3GPP TS 24.501 V15.0.0 (2018-06)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3 (Release 15)

Keywords
5G, 5GS, EPS, stage 3, layer 3, user equipment, network

3GPP

Postal address

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

Internet
http://www.3gpp.org

Contents

Foreword....17
1 Scope....18
2 References....18
3 Definitions and abbreviations....20
3.1 Definitions....20
3.2 Abbreviations....23
4 General....25
4.1 Overview....25
4.2 Coordination between the protocols for 5GS mobility management and 5GS session management....25
4.3 UE domain selection....25
4.3.1 UE's usage setting....25
4.3.2 Domain selection for UE originating sessions / calls....25
4.3.3 Change of UE's usage setting....26
4.3.4 Change or determination of IMS voice availability....26
4.4 NAS security....27
4.4.1 General....27
4.4.2 Handling of 5G NAS security contexts....27
4.4.2.1 General....27
4.4.2.2 Establishment of a mapped 5G NAS security context during inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode....29
4.4.2.3 Establishment of secure exchange of NAS messages....29
4.4.2.4 Change of security keys....30
4.4.3 Handling of NAS COUNT and NAS sequence number....31
4.4.3.1 General....31
4.4.3.2 Replay protection....31
4.4.3.3 Integrity protection and verification....31
4.4.3.4 Ciphering and deciphering....32
4.4.3.5 NAS COUNT wrap around....32
4.4.4 Integrity protection of NAS signalling messages....32
4.4.4.1 General....32
4.4.4.2 Integrity checking of NAS signalling messages in the UE....33
4.4.4.3 Integrity checking of NAS signalling messages in the AMF....33
4.4.5 Ciphering of NAS signalling messages....35
4.5 Unified access control....36
4.5.1 General....36
4.5.2 Determination of the access identities and access category associated with a request for access....37
4.5.3 Operator-defined access categories....38
4.5.4 Access control and checking....39
4.5.4.1 Access control and checking in 5GMM-IDLE mode....39
4.5.4.2 Access control and checking in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication....40
4.5.5 Exception handling and avoiding double barring....41
4.5.6 Mapping between access categories/access identities and RRC establishment cause....43
4.6 Network slicing....43
4.6.1 General....43
4.6.2 Mobility management aspects....44
4.6.2.1 General....44
4.6.2.2 NSSAI storage....44
4.6.3 Session management aspects....45
4.6.3.1 General....45
4.7 NAS over non-3GPP access....46
4.7.1 General....46
4.7.2 5GS mobility management aspects....46
4.7.2.1 General....46

4.7.2.2 Establishment cause for non-3GPP access 46
4.7.3 5GS session management aspects 47
4.8 Interworking with E-UTRAN connected to EPC 47
4.8.1 General 47
4.8.2 Single-registration mode 47
4.8.2.1 General 47
4.8.2.2 Single-registration mode with N26 interface 47
4.8.2.3 Single-registration mode without N26 interface 47
4.8.3 Dual-registration mode 48
4.8.4 Core Network selection 49
4.9 Disabling and re-enabling of UE's N1 mode capability 50
4.9.1 General 50
4.9.2 Disabling and re-enabling of UE's N1 mode capability for 3GPP access 50
4.9.3 Disabling and re-enabling of UE's N1 mode capability for non-3GPP access 50

5 Elementary procedures for 5GS mobility management 51
5.1 Overview 51
5.1.1 General 51
5.1.2 Types of 5GMM procedures 51
5.1.3 5GMM sublayer states 52
5.1.3.1 General 52
5.1.3.2 5GMM sublayer states 52
5.1.3.2.1 5GMM sublayer states in the UE 52
5.1.3.2.1.1 General 52
5.1.3.2.1.2 Main states 53
5.1.3.2.1.2.1 5GMM-NULL 53
5.1.3.2.1.2.2 5GMM-DEREGISTERED 53
5.1.3.2.1.2.3 5GMM-REGISTERED-INITIATED 53
5.1.3.2.1.2.4 5GMM-REGISTERED 53
5.1.3.2.1.2.5 5GMM-DEREGISTERED-INITIATED 53
5.1.3.2.1.2.6 5GMM-SERVICE-REQUEST-INITIATED 53
5.1.3.2.1.3 Substates of state 5GMM-DEREGISTERED 54
5.1.3.2.1.3.1 General 54
5.1.3.2.1.3.2 5GMM-DEREGISTERED.NORMAL-SERVICE 54
5.1.3.2.1.3.3 5GMM-DEREGISTERED.LIMITED-SERVICE 54
5.1.3.2.1.3.4 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION 54
5.1.3.2.1.3.5 5GMM-DEREGISTERED.PLMN-SEARCH 54
5.1.3.2.1.3.6 5GMM-DEREGISTERED.NO-SUPI 54
5.1.3.2.1.3.7 5GMM-DEREGISTERED.NO-CELL-AVAILABLE 54
5.1.3.2.1.3.8 5GMM-DEREGISTERED.eCALL-INACTIVE 55
5.1.3.2.1.4 Substates of state 5GMM-REGISTERED 55
5.1.3.2.1.4.1 General 55
5.1.3.2.1.4.2 5GMM-REGISTERED.NORMAL-SERVICE 55
5.1.3.2.1.4.3 5GMM-REGISTERED.NON-ALLOWED-SERVICE 55
5.1.3.2.1.4.4 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE 55
5.1.3.2.1.4.5 5GMM-REGISTERED.LIMITED-SERVICE 56
5.1.3.2.1.4.6 5GMM-REGISTERED.PLMN-SEARCH 56
5.1.3.2.1.4.7 5GMM-REGISTERED.NO-CELL-AVAILABLE 56
5.1.3.2.2 5GS update status in the UE 56
5.1.3.2.3 5GMM sublayer states in the network side 56
5.1.3.2.3.1 General 56
5.1.3.2.3.2 5GMM-DEREGISTERED 57
5.1.3.2.3.3 5GMM-COMMON-PROCEDURE-INITIATED 57
5.1.3.2.3.4 5GMM-REGISTERED 57
5.1.3.2.3.5 5GMM-DEREGISTERED-INITIATED 57
5.1.4 Coordination between 5GMM and EMM 57
5.1.4.1 General 57
5.1.4.2 Coordination between 5GMM and EMM with N26 interface 57
5.1.4.3 Coordination between 5GMM and EMM without N26 interface 58
5.2 Behaviour of the UE in state 5GMM-DEREGISTERED and state 5GMM-REGISTERED 58
5.2.1 General 58
5.2.2 UE behaviour in state 5GMM-DEREGISTERED 58

5.2.2.1 General ... 58
5.2.2.2 Primary substate selection ... 59
5.2.2.2.1 Selection of the substate after power on ... 59
5.2.2.2 Detailed description of UE behaviour in state 5GMM-DEREGISTERED ... 59
5.2.2.2.1 NORMAL-SERVICE ... 59
5.2.2.2.2 LIMITED-SERVICE ... 59
5.2.2.2.3 ATTEMPTING-REGISTRATION ... 59
5.2.2.2.4 PLMN-SEARCH ... 60
5.2.2.2.5 NO-SUPI ... 60
5.2.2.2.6 NO-CELL-AVAILABLE ... 60
5.2.2.2.7 eCALL-INACTIVE ... 60
5.2.2.3 Substate when back to state 5GMM-DEREGISTERED from another 5GMM state ... 60
5.2.3 UE behaviour in state 5GMM-REGISTERED ... 61
5.2.3.1 General ... 61
5.2.3.2 Detailed description of UE behaviour in state 5GMM-REGISTERED ... 61
5.2.3.2.1 NORMAL-SERVICE ... 61
5.2.3.2.2 NON-ALLOWED-SERVICE ... 61
5.2.3.2.3 ATTEMPTING-REGISTRATION-UPDATE ... 61
5.2.3.2.4 LIMITED-SERVICE ... 62
5.2.3.2.5 PLMN-SEARCH ... 62
5.2.3.2.6 NO-CELL-AVAILABLE ... 62
5.3 General on elementary 5GMM procedures ... 62
5.3.1 5GMM modes and N1 NAS signalling connection ... 62
5.3.1.1 Establishment of the N1 NAS signalling connection ... 62
5.3.1.2 Release of the N1 NAS signalling connection ... 63
5.3.1.3 5GMM-CONNECTED mode with RRC inactive indication ... 65
5.3.2 Permanent identifiers ... 66
5.3.3 Temporary identities ... 66
5.3.4 Registration areas ... 67
5.3.5 Service area restrictions ... 67
5.3.6 Mobile initiated connection only mode ... 69
5.3.7 Handling of the periodic registration update timer and mobile reachable timer ... 70
5.3.8 Handling of timer T3502 ... 71
5.3.9 Handling of NAS level mobility management congestion control ... 71
5.3.10 Handling of DNN based congestion control ... 72
5.3.11 Handling of S-NSSAI based congestion control ... 72
5.3.12 Handling of local emergency numbers ... 72
5.3.13 Lists of 5GS forbidden tracking areas ... 73
5.3.14 List of equivalent PLMNs ... 73
5.3.15 Transmission failure abnormal case in the UE ... 73
5.4 5GMM common procedures ... 74
5.4.1 Primary authentication and key agreement procedure ... 74
5.4.1.1 General ... 74
5.4.1.2 EAP based primary authentication and key agreement procedure ... 74
5.4.1.2.1 General ... 74
5.4.1.2.2 EAP-AKA' related procedures ... 76
5.4.1.2.2.1 General ... 76
5.4.1.2.2.2 Initiation ... 77
5.4.1.2.2.3 UE successfully authenticates network ... 77
5.4.1.2.2.4 Errors when handling EAP-request/AKA'-challenge message ... 77
5.4.1.2.2.5 Network successfully authenticates UE ... 78
5.4.1.2.2.6 UE handling EAP-AKA' notification ... 78
5.4.1.2.2.7 Network sending EAP-success message ... 78
5.4.1.2.2.8 UE handling EAP-success message ... 78
5.4.1.2.2.9 Network not successfully authenticates UE ... 78
5.4.1.2.2.10 Network sending EAP-failure message ... 78
5.4.1.2.2.11 UE handling EAP-success ... 78
5.4.1.2.3 EAP-TLS related procedures ... 79
5.4.1.2.3.1 General ... 79
5.4.1.2.4 EAP message reliable transport procedure ... 79
5.4.1.2.4.1 General ... 79

5.4.1.2.4.2 EAP message reliable transport procedure initiation by the network 79
5.4.1.2.4.3 EAP message reliable transport procedure accepted by the UE 79
5.4.1.2.4.4 Abnormal cases on the network side 80
5.4.1.2.4.5 Abnormal cases in the UE 80
5.4.1.2.5 EAP result message transport procedure 80
5.4.1.2.5.1 General 80
5.4.1.2.5.2 EAP result message transport procedure initiation by the network 80
5.4.1.3 5G AKA based primary authentication and key agreement procedure 81
5.4.1.3.1 General 81
5.4.1.3.2 Authentication initiation by the network 81
5.4.1.3.3 Authentication response by the UE 82
5.4.1.3.4 Authentication completion by the network 83
5.4.1.3.5 Authentication not accepted by the network 83
5.4.1.3.6 Authentication not accepted by the UE 83
5.4.1.3.7 Abnormal cases 84
5.4.2 Security mode control procedure 87
5.4.2.1 General 87
5.4.2.2 NAS security mode control initiation by the network 88
5.4.2.3 NAS security mode command accepted by the UE 89
5.4.2.4 NAS security mode control completion by the network 90
5.4.2.5 NAS security mode command not accepted by the UE 90
5.4.2.6 Abnormal cases in the UE 91
5.4.2.7 Abnormal cases on the network side 91
5.4.3 Identification procedure 91
5.4.3.1 General 91
5.4.3.2 Identification initiation by the network 92
5.4.3.3 Identification response by the UE 92
5.4.3.4 Identification completion by the network 92
5.4.3.5 Abnormal cases in the UE 92
5.4.3.6 Abnormal cases on the network side 92
5.4.4 Generic UE configuration update procedure 93
5.4.4.1 General 93
5.4.4.2 Generic UE configuration update procedure initiated by the network 94
5.4.4.3 Generic UE configuration update accepted by the UE 95
5.4.4.4 Generic UE configuration update completion by the network 96
5.4.4.5 Abnormal cases in the UE 96
5.4.4.6 Abnormal cases on the network side 97
5.4.5 NAS transport procedure(s) 97
5.4.5.1 General 97
5.4.5.2 UE-initiated NAS transport procedure 98
5.4.5.2.1 General 98
5.4.5.2.2 UE-initiated NAS transport procedure initiation 98
5.4.5.2.3 UE-initiated NAS transport of messages accepted by the network 99
5.4.5.2.4 UE-initiated NAS transport of messages not accepted by the network 102
5.4.5.2.5 Abnormal cases on the network side 103
5.4.5.3 Network-initiated NAS transport procedure 104
5.4.5.3.1 General 104
5.4.5.3.2 Network-initiated NAS transport procedure initiation 105
5.4.5.3.3 Network-initiated NAS transport of messages 106
5.4.6 5GMM status procedure 107
5.4.6.1 General 107
5.4.6.2 5GMM status received in the UE 107
5.4.6.3 5GMM status received in the network 107
5.5 5GMM specific procedures 107
5.5.1 Registration procedure 107
5.5.1.1 General 107
5.5.1.2 Registration procedure for initial registration 108
5.5.1.2.1 General 108
5.5.1.2.2 Initial registration initiation 108
5.5.1.2.3 5GMM common procedure initiation 110
5.5.1.2.4 Initial registration accepted by the network 111

5.5.1.2.5 Initial registration not accepted by the network 114
5.5.1.2.6 Initial registration for emergency services not accepted by the network 115
5.5.1.2.7 Abnormal cases in the UE 116
5.5.1.2.8 Abnormal cases on the network side 117
5.5.1.3 Registration procedure for mobility and periodic registration update 118
5.5.1.3.1 General 118
5.5.1.3.2 Mobility and periodic registration update initiation 119
5.5.1.3.3 5GMM common procedure initiation 122
5.5.1.3.4 Mobility and periodic registration update accepted by the network 122
5.5.1.3.5 Mobility and periodic registration update not accepted by the network 126
5.5.1.3.6 Abnormal cases in the UE 128
5.5.1.3.7 Abnormal cases on the network side 129
5.5.2 De-registration procedure 129
5.5.2.1 General 129
5.5.2.2 UE-initiated de-registration procedure 130
5.5.2.2.1 UE-initiated de-registration procedure initiation 130
5.5.2.2.2 UE-initiated de-registration procedure completion - common procedure 131
5.5.2.2.3 UE-initiated de-registration procedure completion for 5GS services over 3GPP access 131
5.5.2.2.4 UE-initiated de-registration procedure completion for 5GS services non-3GPP access 131
5.5.2.2.5 UE-initiated de-registration procedure completion for 5GS services over both 3GPP access and non-3GPP access 132
5.5.2.2.6 Abnormal cases in the UE 132
5.5.2.2.7 Abnormal cases in the network side 133
5.5.2.3 Network-initiated de-registration procedure 133
5.5.2.3.1 Network-initiated de-registration procedure initiation 133
5.5.2.3.2 Network-initiated de-registration procedure completion by the UE 134
5.5.2.3.3 Network-initiated de-registration procedure completion by the network 136
5.5.2.3.4 Abnormal cases in the UE 136
5.5.2.3.5 Abnormal cases in the network side 136
5.5.3 eCall inactivity procedure 137
5.6 5GMM connection management procedures 138
5.6.1 Service request procedure 138
5.6.1.1 General 138
5.6.1.2 Service request procedure initiation 139
5.6.1.3 Common procedure initiation 141
5.6.1.4 Service request procedure accepted by the network 141
5.6.1.5 Service request procedure not accepted by the network 141
5.6.1.6 Service request procedure for initiating a PDU session for emergency services not accepted by the network 143
5.6.1.7 Abnormal cases in the UE 144
5.6.1.8 Abnormal cases on the network side 145
5.6.2 Paging procedure 146
5.6.2.1 General 146
5.6.2.2 Paging for 5GS services 146
5.6.2.2.1 General 146
5.6.2.2.2 Abnormal cases on the network side 147
5.6.2.2.3 Abnormal cases in the UE 147
5.6.3 Notification procedure 147
5.6.3.1 General 147
5.6.3.2 Notification procedure initiation 147
5.6.3.3 Notification procedure completion 148
5.6.3.4 Abnormal cases on the network side 149

