVCC from E-UTRAN to cdma2000® 1x CS supported (see 3GPP TS 23.216 [8]) Location services (LCS) notification mechanisms capability (octet 7, bit 3) 0 LCS notification mechanisms not supported 1 LCS notification mechanisms supported (see 3GPP TS 24.171 [13C]) LTE Positioning Protocol (LPP) capability (octet 7, bit 4) 0 LPP not supported 1 LPP supported (see 3GPP TS 36.355 [22A]) 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
EEA0	128-EEA1	128-EEA2	EEA3	EEA4	EEA5	EEA6	EEA7	octet 3
EIA0	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 EEA0 supported (octet 3, bit 8)
0 EPS encryption algorithm EEA0 not supported
1 EPS encryption algorithm 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)
EPS integrity algorithm EIA0 supported (octet 4, bit 8)
0 EPS integrity algorithm EIA0 not supported
1 EPS integrity algorithm EIA0 supported
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

9.9.3.37 Emergency Number List

See subclause 10.5.3.13 in 3GPP TS 24.008 [13].

9.9.3.38 CLI

The purpose of the CLI information element is to convey information about the calling line for a terminated call to a CS fallback capable UE.

The CLI information element is coded as shown in figure 9.9.3.38.1 and table 9.9.3.38.1.

The CLI is a type 4 information element with a minimum length of 3 octets and a maximum length of 14 octets.

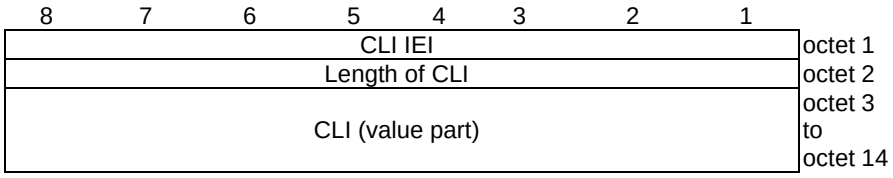


Figure 9.9.3.38.1: CLI information element

Table 9.9.3.38.1: CLI information element

CLI (value part) The coding of the CLI value part is the same as for octets 3 to 14 of the Calling party BCD number information element defined in subclause 10.5.4.9 of 3GPP TS 24.008 [13].

9.9.3.39 SS Code

The purpose of the SS code information element is to convey information related to a network initiated supplementary service request to a CS fallback capable UE.

The SS Code information element is coded as shown in figure 9.9.3.39.1 and table 9.9.3.39.1.

The SS Code is a type 3 information element with 2 octets length.

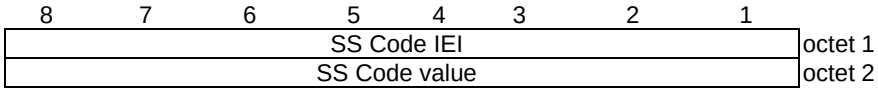


Figure 9.9.3.39.1: SS Code information element

Table 9.9.3.39.1: SS Code information element

SS Code value The coding of the SS Code value is given in subclause 17.7.5 of 3GPP TS 29.002 [15B].

9.9.3.40 LCS indicator

The purpose of the LCS indicator information element is to indicate that the origin of the message is due to a LCS request and the type of this request to a CS fallback capable UE.

The LCS indicator information element is coded as shown in figure 9.9.3.40.1 and table 9.9.3.40.1.

The LCS indicator is a type 3 information element with 2 octets length.

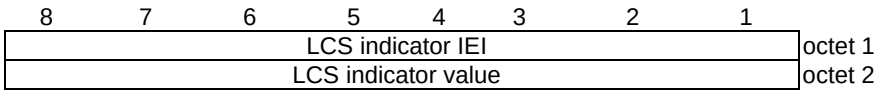


Figure 9.9.3.40.1: LCS indicator information element

Table 9.9.3.40.1: LCS indicator information element

LCS indicator value Bits	
8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	Normal, unspecified in this version of the protocol.
0 0 0 0 0 0 0 1	MT-LR
0 0 0 0 0 0 1 0	
to	Normal, unspecified in this version of the protocol
1 1 1 1 1 1 1 1	

9.9.3.41 LCS client identity

The purpose of the LCS client identity information element is to convey information related to the client of a LCS request for a CS fallback capable UE.

The LCS client identity information element is coded as shown in figure 9.9.3.41.1 and table 9.9.3.41.1.

The LCI client identity is a type 4 information element with a minimum length of 3 octets and a maximum length of 257 octets.

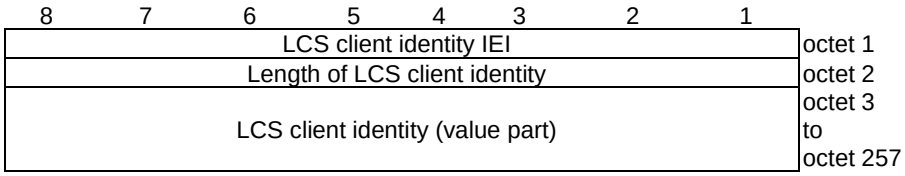


Figure 9.9.3.41.1: LCS client identity information element

Table 9.9.3.41.1: LCS client identity information element

LCS client identity (value part) The coding of the value part of the LCS client identity is given in subclause 17.7.13 of 3GPP TS 29.002 [15B].

9.9.3.42 Generic message container type

The purpose of the generic message container type information element is to specify the type of message contained in the generic message container IE.

The generic message container type information element is coded as shown in table 9.9.3.42.1.

Table 9.9.3.42.1: Generic message container type information element

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	LTE Positioning Protocol (LPP) message container (see 3GPP TS 36.355 [22A])
0 0 0 0 0 0 1 0	Location services message container (see 3GPP TS 24.171 [13C])
0 0 0 0 0 0 1 1 to 0 1 1 1 1 1 1 1	Unused
1 0 0 0 0 0 0 0 to 1 1 1 1 1 1 1 1	Reserved

9.9.3.43 Generic message container

This information element is used to encapsulate the application message transferred between the UE and the network.The generic message container information element is coded as shown in figure 9.9.3.43.1 and and table 9.9.3.43.1.

The generic message container is a type 6 information element.

8 7 6 5 4 3 2 1

Generic message container IEI	octet 1
Length of generic message container contents	octet 2 octet 3
Generic message container contents	octet 4 octet n

Figure 9.9.3.43.1: Generic message container information element

Table 9.9.3.43.1: Generic message container information element

Generic message container contents (octet 4 to octet n); Max value of 65535 octets The coding of the contents of the generic message container is dependent on the particular application.

9.9.3.44 Voice domain preference and UE's usage setting

See subclause 10.5.5.28 in 3GPP TS 24.008 [13].

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 initial subscribed APN-AMBR when the UE establishes a PDN connection or 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. Octets 5-8 are optional. If octet 5 is included, then octet 6 shall also be included, and octets 7-8 may be included. If octet 7 is included, then octet 8 shall also be included. The length of the APN-AMBR IE can be either 4 octets, 6 octets or 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

All other values shall be interpreted as '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 1 1 1 1 1 1 1 0	the APN-AMBR for downlink and APN-AMBR for downlink (extended) in octets 3 and 5), giving a range of 256 Mbps to 65280 Mbps.
1 1 1 1 1 1 1 1	This value shall be interpreted as '0 0 0 0 0 0 0 0' in this version of the specification.

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. Octets 4-11 are optional. If octet 4 is included, then octets 5-7 shall also be included, and octets 8-11 may be included. If octet 8 is included, then octets 4-11 shall also be included. The length of the EPS QoS IE can be either 3 octets, 7 octets or 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] and 3GPP TS 29.212 [16A])
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	Reserved
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
0 0 0 0 1 0 1 0 to 0 1 1 1 1 1 1 1	Reserved
1 0 0 0 0 0 0 0 to 1 1 1 1 1 1 1 0	Operator-specific QCIs
1 1 1 1 1 1 1 1	Reserved

The network shall consider all other values not explicitly defined in this version of the protocol as unsupported.

If the UE receives a QCI value that it does not understand, the UE shall choose a QCI value from the set of QCI values defined in this version of the protocol (see 3GPP TS 23.203 [7] and 3GPP TS 29.212 [16A]) and associated with:

- GBR bearers if the IE includes a guaranteed bit rate value; and

- non-GBR bearers if the IE does not include a guaranteed bit rate value.

The UE shall use this chosen QCI value for internal operations only. The UE shall use the received QCI value in subsequent NAS signalling procedures.