6 Elementary procedures for 5GS session management 149
6.1 Overview 149
6.1.1 General 149
6.1.2 Types of 5GSM procedures 150
6.1.3 5GSM sublayer states 150
6.1.3.1 General 150
6.1.3.2 5GSM sublayer states in the UE 151
6.1.3.2.1 Overview 151
6.1.3.2.2 PDU SESSION INACTIVE 151

6.1.3.2.3 PDU SESSION ACTIVE PENDING 151
6.1.3.2.4 PDU SESSION ACTIVE 151
6.1.3.2.5 PDU SESSION INACTIVE PENDING 151
6.1.3.2.6 PDU SESSION MODIFICATION PENDING 151
6.1.3.2.7 PROCEDURE TRANSACTION INACTIVE 152
6.1.3.2.8 PROCEDURE TRANSACTION PENDING 152
6.1.3.3 5GSM sublayer states in the network side 152
6.1.3.3.1 Overview 152
6.1.3.3.2 PDU SESSION INACTIVE 152
6.1.3.3.3 PDU SESSION ACTIVE 153
6.1.3.3.4 PDU SESSION INACTIVE PENDING 153
6.1.3.3.5 PDU SESSION MODIFICATION PENDING 153
6.1.3.3.6 PROCEDURE TRANSACTION INACTIVE 153
6.1.3.3.7 PROCEDURE TRANSACTION PENDING 153
6.1.4 Coordination between 5GSM and ESM 153
6.1.4.1 Coordination between 5GSM and ESM with N26 interface 153
6.1.4.2 Coordination between 5GSM and ESM without N26 interface 155
6.2 General on elementary 5GSM procedures 157
6.2.1 Principles of PTI handling for 5GSM procedures 157
6.2.2 PDU session types 158
6.2.3 PDU session management 158
6.2.4 IP address allocation 159
6.2.4.1 General 159
6.2.4.2 IP address allocation via NAS signalling 159
6.2.5 Quality of service 160
6.2.5.1 General 160
6.2.5.1.1 QoS rules 160
6.2.5.1.1.1 General 160
6.2.5.1.1.2 Signalled QoS rules 160
6.2.5.1.1.3 Derived QoS rules 162
6.2.5.1.2 Session-AMBR 162
6.2.5.1.3 UL user data packet matching 162
6.2.5.1.4 Reflective QoS 163
6.2.5.1.4.1 General 163
6.2.5.1.4.2 Derivation of packet filter for UL direction from DL user data packet 163
6.2.5.1.4.3 Creating a derived QoS rule by reflective QoS in the UE 165
6.2.5.1.4.4 Updating a derived QoS rule by reflective QoS in the UE 165
6.2.5.1.4.5 Deleting a derived QoS rule in the UE 165
6.2.5.1.4.6 Ignoring RQI in the UE 165
6.2.6 Local area data network (LADN) 165
6.2.7 Handling of DNN based congestion control 166
6.2.8 Handling of S-NSSAI based congestion control 166
6.2.9 Interaction with upper layers 167
6.2.9.1 General 167
6.2.9.2 URSP 167
6.2.10 Handling of 3GPP PS data off 167
6.3 Network-requested 5GSM procedures 168
6.3.1 PDU session authentication and authorization procedure 168
6.3.1.1 General 168
6.3.1.2 PDU EAP message reliable transport procedure 170
6.3.1.2.1 PDU EAP message reliable transport procedure initiation 170
6.3.1.2.2 PDU EAP message reliable transport procedure accepted by the UE 171
6.3.1.2.3 Abnormal cases on the network side 171
6.3.1.2.4 Abnormal cases in the UE 171
6.3.1.3 PDU EAP result message transport procedure 171
6.3.1.3.1 PDU EAP result message transport procedure initiation 171
6.3.2 Network-requested PDU session modification procedure 172
6.3.2.1 General 172
6.3.2.2 Network-requested PDU session modification procedure initiation 172
6.3.2.3 Network-requested PDU session modification procedure accepted by the UE 173
6.3.2.4 Network-requested PDU session modification procedure not accepted by the UE 174

6.3.2.5 Abnormal cases on the network side 175
6.3.2.6 Abnormal cases in the UE 175
6.3.3 Network-requested PDU session release procedure 176
6.3.3.1 General 176
6.3.3.2 Network-requested PDU session release procedure initiation 176
6.3.3.3 Network-requested PDU session release procedure accepted by the UE 177
6.3.3.4 N1 SM delivery skipped 180
6.3.3.5 Abnormal cases on the network side 180
6.3.3.6 Abnormal cases in the UE 181
6.4 UE-requested 5GSM procedures 181
6.4.1 UE-requested PDU session establishment procedure 181
6.4.1.1 General 181
6.4.1.2 UE-requested PDU session establishment procedure initiation 181
6.4.1.3 UE-requested PDU session establishment procedure accepted by the network 184
6.4.1.4 UE requested PDU session establishment procedure not accepted by the network 186
6.4.1.4.1 General 186
6.4.1.4.2 Handling of network rejection due to 5GSM cause #26 192
6.4.1.4.3 Handling of network rejection due to 5GSM cause other than 5GSM cause #26 192
6.4.1.5 Handling the maximum number of established PDU sessions 193
6.4.1.6 Abnormal cases in the UE 193
6.4.1.7 Abnormal cases on the network side 193
6.4.2 UE-requested PDU session modification procedure 194
6.4.2.1 General 194
6.4.2.2 UE-requested PDU session modification procedure initiation 194
6.4.2.3 UE-requested PDU session modification procedure accepted by the network 195
6.4.2.4 UE-requested PDU session modification procedure not accepted by the network 195
6.4.2.5 Abnormal cases in the UE 199
6.4.2.6 Abnormal cases on the network side 200
6.4.3 UE-requested PDU session release procedure 200
6.4.3.1 General 200
6.4.3.2 UE-requested PDU session release procedure initiation 200
6.4.3.3 UE-requested PDU session release procedure accepted by the network 201
6.4.3.4 UE-requested PDU session release procedure not accepted by the network 201
6.4.3.5 Abnormal cases in the UE 201
6.4.3.6 Abnormal cases on the network side 202
6.5 5GSM status procedure 202
6.5.1 General 202
6.5.2 5GSM status received in the UE 202
6.5.3 5GSM status received in the SMF 203
6.6 Miscellaneous procedures 203
6.6.1 Exchange of extended protocol configuration options 203

7 Handling of unknown, unforeseen, and erroneous protocol data 203
7.1 General 203
7.2 Message too short or too long 204
7.2.1 Message too short 204
7.2.2 Message too long 204
7.3 Unknown or unforeseen procedure transaction identity or PDU Session identity 204
7.3.1 Procedure transaction identity 204
7.3.2 PDU Session identity 204
7.4 Unknown or unforeseen message type 204
7.5 Non-semantical mandatory information element errors 205
7.5.1 Common procedures 205
7.5.2 5GS mobility management 205
7.5.3 5GS session management 205
7.6 Unknown and unforeseen IEs in the non-imperative message part 206
7.6.1 IEIs unknown in the message 206
7.6.2 Out of sequence IEs 206
7.6.3 Repeated IEs 206
7.7 Non-imperative message part errors 206
7.7.1 Syntactically incorrect optional IEs 206
7.7.2 Conditional IE errors 206

7.8 Messages with semantically incorrect contents 207
8 Message functional definitions and contents 207
8.1 Overview 207
8.2 5GS mobility management messages 207
8.2.1 Authentication request 207
8.2.1.1 Message definition 207
8.2.1.2 Authentication parameter RAND 208
8.2.1.3 Authentication parameter AUTN 208
8.2.1.4 EAP message 208
8.2.2 Authentication response 208
8.2.2.1 Message definition 208
8.2.2.2 Authentication response parameter 209
8.2.2.3 EAP message 209
8.2.3 Authentication result 209
8.2.3.1 Message definition 209
8.2.4 Authentication failure 210
8.2.4.1 Message definition 210
8.2.4.2 Authentication failure parameter 210
8.2.5 Authentication reject 210
8.2.5.1 Message definition 210
8.2.6 Registration request 211
8.2.6.1 Message definition 211
8.2.6.2 Non-current native NAS key set identifier 212
8.2.6.3 5GMM capability 212
8.2.6.4 UE security capability 212
8.2.6.5 Requested NSSAI 212
8.2.6.6 Last visited registered TAI 212
8.2.6.7 S1 UE network capability 212
8.2.6.8 Uplink data status 212
8.2.6.9 PDU session status 212
8.2.6.10 MICO indication 212
8.2.6.11 UE status 212
8.2.6.12 Additional GUTI 212
8.2.6.13 Allowed PDU session status 213
8.2.6.14 UE's usage setting 213
8.2.6.15 Requested DRX parameters 213
8.2.6.16 EPS NAS message container 213
8.2.6.17 Allowed PDU session status 213
8.2.6.18 Payload container 213
8.2.7 Registration accept 213
8.2.7.1 Message definition 213
8.2.7.2 5G-GUTI 214
8.2.7.3 Equivalent PLMNs 214
8.2.7.4 TAI list 215
8.2.7.5 Allowed NSSAI 215
8.2.7.6 Rejected NSSAI 215
8.2.7.7 Configured NSSAI 215
8.2.7.8 5GS network feature support 215
8.2.7.9 PDU session status 215
8.2.7.10 PDU session reactivation result 215
8.2.7.11 PDU session reactivation result error cause 215
8.2.7.12 LADN information 215
8.2.7.13 MICO indication 215
8.2.7.14 Service area list 216
8.2.7.15 T3512 value 216
8.2.7.16 Non-3GPP de-registration timer value 216
8.2.7.17 T3502 value 216
8.2.7.18 Emergency number list 216
8.2.7.19 Extended emergency number list 216
8.2.7.20 Transparent container 216
8.2.7.21 EAP message 216

8.2.8 Registration complete 216
8.2.8.1 Message definition 216
8.2.8.2 Transparent container 217
8.2.9 Registration reject 217
8.2.9.1 Message definition 217
8.2.9.2 T3346 value 217
8.2.9.3 T3502 value 217
8.2.9.4 EAP message 218
8.2.10 UL NAS transport 218
8.2.10.1 Message definition 218
8.2.10.2 PDU session ID 218
8.2.10.3 Old PDU session ID 218
8.2.10.4 Request type 218
8.2.10.5 S-NSSAI 219
8.2.10.6 DNN 219
8.2.10.7 Additional information 219
8.2.11 DL NAS transport 219
8.2.11.1 Message definition 219
8.2.11.2 PDU session ID 219
8.2.11.3 Additional information 219
8.2.11.4 5GMM cause 220
8.2.11.5 Back-off timer value 220
8.2.12 De-registration request (UE originating de-registration) 220
8.2.12.1 Message definition 220
8.2.13 De-registration accept (UE originating de-registration) 220
8.2.13.1 Message definition 220
8.2.14 De-registration request (UE terminated de-registration) 221
8.2.14.1 Message definition 221
8.2.14.2 5GMM cause 221
8.2.14.3 T3346 value 221
8.2.15 De-registration accept (UE terminated de-registration) 221
8.2.15.1 Message definition 221
8.2.16 Service request 222
8.2.16.1 Message definition 222
8.2.16.2 Uplink data status 222
8.2.16.3 PDU session status 223
8.2.16.4 Allowed PDU session status 223
8.2.17 Service accept 223
8.2.17.1 Message definition 223
8.2.17.2 PDU session status 223
8.2.17.3 PDU session reactivation result 223
8.2.17.4 PDU session reactivation result error cause 224
8.2.17.5 EAP message 224
8.2.18 Service reject 224
8.2.18.1 Message definition 224
8.2.18.2 PDU session status 224
8.2.18.3 T3346 value 224
8.2.18.4 EAP message 224
8.2.19 Configuration update command 225
8.2.19.1 Message definition 225
8.2.19.2 Configuration update indication 225
8.2.19.3 5G-GUTI 225
8.2.19.4 TAI list 226
8.2.19.5 Allowed NSSAI 226
8.2.19.6 Service area list 226
8.2.19.7 Full name for network 226
8.2.19.8 Short name for network 226
8.2.19.9 Local time zone 226
8.2.19.10 Universal time and local time zone 226
8.2.19.11 Network daylight saving time 226
8.2.19.12 LADN information 226

8.2.19.13 MICO indication 226
8.2.19.14 Configured NSSAI 226
8.2.19.15 Rejected NSSAI 226
8.2.20 Configuration update complete 226
8.2.20.1 Message definition 226
8.2.21 Identity request 227
8.2.21.1 Message definition 227
8.2.22 Identity response 227
8.2.22.1 Message definition 227
8.2.23 Notification 228
8.2.23.1 Message definition 228
8.2.24 Notification response 228
8.2.24.1 Message definition 228
8.2.24.2 PDU session status 229
8.2.25 Security mode command 229
8.2.25.1 Message definition 229
8.2.25.2 IMEISV request 230
8.2.25.3 $Hash_{AMF}$ 230
8.2.25.4 Selected EPS NAS security algorithms 230
8.2.25.5 EAP message 230
8.2.26 Security mode complete 230
8.2.26.1 Message definition 230
8.2.26.2 IMEISV 230
8.2.26.3 NAS message container 230
8.2.27 Security mode reject 231
8.6.27.1 Message definition 231
8.2.28 Security protected 5GS NAS message 231
8.2.28.1 Message definition 231
8.2.29 5GMM status 232
8.2.29.1 Message definition 232
8.3 5GS session management messages 232
8.3.1 PDU session establishment request 232
8.3.1.1 Message definition 232
8.3.1.2 PDU session type 233
8.3.1.3 SSC mode 233
8.3.1.4 Maximum number of supported packet filters 233
8.3.1.5 5GSM capability 233
8.3.1.6 SM PDU DN request container 233
8.3.1.7 Extended protocol configuration options 233
8.3.2 PDU session establishment accept 234
8.3.2.1 Message definition 234
8.3.2.2 5GSM cause 234
8.3.2.3 PDU address 234
8.3.2.4 RQ timer value 235
8.3.2.5 S-NSSAI 235
8.3.2.6 Mapped EPS bearer contexts 235
8.3.2.7 EAP message 235
8.3.2.8 Extended protocol configuration options 235
8.3.3 PDU session establishment reject 235
8.3.3.1 Message definition 235
8.3.3.2 Back-off timer value 236
8.3.3.3 Allowed SSC mode 236
8.3.3.4 EAP message 236
8.3.3.5 Extended protocol configuration options 236
8.3.4 PDU session authentication command 236
8.3.4.1 Message definition 236
8.3.4.2 EAP message 236
8.3.4.3 Extended protocol configuration options 236
8.3.5 PDU session authentication complete 237
8.3.5.1 Message definition 237
8.3.5.2 EAP message 237

8.3.5.3 Extended protocol configuration options 237
8.3.6 PDU session authentication result 237
8.3.6.1 Message definition 237
8.3.6.2 EAP message 238
8.3.6.3 Extended protocol configuration options 238
8.3.7 PDU session modification request 238
8.3.7.1 Message definition 238
8.3.7.2 5GSM capability 239
8.3.7.3 Maximum number of supported packet filters 239
8.3.7.4 Requested QoS rules 239
8.3.7.5 Extended protocol configuration options 239
8.3.8 PDU session modification reject 239
8.3.8.1 Message definition 239
8.3.8.2 Back-off timer value 240
8.3.8.3 Extended protocol configuration options 240
8.3.9 PDU session modification command 240
8.3.9.1 Message definition 240
8.3.9.2 5GSM cause 241
8.3.9.3 Session-AMBR 241
8.3.9.4 RQ timer value 241
8.3.9.5 Authorized QoS rules 241
8.3.9.6 Mapped EPS bearer contexts 241
8.3.9.7 Extended protocol configuration options 241
8.3.10 PDU session modification complete 241
8.3.10.1 Message definition 241
8.3.10.2 Extended protocol configuration options 242
8.3.11 PDU session modification command reject 242
8.3.11.1 Message definition 242
8.3.11.2 Extended protocol configuration options 242
8.3.12 PDU session release request 243
8.3.12.1 Message definition 243
8.3.12.2 Extended protocol configuration options 243
8.3.13 PDU session release reject 243
8.3.13.1 Message definition 243
8.3.13.2 Extended protocol configuration options 244
8.3.14 PDU session release command 244
8.3.14.1 Message definition 244
8.3.14.2 Back-off timer value 244
8.3.14.3 EAP message 245
8.3.14.4 Extended protocol configuration options 245
8.3.15 PDU session release complete 245
8.3.15.1 Message definition 245
8.3.15.2 Extended protocol configuration options 245
8.3.16 5GSM status 245
8.3.16.1 Message definition 245

9 General message format and information elements coding 246
9.1 Overview 246
9.2 Extended protocol discriminator 247
9.3 Security header type 247
9.4 PDU session identity 248
9.5 Spare half octet 248
9.6 Procedure transaction identity 248
9.7 Message type 248
9.8 Message authentication code 250
9.9 Sequence number 250
9.10 Other information elements 250
9.10.1 General 250
9.10.2 Common information elements 250
9.10.2.1 Additional information 250
9.10.2.2 EAP message 251
9.10.2.3 GPRS timer 251

9.10.2.4 GPRS timer 2 ... 251
9.10.2.5 GPRS timer 3 ... 251
9.10.2.6 S-NSSAI ... 251
9.10.2.7 S1 mode to N1 mode NAS transparent container ... 252
9.10.3 5GS mobility management (5GMM) information elements ... 254
9.10.3.1 5GMM capability ... 254
9.10.3.2 5GMM cause ... 254
9.10.3.3 5GS identity type ... 255
9.10.3.4 5GS mobile identity ... 256
9.10.3.5 5GS network feature support ... 259
9.10.3.6 5GS registration result ... 260
9.10.3.7 5GS registration type ... 261
9.10.3.8 5GS tracking area identity ... 262
9.10.3.9 5GS tracking area identity list ... 263
9.10.3.10 Access type ... 267
9.10.3.11 Allowed PDU session status ... 267
9.10.3.12 Authentication failure parameter ... 268
9.10.3.13 Authentication parameter AUTN ... 268
9.10.3.14 Authentication parameter RAND ... 268
9.10.3.15 Authentication response parameter ... 268
9.10.3.16 Configuration update indication ... 268
9.10.3.17 Daylight saving time ... 269
9.10.3.18 De-registration type ... 269
9.10.3.19 DNN ... 270
9.10.3.20 DRX parameters ... 270
9.10.3.21 Emergency number list ... 270
9.10.3.22 EPS NAS message container ... 270
9.10.3.23 EPS NAS security algorithms ... 271
9.10.3.24 Extended emergency number list ... 271
9.10.3.25 $Hash_{AMF}$ ... 271
9.10.3.26 IMEISV request ... 271
9.10.3.27 LADN information ... 271
9.10.3.28 MICO indication ... 272
9.10.3.29 NAS key set identifier ... 273
9.10.3.30 NAS message ... 273
9.10.3.31 NAS message container ... 274
9.10.3.32 NAS security algorithms ... 274
9.10.3.33 Network name ... 275
9.10.3.34 NSSAI ... 275
9.10.3.35 Payload container ... 276
9.10.3.36 Payload container type ... 277
9.10.3.37 PDU session identity 2 ... 277
9.10.3.38 PDU session reactivation result ... 277
9.10.3.39 PDU session reactivation result error cause ... 278
9.10.3.40 PDU session status ... 279
9.10.3.41 PLMN list ... 279
9.10.3.42 Rejected NSSAI ... 279
9.10.3.43 Request type ... 280
9.10.3.44 S1 UE network capability ... 281
9.10.3.45 Service area list ... 281
9.10.3.46 Service type ... 285
9.10.3.47 Time zone ... 285
9.10.3.48 Time zone and time ... 286
9.10.3.49 Transparent container ... 286
9.10.3.50 UE security capability ... 286
9.10.3.51 UE's usage setting ... 289
9.10.3.52 UE status ... 289
9.10.3.53 Uplink data status ... 290
9.10.4 5GS session management (5GSM) information elements ... 290
9.10.4.1 5GSM capability ... 290
9.10.4.2 5GSM cause ... 291

9.10.4.3 Allowed SSC mode 292
9.10.4.4 Extended protocol configuration options 293
9.10.4.5 Mapped EPS bearer contexts 293
9.10.4.6 Maximum number of supported packet filters 296
9.10.4.7 PDU address 296
9.10.4.8 PDU session type 297
9.10.4.9 QoS rules 298
9.10.4.10 Session-AMBR 306
9.10.4.11 SM PDU DN request container 307
9.10.4.12 SSC mode 307
9.11 3GPP specific coding information defined within present document 308
9.11.1 Serving network name (SNN) 308

10 List of system parameters 309
10.1 General 309
10.2 Timers of 5GS mobility management 309
10.3 Timers of 5GS session management 314

Annex A (informative): Cause values for 5GS mobility management 316
A.1 Causes related to UE identification 316
A.2 Cause related to subscription options 316
A.3 Causes related to PLMN specific network failures and congestion/authentication failures 317
A.4 Causes related to invalid messages 317

Annex B (informative): Cause values for 5GS session management 319
B.1 Causes related to nature of request 319
B.2 Protocol errors (e.g., unknown message) 320

Annex C (normative): Storage of 5GMM information 322

Annex D (normative): UE policy delivery protocol 323
D.1 General 323
D.2 Procedures 323
D.2.1 Network-requested UE policy management procedure 323
D.2.1.1 General 323
D.2.1.2 Network-requested UE policy management procedure initiation 323
D.2.1.3 Network-requested UE policy management procedure accepted by the UE 324
D.2.1.4 Network-requested UE policy management procedure not accepted by the UE 324
D.2.1.5 Abnormal cases on the network side 325
D.2.1.6 Abnormal cases in the UE 325
D.2.2 UE-initiated UPSI list transport procedure 325
D.2.2.1 General 325
D.2.2.2 UE-initiated UPSI list transport procedure initiation 325
D.2.2.3 UE-initiated UPSI list transport procedure accepted by the network 325
D.2.2.4 Abnormal cases on the network side 325
D.3 UE policy re-assembly at the UE 326
D.4 Message coding rules 326
D.5 Message functional definition and contents 326
D.5.1 Manage UE policy command 326
D.5.1.1 Message definition 326
D.5.2 Manage UE policy complete 326
D.5.2.1 Message definition 326
D.5.3 Manage UE policy command reject 327
D.5.3.1 Message definition 327
D.5.4 UPSI list transport 327
D.5.4.1 Message definition 327
D.6 Information elements coding 328
D.6.1 UE policy delivery protocol message type 328
D.6.2 UE policy section management list 328
D.6.3 UE policy section management result 332
D.6.4 UPSI list 334

Annex E (informative): Change history 336

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 non-access stratum (NAS) procedures in the 5G system (5GS) used by the protocols for:

- mobility management between the user equipment (UE) and the access and mobility management function (AMF) for both 3GPP access and non-3GPP access; and
- session management between the user equipment (UE) and the session management function (SMF) for both 3GPP access and non-3GPP access.

The 5GS mobility management (5GMM) protocol defined in the present document provides procedures for the control of mobility when the user equipment (UE) is using the NG radio access network (NG-RAN) and/or non-3GPP access network. The 5GMM protocol also provides control of security for the NAS protocols.

The 5GS session management (5GSM) protocol defined in the present document provides procedures for the handling of 5GS PDU sessions. 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 the NG-RAN and the evolved universal terrestrial radio access (E-UTRAN) connected to the evolved packet core (EPC) and between the NG-RAN and the non-3GPP access network.

The present document is applicable to the UE, the access and mobility management function (AMF) and to the session management function (SMF) in the 5GS.

The clauses and subclauses in the present document are common for both 3GPP access and non-3GPP access unless it is explicitly stated that they apply to 3GPP access only or non-3GPP access only.

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

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

[2] 3GPP TS 22.101: "Service aspects; Service principles".

[3] 3GPP TS 22.261: "Service requirements for the 5G system; Stage 1".

[4] 3GPP TS 23.003: "Numbering, addressing and identification".

[5] 3GPP TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".

[6] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[7] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".

[8] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[9] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[10] 3GPP TS 23.503: " Policy and Charging Control Framework for the 5G System; Stage 2".

[11] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General aspects".

[12] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

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

[14] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[15] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[16] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3"

[17] 3GPP TS 24.368: "Non-Access Stratum (NAS) configuration Management Object (MO)".

[18] 3GPP TS 24.502: "Access to the 3GPP 5G System (5GS) via non-3GPP access networks; Stage 3".

[19] 3GPP TS 24.5xx: "UE policies for 5G System (5GS); Stage 3".

[20] 3GPP TS 24.623: "Extensive Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".

[21] 3GPP TS 29.507: "5G System; Access and Mobility Policy Control Service; Stage 3".

[22] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[23] 3GPP TS 33.102: "3G security; Security architecture".

[24] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[25] 3GPP TS 36.323: "NR; Packet Data Convergence Protocol (PDCP) specification".

[26] 3GPP TS 36.355: "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP)".

[27] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[28] 3GPP TS 38.304: "New Generation Radio Access Network; User Equipment (UE) procedures in Idle mode".

[29] 3GPP TS 38.323: "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification".

[30] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol Specification".

[31] 3GPP TS 38.413: "NG Radio Access Network (NG-RAN); NG Application Protocol (NGAP)".

[32] IETF RFC 768: "User Datagram Protocol".

[33] IETF RFC 793: "Transmission Control Protocol."

[34] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

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

[36] IETF RFC 4191: "Default Router Preferences and More-Specific Routes".

[37] IETF RFC 4282: "The Network Access Identifier".

[38] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[39] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[40] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[41] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2)".

[42] 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].

5GMM-IDLE mode: In this specification, if the term is used standalone, a UE in 5GMM-IDLE mode means the UE can be either in 5GMM-IDLE mode over 3GPP access or in 5GMM-IDLE mode over non-3GPP access.

5GMM-CONNECTED mode: In this specification, if the term is used standalone, a UE in 5GMM-CONNECTED mode means the UE can be either in 5GMM-CONNECTED mode over 3GPP access or in 5GMM-CONNECTED mode over non-3GPP access.

5GMM-IDLE mode over 3GPP access: A UE is in 5GMM-IDLE mode over 3GPP access when no N1 NAS signalling connection between the UE and network over 3GPP access exists. The term 5GMM-IDLE mode over 3GPP access used in the present document corresponds to the term CM-IDLE state for 3GPP access used in 3GPP TS 23.501 [8].

5GMM-CONNECTED mode over 3GPP access: A UE is in 5GMM-CONNECTED mode over 3GPP access when a N1 NAS signalling connection between the UE and network over 3GPP access exists. The term 5GMM-CONNECTED mode over 3GPP access used in the present document corresponds to the term CM-CONNECTED state for 3GPP access used in 3GPP TS 23.501 [8].

5GMM-IDLE mode over non-3GPP access: A UE is in 5GMM-IDLE mode over non-3GPP access no N1 NAS signalling connection between the UE and network over non-3GPP access exists. The term 5GMM-IDLE mode over non-3GPP access used in the present document corresponds to the term CM-IDLE state for non-3GPP access used in 3GPP TS 23.501 [8].

5GMM-CONNECTED mode over non-3GPP access: A UE is in 5GMM-CONNECTED mode over non-3GPP access when it has N1 NAS signalling connection between the UE and network over non-3GPP access exists. The term 5GMM-CONNECTED mode over non-3GPP access used in the present document corresponds to the term CM-CONNECTED state for non-3GPP access used in 3GPP TS 23.501 [8].

5GS services: Services provided by PS domain. Within the context of this specification, 5GS services is used as a synonym for EPS services.

Access stratum connection: A peer to peer access stratum connection between either the UE and the NG-RAN for 3GPP access or the UE and the N3IWF for non-3GPP access. The access stratum connection for 3GPP access corresponds to an RRC connection via the Uu reference point. The creation of the access stratum connection for non-3GPP access corresponds to the completion of the IKE_SA_INIT exchange (see IETF RFC 7296 [41]) via the NWu reference point.

Always-on PDU session: A PDU session for which user-plane resources have to be activated during every transition from 5GMM-IDLE mode to 5GMM-CONNECTED mode. Such a PDU session is established based on indication from upper layers.

NOTE 1: How the upper layers in the UE are configured to provide an indication is out of scope of the specification.

Editor's note: It is FFS whether any handling is required for access identities, access category or reject cause received in PDU session reactivation result IE due to always-on PDU session.

DNN based congestion control: Type of congestion control at session management level that is applied to reject session management requests from UEs or release PDU sessions when the associated DNN is congested. DNN based congestion control can be activated at the SMF over session management level and also activated at the AMF over mobility management level.

General NAS level congestion control: Type of congestion control at mobility management level that is applied at a general overload or congestion situation in the network, e.g. lack of processing resources.

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

N1 mode: A mode of a UE allowing access to the 5G core network via the 5G access network.

N1 NAS signalling connection: A peer to peer N1 mode connection between UE and AMF. An N1 NAS signalling connection is either the concatenation of an RRC connection via the Uu reference point and an NG connection via the N2 reference point for 3GPP access, or the concatenation of an IPsec tunnel via the NWu reference point and an NG connection via the N2 reference point for non-3GPP access.

PDU address: An IP address assigned to the UE by the packet data network.

PDU session for LADN: A PDU session with a DNN associated with a LADN.

Persistent PDU session: either a non-emergency PDU session contains a GBR QoS flow with QoS equivalent to QoS of teleservice 11 and where there is a radio bearer associated with that PDU session, or an emergency PDU session where there is a radio bearer associated with that PDU session.

NOTE 2: An example of a persistent PDU session is a non-emergency PDU session with 5QI = 1 where there is a radio bearer associated with that context.

Procedure transaction identity: An identity which is dynamically allocated by the UE for the UE-requested 5GSM procedures. The procedure transaction identity is released when the procedure is completed but it should not be released immediately.

Registered for emergency services: A UE is registered for emergency services if it has successfully completed initial registration for emergency services or if it has only one PDU session established which is for emergency services.

Rejected NSSAI: Rejected NSSAI for the current PLMN or rejected NSSAI for the current PLMN and registration area combination.

Rejected NSSAI for the current PLMN: A set of S-NSSAIs which was included in the requested NSSAI by the UE and is sent by the AMF with the rejection cause "S-NSSAI not available in the current PLMN".

Rejected NSSAI for the current PLMN and registration area combination: A set of S-NSSAIs which was included in the requested NSSAI by the UE and is sent by the AMF with the rejection cause "S-NSSAI not available in the current registration area".

Removal of eCall only mode restriction: All the limitations as described in 3GPP TS 22.101 [2] for the eCall only mode do not apply any more.

S-NSSAI-based congestion control: Type of congestion control at session management level that is applied to reject session management requests from UEs or release PDU sessions when the associated S-NSSAI and optionally the associated DNN are congested. . S-NSSAI based congestion control can be activated at the SMF over session management level and also activated at the AMF over mobility management level.

Selected core network type information: A type of core network (EPC or 5GCN) selected by the UE NAS layer in case of an E-UTRA cell connected to both EPC and 5GCN.