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 to 0 0 1 1 1 1 1 1	The maximum bit rate is binary coded in 8 bits, using a granularity of 1 kbps giving a range of values from 1 kbps to 63 kbps in 1 kbps increments.
0 1 0 0 0 0 0 0 to 0 1 1 1 1 1 1 1	The maximum bit rate is 64 kbps + ((the binary coded value in 8 bits – 01000000) * 8 kbps) giving a range of values from 64 kbps to 568 kbps in 8 kbps increments.
1 0 0 0 0 0 0 0 to 1 1 1 1 1 1 1 0	The maximum bit rate is 576 kbps + ((the binary coded value in 8 bits – 10000000) * 64 kbps) giving a range of values from 576 kbps to 8640 kbps in 64 kbps increments.
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.

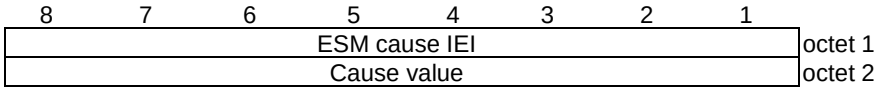


Figure 9.9.4.4.1: ESM cause information element

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	Request rejected by Serving GW or PDN GW
0	0	0	1	1	1	1	1	Request 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	0	1	1	1	Reactivation requested
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	Invalid EPS bearer identity
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	0	1	1	1	1	PTI mismatch
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	0	1	1	0	1	1	1	Multiple PDN connections for a given APN not allowed
0	0	1	1	1	0	0	0	Collision with network initiated request
0	0	1	1	1	0	1	1	Unsupported QCI value
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.

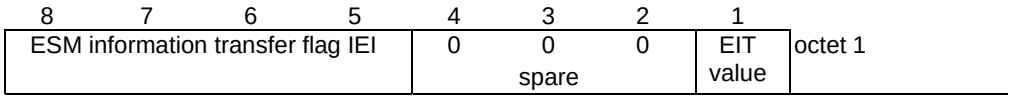


Figure 9.9.4.5.1: ESM information transfer flag information element

Table 9.9.4.5.1: ESM information transfer flag information element

EIT (ESM information transfer)	
Bit	
1	
0	security protected ESM information transfer not required
1	security protected 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 or to identify the EPS bearer (default or dedicated) with which one or more packet filters specified in a traffic flow aggregate are associated.

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.

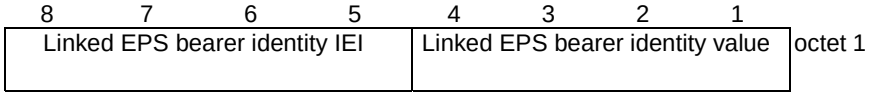


Figure 9.9.4.6.1: Linked EPS bearer identity information element

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].

9.9.4.7A Notification indicator

The purpose of the Notification indicator information element is to inform the UE about an event which is relevant for the upper layer using an EPS bearer context or having requested a procedure transaction.

The Notification indicator information element is coded as shown in figure 9.9.4.7A.1 and table 9.9.4.7A.1.

The Notification indicator is a type 4 information element with 3 octets length.

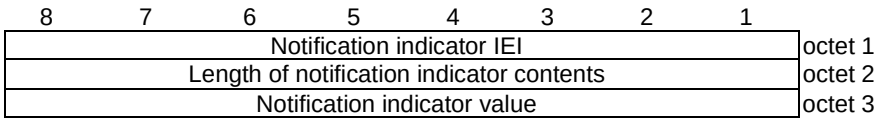


Figure 9.9.4.7A.1: Notification indicator information element

Table 9.9.4.7A.1: Notification indicator information element

Notification indicator value (octet 3) Bits **8 7 6 5 4 3 2 1**	
0 0 0 0 0 0 0 1	SRVCC handover cancelled, IMS session re-establishment required (see 3GPP TS 23.216 [8])
0 0 0 0 0 0 1 0 to 0 1 1 1 1 1 1 1	Unused, shall be ignored if received by the UE
All other values are reserved.	

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.

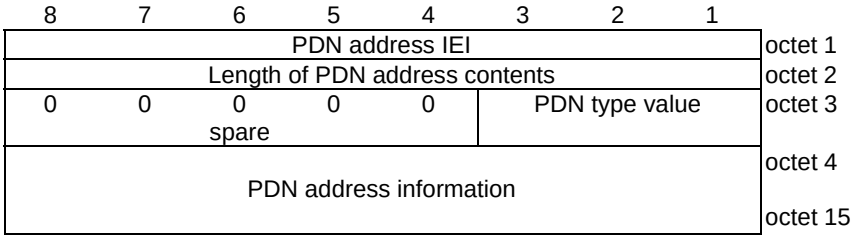


Figure 9.9.4.9.1: PDN address information element

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 4 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.

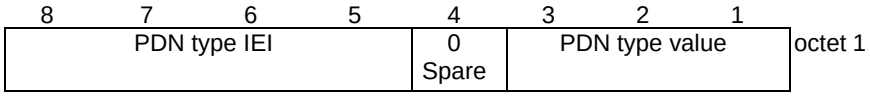


Figure 9.9.4.10.1: PDN type information element

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
1	0	0	unused; shall be interpreted as "IPv6" if received by the network

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 one of more packet filters and their related parameters and operations. The traffic flow 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 bearer contexts. 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 packet filter.

When the traffic flow aggregate description is used in the UE requested bearer resource allocation procedure or the UE requested bearer resource modification procedure, it is associated to a particular procedure identified by a procedure transaction identity (PTI). Therefore, the UE shall release the traffic flow aggregate description when the UE requested bearer resource allocation procedure or the UE requested bearer resource modification procedure is completed. The UE shall not include the packet filters of a particular traffic flow aggregate description in any other traffic flow aggregate description when multiple UE requested bearer resource allocation procedures and/or UE requested bearer resource modification procedures are ongoing in parallel.

The Traffic flow aggregate description information element is encoded using the same format as the Traffic flow template (TFT) information element (see subclause 10.5.6.12 in 3GPP TS 24.008 [13]). When sending this IE in the BEARER RESOURCE ALLOCATION REQUEST message or the BEARER RESOURCE MODIFICATION REQUEST message, the UE shall set the packet filter identifier values to 0 if the packet filters are newly created; otherwise, the UE shall set the packet filter identifier values from those of already assigned packet filter identifiers of the existing EPS bearer, so that they are unique across all packet filters for the EPS bearer context indicated by the EPS bearer identity IE.

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 EMM 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 EMM 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	Default 54 min. NOTE 2 NOTE 5	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 if the UE is not attached for emergency bearer services. Implicit detach from network if the UE is attached for emergency bearer services.
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 sent EXTENDED SERVICE REQUEST sent in case f, g, i and j in subclause 5.6.1.1	Bearers have been set up SERVICE REJECT received	Abort the procedure

T3417ext	10s	EMM-SERVICE-REQUEST-INITIATED	EXTENDED SERVICE REQUEST sent in case d in subclause 5.6.1.1 EXTENDED SERVICE REQUEST sent in case e in subclause 5.6.1.1 and the CSFB response was set to "CS fallback accepted by the UE"	Inter-system change from S1 mode to A/Gb mode or Iu mode is completed Inter-system change from S1 mode to A/Gb mode or Iu mode is failed SERVICE REJECT received	Abort the procedure
T3418	20s	EMM-REGISTERED-INITIATED EMM-REGISTERED EMM-TRACKING-AREA-UPDATING-INITIATED EMM-DEREGISTERED-INITIATED EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (EMM cause = #20 "MAC failure" or #26 "non-EPS authentication unacceptable") sent	AUTHENTICATION REQUEST received	On first expiry, the UE should consider the network as false and follow item f of subclause 5.4.2.7, if the UE is not attached for emergency bearer services. On first expiry, the UE will follow subclause 5.4.2.7 under 'For items c, d, and e:', if the UE is attached for emergency bearer services.
T3420	15s	EMM-REGISTERED-INITIATED EMM-REGISTERED EMM-DEREGISTERED-INITIATED EMM-TRACKING-AREA-UPDATING-INITIATED EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (cause = #21 "synch failure") sent	AUTHENTICATION REQUEST received	On first expiry, the UE should consider the network as false and follow item f of subclause 5.4.2.7, if the UE is not attached for emergency bearer services. On first expiry, the UE will follow subclause 5.4.2.7 under 'For items c, d, and e:', if the UE is attached for emergency bearer services.
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.	Set 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 EMM cause #11, #12, #13, #14 or #15 SERVICE REJECT received with any of the EMM cause #11, #12, #13 or #15 TRACKING AREA UPDATE ACCEPT received after the UE sent TRACKING AREA UPDATE REQUEST in EMM-IDLE mode 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 EMM cause #39 "CS domain temporarily not available"	TRACKING AREA UPDATE REQUEST sent	None

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 #39 "CS domain temporarily not available".