UE configured for high priority access in selected PLMN: A UE configured with one or more access identities equal to 1, 2, or 11-15 applicable in the selected PLMN as specified in subclause 4.5.2. Definition derived from 3GPP TS 22.261 [3].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.122 [5] apply:

Country
EHPLMN
HPLMN
Shared network
Suitable Cell
VPLMN

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.167 [6] apply:

eCall over IMS

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.401 [7] apply:

eCall only mode

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [8] apply:

5G access network
5G core network
5G QoS flow
5G QoS identifier
5G-GUTI
5G System
5G-S-TMSI
Allowed area
Allowed NSSAI
AMF region
AMF set
Configured NSSAI
Local area data network
Network slice
NG-RAN
Non-allowed area
Non-seamless non-3GPP offload
PDU session
PDU session type
PEI
Requested NSSAI
SUPI
SUCI
UE presence in LADN service area

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.301 [15] apply:

EPS services
Non-EPS services

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.501 [24] apply:

5G security context
5G NAS security context
Current 5G security context
Full native 5G security context
K'$_{AME}$
K$_{AMF}$
K$_{ASME}$
Mapped security context
Native 5G security context
Non-current 5G security context
Partial native 5G security context
RES*

For the purposes of the present document, the following terms and definitions given in 3GPP TS 38.413 [31] apply:

NG connection

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].

4G-GUTI	4G-Globally Unique Temporary Identifier
5GCN	5G Core Network
5G-GUTI	5G-Globally Unique Temporary Identifier
5GMM	5GS Mobility Management
5GS	5G System
5GSM	5GS Session Management
5G-S-TMSI	5G S-Temporary Mobile Subscription Identifier
5G-TMSI	5G Temporary Mobile Subscription Identifier
5QI	5G QoS Identifier
AKA	Authentication and Key Agreement
AMBR	Aggregate Maximum Bit Rate
AMF	Access and Mobility Management Function
APN	Access Point Name
DL	Downlink
DN	Data Network
DNN	Data Network Name
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EAP-AKA'	Improved Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement
EPD	Extended Protocol Discriminator
EMM	EPS Mobility Management
EPC	Evolved Packet Core Network
EPS	Evolved Packet System
ESM	EPS Session Management
Gbps	Gigabits per second
GFBR	Guaranteed Flow Bit Rate
GUAMI	Globally Unique AMF Identifier
IP-CAN	IP-Connectivity Access Network
KSI	Key Set Identifier
LADN	Local Area Data Network
LMF	Location Management Function
LPP	LTE Positioning Protocol
Mbps	Megabits per second
MFBR	Maximum Flow Bit Rate
MICO	Mobile Initiated Connection Only
N3IWF	Non-3GPP Inter-Working Function
NAI	Network Access Identifier
NR	New Radio
ngKSI	Key Set Identifier for Next Generation Radio Access Network
NSSAI	Network Slice Selection Assistance Information
PTI	Procedure Transaction Identity
QFI	QoS Flow Identifier
QoS	Quality of Service
QRI	QoS Rule Identifier
RQA	Reflective QoS Attribute
RQI	Reflective QoS Indication
(R)AN	(Radio) Access Network
S-NSSAI	Single NSSAI
SA	Security Association
SNN	Serving Network Name
SMF	Session Management Function
TA	Tracking Area
TAC	Tracking Area Code

TAI	Tracking Area Identity
Tbps	Terabits per second
UL	Uplink
UPDP	UE Policy Delivery Protocol
UPSC	UE Policy Section Code
UPSI	UE Policy Section Identifier
URN	Uniform Resource Name
URSP	UE Route Selection Policy

4 General

4.1 Overview

4.2 Coordination between the protocols for 5GS mobility management and 5GS session management

A 5GS session management (5GSM) message is piggybacked in specific 5GS mobility management (5GMM) transport messages. To this purpose, the 5GSM messages can be transmitted in an information element in the 5GMM transport messages. In this case, the UE, the AMF and the SMF execute the 5GMM procedure and the 5GSM procedure in parallel. The success of the 5GMM procedure is not dependent on the success of the piggybacked 5GSM procedure.

The UE can only initiate the 5GSM procedure when there is a 5GMM context established at the UE and the AMF can only forward the 5GSM message for the 5GSM procedure initiated by the SMF when there is a 5GMM context established at the AMF.

Except for the 5GMM procedures piggybacking 5GSM messages, during 5GMM procedures the UE and the AMF shall suspend the transmission of 5GSM messages.

4.3 UE domain selection

4.3.1 UE’s usage setting

The UE’s usage setting defined in 3GPP TS 24.301 [15] applies to voice capable UEs in 5GS and indicates whether the UE has preference for voice services over data services or vice-versa, where:

a) voice services include IMS voice; and

b) data services include any kind of user data transfer without a voice media component.

The UE’s usage setting can be set to:

a) "voice centric"; or

b) "data centric".

If the UE is capable of S1 mode, there is a single UE’s usage setting at the UE which applies to both 5GS and EPS.

4.3.2 Domain selection for UE originating sessions / calls

The behaviour of the UE for domain selection is determined by:

a) the UE usage setting;

b) the availability of IMS voice; and

c) whether the UE operates in single-registration mode or dual-registration mode (see 3GPP TS 23.501 [8]).

In the present document, "IMS voice not available" is determined per access type independently, i.e. 3GPP access or non-3GPP access.

In the present document, "IMS voice not available" refers to one of the following conditions:

a) the UE does not support IMS voice;

b) the UE supports IMS voice, but the network indicates in the REGISTRATION ACCEPT message that IMS voice over PS sessions are not supported; or

c) the UE supports IMS voice, the network indicates in the REGISTRATION ACCEPT message that IMS voice over PS sessions are supported, but the upper layers:

1) provide no indication that the UE is available for voice call in the IMS within a manufacturer determined period of time; or

2) indicate that the UE is not available for voice calls in the IMS.

NOTE: If conditions a and b evaluate to false, the upper layers need time to attempt IMS registration. In the event an indication from the upper layers that the UE is available for voice calls in the IMS takes longer than the manufacturer determined period of time (e.g. due to delay when attempting IMS registration or due to delay in obtaining a QoS flow for SIP signalling), the NAS layer assumes the UE is not available for voice calls in the IMS.

Other conditions may exist but these are implementation specific.

In the present document, "IMS voice available" applies when "IMS voice not available" does not apply.

When IMS voice is not available over 3GPP access, if the UE's usage setting is "voice centric", the UE operates in single-registration mode, and the UE:

- does not have a persistent PDU session, the UE shall disable the N1 mode capability for 3GPP access (see subclause 4.9.2), and attempt to select an E-UTRA cell connected to EPC. If such a cell is found, the UE shall then perform voice domain selection procedures as defined in 3GPP TS 24.301 [15]; and

- has a persistent PDU session, then the UE waits until the radio bearer associated with the persistent PDU session has been released. When the radio bearer associated with the persistent PDU session has been released and the UE operates in single-registration mode, the UE's usage setting is "voice centric" with "IMS voice not available", the UE shall attempt to select an E-UTRA cell connected to EPC and disable the N1 mode capability for 3GPP access (see subclause 4.9). If such a cell is found, the UE shall then perform voice domain selection procedures as defined in 3GPP TS 24.301 [15].

4.3.3 Change of UE's usage setting

If the UE operates in single-registration mode, whenever the UE's usage setting changes, the UE shall execute procedures according to table 4.3.3.1:

Table 4.3.3.1: Change of UE's usage setting for a UE in single-registration mode

UE's usage setting change	Procedure to execute
From "data centric" to "voice centric" and "IMS voice not available" over 3GPP access	Disable the N1 mode capability for 3GPP access (see subclause 4.9.2)
From "voice centric" to "data centric" and the N1 mode capability for 3GPP access is disabled at the UE	Re-enable the N1 mode capability for 3GPP access (see subclause 4.9.2)

4.3.4 Change or determination of IMS voice availability

If the UE operates in single-registration mode, whenever the IMS voice availability is determined or changes, the UE shall execute procedures according to table 4.3.4.1:

Table 4.3.4.1: Change of IMS voice availability for a UE in single-registration mode

Change of IMS voice available condition	Procedure to execute
"IMS voice not available" over 3GPP access and the UE's usage setting is "voice centric"	Disable the N1 mode capability (see subclause 4.9.2)

4.4 NAS security

4.4.1 General

This clause describes the principles for the handling of 5G NAS security contexts in the UE and in the AMF and the procedures used for the security protection of NAS messages between the UE and the AMF. Security protection involves integrity protection and ciphering of the 5GMM and 5GSM NAS messages.

The signalling procedures for the control of NAS security are part of the 5GMM 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 AMF so that it always selects the "null ciphering algorithm", NEA0.

4.4.2 Handling of 5G NAS security contexts

4.4.2.1 General

The security parameters for authentication, integrity protection and ciphering are tied together in a 5G NAS security context and identified by a key set identifier (ngKSI). The relationship between the security parameters is defined in 3GPP TS 33.501 [24].

Before security can be activated, the AMF and the UE need to establish a 5G NAS security context. Usually, the 5G NAS security context is created as the result of a primary authentication and key agreement procedure between the AMF and the UE. Alternatively, during inter-system change from S1 mode to N1 mode, the AMF and the UE derive a mapped 5G NAS security context from an EPS security context that has been established while the UE was in S1 mode.

The 5G NAS security context is taken into use by the UE and the AMF, when the AMF initiates an NAS security mode control procedure or during the inter-system change procedure from S1 mode to N1 mode. The 5G NAS security context which has been taken into use by the network most recently is called current 5G NAS security context. This current 5G NAS security context can be of type native or mapped, i.e. originating from a native 5G NAS security context or mapped 5G NAS security context.

The key set identifier ngKSI is assigned by the AMF either during the primary authentication and key agreement procedure or, for the mapped 5G NAS security context, during the inter-system change procedure. The ngKSI consists of a value and a type of security context parameter indicating whether a 5G NAS security context is a native 5G NAS security context or a mapped 5G NAS security context. When the 5G NAS security context is a native 5G NAS security context, the ngKSI has the value of KSI_{AMF}, and when the current 5G NAS security context is of type mapped, the ngKSI has the value of KSI_{ASME}.

The 5G NAS security context which is indicated by an ngKSI can be taken into use to establish the secure exchange of NAS messages when a new N1 NAS signalling connection is established without executing a new primary authentication and key agreement procedure (see subclause 5.4.1) or when the AMF initiates a security mode control procedure. For this purpose the initial NAS messages (i.e. REGISTRATION REQUEST, DEREGISTRATION REQUEST and SERVICE REQUEST) and the SECURITY MODE COMMAND message contain an ngKSI in the NAS key set identifier IE indicating the current 5G NAS security context used to integrity protect the NAS message.

In the present document, when the UE is required to delete an ngKSI, the UE shall set the ngKSI to the value "no key is available" and consider also the associated keys K_{AMF} or K'_{AMF}, 5G NAS ciphering key and 5G NAS integrity key invalid (i.e. the 5G NAS security context associated with the ngKSI 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).

As described in the subclause 4.8 in order to interwork with E-UTRAN connected to EPC, the UE supporting both S1 mode and N1 mode can operate in either single-registration mode or dual-registration mode. A UE operating in dual-registration mode shall independently maintain and use both EPS security context (see 3GPP TS 24.301 [15]) and 5G NAS security context. During inter-system change to S1 mode, the UE operating in dual-registration mode shall take into use an EPS security context and follow the handling of this security context as specified in 3GPP TS 24.301 [15]. However, during inter-system change to N1 mode, the UE operating in dual-registration mode shall take into use a 5G NAS security context and follow the handling of this security context as described in the present specification. A UE operating in single-registration mode shall maintain and use only 5G NAS security context and follow the handling of this security context as described in the present specification.

The UE and the AMF need to be able to maintain two 5G NAS security contexts simultaneously, i.e. a current 5G NAS security context and a non-current 5G NAS security context, since:

a) after a 5G re-authentication, the UE and the AMF can have both a current 5G NAS security context and a non-current 5G NAS security context which has not yet been taken into use (i.e. a partial native 5G NAS security context); and

b) after an inter-system change from S1 mode to N1 mode, the UE and the AMF can have both a mapped 5G NAS security context, which is the current 5G NAS security context, and a non-current native 5G NAS security context that was created during a previous access in N1 mode.

The number of 5G NAS security contexts that need to be maintained simultaneously by the UE and the AMF is limited by the following requirements:

a) After a successful 5G (re-)authentication, which creates a new partial native 5G NAS security context, the AMF and the UE shall delete the non-current 5G NAS security context, if any;

b) When a partial native 5G NAS security context is taken into use through a security mode control procedure, the AMF and the UE shall delete the previously current 5G NAS security context;

c) When the AMF and the UE create a 5G NAS security context using null integrity and null ciphering algorithm during an initial registration procedure for emergency services, or a registration procedure for mobility and periodic registration update for a UE that has a PDU session for emergency services (see subclause 5.4.2.2), the AMF and the UE shall delete the previous current 5G NAS security context;

d) When a new mapped 5G NAS security context or 5G NAS security context created using null integrity and null ciphering algorithm is taken into use during the inter-system change from S1 mode to N1 mode, the AMF and the UE shall not delete the previously current native 5G NAS security context, if any. Instead, the previously current native 5G NAS security context shall become a non-current native 5G NAS security context, and the AMF and the UE shall delete any partial native 5G NAS security context;

   If no previously current native 5G NAS security context exists, the AMF and the UE shall not delete the partial native 5G NAS security context, if any;

e) When the AMF and the UE derive a new mapped 5G NAS security context during inter-system change from S1 mode to N1 mode, the AMF and the UE shall delete any existing current mapped 5G NAS security context;

f) When a non-current full native 5G NAS security context is taken into use by a security mode control procedure, then the AMF and the UE shall delete the previously current mapped 5G NAS security context; and

g) When the UE or the AMF moves from 5GMM-REGISTERED to 5GMM-DEREGISTERED state, if the current 5G NAS security context is a mapped 5G NAS security context and a non-current full native 5G NAS security context exists, then the non-current 5G NAS security context shall become the current 5G NAS security context. Furthermore, the UE and the AMF shall delete any mapped 5G NAS security context or partial native 5G NAS security context.

The UE shall mark the 5G NAS security context on the USIM or in the non-volatile memory as invalid when the UE initiates an initial registration procedure as described in subclause 5.5.1,2 or when the UE leaves state 5GMM-DEREGISTERED for any other state except 5GMM-NULL.

The UE shall store the current native 5G NAS security context as specified in annex C and mark it as valid only when the UE enters state 5GMM-DEREGISTERED from any other state except 5GMM-NULL or when the UE aborts the initial registration procedure without having left 5GMM-DEREGISTERED.

4.4.2.2 Establishment of a mapped 5G NAS security context during inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode

In order for the UE operating in single-registration mode to derive a mapped 5G NAS security context for an inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, the AMF shall generate an ngKSI using the downlink NAS COUNT and the K'_{ASME} as indicated in 3GPP TS 33.501 [24]. The AMF shall include the message authentication code, selected NAS algorithms, downlink NAS COUNT, replayed UE security capabilities and generated ngKSI in the S1 to N1 NAS transparent container IE (see subclause 9.10.2.7). The AMF shall derive the 5G NAS keys from the K'_{ASME}.

When the UE operating in single-registration mode receives the command to perform handover to NG-RAN, the UE shall derive $K'_{AMF,}$ as indicated in 3GPP TS 33.501 [24], using the K'_{ASME} received in the S1 mode to N1 mode NAS transparent container IE. Furthermore, the UE shall associate the derived K'_{AMF} with the received KSI_{ASME} and derive the 5G NAS keys from the K'_{ASME}.

When the UE operating in single-registration mode has a PDU session for emergency services and has no current EPS security context, the AMF shall set 5G-IA0 and 5G-EA0 as the selected NAS security algorithms in the S1 mode to N1 mode NAS transparent container IE. The AMF shall create a locally generated the K'_{AMF}. The AMF shall set the ngKSI value of the associated security context to "000" and the type of security context flag to "mapped security context" in the S1 mode to N1 mode NAS transparent container IE.

When the UE operating in single-registration mode receives the command to perform handover to NG-RAN (see 3GPP TS 38.331 [30]) and has a PDU connection for emergency services, if 5G-IA0 and 5G-EA0 as the selected NAS security algorithms are included in the S1 mode to N1 mode NAS transparent container IE, the UE shall create a locally generated K'_{AMF}. Furthermore, the UE shall set the ngKSI value of the associated security context to the KSI value received.