NOTE 5: The default value of this timer is used if the network does not indicate a value in the TRACKING AREA UPDATE ACCEPT message and the UE does not have a stored value for this timer.

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 for EPS services initiated	Paging procedure for EPS services 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 TRACKING AREA UPDATE ACCEPT sent with TMSI 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 if the UE is not attached for emergency bearer services. Implicitly detach the UE which is attached for emergency bearer services.
Implicit detach timer	NOTE 3	All except EMM-DEREGISTERED	The mobile reachable timer expires while the network is in EMM-IDLE mode	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.
NOTE 3: The value of this timer is network dependent. If ISR is activated, the default value of this timer is 4 minutes greater than T3423.

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	8s	PROCEDURE TRANSACTION PENDING	BEARER RESOURCE ALLOCATION REQUEST sent	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE ALLOCATION REJECT received	Retransmission of BEARER RESOURCE ALLOCATION REQUEST
T3481	8s	PROCEDURE TRANSACTION PENDING	BEARER RESOURCE MODIFICATION REQUEST sent	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or DEACTIVATE EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE MODIFICATION REJECT received	Retransmission of BEARER RESOURCE MODIFICATION REQUEST
T3482	8s	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	8s	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	8s	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	PROCEDURE TRANSACTION PENDING	ESM INFORMATION REQUEST sent	ESM INFORMATION RESPONSE received	Retransmission of ESM INFORMATION REQUEST on 1st and 2nd expiry only
T3495	8s	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.

Annex A (informative): Cause values for EPS mobility management

A.1 Causes related to UE identification

Cause #2 – IMSI unknown in HSS

This EMM cause is sent to the UE if the UE is not known (registered) in the HSS. This EMM cause does not affect operation of the EPS service, although is may be used by an EMM procedure.

Cause #3 – Illegal UE

This EMM 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 #6 – Illegal ME

This EMM cause is sent to the UE if the ME used is not acceptable to the network, e.g. blacklisted.

Cause #9 – UE identity cannot be derived by the network.

This EMM cause is sent to the UE when the network cannot derive the UE's identity from the GUTI/S-TMSI/P-TMSI and RAI e.g. no matching identity/context in the network or failure to validate the UE's identity due to integrity check failure of the received message.

Cause #10 – Implicitly detached

This EMM 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 #5 – IMEI not accepted

This cause is sent to the UE if the network does not accept an attach procedure for emergency bearer services using an IMEI.

Cause #7 – EPS services not allowed

This EMM cause is sent to the UE when it is not allowed to operate EPS services.

Cause #8 – EPS services and non-EPS services not allowed

This EMM cause is sent to the UE when it is not allowed to operate either EPS or non-EPS services.

Cause #11 – PLMN not allowed

This EMM cause is sent to the UE if it requests attach or tracking area updating in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate.

Cause #12 – Tracking area not allowed

This EMM 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 EMM 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 #13 – Roaming not allowed in this tracking area

This EMM 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 #14 – EPS services not allowed in this PLMN

This EMM 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 #15 – No suitable cells in tracking area

This EMM 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 #25 – Not authorized for this CSG

This EMM cause is sent to the UE if it requests access in a CSG cell with CSG ID where the UE either has no subscriptionto operate or the UE's subscription has expired and it should find another cell in the same PLMN.

Cause #40 – No EPS bearer context activated

This EMM cause is sent to the UE, if during a tracking area updating procedure the MME detects that there is no active EPS bearer context in the network.

A.3 Causes related to PLMN specific network failures and congestion/authentication failures

Cause #16 – MSC temporarily not reachable

This EMM 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 #17 – Network failure

This EMM cause is sent to the UE if the MME cannot service an UE generated request because of PLMN failures.

Cause #18 – CS domain not available

This EMM cause is sent to the UE if the MME cannot service an UE generated request because of no availability of CS domain.

Cause #19 – ESM failure

This EMM cause is sent to the UE when there is a failure in the ESM message contained in the EMM message.

Cause #20 – MAC failure

This EMM 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 #21 – Synch failure

This EMM 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 #22 – Congestion

This EMM cause is sent to the UE because of congestion in the network (e.g. no channel, facility busy/congested etc.).

Cause #23 – UE security capabilities mismatch

This EMM cause is sent to the network if the UE detects that the UE security capability does not match the one sent back by the network.

Cause #24 – Security mode rejected, unspecified

This EMM cause is sent to the network if the security mode command is rejected by the UE if the UE detects that the $nonce_{UE}$ does not match the one sent back by the network or for unspecified reasons.

Cause #26 – Non-EPS authentication unacceptable

This EMM cause is sent to the network in S1 mode if the "separation bit" in the AMF field of AUTN is set to 0 in the AUTHENTICATION REQUEST message (see 3GPP TS 33.401 [19]).

Cause #39 – CS domain temporarily not available

This EMM cause is sent to the UE when the CS fallback or 1xCS fallback request cannot be served temporarily due to O&M reasons.

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 #8 – Operator Determined Barring

This ESM cause is used by the network to indicate that the requested service was rejected by the MME due to Operator Determined Barring.

Cause #26 – Insufficient resources

This ESM cause is used by the UE or by the network to indicate that the requested service cannot be accepted due to insufficient resources.

Cause #27 – Unknown or missing access point name

This ESM 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 #28 – Unknown PDN type

This ESM 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 #29 – User authentication failed

This ESM 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 #30 – Request rejected by Serving GW or PDN GW

This ESM cause is used by the network to indicate that the requested service or operation or the request for a resource was rejected by the Serving GW or PDN GW.

Cause #31 – Request rejected, unspecified

This ESM cause is used by the network to indicate that the requested service or operation or the request for a resource was rejected due to unspecified reasons.

Cause #32 – Service option not supported

This ESM cause is used by the network when the UE requests a service which is not supported by the PLMN.

Cause #33 – Requested service option not subscribed

This ESM cause is sent when the UE requests a service option for which it has no subscription.

Cause #34 – Service option temporarily out of order

This ESM 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 #35 – PTI already in use

This ESM 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 #36 – Regular deactivation

This ESM cause is used to indicate a regular UE or network initiated release of EPS bearer resources.

Cause #37 – EPS QoS not accepted

This ESM cause is used by the network if the new EPS QoS cannot be accepted that was indicated in the UE request.

Cause #38 – Network failure

This ESM cause is used by the network to indicate that the requested service was rejected due to an error situation in the network.

Cause #39 – Reactivation requested

This ESM cause is used by the network to request an EPS bearer context reactivation.

Cause #41 – Semantic error in the TFT operation.

This ESM 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 #42 – Syntactical error in the TFT operation.

This ESM 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 #43 – Invalid EPS bearer identity

This ESM cause is used by the network or the UE to indicate that the EPS bearer identity value provided to it is not a valid value for the received message or the EPS bearer context identified by the linked EPS bearer identity IE in the request is not active.

Cause #44 – Semantic errors in packet filter(s)

This ESM 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 #45 – Syntactical error in packet filter(s)

This ESM 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 #46 – EPS bearer context without TFT already activated

This ESM cause is used by the network or the UE to indicate that it has already activated an EPS bearer context without TFT.

Cause #47 – PTI mismatch

This ESM cause is used by the UE to indicate that the PTI value which is included in the ESM message that the UE receives does not match a PTI in use.

Cause #49 – Last PDN disconnection not allowed

This ESM 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 #50 – PDN type IPv4 only allowed

This ESM cause is used by the network to indicate that only PDN type IPv4 is allowed for the requested PDN connectivity.

Cause #51 – PDN type IPv6 only allowed

This ESM cause is used by the network to indicate that only PDN type IPv6 is allowed for the requested PDN connectivity.

Cause #52 – single address bearers only allowed

This ESM 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 #53 – ESM information not received

This ESM cause is used by the network to indicate that the PDN connectivity procedure was rejected due to the ESM information was not received.

Cause #54 – PDN connection does not exist

This ESM cause is used by the network at handover from a non-3GPP access network to indicate that the MME does not have any information about the requested PDN connection.

Cause #55 – Multiple PDN connections for a given APN not allowed

This ESM cause is used by the network to indicate that the PDN connectivity procedure was rejected due to multiple PDN connections for a given APN are not allowed.