If the inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode is not completed successfully, the AMF and the UE operating in single-registration mode shall delete the new mapped 5G NAS 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 AMF during the registration 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 AMF are sent integrity protected using the current 5G security algorithms, and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered using the current 5G security algorithms.

During inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode, secure exchange of NAS messages is established between the AMF and the UE by:

a) the transmission of NAS security related parameters encapsulated in the AS signalling from the AMF to the UE triggering the inter-system change in 5GMM-CONNECTED mode (see 3GPP TS 33.501 [24]). The UE uses these parameters to generate the mapped 5G NAS security context; and,

b) after the inter-system change in 5GMM-CONNECTED mode, the transmission of a REGISTRATION REQUEST message from the UE to the AMF. The UE shall send this message integrity protected using the mapped 5G NAS security context, but unciphered. From this time onward, all NAS messages exchanged between the UE and the AMF are sent integrity protected using the mapped 5G NAS security context, and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered using the mapped 5G NAS security context.

The secure exchange of NAS messages shall be continued after N1 mode to N1 mode handover. It is terminated after inter-system change from N1 mode to S1 mode or when the NAS signalling connection is released.

When a UE in 5GMM-IDLE mode, after an inter-system change from S1 mode to N1 mode, establishes a new NAS signalling connection, and has a valid current 5G NAS security context, the UE shall transmit the initial NAS message integrity protected with the current 5G NAS security context. The UE shall include the ngKSI indicating the current 5G NAS security context value in the initial NAS message. The AMF shall check whether the ngKSI included in the initial NAS message belongs to a 5G NAS security context available in the AMF, and shall verify the MAC of the NAS message. If the verification is successful, the AMF deletes the security context received from the source MME, and the AMF may re-establish the secure exchange of NAS messages:

a) by replying with a NAS message that is integrity protected and ciphered using the current 5G NAS security context. From this time onward, all NAS messages exchanged between the UE and the AMF are sent integrity protected and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered; or

b) by initiating a security mode control procedure. This can be used by the AMF to take a non-current 5G NAS security context into use or to modify the current 5G NAS security context by selecting new NAS security algorithms.

When a UE in 5GMM-IDLE mode establishes a new NAS signalling connection and has a valid current 5G NAS security context, the UE shall transmit the initial NAS message integrity protected with the current 5G NAS security context, but unciphered. The UE shall include the ngKSI indicating the current 5G NAS security context value in the initial NAS message. The AMF shall check whether the ngKSI included in the initial NAS message belongs to a 5G NAS security context available in the AMF, and shall verify the MAC of the NAS message. If the verification is successful, the AMF may re-establish the secure exchange of NAS messages:

a) by replying with a NAS message that is integrity protected and ciphered using the current 5G NAS security context. From this time onward, all NAS messages exchanged between the UE and the AMF are sent integrity protected and except for the messages specified in subclause 4.4.5, all NAS messages exchanged between the UE and the AMF are sent ciphered; or

b) by initiating a security mode control procedure. This can be used by the AMF to take a non-current 5G NAS security context into use or to modify the current 5G NAS security context by selecting new NAS security algorithms.

When a UE in 5GMM-IDLE mode establishes a new NAS signalling connection, has no current 5G NAS security context and performs a registration procedure after an inter-system change in idle mode from S1 mode to N1 mode, the UE shall send the REGISTRATION REQUEST message without integrity protection and encryption. The AMF may create a fresh mapped 5G NAS security context or may trigger a primary authentication and key agreement procedure to create a fresh native 5G NAS security context. The newly created 5G NAS security context is taken into use by initiating a security mode control procedure and this context becomes the current 5G NAS security context in both the UE and the AMF. This re-establishes the secure exchange of NAS messages.

4.4.2.4 Change of security keys

When the AMF initiates a re-authentication to create a new 5G NAS security context, the messages exchanged during the authentication procedure are integrity protected and ciphered using the current 5G NAS security context, if any.

Both UE and AMF shall continue to use the current 5G NAS security context, until the AMF initiates a security mode control procedure. The SECURITY MODE COMMAND message sent by the AMF includes the ngKSI of the new 5G NAS security context to be used. The AMF shall send the SECURITY MODE COMMAND message integrity protected with the new 5G NAS security context, but unciphered. When the UE responds with a SECURITY MODE COMPLETE message, it shall send the message integrity protected and ciphered with the new 5G NAS security context.

The AMF can also modify the current 5G NAS security context or take the non-current native 5G NAS security context, if any, into use, by sending a SECURITY MODE COMMAND message including the ngKSI of the 5G NAS security context to be modified and including a new set of selected NAS security algorithms. In this case the AMF shall send the SECURITY MODE COMMAND message integrity protected with the modified 5G NAS 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 5G NAS security context.

4.4.3 Handling of NAS COUNT and NAS sequence number

4.4.3.1 General

Each 5G NAS security context shall be associated with two separate counters NAS COUNT per access type in the same PLMN: one related to uplink NAS messages and one related to downlink NAS messages. If the 5G NAS security context is used for access via both 3GPP and non-3GPP access in the same PLMN, there are two NAS COUNT counter pairs associated with the 5G NAS security context. The NAS COUNT counters use 24 bit internal representation and are independently maintained by UE and AMF. 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 AMF 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, except for the initial NAS messages if the lower layers indicated the failure to establish the RRC connection (see 3GPP TS 38.331 [30]). 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.

During the handover from E-UTRAN to NG-RAN, when a mapped 5G NAS security context is derived and taken into use, the AMF shall set both the uplink and downlink NAS COUNT counters of this 5G NAS security context to zero. The UE shall set both the uplink and downlink NAS COUNT counters to zero.

During the handover from NG-RAN to E-UTRAN the AMF signals the current downlink NAS COUNT value in a NAS security transparent container (see subclause 9.10.2.x).

During handover to or from NG-RAN, the AMF shall increment downlink NAS COUNT by one after it has created a NAS security transparent container (see subclause 9.10.2.7).

NOTE: During the handover from E-UTRAN to NG-RAN, the NAS security transparent container (see subclause 9.10.2.7) is treated as an implicit SECURITY MODE COMMAND message for the UE and the AMF, and therefore the AMF 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 5G NAS security context for the purpose of the NAS COUNT handling.

4.4.3.2 Replay protection

Replay protection shall be supported for received NAS messages both in the AMF 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 assures that one and the same NAS message is not accepted twice by the receiver. Specifically, for a given 5G 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 5G-IA0 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 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 33.501 [24], and the integrity protection shall include octet 7 to n of the security protected 5GS NAS message, i.e. the sequence number IE and the NAS message IE. In addition to the data that is to be integrity protected, the BEARER ID, DIRECTION bit, NAS COUNT and 5G NAS are input to the integrity protection algorithm. These parameters are described in 3GPP TS 33.501 [24].

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 5G-IA0 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 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 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 AMF detects that either its downlink NAS COUNT or the UE's uplink NAS COUNT is "close" to wrap around, (close to 2^{24}), the AMF shall take the following actions:

- If there is no non-current native 5G NAS security context with sufficiently low NAS COUNT values, the AMF shall initiate a new primary authentication and key agreement procedure with the UE, leading to a new established 5G NAS security context and the NAS COUNT being reset to 0 in both the UE and the AMF when the new 5G NAS security context is activated;

- Otherwise, the AMF can activate a non-current native 5G NAS security context with sufficiently low NAS COUNT values or initiate a new primary authentication and key agreement procedure as specified above.

If for some reason a new K_{AMF} has not been established using primary authentication and key agreement procedure before the NAS COUNT wraps around, the node (AMF 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 ngKSI indicating the current 5G NAS security context.

When the 5G-IA0 is used as the NAS integrity algorithm, the UE and the AMF shall allow NAS COUNT wrap around. If NAS COUNT wrap around occurs, the following requirements apply:

a) the UE and the AMF shall continue to use the current 5G NAS security context;

b) the AMF shall not initiate the primary authentication and key agreement procedure;

c) the AMF shall not release the NAS signalling connection; and

d) 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 5GMM NAS messages once a valid 5G NAS security context exists and has been taken into use. For the network, integrity protected signalling is mandatory for the 5GMM NAS messages once a secure exchange of 5GS 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"5G-IA0 (see subclause 9.10.3.32) in the current 5G NAS security context is only allowed for an unauthenticated UE for which establishment of emergency services is allowed. For setting the security header type in outbound NAS messages, the UE and the AMF shall apply the same rules irrespective

of whether the "null integrity protection algorithm" or any other integrity protection algorithm is indicated in the 5G NAS security context.

If the "null integrity protection algorithm"5G-IA0 has been selected as an 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 33.501 [24].

When a NAS message needs to be sent both ciphered and integrity protected, the NAS message is first ciphered and then the ciphered NAS message and the NAS sequence number are integrity protected by calculating the MAC.

NOTE: NAS messages that are ciphered with the "null ciphering algorithm" 5G-EA0 are regarded as ciphered (see subclause 4.4.5).

When a NAS message needs to be sent only integrity protected and unciphered, the unciphered NAS message and the NAS sequence number are integrity protected by calculating the MAC.

When during a 5GMM procedure a 5GSM message is piggybacked in a 5GMM 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 5GMM entity in the UE or forwarded to the 5GSM entity, unless the network has established secure exchange of 5GS NAS messages for the NAS signalling connection:

a) IDENTITY REQUEST (if requested identification parameter is SUCI);

b) AUTHENTICATION REQUEST;

c) AUTHENTICATION RESULT;

d) AUTHENTICATION REJECT;

e) REGISTRATION REJECT;

f) DEREGISTRATION ACCEPT (for non switch off); and

g) SERVICE REJECT.

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

Integrity protection is never applied directly to 5GSM messages, but to the 5GMM message in which the 5GSM message is included.

The network can provide the transparent container IE during the registration procedure to the UE in the REGISTRATION ACCEPT message. The transparent container IE is integrity protected by the HPLMN as specified in 3GPP TS 33.501 [24]. If the transparent container IE does not successfully pass the integrity check (see 3GPP TS 33.501 [24]), then the UE can abort the registration procedure before performing PLMN selection as specified in subclause 5.5.1.2.4 and subclause 5.5.1.3.4.

Once the secure exchange of NAS messages has been established, the receiving 5GMM 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 5.4.2.5. 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 AMF

Except the messages listed below, no NAS signalling messages shall be processed by the receiving 5GMM entity in the AMF or forwarded to the 5GSM entity, unless the secure exchange of NAS messages has been established for the NAS signalling connection:

a) REGISTRATION REQUEST;

b) IDENTITY RESPONSE (if requested identification parameter is SUCI);

c) AUTHENTICATION RESPONSE;

d) AUTHENTICATION FAILURE;

e) SECURITY MODE REJECT;

f) DEREGISTRATION REQUEST; and

g) DEREGISTRATION ACCEPT;

NOTE 1: The REGISTRATION REQUEST message is sent by the UE without integrity protection, if the registration procedure is initiated due to an inter-system change in 5GMM-IDLE mode and no current 5G NAS security context is available in the UE. The other messages are accepted by the AMF without integrity protection, as in certain situations they are sent by the UE before security can be activated.

NOTE 2: The DEREGISTRATION REQUEST message can be sent by the UE without integrity protection, e.g. if the UE is registered for emergency services and there is no shared 5G NAS security context available, or if due to user interaction a registration procedure is cancelled before the secure exchange of NAS messages has been established. For these cases the network can attempt to use additional criteria (e.g. whether the UE is subsequently still performing periodic registration update or still responding to paging) before marking the UE as 5GMM-DEREGISTERED.

Integrity protection is never applied directly to 5GSM messages, but to the 5GMM message in which the 5GSM message is included.

Once a current 5G NAS security context exists, until the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving 5GMM entity in the AMF 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 5G NAS security context is not available in the network:

a) REGISTRATION REQUEST;

b) IDENTITY RESPONSE (if requested identification parameter is SUCI);

c) AUTHENTICATION RESPONSE;

d) AUTHENTICATION FAILURE;

e) SECURITY MODE REJECT;

f) DEREGISTRATION REQUEST;

g) DEREGISTRATION ACCEPT; and

h) SERVICE REQUEST;

NOTE 3: These messages are processed by the AMF 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 a 5G NAS security context that is no longer available in the network.

If a REGISTRATION REQUEST message fails the integrity check and it is not an registration request for emergency services, the AMF shall authenticate the subscriber before processing the registration request any further. Additionally, the AMF shall initiate a security mode control procedure, and include a $HASH_{AMF}$ IE in the SECURITY MODE COMMAND message as specified in subclause 5.4.2.2. For the case when the registration procedure is for emergency services see subclause 5.5.1.2.3 and subclause 5.4.1.3.5.

If a DEREGISTRATION REQUEST message fails the integrity check, the AMF shall proceed as follows:

- If it is not a deregistration request due to switch off, and the AMF can initiate an authentication procedure, the AMF should authenticate the subscriber before processing the deregistration request any further.

- If it is a deregistration request due to switch off, or the AMF does not initiate an authentication procedure for any other reason, the AMF may ignore the deregistration request and remain in state 5GMM-REGISTERED.

NOTE 4: The network can attempt to use additional criteria (e.g. whether the UE is subsequently still performing periodic registration update or still responding to paging) before marking the UE as 5GMM-DEREGISTERED.

If a REGISTRATION REQUEST message fails the integrity check and the UE provided EPS NAS message container IE which was successfully verified by the source MME, the AMF may create a mapped 5G NAS security context and initiate a security mode control procedure to take the new mapped 5G NAS security context into use; otherwise if the UE has only a PDU session for non-emergency services established, the AMF shall initiate a primary authentication and key agreement procedure to create a new native 5G NAS security context. Additionally, the AMF shall initiate a security mode control procedure, and include a $HASH_{AMF}$ IE in the SECURITY MODE COMMAND message as specified in subclause 5.4.2.2. For the case when the UE has a PDU session for emergency services see subclause 5.5.1.3.3 and subclause 5.4.1.3.5.

If a SERVICE REQUEST message fails the integrity check and the UE has only PDU sessions for non-emergency services established, the AMF shall send the SERVICE REJECT message with 5GMM cause #9 "UE identity cannot be derived by the network" and keep the 5GMM-context and 5G NAS security context unchanged. For the case when the UE has a PDU session for emergency services and integrity check fails, the AMF may skip the authentication procedure even if no 5G NAS security context is available and proceed directly to the execution of the security mode control procedure as specified in subclause 5.4.2. After successful completion of the service request procedure, the network shall release all non-emergency PDU sessions locally. The emergency PDU sessions shall not be released.

Once the secure exchange of NAS messages has been established for the NAS signalling connection, the receiving 5GMM entity in the AMF 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 AMF 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 AMF configuration. When operation of the network without ciphering is configured, the AMF shall indicate the use of "null ciphering algorithm" 5G-EA0 (see subclause 9.10.3.32) in the current 5G NAS security context for all UEs. For setting the security header type in outbound NAS messages, the UE and the AMF shall apply the same rules irrespective of whether the "null ciphering algorithm" or any other ciphering algorithm is indicated in the 5G NAS security context.

When the UE establishes a new N1 NAS signalling connection, it shall send the initial NAS message unciphered.

The UE shall send the REGISTRATION 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 N1 NAS signalling connection. From this time onward, unless explicitly defined, the UE shall send all NAS messages ciphered until the N1 NAS signalling connection is released, or the UE performs inter-system change to S1 mode.

The AMF shall start ciphering and deciphering of NAS messages as described in subclause 4.4.3.4. From this time onward, except for the SECURITY MODE COMMAND message, the AMF shall send all NAS messages ciphered until the N1 NAS signalling connection is released, or the UE performs inter-system change to S1 mode.

Ciphering is never applied directly to 5GSM messages, but to the 5GMM message in which the 5GSM message is included.

Once the encryption of NAS messages has been started between the AMF 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"5G-EA0 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 33.501 [24].