Cause #56 – Collision with network initiated request

This ESM cause is used by the network to indicate that the network has already initiated the activation, modification or deactivation of bearer resources which was requested by the UE.

Cause #59 – Unsupported QCI value

This ESM cause is used by the network if the QCI indicated in the UE request cannot be supported.

Cause #81 – Invalid PTI value

This ESM cause is used by the network or UE to indicate that the PTI provided to it is unassigned or reserved.

Cause #112 – APN restriction value incompatible with active EPS bearer context.

This ESM 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 #95 – Semantically incorrect message

This ESM cause is used to report receipt of a message with semantically incorrect contents.

Cause #96 – Invalid mandatory information

This ESM cause indicates that the equipment sending this ESM cause has received a message with a non-semantical mandatory IE error.

Cause #97 – Message type non-existent or not implemented

This ESM cause indicates that the equipment sending this ESM 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 ESM cause.

Cause #98 – Message type not compatible with protocol state

This ESM cause indicates that the equipment sending this ESM cause has received a message not compatible with the protocol state.

Cause #99 – Information element non-existent or not implemented

This ESM cause indicates that the equipment sending this ESM 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 ESM cause. However, the information element is not required to be present in the message in order for the equipment sending the ESM cause to process the message.

Cause #100 – Conditional IE error

This ESM cause indicates that the equipment sending this cause has received a message with conditional IE errors.

Cause #101 – Message not compatible with protocol state

This ESM cause indicates that a message has been received which is incompatible with the protocol state.

Cause #111 – Protocol error, unspecified

This ESM cause is used to report a protocol error event only when no other ESM 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;
- Operator CSG list; and
- EPS security context parameters from a full native EPS security context (see 3GPP TS 33.401 [19]).

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 except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM. The allowed CSG list is stored in a non-volatile memory in the ME if the UE supports CSG selection. 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.

The following EMM parameter shall be stored in a non-volatile memory in the ME together with the IMSI from the USIM:

- TIN.

This EMM parameter can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory of the ME; else the UE shall delete the EMM parameter.

If the UE is attached for emergency bearer services, the UE shall not store the EMM parameters described in this annex on the USIM or in non-volatile memory. Instead the UE shall temporarily store these parameters locally in the ME and the UE shall delete these parameters when the UE is detached.

Annex D (normative): Establishment cause (S1 mode only)

D.1 Mapping of NAS procedure to RRC establishment cause (S1 mode only)

When EMM requests the establishment of a NAS-signalling connection, the RRC establishment cause used by the UE shall be selected according to the NAS procedure as specified in table D.1.1. The EMM shall also indicate to the lower layer for the purpose of access control, the call type associated with the RRC establishment cause as specified in table D.1.1.

Table D.1.1: Mapping of NAS procedure to establishment cause and call type

NAS procedure	RRC establishment cause (according 3GPP TS 36.331 [22])	Call type
Attach	If an ATTACH REQUEST has EPS attach type not set to "EPS emergency attach", the RRC establishment cause shall be set to MO signalling except when the UE initiates attach procedure to establish emergency bearer services. (See Note 1)	"originating signalling"
	If an ATTACH REQUEST has EPS attach type set to "EPS emergency attach" or if the ATTACH REQUEST has EPS attach type not set to "EPS emergency attach" but the UE initiates the attach procedure on receiving request from upper layer to establish emergency bearer services, the RRC establishment cause shall be set to Emergency call. (See Note 1)	"emergency calls"
Tracking Area Update	If the UE does not have a PDN connection established for emergency bearer services and is not initiating a PDN CONNECTIVITY REQUEST that has request type set to "emergency, the RRC establishment cause shall be set to MO signalling. (See Note 1)	"originating signalling"
	If the UE has a PDN connection established for emergency bearer services or is initiating a PDN CONNECTIVITY REQUEST that has request type set to "emergency", the RRC establishment cause shall be set to Emergency call. (See Note 1)	"emergency calls"
Detach	MO signalling (See Note 1)	"originating signalling"
Service Request	If a SERVICE REQUEST is to request user plane radio resources, the RRC establishment cause shall be set to MO data. (See Note 1)	"originating calls"
	If a SERVICE REQUEST is to request user plane radio resources for emergency bearer services, the RRC establishment cause shall be set to Emergency call. (See Note 1)	"emergency calls"
	If a SERVICE REQUEST is to request resources for UL signalling, the RRC establishment cause shall be set to MO data. (See Note 1)	"originating calls"
	If the SERVICE REQUEST is triggered by a PDN CONNECTIVITY REQUEST that has request type set to "emergency", the RRC establishment cause shall be set to Emergency call. (See Note 1)	"emergency calls"

	If a SERVICE REQUEST is a response to paging where the CN domain indicator is set to "PS", the RRC establishment cause shall be set to MT access. (See Note 1)	"terminating calls"
	If an EXTENDED SERVICE REQUEST has service type set to "mobile originating CS fallback or 1xCS fallback", the RRC establishment cause shall be set to MO data. (See Note1).	"originating calls"
	If an EXTENDED SERVICE REQUEST is a response to paging for CS fallback, service type set to "mobile terminating CS fallback or 1xCS fallback", the RRC establishment cause shall be set to MT access. (See Note1, Note 2).	"terminating calls"
	If an EXTENDED SERVICE REQUEST has service type set to "mobile originating CS fallback emergency call or 1xCS fallback emergency call", the RRC establishment cause shall be set to Emergency call. (See Note1).	"emergency calls"

Note 1: For these NAS procedures initiated by UEs of access class 12, 13 or 14 in their home country, the RRC establishment cause will be set to "High priority access AC 11 – 15". For this purpose the home country is defined as the country of the MCC part of the IMSI, see 3GPP TS 22.011 [1A].
For these NAS procedures initiated by UE of access class 11 or 15 in their HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present), the RRC establishment cause will be set to "High priority access AC 11 – 15".
Note 2: This is not applicable for mobile terminating 1xCS fallback.

NOTE: The RRC establishment cause can be used by the network to prioritise the connection establishment request from the UE at high load situations in the network.

Annex E (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
2009-03	CT-43	CP-090153	0003	2	Clarification of the timer T3413 in paging procedure for CSFB	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0004	2	Clarification of the abnormal case in UE requested PDN connectivity procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0006	1	Clarification on expiration of T3417	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0010	1	Clean up the unuseful definition and complete sentence	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0011	1	Cleanup the definition of the TAI list	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0015	1	Updating the identities of forbidden tracking areas	8.0.0	8.1.0
2009-03	CT-43	CP-090153	0017	2	the handling of the UE after the EPS detach only	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0019	2	Resolve editors'notes for NAS security	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0022	1	APN-AMBR Clarifications	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0023	2	State change to EMM-DEREGISTERED for non-3GPP access	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0025	2	Updating the APN-AMBR of the UE after inter-system handover to S1 mode	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0027	2	Provision of RRC establishment cause values by EPS NAS	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0034	2	Update to Paging using IMSI procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0035	1	Update the PDN address IE to Mandatory	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0037	1	Update to the detach procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0039	3	Security and inter RAT mobility to E-UTRAN	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0040	1	KSI inclusion in Detach Request	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0044	1	Editorials on security issues	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0045	2	Behaviour on Service Reject(cause#10), relationship between SM and ESM state machines, inclusion of PDP context parameters	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0046	2	Clarifications on issues for bearer context states	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0050		Remove Editors Note for TAI length	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0051	1	Correct use of cdma terminology	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0059	1	Addition of actions on receiving an ESM STATUS message	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0060	1	Addition of the definition of casue value #47 (PTI mismatch)	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0061	1	Editorial corrections on the definition of default bearer and the ESM message names	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0062	2	Correction to error cause value #9 and integrity check failure	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0064		IPv6 interface identifier coding	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0066	3	Clarification for local release of bearers	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0068	1	Corrections for Attach failure procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0069	2	Re-transmission of EMM DL NAS message handling due to handover	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0070	2	Re-transmission of ESM DL NAS message handling due to handover	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0071		Paging for EPS services using IMSI and DRX	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0075	2	Coordination of ESM and EMM sublayers for supporting ISR	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0076	1	Handling of TAI list at the UE	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0078	2	UE specific DRX Parameter handling in ATTACH/TAU procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0081	1	Handling of security context during state transitions	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0082	2	Trigger for initiating ciphering protection	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0085	2	UE action related to ISR local deactivation	8.0.0	8.1.0
2009-03	CT-43	CP-090153	0088	3	Clarification on CLI usage	8.0.0	8.1.0
2009-03	CT-43	CP-090153	0092	1	Abnormal case handling for Extended Service request	8.0.0	8.1.0
2009-03	CT-43	CP-090259	0093	4	UE behaviour when UE support of CSG selection is optional	8.0.0	8.1.0
2009-03	CT-43	CP-090153	0094	2	Conditions for initiating TAU and combined TAU	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0095	1	Corrections for attach and TAU attempt counters	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0096	1	Network initiated detach procedure corrections	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0097	1	EMM states cleanup	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0099	2	Supervision timer and corrections for the extended service request procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090153	0100	1	Corrections for combined attach procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090153	0102	2	Definition of NAS Message Container and Removal of Editor's Note	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0103	1	Adding missing procedure figure to Service Request	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0104	1	Introduction of the Local Emergency Numbers List	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0105	2	New cause value for separation bit failure in authentication	8.0.0	8.1.0

2009-03	CT-43	CP-090153	0106	3	Solving editor's notes in Annex A.3	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0109	2	Update on security procedure section	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0112	1	Clarification on Dedicated bearer setup procedure failure	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0116	1	New ESM cause value for collision with network initiated request	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0117	1	Populating PDN type IE value in PDN CONNECTIVITY REQUEST message	8.0.0	8.1.0
2009-03	CT-43	CP-090153	0119	2	Extended service request for 1xCSFB	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0125	1	ODB Error Cause Clarification	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0128		NAS recovery on/off mechanism(LTE)	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0129	1	Introduce definition of EPS services and non-EPS services	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0131	1	Proposal of UE GMM and MM behavior on reception of error cause #9 when UE executed TAU, combined TAU and Service Request	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0135	1	Clarifications on IP address handling	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0136	1	Unsuccessful cases for pre-registration	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0137	2	Use of P-TMSI for the attach procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0138		Cleanup of editor's notes	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0139	1	Correction of the paging procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0140	1	Cleanup of editor's notes for ESM abnormal cases	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0141		Definition of ESM cause #54	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0142		Definition of security related IEs for inter-system handover	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0143		Removal of ISR bit from UE network capability	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0144		Correction of detach procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0145	1	Addition of text for subclause 4.1, Overview	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0146	1	Addition of text for subclause 6.1.1, General	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0147	1	Addition of text for subclause 6.1.2, Types of ESM procedures	8.0.0	8.1.0
2009-03	CT-43	CP-090157	0152		Correction of cause#25 handling	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0153		Description of procedure transaction states for the network	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0154	1	Moving the description of the eKSI to subclause 4.4	8.0.0	8.1.0
2009-03	CT-43	CP-090129	0155	3	CS Service Notification	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0158	1	E9.04, removal of Editor's note in 9.5	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0159		E4.03 and E9.05, removal of Editor's notes in 4.3.3.1 and 9.6	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0160	2	Inclusion of APN in PDN connectivity request	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0162	2	Clarification on local EPS bearer context deactivation	8.0.0	8.1.0
2009-03	CT-43	CP-090131	0163	2	Unciphered network operation	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0164		ESM cause value #53 missing in 6.5.1.4	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0165	1	Reservation of "reserved" and "unused" code points	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0166		Editorial modification to add a "new line" character	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0167	2	Activation of dedicated bearers during attach procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0168	2	Additions to " EPS bearer context deactivation initiated by the network"	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0170		Removal of EN for TAU reject (cause #12)	8.0.0	8.1.0
2009-03	CT-43	CP-090130	0171	2	Security Terminolgy Change to Reflect 33.401	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0172	1	Alignment of cause representation	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0173		Correction of fields within Detach type IE	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0174		Deletion of editor's note for 2 digit MNC	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0176	2	Clarification of the network behaviour on SMC rejection	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0178	1	Add an abnormal case in the dedicated EPS bearer context activation procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0181	3	Clarify the collison between detach and service request procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090127	0186	1	Correction of QCI	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0187		Clarifications related to the use of "active flag"	8.0.0	8.1.0
2009-03	CT-43	CP-090153	0189	1	Corrections for CS/PS mode 1 and CS/PS mode 2 of operation	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0195	1	ESM information transfer flag	8.0.0	8.1.0
2009-03	CT-43	CP-090125	0198		Attach attempt counter	8.0.0	8.1.0
2009-03	CT-43	CP-090128	0199	1	Error correction in reference for timer T3412 in TAU procedure	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0201	1	Clarifications for request type	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0203	1	Clarification of the use of NAS security header	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0205	1	Proposal of UE GMM and MM behavior on reception of error cause #10 when UE executed TAU, combined TAU and Service Request	8.0.0	8.1.0
2009-03	CT-43	CP-090126	0206		Definition of T3480, T3485, T3486, T3495 timer duration; Corrections on EPS bearer identity checking	8.0.0	8.1.0
2009-03	CT-43	CP-090215	0207	3	Clarification of UE requested ESM procedures	8.0.0	8.1.0
2009-03	CT-43	CP-090157	0208		Corrections to CSG related NAS behavior	8.0.0	8.1.0
2009-06	CT-44	CP-090421	0190	1	Cleanup for transport of NAS messages procedure	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0210	1	TAU handling	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0214		NAS security parameters for inter system handovers	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0216	2	Transmission failure of EMM messages	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0217	1	Clarifications on protocol discriminator for security protected NAS message	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0219	1	Clarifications related PDN disconnect request, ESM information	8.1.0	8.2.0

					request, EPS bearer context modification request and bearer resource allocation request procedures		
2009-06	CT-44	CP-090410	0220		Service Reject(cause #12)	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0227	1	Security context cleanup at Security Mode Reject	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0228	2	Removal of KSIASME from TAU accept	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0229		Add missing LV-E format	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0230		New value for ESM timer T3482	8.1.0	8.2.0
2009-06	CT-44	CP-090410	0231		EPS mobile identity octet numbering	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0232	2	PDN connectivity reject cause value corrections	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0233	1	MME handling of lower layer failure during the attach procedure	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0239	1	Null ciphering algorithm	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0242	1	EPS security modification	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0243	2	Clarification regarding bearer resource allocation procedure, EPS bearer identity and PTI in several ESM messages.	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0244	1	Removal of default PDN	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0245	2	Add description of cause #40 in Annex A	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0246	2	Correct the UE behavior of handling ESM message	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0247	1	Clarify the UE behavior upon reception of some reject messages	8.1.0	8.2.0
2009-06	CT-44	CP-090498	0251	5	eKSI definition in NAS messages	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0252	1	eKSI in Service Request message	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0257		Remove unused ESM cause value #40 – "Feature not supported"	8.1.0	8.2.0
2009-06	CT-44	CP-090421	0260	1	Abnormal case handling for Extended Service request in 1xCSFB	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0269	1	Resolution of Editor's Note in subclause 5.4.4.2	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0272		Update the cause of start and stop of T3413	8.1.0	8.2.0
2009-06	CT-44	CP-090421	0274		The collison handling for Extended Service Request	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0275		Handling of undefined QCI values	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0276	1	Relation between HNP and HA delivered through PCO	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0277		Corrections on abnormal case in UE requested PDN connectivity procedure	8.1.0	8.2.0
2009-06	CT-44	CP-090411	0280	1	Correction of UE requested resource procedures	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0282	1	More precise general text for UE requested PDN connectivity procedure	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0283		Alignment of cause representation	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0284		Text clean up in 24.301	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0292	1	Correction for the main state change in the UE	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0293	1	Correction for implicit detach timer	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0296	1	Clarification on Local Network initiated detach procedure without EMM signalling	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0300	2	Correction for the EPS mobile identity	8.1.0	8.2.0
2009-06	CT-44	CP-090421	0301		Impacts of successful combined registration on forbidden LAs lists	8.1.0	8.2.0
2009-06	CT-44	CP-090421	0302		CS/PS mode 1 UE behaviour on reception of cause #18	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0303		Corrections on handling of UE network capability	8.1.0	8.2.0
2009-06	CT-44	CP-090421	0304		Cleanup for EMM procedures	8.1.0	8.2.0
2009-06	CT-44	CP-090421	0306	1	Handling of non-semantical mandatory information element errors in the PDN DISCONNNECT REQUEST message.	8.1.0	8.2.0
2009-06	CT-44	CP-090421	0309	2	Clarification on the registered PLMN for Network Sharing	8.1.0	8.2.0
2009-06	CT-44	CP-090421	0312	1	Definition of kbps	8.1.0	8.2.0
2009-06	CT-44	CP-090421	0315	2	Sending UE Id in the CS Service Notification	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0318	1	Clarification of EPS QoS length	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0319		Removal of unnecessary TAU procedure after abnormal bearer allocation failure	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0320	1	Set of minor corrections to TS 24.301	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0321	2	Clarifications to 24.301	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0322	1	Set of corrections to security procedure	8.1.0	8.2.0
2009-06	CT-44	CP-090412	0328		Clarification on access class applicability	8.1.0	8.2.0
2009-06	CT-44				Correction of minor typo	8.2.0	8.2.1
2009-09	CT-45	CP-090650	0226	7	Correcting ESM and SM coordination	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0255	4	Definition of valid GUTI	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0266	3	Clarification of T3212	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0310	6	TFT for default bearer	8.2.1	8.3.0
2009-09	CT-45	CP-090630	0329	9	Corrections in TFT checks	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0330	4	Resynchronization of EPS bearer contexts on TAU without active flag	8.2.1	8.3.0
2009-09	CT-45	CP-090652	0333	2	Inclusion of GERAN/UTRAN parameters in ESM messages	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0337	1	Clarifications on usage of EPS security context	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0338	1	BCM mode notification for LTE UE	8.2.1	8.3.0
2009-09	CT-45	CP-090677	0340		Update to the CSG ID definition	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0344		Replacing "MS" by "UE"	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0345	1	Correction of error handling	8.2.1	8.3.0
2009-09	CT-45	CP-090677	0346	1	Clarifications related to manual CSG selection	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0358	2	Handling of UE's usage setting, voice setting and VoIMS indicator – 24.301	8.2.1	8.3.0