4.5 Unified access control

4.5.1 General

When the UE wants to access the 5GS, the UE first performs access control checks to determine if the access is allowed. Access control checks shall be perfomed for the access attempts defined by the following list of events:

a) the UE is in 5GMM-IDLE mode over 3GPP access and an event that requires a transition to 5GMM-CONNECTED mode occurs; and

b) the UE is in 5GMM-CONNECTED mode over 3GPP access or 5GMM-CONNECTED mode with RRC inactive indication and one of the following events occurs:

   1) 5GMM receives an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication from upper layers;

   2) 5GMM receives a request from upper layers to send a mobile originated SMS over NAS unless the request triggered a service request procedure to transition the UE from 5GMM-IDLE mode to 5GMM-CONNECTED mode;

   3) 5GMM receives a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session establishment unless the request triggered a service request procedure to transition the UE from 5GMM-IDLE mode to 5GMM-CONNECTED mode;

   4) 5GMM receives a request from upper layers to send an UL NAS TRANSPORT message for the purpose of PDU session modification unless the request triggered a service request procedure to transition the UE from 5GMM-IDLE mode to 5GMM-CONNECTED mode; and

   5) 5GMM receives a request to re-establish the user-plane resources for an existing PDU session.

NOTE 1: 5GMM specific procedures initiated by NAS in 5GMM-CONNECTED mode are not subject to access control, e.g. a registration procedure after PS handover will not be prevented by access control (see subclause 5.5).

Editor's note: Whether other events need to be considered in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication, is FFS.

When the NAS detects one of the above events, the NAS needs to perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

NOTE 2: The NAS is aware of the above events through indications provided by upper layers or when determing the need to start 5GMM procedures through normal NAS behaviour, or both.

To determine the access identities and the access category for a request, the NAS checks the reason for access, types of service requested and profile of the UE including UE configurations, against a set of access identities and access categories defined in 3GPP TS 22.261 [3], namely:

a) a set of standardized access identities;

b) a set of standardized access categories; and

c) a set of operator-defined access categories, if available.

For the purpose of determining the applicable access identities from the set of standardized access identities defined in 3GPP TS 22.261 [3], the NAS shall follow the requirements set out in subclause 4.5.2 and the rules and actions defined in table 4.5.2.1.

For the purpose of determining the applicable access category from the set of standardized access categories and operator-defined access categories defined in 3GPP TS 22.261 [3], the NAS shall follow the requirements set out in subclause 4.5.2 and the rules and actions defined in table 4.5.2.2.

4.5.2 Determination of the access identities and access category associated with a request for access

When the UE needs to initiate an access attempt in one of the events listed in subclause 4.5.1, the UE shall determine one or more access identities from the set of standardized access identities, and one access category from the set of standardized access categories and operator-defined access categories, to be associated with that access attempt.

The set of the access identities applicable for the request is determined by the UE in the following way:

a) for each of the access identities 1, 2, 11, 12, 13, 14 and 15 in table 4.5.2.1, the UE shall check whether the access identity is applicable in the selected PLMN, if a new PLMN is selected, or otherwise if it is applicable in the RPLMN or equivalent PLMN; and

b) if none of the above access identities is applicable, then access identity 0 is applicable.

Table 4.5.2.1: Access identities

Access Identity number	UE configuration
0	UE is not configured with any parameters from this table
1 (NOTE 1)	UE is configured for multimedia priority service (MPS).
2 (NOTE 2)	UE is configured for mission critical service (MCS).
3-10	Reserved for future use
11 (NOTE 3)	Access Class 11 is configured in the UE.
12 (NOTE 3)	Access Class 12 is configured in the UE.
13 (NOTE 3)	Access Class 13 is configured in the UE.
14 (NOTE 3)	Access Class 14 is configured in the UE.
15 (NOTE 3)	Access Class 15 is configured in the UE.
NOTE 1: Access identity 1 is used by UEs configured for MPS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present), visited PLMNs of the home country, and configured visited PLMNs outside the home country.	
NOTE 2: Access identity 2 is used by UEs configured for MCS, in the PLMNs where the configuration is valid. The PLMNs where the configuration is valid are HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present).	
NOTE 3: Access identities 11 and 15 are valid in HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present). Access Identities 12, 13 and 14 are valid in HPLMN and visited PLMNs of home country only. For this purpose the home country is defined as the country of the MCC part of the IMSI.	

Editor's note: The definition and configuration of Access Classes 11 to 15 for 5GS is FFS.

Editor's note: How the UE is configured for MPS and MCS is FFS.

The UE uses the MPS indicator bit of the 5GS network feature support IE to determine if access identity 1 is valid when the UE is not in the country of its HPLMN (see 3GPP TS 23.122 [5]). Processing of the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message is described in subclause 5.5.1.2.4 and subclause 5.5.1.3.4. The UE shall not consider access identity 1 to be valid when the UE is not in the country of its HPLMN prior to receiving the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message being set to "Access identity 1 valid in RPLMN or equivalent PLMN".

When the UE is in the country of its HPLMN, the contents of the USIM files EF_{UAC_AIC} and EF_{ACC} as specified in 3GPP TS 31.102 [22] and the rules specified in table 4.5.2.1 are used to determine the applicability of access identity 1 and access classes 11 - 15. When the UE is not in the country of its HPLMN, the contents of the USIM files EF_{UAC_AIC} and EF_{ACC} are not applicable.

In order to determine the access category applicable for the access attempt, the NAS shall check the rules in table 4.5.2.2, and use the access category for which there is a match for barring check. If the access attempt matches more than one rule, the access category of the lowest rule number shall be selected.

Table 4.5.2.2: Mapping table for access categories

Rule #	Type of access attempt	Requirements to be met	Access Category
1	Response to paging	Access attempt is for MT access	0 (= MT_acc)
2	Emergency	UE is attempting access for an emergency session (NOTE 1, NOTE 2)	2 (= emergency)
3	Access attempt for operator-defined access category	UE was provided with operator-defined access categories for the current PLMN, and access attempt is matching criteria of an operator-defined access category	32-63 (= based on operator classification)
4	Access attempt for delay tolerant service	UE is configured for NAS signalling low priority, the PLMN is broadcasting one of the categories a, b or c, and the UE is a member of the broadcasted category in the selected PLMN or RPLMN/equivalent PLMN (NOTE 3, NOTE 5)	1 (= delay tolerant)
5	MO MMTel voice call	Access attempt is for MO MMTel voice call or for NAS signalling connection recovery during ongoing MO MMTel voice call (NOTE 2)	4 (= MO MMTel voice)
6	MO MMTel video call	Access attempt is for MO MMTel video call or for NAS signalling connection recovery during ongoing MO MMTel video call (NOTE 2)	5 (= MO MMTel video)
7	MO SMS over NAS or MO SMSoIP	Access attempt is for MO SMS over NAS (NOTE 4) or MO SMS over SMSoIP transfer or for NAS signalling connection recovery during ongoing MO SMS or SMSoIP transfer (NOTE 2)	6 (= MO SMS and SMSoIP)
8	UE NAS initiated 5GMM specific procedures	Access attempt is for MO signalling	3 (= MO_sig)
9	UE NAS initiated 5GMM connection management procedures or 5GMM NAS transport procedure	Access attempt is for MO data	7 (= MO_data)

NOTE 1: This includes 5GMM specific procedures while the service is ongoing and 5GMM connection management procedures required to establish a PDU session with request type = "initial emergency request" or "existing emergency PDU session", or to re-establish user-plane resources for such a PDU session. This further includes the service request procedure initiated with a SERVICE REQUEST message with the Service type IE set to "emergency services fallback".

NOTE 2: Access for the purpose of NAS signalling connection recovery during an ongoing service is mapped to the access category of the ongoing service in order to derive an RRC establishment cause, but barring checks will be skipped for this access attempt.

NOTE 3: If the UE selects a new PLMN, then the selected PLMN is used to check the membership; otherwise the UE uses the RLPMN or a PLMN equivalent to the RPLMN.

NOTE 4: This includes the 5GMM connection management procedures triggered by the UE-initiated NAS transport procedure for transporting the MO SMS.

NOTE 5: The UE configured for NAS signalling low priority is not supported in this release of specification.

4.5.3 Operator-defined access categories

Operator-defined access categories can be signalled to the UE using NAS signalling. Each operator-defined access category consists of the following parameters:

Editor's note: The encoding of the operator-defined access categories is FFS.

Editor's note: Whether the operator-defined access categories are sent to the UE in a CONFIGURATION UPDATE COMMAND message, a DL NAS TRANSPORT message or another NAS message is FFS.

a) a precedence value which indicates in which order the UE shall evaluate the operator-defined categories for a match;

b) an access category number in the 32-63 range that uniquely identifies the access category in the PLMN in which the access categories are being sent to the UE; and

c) one or more access category criteria type and associated access category criteria type values. The access category criteria type can be set to one of the following:

1) DNN name;

2) 5QI;

Editor's note: Whether the 5QI is a suitable access category criteria type is FFS.

3) OS Id + OS App Id of application triggering the access attempt; or

4) S-NSSAI; and

d) optionally, a standardized access category, that is used in combination with the access identities to determine the establishment cause.

Editor's note: Other access category criteria types, in particular whether QFI is a suitable parameter, are FFS.

Editor's note: When the standardized access category, that is used in combination with the access identities to determine the establishment cause, is not provided, then it is FFS how the UE derives RRC establishment cause.

NOTE: An access category criteria type can be associated with more than one access category criteria values. In this case, the access attempt matches the access category if the access criteria for the access attempt match any of the associated access criteria type values.

If the UE is configured with operator-defined access categories for a PLMN, then access control in 5GMM-IDLE mode will only be performed for the event a) defined in subclause 4.5.1.

If the UE is configured with operator-defined access categories for a PLMN, then access control in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication will only be performed for the events 1) to 5) defined in subclause 4.5.1.

Upon receiving a NAS signalling message with operator-defined access category definitions, the UE shall store the operator-defined access category definitions for the registered PLMN.

4.5.4 Access control and checking

4.5.4.1 Access control and checking in 5GMM-IDLE mode

When the UE is in 5GMM-IDLE mode, upon receiving a request from the upper layers for an access attempt, the NAS shall categorize the access attempt into access identities and an access category following subclause 4.5.2, table 4.5.2.1 and table 4.5.2.2, and subclause 4.5.3, and provide the applicable access identities and the access category to the lower layers for the purpose of access control checking. In this request to the lower layer the NAS can also provide to the lower layer the RRC establishment cause determined as specified in subclause 4.5.6 of this specification.

NOTE 1: The access barring check is performed by the lower layers.

NOTE 2: As an implementation option, the NAS can provide the RRC establishment cause to the lower layers after being informed by the lower layers that the access attempt is allowed.

If the lower layers indicate that the access attempt is allowed, the NAS shall initiate the procedure to send the initial NAS message for the access attempt.

If the lower layers indicate that the access attempt is barred, the NAS shall not initiate the procedure to send the initial NAS message for the access attempt. Additionally, if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication, the NAS shall notify the upper layers that the access attempt is barred. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated , the NAS may initiate the procedure to send the initial NAS message, if still needed.

NOTE 3: Barring timers, on a per access category basis, is run by the lower layers. At expiry of barring timers, the indication of alleviation of access barring is indicated to the NAS on a per access category basis.

4.5.4.2 Access control and checking in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication

When the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication, upon detecting one of events 1) through 5) listed in subclause 4.5.1, the NAS shall categorize the corresponding access attempt into access identities and an access category following subclause 4.5.2, table 4.5.2.1 and table 4.5.2.2, and subclause 4.5.2.3, and provide the access identities and the access category to the lower layers for the purpose of access control checking. In this request to the lower layer the NAS can also provide to the lower layer the RRC establishment cause determined as specified in subclause 4.5.6 of this specification.

NOTE 1: As an implementation option, the NAS can provide the RRC establishment cause to the lower layers after being informed by the lower layers that the access attempt is allowed.

If the lower layers indicate that the access attempt is allowed, the NAS shall take the following action depending on the event which triggered the access attempt:

Editor's note: It is FFS whether the NAS layeris involved in determining t the RRC resume cause when transiting over 3GPP access from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-CONNECTED mode due to an uplink use-data packet via re-activated PDU session.

a) if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication, the NAS shall notify the upper layers that the access attempt is allowed;

b) if the event which triggered the access attempt was a request from upper layers to send a mobile originated SMS over NAS, 5GMM shall initiate the NAS transport procedure as specified in subclause 5.4.5 to send the SMS in an UL NAS TRANSPORT message;

c) if the event which triggered the access attempt was a request from upper layers to establish a new PDU session, 5GMM shall initiate the NAS transport procedure as specified in subclause 5.4.5 to send the PDU SESSION ESTABLISHMENT REQUEST message;

d) if the event which triggered the access attempt was a request from upper layers to modify an existing PDU session, 5GMM shall initiate the NAS transport procedure as specified in subclause 5.4.5 to send the PDU SESSION MODIFICATION REQUEST message; and

e) if the event which triggered the access attempt was a request to re-establish the user-plane resources for an existing PDU session, 5GMM shall initiate the service request procedure as specified in subclause 5.6.1.

If the lower layers indicate that the access attempt is barred, the NAS shall take the following action depending on the event which triggered the access attempt:

a) if the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication, the NAS shall notify the upper layers that the access attempt is barred. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS shall notify the upper layers that the barring is alleviated for the access category;

NOTE 2: In this case prohibiting the initiation of the MMTEL voice session, MMTEL video session or prohibiting sending of the SMS over IP is performed by the upper layers.

b) if the event which triggered the access attempt was a request from upper layers to send a mobile originated SMS over NAS, 5GMM shall not initiate the NAS transport procedure as specified in subclause 5.4.5 to send the SMS in an UL NAS TRANSPORT message. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, 5GMM may initiate the NAS transport procedure as specified in subclause 5.4.5 to send the SMS in an UL NAS TRANSPORT message, if still needed;

c) if the event which triggered the access attempt was a request from upper layers to establish a new PDU session, 5GMM shall not initiate the NAS transport procedure to send the PDU SESSION ESTABLISHMENT REQUEST message. Upon receiving an indication from the lower layers that the barring is alleviated for the

access category with which the access attempt was associated, the NAS may initiate the NAS transport procedure as specified in subclause 5.4.5, if still needed;

d) if the event which triggered the access attempt was a request from upper layers to modify an existing PDU session modification, 5GMM shall not initiate the NAS transport procedure to send the PDU SESSION MODIFICATION REQUEST message. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS may initiate the NAS transport procedure as specified in subclause 5.4.5, if still needed; and

e)- if the event which triggered the access attempt was a request to re-establish the user-plane resources for an existing PDU session, the NAS shall not initiate the service request procedure as specified in subclause 5.6.1. Upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS may initiate the service request procedure as specified in subclause 5.6.1, if still needed.

4.5.5 Exception handling and avoiding double barring

There are several services for which the NAS needs to be informed when the service starts and stops,

- because, while the service is ongoing, the mapping of other access attempts to a specific access category can be affected; and
- in order to avoid double barring at the start of these services.

These services are:

a) emergency service;

b) MMTEL voice;

c) MMTEL video;

d) SMSoIP; and

e) SMS over NAS.

The UE considers an emergency service a) as started when 5GMM receives a request from upper layers to register for emergency services or to establish a PDU session with request type = "initial emergency request" or "existing emergency PDU session". It considers the emergency service as stopped when this PDU session is released.

In addition, the UE considers an emergency service a) as started when the 5GMM receives a request for emergency services from the upper layer and performs emergency services fallback as specified in subclause 4.13.4.2 of 3GPP TS 23.502 [9]. In this case, the UE considers the emergency service as stopped when:

- the PDU session for emergency services established during the emergency services fallback is released if the UE has moved to an E-UTRA cell connected to 5GCN; or
- the service request procedure involved in the emergency services fallback is completed otherwise.

While an emergency service a) is ongoing, any access attempt triggered by the initiation of a registration, de-registration or service request procedure is mapped to access category 2 = emergency.

Once the emergency service has successfully passed access control, then as long as the service is ongoing, the following access attempts are allowed to proceed without further access control checking in order to avoid double barring:

- any service request procedure related to the PDU session associated with request type = "initial emergency request" or "existing emergency PDU session"; and
- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery.

NOTE 1: Although the access control checking is skipped, the mapping is performed in order to derive an RRC establishment cause.