2009-09	CT-45	CP-090653	0362	2	Storing EPS security parameters	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0370	2	Clarification on CSFB using redirection	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0372	5	Disabling E-UTRAN capability for the voice centric UE	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0374	2	Detach procedure for the last PDN disconnect by the network	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0375	1	Correction for network abnormal case - Attach and TAU procedures collision	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0376	2	Correction for abnormal case on network side due to lower layer failure	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0379	4	Inclusion of Old P-TMSI signature IE in ATTACH REQUEST and TRACKING AREA UPDATE REQUEST	8.2.1	8.3.0
2009-09	CT-45	CP-090652	0380	1	Interaction between S1 mode and A/Gb or Iu mode	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0381	1	Selected PLMN identity at NAS signalling connection establishment	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0382	4	Aligning UE modes of operation definition with stage 2 principles for CS domain and IM CN Subsystem selection	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0388	2	Corrections for abnormal case of GUTI REALLOCATION procedure	8.2.1	8.3.0
2009-09	CT-45	CP-090677	0389	1	The abnormal case of detach for CSG	8.2.1	8.3.0
2009-09	CT-45	CP-090652	0391	2	Handling of unknown QCI in the network	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0393	1	Corrections for TAU complete initiation	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0395	1	Corrections for Combined TAU procedure initiation	8.2.1	8.3.0
2009-09	CT-45	CP-090652	0396	1	NAS COUNT estimation correction	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0397	2	Security protection of Security mode reject	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0398	1	Rename of ESM cause #30 and #31	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0400	2	Abnormal case of combined default bearer and dedicated bearer	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0405	1	Clarification of behavior upon reception of ESM cause #43	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0407	1	Correcting service type and EPS update type	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0408		Addition of missing LV-E format	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0409	1	Clarification on APN-AMBR IE description	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0411	2	Clarification on abnormal cases in the UE for a few ESM procedures	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0413	1	Correction for the misplaced ESM message	8.2.1	8.3.0
2009-09	CT-45	CP-090733	0415	1	Additional triggers for tracking area update procedure	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0417	2	Deletion of mapped context after detach	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0419	1	Corrections to EPS security context handling	8.2.1	8.3.0
2009-09	CT-45	CP-090652	0425	2	Providing the MSISDN to the MS	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0426		Correction QCI within EPS quality of service information	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0428		Removal of inclusion of cause#46 in some ESM reject messages	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0429		Correction of definition of Linked EPS bearer identity IE	8.2.1	8.3.0
2009-09	CT-45	CP-090652	0430	1	MME and network synchronisation during TAU	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0439	2	Clarification to UE requested bearer modification procedure	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0442		Dependency between transport of NAS messages procedure and other EMM procedures	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0447	1	Correction for EPS update status change	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0448	2	Security handling of TAU	8.2.1	8.3.0
2009-09	CT-45	CP-090651	0449	1	Correction for the usage of Additional GUTI IE	8.2.1	8.3.0
2009-09	CT-45	CP-090674	0452	1	Corrections for detach procedure	8.2.1	8.3.0
2009-09	CT-45	CP-090675	0459	1	Paging for SMS messages	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0461	1	Clarification of the abnormal case in the attach procedure	8.2.1	8.3.0
2009-09	CT-45	CP-090652	0469	1	Miscelleneous corrections to references and incorrect aspects of the specification	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0479	2	Radio capability handling	8.2.1	8.3.0
2009-09	CT-45	CP-090653	0481	3	UE handling unknown QCI value received from the network	8.2.1	8.3.0
2009-09	CT-45	CP-090652	0482	1	Local deactivation of GBR EPS bearer context at MME during RLF	8.2.1	8.3.0
2009-09	CT-45	CP-090682	0487	1	Graphs for paging procedures	8.2.1	8.3.0
2009-09	CT-45	CP-090650	0490		Clarification of bearer context deactivation procedure and correction for ESM cause name	8.2.1	8.3.0
2009-09	CT-45	CP-090675	0494	1	Parameters for SMS over SGs charging	8.2.1	8.3.0
2009-09	CT-45	CP-090682	0331	2	Clarifications related to security mode control procedure	8.3.0	9.0.0
2009-09	CT-45	CP-090694	0341	2	Paging Optimization	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0342	1	Including call type "emergency calls"	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0343	1	Introducing reject cause value for emergency service over EPS	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0347	3	Bearer resource allocation for emergency service	8.3.0	9.0.0
2009-09	CT-45	CP-090690	0348	4	PDN Connection for emergency service	8.3.0	9.0.0
2009-09	CT-45	CP-090690	0349	3	Types of EMM procedures for emergency service	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0351	3	Authentication failure for emergency service	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0352	2	Limited service state attach for emergency service	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0353	4	Emergency service security	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0356	2	Emergency service authentication	8.3.0	9.0.0
2009-09	CT-45	CP-090682	0366	2	Clarify terminology of PTI assignment in bearer context	8.3.0	9.0.0
2009-09	CT-45	CP-090690	0422	1	Null algorithm for integrity protection	8.3.0	9.0.0
2009-09	CT-45	CP-090690	0433	2	UE states and attach for emergency services	8.3.0	9.0.0

2009-09	CT-45	CP-090690	0440	1	Update the forbidden TAI list in the limited state	8.3.0	9.0.0
2009-09	CT-45	CP-090690	0441	1	Bearer resource modification for emergency bearer	8.3.0	9.0.0
2009-09	CT-45	CP-090690	0444	1	Support indications for IMS Voice over PS session and emergency call	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0456	2	Clarification about the UE handling with the TAI list in the forbidden TA	8.3.0	9.0.0
2009-09	CT-45	CP-090690	0464	1	GUTI allocation for the UE without USIM	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0466	2	Handling of attach rejection for emergency service	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0468	2	Deactivating non-emergency bearers	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0473	3	Limited service state attach for emergency service	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0474	1	Detach on timeout for emergency service	8.3.0	9.0.0
2009-09	CT-45	CP-090689	0476	1	HSS detach request and deactivate non-emergency bearers	8.3.0	9.0.0
2009-09	CT-45	CP-090694	0483	1	Update of allowed CSG list after successful manual selection of a CSG cell in a different PLMN	8.3.0	9.0.0
2009-09	CT-45	CP-090682	0493	1	Discard unencrypted NAS messages	8.3.0	9.0.0
2009-12	CT-46	CP-090922	0485	5	ESM retransmission and PTI mismatch issue	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0496	2	Stop paging optimization for emergency attached UE	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0497	4	RRC establishment cause for Emergency Service	9.0.0	9.1.0
2009-12	CT-46	CP-090935	0498	3	Clarification on the Closed mode CSG cell	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0499	2	Corrections for description of UE behaviour in state EMM-REGISTERED	9.0.0	9.1.0
2009-12	CT-46	CP-090935	0500	3	Operator CSG List	9.0.0	9.1.0
2009-12	CT-46	CP-090899	0505	1	Mapped QCI Handling in UE	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0507	1	Correction on Timer handling	9.0.0	9.1.0
2009-12	CT-46	CP-090898	0512		Correction of criterion to trigger TAU	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0513	1	Specification of EPS emergency bearer services attach rules	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0515	4	TAU authentication while attached for emergency services	9.0.0	9.1.0
2009-12	CT-46	CP-090915	0518	3	UE mode of operation selection corrections and additions	9.0.0	9.1.0
2009-12	CT-46	CP-090935	0521	4	Processing the reject cause code #25 for the Operator CSG List	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0523		Deactivating non-emergency bearers	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0524	3	Clarification for TAU trigger for NAS recovery	9.0.0	9.1.0
2009-12	CT-46	CP-090916	0526	4	Correction to the SMS paging procedure	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0529	1	Correction to conditions for EMM initiating service request	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0530		EMM state machine on the UE side for emergency attach	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0534	4	EPS security context storage while emergency EPS security context exists	9.0.0	9.1.0
2009-12	CT-46	CP-090899	0540	2	From MBR of default PDP context to APN-AMBR of default EPS bearer	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0542	1	Correction of length values for ESM message container IEIs	9.0.0	9.1.0
2009-12	CT-46	CP-090898	0546	1	Correction to SMC procedure for establishment of mapped EPS security context in EMM-IDLE	9.0.0	9.1.0
2009-12	CT-46	CP-090898	0548	1	Correction to establishment of mapped EPS security context during inter-sytem handover	9.0.0	9.1.0
2009-12	CT-46	CP-090898	0550	1	Correction to the storage of the EPS security context	9.0.0	9.1.0
2009-12	CT-46	CP-090898	0552	4	Correction to the EPS security context handling	9.0.0	9.1.0
2009-12	CT-46	CP-090898	0554	2	Correction to the EPS authentication procedure	9.0.0	9.1.0
2009-12	CT-46	CP-090899	0556	4	Transition to the EMM-DEREGISTERED state and EPS security context actions	9.0.0	9.1.0
2009-12	CT-46	CP-090898	0562	4	Clarification of local detach	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0563	2	Clarifications on EPS security and minor corrections	9.0.0	9.1.0
2009-12	CT-46	CP-090916	0564	4	Combined Attach and TAU for "SMS only" and "CS fallback not preferred", and related UE behaviour	9.0.0	9.1.0
2009-12	CT-46	CP-090916	0569	2	Ignoring paging for CS fallback to A/Gb or Iu mode by an SMS only UE	9.0.0	9.1.0
2009-12	CT-46	CP-090899	0571	3	Default value for T3412	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0574	2	Enhanced CS fallback to 1xRTT	9.0.0	9.1.0
2009-12	CT-46	CP-090900	0576	5	NAS count handling in idle mode inter-RAT mobility	9.0.0	9.1.0
2009-12	CT-46	CP-090900	0578	2	NAS count handling on inter-RAT mobility	9.0.0	9.1.0
2009-12	CT-46	CP-090899	0580		Integrity protection of DETACH REQUEST	9.0.0	9.1.0
2009-12	CT-46	CP-090926	0581	4	Generic Transport of NAS messages	9.0.0	9.1.0
2009-12	CT-46	CP-090915	0584	1	Clarification of disabling E-UTRAN capabilities	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0585	1	Handling of only Emergency Bearers existing scenarios	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0588	1	Remove Support of Emergency HO from HRPD to E-UTRAN	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0589	1	EMM context handling for emergency attach	9.0.0	9.1.0
2009-12	CT-46	CP-090916	0590	2	Detach for "SMS only"	9.0.0	9.1.0
2009-12	CT-46	CP-090915	0592	1	1xCSFB triggers for RRC establishment	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0593	2	Detach with re-attach required	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0594		Paging cycles for EPS using S-TMSI	9.0.0	9.1.0
2009-12	CT-46	CP-090900	0598	1	Defining the value of NAS COUNTs	9.0.0	9.1.0
2009-12	CT-46	CP-090898	0602		Correcting the handling of multiple authentication failures in the UE	9.0.0	9.1.0
2009-12	CT-46	CP-090899	0604	1	Handling of missing NAS Securirty Mode Complete when generating mapped context	9.0.0	9.1.0

2009-12	CT-46	CP-090900	0606	1	Security handling when NAS COUNT wrap around	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0607	2	Deactivate non-EMC bearers with CSG ID not in allowed CSG list	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0611	1	Introduction of generic notification procedure	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0615	1	Clarifications on security	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0618	1	Rules for integrity protection with NULL algorithm	9.0.0	9.1.0
2009-12	CT-46	CP-090899	0620	1	TFT corrections	9.0.0	9.1.0
2009-12	CT-46	CP-090922	0621	2	Interpretation of GPRS timer value of 0	9.0.0	9.1.0
2009-12	CT-46	CP-090930	0625	1	Handling authentication failure during TAU	9.0.0	9.1.0
2009-12	CT-46	CP-090935	0626	1	Removal of definition of Allowed CSG list	9.0.0	9.1.0
2009-12	CT-46	CP-090916	0629	1	Abnormal cases in the UE for "SMS only" and "CS Fallback not preferred"	9.0.0	9.1.0
2009-12	CT-46	CP-090898	0633	2	Correction to the NAS security mode control procedure	9.0.0	9.1.0
2009-12	CT-46	CP-091054	0637	2	Alignment with TS23.401 caused by changing the term CSFB to "CSFB and SMS over SGs".	9.0.0	9.1.0
2009-12	CT-46	CP-090919	0567	5	Protecting the allowed CSG list	9.0.0	9.1.0
2010-03	CT-47	CP-100144	0587	3	Deactive ISR for UE attached for emergency bearer services	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0624	3	EPS Bearer Context Synchronization during Extended Service Request	9.1.0	9.2.0
2010-03	CT-47	CP-100106	0639	1	Correction of MME DL NAS COUNT at handover	9.1.0	9.2.0
2010-03	CT-47	CP-100139	0640	1	Inclusion of routing identifier for generic NAS transport	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0641		Tracking Area Update Procedure	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0642	1	UE Initiated Detach Procedure	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0643		UE Substate PLMN Search	9.1.0	9.2.0
2010-03	CT-47	CP-100106	0647	2	Security at idle mobility from E-UTRAN to UTRAN/GERAN	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0657		UE behavior after EPS bearer context deactivation	9.1.0	9.2.0
2010-03	CT-47	CP-100106	0660	2	Correction of used parameter in coordination between ESM and SM	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0664	1	Store EPS security context at state transition to EMM-DEREGISTERED	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0665	1	Definition of attached for emergency bearer service	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0667	2	Defining Selective camping capability IE	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0668	1	Security handling when NAS COUNT wrap around	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0670	1	Deletion of RAND and RES in the UE	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0671	1	Add packet filters to existing TFT	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0672	1	CSG subcription expiration and non-emergency bearer deactivation	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0673		Clarification of IMEI used for EMC attach	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0674	1	Correction on the security protection of the NAS message	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0675	1	Handling of authentication failure in EMC cases	9.1.0	9.2.0
2010-03	CT-47	CP-100106	0677	2	EPS security context handling in detach procedure	9.1.0	9.2.0
2010-03	CT-47	CP-100106	0679	1	Re-Authentication after intergity check failure of TAU Request	9.1.0	9.2.0
2010-03	CT-47	CP-100148	0682		Use of Cause #25 when UE's subscription to CSG has expired – 24.301	9.1.0	9.2.0
2010-03	CT-47	CP-100106	0685		Correction on E-UTRAN Deactivate ISR timer	9.1.0	9.2.0
2010-03	CT-47	CP-100139	0686	1	Retransmission of non-transmistted LPP PDUs	9.1.0	9.2.0
2010-03	CT-47	CP-100106	0693	2	TAU request and ciphering in connected mode	9.1.0	9.2.0
2010-03	CT-47	CP-100139	0696	2	CS Fallback for MO-LR in Rel9	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0700	1	Add reactivation requested cause code to EPS	9.1.0	9.2.0
2010-03	CT-47	CP-100106	0702	1	Deletion of mapped EPS security context when I-RAT HO fails	9.1.0	9.2.0
2010-03	CT-47	CP-100126	0704		UE behaviour corrections for 'SMS only'	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0705		Definition of non-emergency EPS bearer context	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0711	2	Pre Rel8 QoS mapping when this QoS is not received while on E-UTRAN	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0713	1	Clarification of Integrity protection of Service Request in section 4.4.3.3	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0714	1	No reset of DL NAS Count on Security Mode Command accepted by the UE	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0716	2	Attach for emergency bearer services to a network not supporting EM BS	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0718	1	Security Mode Command using NULL algos during TAU for normal attached UE	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0720	1	Retransmission of PDN connectivity request for emergency bearer services	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0724		Correction of access class bit 10 handling	9.1.0	9.2.0
2010-03	CT-47	CP-100144	0725	2	Mobility aspects of Emergency attached UEs	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0726	1	Arrange definitions in alphabetical order	9.1.0	9.2.0
2010-03	CT-47	CP-100062	0708	3	Authentication Procedure after Inter PLMN Handover	9.1.0	9.2.0
2010-03	CT-47	CP-100134	0727	3	Alignment of TAI list boundary with 2G/3G LA boundary	9.1.0	9.2.0
2010-03	CT-47	CP-100210	0730	2	Correct terminating domain selection for IMS voice UEs	9.1.0	9.2.0
2010-06	CT#48	CP-100354	0722	3	Avoiding rejection of a CS fallback due to CSG subscription expiry	9.2.0	9.3.0
2010-06	CT#48	CP-100354	0735	1	eKSI value setting for no valid EPS security context	9.2.0	9.3.0
2010-06	CT#48	CP-100360	0736	4	Authentication procedure for emergency services	9.2.0	9.3.0