Editor's note: If MT LCS are used during an emergency service to locate the UE, the 5GMM will transfer LCS messages to the network. It is FFS based on which criteria the UE will determine to skip access control for these messages.

For services b) to e) the 5GMM receives explicit start and stop indications from the upper layers.

Editor's note: Whether explicit start and stop indications for SMS over NAS need to be defined is FFS.

Once the service has successfully passed access control, then as long as the service is ongoing, the following access attempts are allowed to proceed without further access control checking in order to avoid double barring:

- for services b), c) and d), any service request procedure related to the PDU session established for DNN = "IMS"; and

Editor's note: It has been observed that some operators use an APN different from "IMS" for SMSoIP. How to handle that case when a DNN different from "IMS" is used, is FFS.

- for services b), c), d) and e), any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery.

While an MMTEL voice call is ongoing:

- any service request procedure related to the PDU session established for DNN = "IMS" is mapped to access category 4; and

- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery is mapped to access category 4.

While an MMTEL video call is ongoing and no MMTEL voice call is ongoing:

- any service request procedure related to the PDU session established for DNN = "IMS" is mapped to access category 5; and

- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery is mapped to access category 5.

While an SMS over IMS is ongoing, no MMTEL video call is ongoing and no MMTEL voice call is ongoing:

- any service request procedure related to the PDU session established for DNN = "IMS" is mapped to access category 6; and

- any:

  1) service request procedure; or

  2) registration procedure;

initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery is mapped to access category 6.

While an SMS over NAS is ongoing, no SMS over IMS is ongoing, no MMTEL video call is ongoing and no MMTEL voice call is ongoing:

- any:

  1) service request procedure; or

  2) registration procedure;

  initiated in 5GMM-IDLE mode for the purpose of NAS signalling connection recovery is mapped to access category 6.

NOTE 2: Although the access control checking is skipped, the mapping is performed in order to derive an RRC establishment cause.

If an access category is determined and the access control checking is skipped, the NAS shall determine the establishment cause from one or more determined access identities and the access category as specified in subclause 4.5.6, the NAS shall initiate the procedure to send the initial NAS message for the access attempt and shall provide the establishment cause to lower layers.

4.5.6 Mapping between access categories/access identities and RRC establishment cause

When 5GMM requests the establishment of a NAS-signalling connection, the RRC establishment cause used by the UE shall be selected according to one or more determined access identities and the access category as specified in table 4.5.6.1. If the determined access category is an operator-defined access category and there is a standardized access category associated with the operator-defined access category as specified in subclause 4.5.3, the RRC establishment cause used by the UE is selected according to one or more determined access identities and the standardized access category associated with the operator-defined access category.

Table 4.5.6.1: Mapping table for access identities/access categories and RRC establishment cause

Access identities	Access categories	RRC establishment cause is set to
0	0 (= MT_acc)	MT access
	1 (= delay tolerant)	FFS
	2 (= emergency)	Emergency call
	3 (= MO_sig)	MO signalling
	4 (= MO MMTel voice)	MO voice call
	5 (= MO MMTel video)	FFS
	6 (= MO SMS and SMSoIP)	FFS
	7 (= MO_data)	MO data
1	Any category	"High priority access"
2	Any category	"High priority access"
11, 15	Any category	"High priority access"
12,13,14,	Any category	"High priority access"
NOTE: See subclause 4.5.2, table 4.5.2.1 for use of the access identities of 0, 1, 2, and 11-15.		

Editor's note: It is FFS how to determine RRC establishment causes for the access category 1, 5, 6.

4.6 Network slicing

4.6.1 General

The 5GS supports network slicing as described in 3GPP TS 23.501 [8]. Within a PLMN, a network slice is identified by an S-NSSAI, which is comprised of a slice/service type (SST) and a slice differentiator (SD). Inclusion of an SD in an S-NSSAI is optional. A set of one or more S-NSSAIs is called the NSSAI. The following NSSAIs are defined in 3GPP TS 23.501 [8]:

a) configured NSSAI;

b) requested NSSAI;

c) allowed NSSAI; and

d) subscribed S-NSSAIs;

The following NSSAIs are defined in the present document:

a) rejected NSSAI for the current PLMN; and

b) rejected NSSAI for the current PLMN and registration area combination.

The HPLMN may configure a UE with the configured NSSAI per PLMN. In addition, the HPLMN may configure a UE with a configured NSSAI not associated with a PLMN. The UE shall have a single configured NSSAI not associated with a PLMN and consider the configured NSSAI as valid in a PLMN for which the UE has neither configured NSSAI nor allowed NSSAI.

The allowed NSSAI is managed per access type independently, i.e. 3GPP access or non-3GPP access.

4.6.2 Mobility management aspects

4.6.2.1 General

Upon registration to a PLMN, the UE shall send to the AMF the requested NSSAI which includes one or more S-NSSAIs of the allowed NSSAI for the PLMN or the configured NSSAI and corresponds to the network slice(s) to which the UE wants to register if:

a) the UE has a configured NSSAI for the current PLMN;

b) the UE has an allowed NSSAI for the current PLMN; or

c) the UE has neither allowed NSSAI for the current PLMN nor configured NSSAI for the current PLMN and has a configured NSSAI not associated with a PLMN.

The UE NAS shall also provide the lower layers with the requested NSSAI, if available and the UE is in 5GMM-IDLE mode. If the UE has neither a configured NSSAI nor an allowed NSSAI valid for a PLMN and does not have any configured NSSAI that is not associated with any PLMN, the UE does not send a requested NSSAI when requesting registration towards the PLMN. In roaming scenarios the UE may also provide the mapping of each S-NSSAI of the requested NSSAI to the S-NSSAIs of the configured NSSAI for the HPLMN, if available. The AMF verifies if the requested NSSAI is permitted based on the subscribed S-NSSAIs in the UE subscription and optionally the mapping information provided by the UE, and if so then the AMF shall provide the UE with the allowed NSSAI for the PLMN, and may also provide the UE with the mapping of each S-NSSAI of the allowed NSSAI for the PLMN to the S-NSSAI(s) of the configured NSSAI for the HPLMN if available. The AMF shall not provide the UE with the mapping of multiple S-NSSAIs of the allowed NSSAI to the same S-NSSAI of the configured NSSAI for the HPLMN. The AMF may also query the NSSF to determine the allowed NSSAI for a given registration area as defined in 3GPP TS 23.501 [8].

The set of network slice(s) for a UE can be changed at any time while the UE is registered to a PLMN, and the change may be initiated by the network, or the UE. In this case, the allowed NSSAI and associated registration area may be changed during the registration procedure. The network may notify the UE of the change of the supported network slice(s) in order to trigger the registration procedure. Change in the allowed NSSAI may lead to AMF relocation subject to operator policy. See subclause 5.4.4 describing the generic UE configuration update procedure for further details.

4.6.2.2 NSSAI storage

If available, the configured NSSAI(s) shall be stored in a non-volatile memory in the ME as specified in annex C.

Each of the configured NSSAI stored in the UE is a set composed of at most 16 S-NSSAIs. Each of the allowed NSSAI stored in the UE is a set composed of at most 8 S-NSSAIs and is associated with a PLMN identity and an access type. Each of the configured NSSAI, and the rejected NSSAI is associated with a PLMN identity. The S-NSSAI(s) in the rejected NSSAI for the current PLMN and registration area combination are further associated with a registration area where the rejected S-NSSAI(s) is not available. The S-NSSAI(s) in the rejected NSSAI for the current PLMN shall be considered rejected for the current PLMN regardless of the access type. There shall be no duplicated PLMN identities in

each of the list of configured NSSAI(s), allowed NSSAI(s), rejected NSSAI(s) for the current PLMN, and rejected NSSAI(s) for the current PLMN and registration area combination.

The UE stores NSSAIs as follows:

a) The configured NSSAI shall be stored until a new configured NSSAI is received for a given PLMN. The network may provide to the UE the mapping of each S-NSSAI of the new configured NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN which shall also be stored in the UE. When the UE is provisioned with a new configured NSSAI for a PLMN, the UE shall:

   1) replace any stored configured NSSAI for this PLMN with the new configured NSSAI for this PLMN;

   2) delete any stored mapping of each S-NSSAI of the configured NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN and, if available, store the mapping of each S-NSSAI of the new configured NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN;

   3) delete any stored allowed NSSAI for this PLMN and, if available, the stored mapping of each S-NSSAI of the allowed NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN, if the UE received the new configured NSSAI for this PLMN and the "registration requested" indication in the same CONFIGURATION UPDATE COMMAND message but without any new allowed NSSAI for this PLMN included; and

   4) delete any rejected NSSAI for the current PLMN, and rejected NSSAI for the current PLMN and registration area combination.

   If the UE receives an S-NSSAI associated with a PLMN ID from the network during the PDN connection establishment procedure in EPS as specified in 3GPP TS 24.301 [15], the UE may store the received S-NSSAI in the configured NSSAI for the PLMN identified by the PLMN ID associated with the S-NSSAI, if not already in the configured NSSAI.

b) The allowed NSSAI shall be stored until a new allowed NSSAI is received for a given PLMN. The network may provide to the UE the mapping of each S-NSSAI of the new allowed NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN (see subclauses 5.5.1.2 and 5.5.1.3) which shall also be stored in the UE. When a new allowed NSSAI for a PLMN is received, the UE shall:

   1) replace any stored allowed NSSAI for this PLMN with the new allowed NSSAI for this PLMN; and

   2) delete any stored mapping of each S-NSSAI of the allowed NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN and, if available, store the mapping of each S-NSSAI of the new allowed NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN.

   The UE shall remove, if any, the stored rejected S-NSSAI(s) which is/are included in the new allowed NSSAI for the current PLMN.

NOTE: Whether the UE stores the allowed NSSAI and the mapping of the allowed NSSAI to the configured NSSAI for the HPLMN also when the UE is switched off is implementation specific.

c) When the UE receives the S-NSSAI(s) included in rejected NSSAI in the REGISTRATION ACCEPT message or in the CONFIGURATION UPDATE COMMAND message, the UE shall store the S-NSSAI(s) into the rejected NSSAI based on the associated rejection cause(s). Once the UE is deregistered over all access types, the rejected NSSAI for the current PLMN shall be deleted. Once the UE is deregistered over an access type, the rejected NSSAI for the current PLMN and registration area combination corresponding to the access type shall be deleted. The UE shall delete, if any, the stored rejected NSSAI for the current PLMN and registration area combination if the UE moves out of the registration area.

4.6.3 Session management aspects

4.6.3.1 General

In order to enable PDU transmission in a network slice, the UE may request establishment of a PDU session in a network slice towards a data network (DN) which is associated with an S-NSSAI and a data network name (DNN) if there is no established PDU session adequate for the PDU transmission. The S-NSSAI included is part of allowed NSSAI of the serving PLMN, which is an S-NSSAI value valid in the serving PLMN, and in roaming scenarios the

mapped configured S-NSSAI(s) for the HPLMN is also included for the PDU session if available. See subclause 6.4.1 for further details. The UE determines whether to establish a new PDU session or use one of the established PDU session(s) based on the URSP rules which include S-NSSAIs, if any (see subclause 6.2.9).

4.7 NAS over non-3GPP access

4.7.1 General

From the UE's NAS perspective, in general the procedures and messages defined for 5GMM and 5GSM are used over non-3GPP access as over 3GPP access. However, a number of aspects are different as described in the following subclauses.

4.7.2 5GS mobility management aspects

4.7.2.1 General

The mobility management procedures defined over 3GPP access are re-used over non-3GPP access with the following exceptions:

a) the registration status of the UE's 3GPP access and non-3GPP access 5GMM state machine instances are independent and can be different;

b) single-registration mode and dual-registration mode do not apply for 5GMM over non-3GPP access;

c) the RPLMN over non-3GPP access can be different from the RPLMN over 3GPP access. The MCC of the RPLMN over 3GPP access and the MCC of the RPLMN over the non-3GPP access can also be different;

d) the registration for 3GPP access and for non-3GPP access are performed separately. Like for 3GPP access, an access stratum connection exists before the UE can perform the registration procedure for non-3GPP access. As over non-3GPP access the 5GS operates one single common registration area for an entire PLMN, which is associated with the operator-specific N3GPP TAI for the PLMN, list management of registration areas is not required, and registration updating due to registration area change with the registered PLMN is not performed. Furthermore, the periodic registration update procedure is also not performed. New registration at change of PLMN is required;

e) the 5GMM over non-3GPP access considers that the N1 NAS signalling connection is established when the lower layers indicate that the access stratum connection is established succcessfully;

f) the UE-initiated service request procedure via non-3GPP access is supported. Upon indication from the lower layers of non-3GPP access, that the access stratum connection is established between the UE and the network, the UE in 5GMM-REGISTERED state and in 5GMM-IDLE mode over non-3GPP access shall initiate the service request procedure via non-3GPP access. The UE may indicate with the service request message the PDU session(s) associated with non-3GPP access to re-activate user-plane resources for which the UE has pending user data to be sent;

g) paging procedure is not performed via non-3GPP access;

h) service area restrictions do not apply for non-3GPP access; and

i) the establishment cause for non-3GPP access is determined according to subclause 4.7.2.2.

4.7.2.2 Establishment cause for non-3GPP access

When establishment of a N1 NAS signalling connection over non-3GPP access is initiated, the UE shall determine one or more access identities to be associated with the establishment of the N1 NAS signalling connection as specified in subclause 4.5.2 and table 4.5.2.1, shall select the establishment cause from the determined one or more access identities and the event which triggered initiation of the NAS signalling connection over non-3GPP access as specified in table 4.7.2.2.1 and shall provide the selected establishment cause to the lower layers.

Table 4.7.2.2.1: Mapping table for determination of establishment cause for non-3GPP access

Access identities	Type of access attempt	Requirements to be met	Establishment cause
0	Emergency	UE is attempting access for an emergency session (NOTE 1)	Emergency call
	UE NAS initiated 5GMM specific procedures	Access attempt is for MO signalling	MO signalling
	UE NAS initiated 5GMM connection management procedures or 5GMM NAS transport procedure	Access attempt is for MO data	MO data
1	Any	Any	"High priority access"
2	Any	Any	"High priority access"
11, 15	Any	Any	"High priority access"
12,13,14,	Any	Any	"High priority access"
NOTE 1: This includes 5GMM specific procedures while the service is ongoing and 5GMM connection management procedures required to establish a PDU session with request type = "initial emergency request" or "existing emergency PDU session", or to re-establish radio bearers for such a PDU session.			
NOTE 2: See subclause 4.5.2, table 4.5.2.1 for use of the access identities of 0, 1, 2, and 11-15.			

4.7.3 5GS session management aspects

The session management procedures defined over 3GPP access are re-used over non-3GPP access.

4.8 Interworking with E-UTRAN connected to EPC

4.8.1 General

In order to interwork with E-UTRAN connected to EPC, the UE supporting both S1 mode and N1 mode can operate in single-registration mode or dual-registration mode (see 3GPP TS 23.501 [8]). Support of single-registration mode is mandatory for UEs supporting both S1 mode and N1 mode.

During the EPS attach procedure (3GPP TS 24.301 [15]) or initial registration procedure (see subclause 5.5.1.2), the mode for inter-system interworking is selected if the UE supports both S1 mode and N1 mode, and the network supports inter-system interworking.

4.8.2 Single-registration mode

4.8.2.1 General

If the UE receives the indication that interworking without N26 is not supported, the UE operates as described in subclause 4.8.2.2. If the UE receives the indication that interworking without N26 is supported and the UE does not support dual-registration mode, the UE operates as described in subclause 4.8.2.3.

4.8.2.2 Single-registration mode with N26 interface

See subclause 5.1.4.2 for coordination between 5GMM and EMM and subclause 6.1.4.1 for coordination between 5GSM and ESM.