2010-06	CT#48	CP-100360	0746	2	Handover to EUTRAN including NULL algos	9.2.0	9.3.0
2010-06	CT#48	CP-100360	0748	1	Authentication failure by UE while it has a PDN connection for emergency bearer services	9.2.0	9.3.0
2010-06	CT#48	CP-100362	0749	3	Add HeNB name	9.2.0	9.3.0
2010-06	CT#48	CP-100354	0751	1	Correction on request type	9.2.0	9.3.0
2010-06	CT#48	CP-100354	0752	1	Correction of conditions for TAU and ISR deactivation for T-ADS	9.2.0	9.3.0
2010-06	CT#48	CP-100354	0753	2	CSFB corrections in Service request procedure	9.2.0	9.3.0
2010-06	CT#48	CP-100354	0754	1	No NAS retransmission of SMS messages	9.2.0	9.3.0
2010-06	CT#48	CP-100348	0757	1	Voice domain preference alignments	9.2.0	9.3.0
2010-06	CT#48	CP-100354	0759		Update status for cause #9 and #10	9.2.0	9.3.0
2010-06	CT#48	CP-100349	0761	1	Combined TAU trigger after SRVCC	9.2.0	9.3.0
2010-06	CT#48	CP-100354	0763	1	Cause #39	9.2.0	9.3.0
2010-06	CT#48	CP-100360	0767	3	Clarification to establishment cause used by a UE in case of EMC procedure.	9.2.0	9.3.0
2010-06	CT#48	CP-100360	0768	2	Clarifications to expirey of Periodic RAU and mobile Reachable timer in case of EMC	9.2.0	9.3.0
2010-06	CT#48	CP-100350	0770	2	Clarification to network initiated detach procedure with cause #25	9.2.0	9.3.0
2010-06	CT#48	CP-100360	0771	1	Handling EPS Security Contexts	9.2.0	9.3.0
2010-06	CT#48	CP-100348	0775	2	Correction to UE mode of operation	9.2.0	9.3.0
2010-06	CT#48	CP-100339	0777	3	Correction to mapping of EPS QoS to pre-Rel-8 QoS	9.2.0	9.3.0
2010-06	CT#48	CP-100354	0783	1	Correction of selective camping IE inclusion requirement for 1x CS fallback capable UE	9.2.0	9.3.0
2010-06	CT#48	CP-100360	0784	2	Emergency attach reject from EMM in shared networks	9.2.0	9.3.0
2010-09	CT#49	CP-100501	0739	4	Corrections to UE mode of operation selection taking into account the UE's availability for voice calls in the IMS	9.3.0	9.4.0
2010-09	CT#49	CP-100506	0786	2	Handling of Detach Procedure for non-EPS services on a CSG cell which is no longer valid for the UE.and IMS EMG call is active.	9.3.0	9.4.0
2010-09	CT#49	CP-100506	0787	1	Emergency security context creation at standalone SMC	9.3.0	9.4.0
2010-09	CT#49	CP-100501	0789	1	Adding spec reference to ensure QoS alignment	9.3.0	9.4.0
2010-09	CT#49	CP-100506	0794	2	Skip Authentication for Emergency Services	9.3.0	9.4.0
2010-09	CT#49	CP-100506	0797	1	Clarification to timer T3418 and T3420 timer description in EMC case.	9.3.0	9.4.0
2010-09	CT#49	CP-100501	0812	2	On UE handling of 1xCSFB failure due to lower layer failure	9.3.0	9.4.0
2010-09	CT#49	CP-100501	0820	1	Allowing the UE to send a request for emergency call when the timer T3442 is running	9.3.0	9.4.0
2010-09	CT#49	CP-100495	0832	3	Correction on CS Fallback procedure using Release with Redirection	9.3.0	9.4.0
2010-09	CT#49	CP-100506	0842	1	Clarification to an emergency PDN connection establishment procedure.	9.3.0	9.4.0
2010-09	CT#49	CP-100506	0844	1	Handling of collision of Network Initiated Detach procdure with Service Request procedure and TAU procedure.	9.3.0	9.4.0
2010-09	CT#49	CP-100495	0850	1	No EPS bearer context activated during combined tracking area update	9.3.0	9.4.0
2010-09	CT#49	CP-100485	0852	1	Context transfer on inter-system change from A/Gb mode or Iu mode	9.3.0	9.4.0
2010-09	CT#49	CP-100506	0854	1	Skip authentication during TAU in EMC cases	9.3.0	9.4.0
2010-09	CT#49	CP-100506	0859	1	Local bearer deactivation and UE status	9.3.0	9.4.0
2010-09	CT#49	CP-100501	0868	1	Inclusion of transaction identifier	9.3.0	9.4.0
2010-09	CT#49	CP-100501	0871	1	Alignment with 23.401 for ESM cause value #52 "single address bearers only allowed"	9.3.0	9.4.0
2010-12	CT#50	CP-100747	0897	1	Deleting equivalent PLMNs list in EMC case	9.4.0	9.5.0
2010-12	CT#50	CP-100740	0930	1	ISR deactivation before TAU when UE moves from PMM-CONNECTED to E-UTRAN	9.4.0	9.5.0
2010-12	CT#50	CP-100742	0935	1	Correction in the use of cause value #2 in detach collision cases	9.4.0	9.5.0
2010-12	CT#50	CP-100747	0948	1	Correction on EMM authentication failure for EMC services	9.4.0	9.5.0
2011-03	CT#51	CP-110174	0979	1	Service request initiation for dual rx 1xCSFB UE	9.5.0	9.6.0
2011-03	CT#51	CP-110171	1017		Correction to detection of CSG cell based on CSG ID – 24.301	9.5.0	9.6.0
2011-03	CT#51	CP-110163	1020	3	Sending ESM messages together with Service request procedure	9.5.0	9.6.0
2011-03	CT#51	CP-110253	1028	4	Clarification to RRC establishment cause when device is attaching for emergency bearer services.	9.5.0	9.6.0
2011-06	CT#52	CP-110455	1041		Correction on encoding of CS-LCS in EPS network feature support IE	9.6.0	9.7.0
2011-06	CT#52	CP-110446	1053		Manipulation of CSG ID entries (in ACL and OCL) and the associated PLMNID - LTE	9.6.0	9.7.0
2011-06	CT#52	CP-110453	1073	1	Modification of NAS security context storage	9.6.0	9.7.0
2011-09	CT#54	CP-110665	1205	1	Reject Cause handling while UE attaching for emergency bearer services	9.7.0	9.8.0
2012-03	CT#55	CP-120102	1319	2	Re-attach for emergency bearer service	9.8.0	9.9.0
2012-06	CT#56	CP-120296	1383	1	Ensuring add filter resource modification targets a single traffic flow aggregate	9.9.0	9.10.0
2013-03	CT#59	CP-130099	1609	2	Inclusion of PLMN ID for the CS domain	9.10.0	9.11.0

History

Document history		
V9.1.0	January 2010	Publication
V9.2.0	April 2010	Publication
V9.3.0	June 2010	Publication
V9.4.0	October 2010	Publication
V9.5.0	January 2011	Publication
V9.6.0	March 2011	Publication
V9.7.0	June 2011	Publication
V9.8.0	October 2011	Publication
V9.9.0	March 2012	Publication
V9.10.0	July 2012	Publication
V9.11.0	April 2013	Publication