4.8.2.3 Single-registration mode without N26 interface

At inter-system change from N1 mode to S1 mode in EMM-IDLE mode when:

a) the UE supports non-IP PDN type and at least one PDU session is active; or

b) the UE does not support non-IP PDN type and at least one PDU session context of IPv4, IPv6 or IPv4v6 PDU session type is active,

the UE shall proceed as follows:

a) if the UE supports sending an ATTACH REQUEST message containing a PDN CONNECTIVITY REQUEST message with request type set to "handover" to transfer a PDU session from N1 mode to S1 mode and the UE has received an "interworking without N26 supported" indication from the network, the UE shall:

   1) enter substates EMM-DEREGISTERED.NORMAL-SERVICE and 5GMM-REGISTERED.NO-CELL-AVAILABLE;

   2) map each PDU session supporting interworking to EPS to the default EPS bearer context of the corresponding PDN connection(s) and set the state of each default EPS bearer context, as specified in subclause 6.1.4.2; and

   3) initiate an EPS attach procedure and include a PDN CONNECTIVITY REQUEST message with request type set to "handover" in the ATTACH REQUEST message to activate a default EPS bearer context for one of the active PDU session contexts.

   After successful completion of the EPS attach procedure, the UE shall attempt to activate each of the other default EPS bearer contexts, if any, by initiating a stand-alone PDN connectivity procedure with request type set to "handover" in the PDN CONNECTIVITY REQUEST message; and

b) otherwise, enter substates EMM-REGISTERED.NORMAL-SERVICE and 5GMM-REGISTERED.NO-CELL-AVAILABLE and initiate a tracking area update procedure (see 3GPP TS 24.301 [15]).

At inter-system change from N1 mode to S1 mode in EMM-IDLE mode when:

a) the UE supports non-IP PDN type and no PDU session is active; or

b) the UE does not support non-IP PDN type and no PDU session context of IPv4, IPv6 or IPv4v6 PDU session type is active,

the UE shall enter substates EMM-DEREGISTERED.NORMAL-SERVICE and 5GMM-DEREGISTERED.NO-CELL-AVAILABLE, and initiate an attach procedure.

At inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode, the UE shall:

a) enter substate 5GMM-REGISTERED.NORMAL-SERVICE and substate EMM-REGISTERED.NO-CELL-AVAILABLE;

b) map the default EPS bearer context(s) of the PDN connection(s), if any, to the corresponding PDU session(s) and set the state of each PDU session, as specified in subclause 6.1.4.2; and

c) initiate the registration procedure for mobility and periodic registration update indicating "mobility registration updating" in the 5GS registration type IE of the REGISTRATION REQUEST message (see subclause 5.5.1.3).

After having successfully registered in N1 mode the UE shall:

a) if the UE supports the PDU session establishment procedure with request type set to "existing PDU session" to transfer a PDN connection from S1 mode to N1 mode and the UE has received an "interworking without N26 supported" indication from the network, attempt to transfer all existing PDN connections, if any, from S1 mode to N1 mode by initiating the PDU session establishment procedure with request type set to "existing PDU session"; and

b) otherwise, establish PDU sessions corresponding to all existing PDN connections, if any, by initiating the PDU session establishment procedure with request type set to "initial request".

See subclause 5.1.4.3 for coordination between 5GMM and EMM and subclause 6.1.4.2 for coordination between 5GSM and ESM.

4.8.3 Dual-registration mode

If both 5GMM and EMM are enabled, a UE, which is capable of N1 mode and S1 mode and is operating in the dual-registration mode shall maintain independent registrations for 5GMM and EMM independently. Coordination between 5GMM and EMM is not needed, except as specified in the present subclause.

a) A UE operating in the dual-registration mode may register to N1 mode only, S1 mode only, or to both N1 mode and S1 mode.

b) When the UE decides to operate in dual-registration mode (see subclause 5.5.1.2.4), NAS informs the lower layers about this.

c) If a UE is registered in N1 mode only, then for registration in S1 mode it shall use the same PLMN to which it is registered in N1 mode or an equivalent PLMN.

d) If a UE is registered in S1 mode only, then for registration in N1 mode it shall use the same PLMN to which it is registered in S1 mode or an equivalent PLMN.

Editor's note: When the UE registers in the other mode, it can receive an equivalent PLMN which is different from the equivalent PLMN list already stored in the UE. The handling of these 2 lists, e.g. whether they are maintained independently or whether the new one overrides the old one, is FFS. Furthermore, if the UE is registered in both N1 mode and S1 mode, then due to the UE's mobility the PLMNs to which the UE is registered in N1 mode and S1 mode, respectively, can become non-equivalent PLMNs. The UE reaction for this case is FFS.

When no PDU session is active and the UE has not registered to S1 mode yet, the UE may initiate the attach procedure if EMM-REGISTERED without PDN connection is not supported by the MME. If EMM-REGISTERED without PDN connection is supported by the MME, the UE may initiate either the attach procedure without PDN connection establishment or the attach procedure with PDN connection establishment.

When at least one PDU session is active and the UE has not registered to S1 mode yet, the UE may initiate the attach procedure. If necessary, the UE may transfer an active PDU session from N1 mode to S1 mode by initiating the attach procedure with request type set to "handover" in the PDN CONNECTIVITY REQUEST message. After successfully attached in S1 mode, if necessary, the UE may transfer other active PDU sessions from N1 mode to S1 mode by initiating the PDN connectivity procedure with request type set to "handover" in the PDN CONNECTIVITY REQUEST message.

NOTE 1: It is up to UE implementation to determine which active PDU session is transferred from N1 mode to S1 mode.

When the UE has not registered to N1 mode, the UE may initiate the initial registration procedure. After successfully registered in N1 mode, if necessary, the UE may transfer one or more active PDN connections from S1 mode to N1 mode by initiating the PDU session establishment procedure with request type set to "existing PDU session".

NOTE 2: It is up to UE implementation to determine which active PDN connection is transferred from S1 mode to N1 mode.

If both the UE and the MME support EMM-REGISTERED without PDN connection, the UE that transferred all PDN connections to the 5GS, may stay in state EMM-REGISTERED. Otherwise, the UE shall enter state EMM-DEREGISTERED upon transferring all PDN connection to the 5GS.

See subclause 6.1.4 for coordination between 5GSM and ESM.

4.8.4 Core Network selection

If the UE is capable of both N1 mode and S1 mode, when the UE needs to use one or more functionalities not supported in 5GS but supported in EPS and the UE is in 5GMM-IDLE mode, the UE may disable the N1 mode capability for 3GPP access (see subclause 4.9.2).

If the UE is capable of both N1 mode and S1 mode and lower layers provide an indication that the current E-UTRA cell is connected to both EPC and 5GCN, the UE shall select a core network type (EPC or 5GCN) based on the PLMN selection procedures as specified in 3GPP TS 23.122 [5] and provide the selected core network type information to the lower layer during the initial registration procedure.

NOTE: If the PLMN selection information provisioned in the USIM does not contain any prioritization between E-UTRAN and NG-RAN for a PLMN, which core network type to select for that PLMN is up to UE implementation.

4.9 Disabling and re-enabling of UE's N1 mode capability

4.9.1 General

The UE shall re-enable the N1 mode capability when the UE powers off and powers on again or the USIM is removed.

As an implementation option, the UE may start a timer for re-enabling N1 mode capability, after the N1 mode capability was disabled. On the expiry of this timer, the UE should re-enable the N1 mode capability.

4.9.2 Disabling and re-enabling of UE's N1 mode capability for 3GPP access

When the UE supporting both N1 mode and S1 mode is disabling the N1 mode capability for 3GPP access, it should proceed as follows:

a) select an E-UTRA cell connected to EPC of the registered PLMN or a PLMN from the list of equivalent PLMNs;

b) if an E-UTRA cell connected to EPC of the registered PLMN or a PLMN from the list of equivalent PLMNs cannot be found, the UE may select another RAT of the registered PLMN or a PLMN from the list of equivalent PLMNs that the UE supports;

c) if another RAT of the registered PLMN or a PLMN from the list of equivalent PLMNs cannot be found, or the UE does not have a registered PLMN, then perform PLMN selection as specified in 3GPP TS 23.122 [5]; or

d) if no other allowed PLMN and RAT combinations are available, then the UE may re-enable the N1 mode capability for 3GPP access and remain camped in NG-RAN of the registered PLMN, and may periodically scan for another PLMN and RAT combination which can provide EPS services or non-EPS services (if the UE supports non-EPS services).

When the UE supporting both N1 mode and S1 mode needs to stay in E-UTRA connected to EPC (e.g. due to the domain selection for UE originating sessions as specified in subclause 4.3.2), in order to prevent unwanted handover or cell reselection from E-UTRA connected to EPC to NG-RAN connected to 5GCN, the UE operating in single-registration mode shall disable the N1 mode capability for 3GPP access and:

a) shall set the N1mode bit to "N1 mode not supported" in the UE network capability IE (see 3GPP TS 24.301 [15]) of the ATTACH REQUEST message and the TRACKING AREA UPDATE REQUEST message in EPC; and

b) the UE NAS layer shall indicate the access stratum layer(s) of disabling of the N1 mode capability for 3GPP access.

NOTE: The UE can only disable the N1 mode capability for 3GPP access when in 5GMM-IDLE mode.

The UE shall re-enable the N1 mode capability for 3GPP access when the UE performs PLMN selection.

If the disabling of N1 mode capability for 3GPP access was due to IMS voice is not available over 3GPP access and the UE’s usage setting is "voice centric", the UE shall re-enable the N1 mode capability for 3GPP access when the UE’s usage setting is changed from "voice centric" to "data centric" or when the IMS voice becomes available in 5GS, as specified in subclauses 4.3.3 and 4.3.4.

The UE should memorize the identity of the PLMN where N1 mode capability for 3GPP access was disabled and should not consider this PLMN in subsequent PLMN selections as specified in 3GPP TS 23.122 [5].

If the UE attempts to establish a PDU session for emergency services in a PLMN where N1 mode capability was disabled due to the UE's registration attempt counter have reached 5, the UE may enable N1 mode capability for that PLMN memorized by the UE.

4.9.3 Disabling and re-enabling of UE's N1 mode capability for non-3GPP access

Editor's note: The content of this subclause is still to be determined.

5 Elementary procedures for 5GS mobility management

5.1 Overview

5.1.1 General

The main function of the 5GS mobility management (5GMM) sublayer is to support the identification, security, mobility of a UE as well as generic message transport.

A further function of the 5GMM sublayer is to provide connection management services to the other sublayer(s).

Editor's note: Sublayer design can be revisited after the protocol framework is identified.

5.1.2 Types of 5GMM procedures

Depending on how they can be initiated, three types of 5GMM procedures can be distinguished:

a) 5GMM common procedures

5GMM common procedure can always be initiated when the UE is in 5GMM-CONNECTED mode. The procedures belonging to this type are:

1) Initiated by the network:

i) network-initiated NAS transport.

ii) primary authentication and key agreement procedure

iii) security mode control;

iv) generic UE configuration update

v) identification

2) Initiated by the UE:

UE-initiated NAS transport.

3) Initiated by the UE or the network and used to report certain error conditions detected upon receipt of 5GMM protocol data:

5GMM status.

b) 5GMM specific procedures:

At any time only one UE initiated 5GMM specific procedure can be running for each of the access network(s) that the UE is camping in. The procedures belonging to this type are:

1) Initiated by the UE and used e.g. to register to the network for 5GS services and establish a 5GMM context, to update the location/parameter(s) of the UE:

registration.

2) Initiated by the UE or the network and used to deregister from the network for 5GS services and to release a 5GMM context:

de-registration.

3) Initiated by the UE and used to deregister from the network for 5GS services and to release a 5GMM context:

eCall inactivity procedure.

c) 5GMM connection management procedures:

1) 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 5GMM specific procedure is ongoing for each of the access network(s) that the UE is camping in.

2) Initiated by the network and used to request the establishment of an N1 NAS signalling connection or to prompt the UE to perform re-registration if necessary as a result of a network failure or to request re-establishment of the PDU session(s) associated with non-3GPP access over 3GPP access; not applicable for the non-3GPP access network:

paging.

3) Initiated by the network and used to request re-establishment the PDU session(s) associated with non-3GPP access over 3GPP access when the UE is in 5GMM-CONNECTED mode over 3GPP access and in 5GMM-IDLE mode over non-3GPP access; or

Initiated by the network and used to request re-establishment of the PDU session(s) associated with 3GPP access over 3GPP access when the UE is in 5GMM-CONNECTED mode over non-3GPP access and in 5GMM-IDLE mode over 3GPP access:

notification.

5.1.3 5GMM sublayer states

5.1.3.1 General

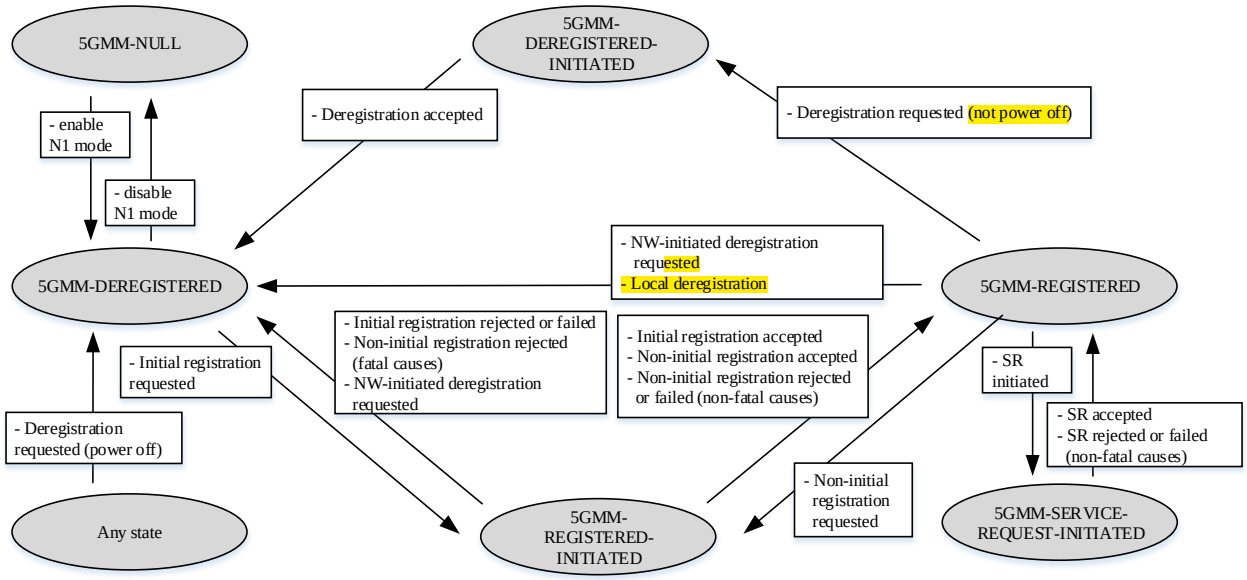
In the following subclauses, the 5GS mobility management (5GMM) sublayer of the UE and the network is described by means of different state machines. The 5GMM sublayer states is managed per access type independently, i.e. 3GPP access or non-3GPP access. In subclause 5.1.3.2, the states of the 5GMM sublayer are introduced.

5.1.3.2 5GMM sublayer states

5.1.3.2.1 5GMM sublayer states in the UE

5.1.3.2.1.1 General

In the following subclauses, the possible 5GMM sublayer states of the UE are described and shown in Figure 5.1.3.2.1.1.1.



NOTE: Not all possible transitions are shown in this figure.
Editor's note: The fatal causes and non-fatal causes used in the 5GMM procedures are FFS.

Figure 5.1.3.2.1.1.1: 5GMM main states in the UE

5.1.3.2.1.2 Main states

5.1.3.2.1.2.1 5GMM-NULL

5GS services are disabled in the UE. No 5GS mobility management function shall be performed in this state.

5.1.3.2.1.2.2 5GMM-DEREGISTERED

In the state 5GMM-DEREGISTERED, no 5GMM context has been established and the UE location is unknown to the network and hence it is unreachable by a network. In order to establish a 5GMM context, the UE shall start the initial registration procedure.

5.1.3.2.1.2.3 5GMM-REGISTERED-INITIATED

A UE enters the state 5GMM-REGISTERED-INITIATED after it has started the initial registration procedure or the non-initial registration procedure, and is waiting for a response from the network.

5.1.3.2.1.2.4 5GMM-REGISTERED

In the state 5GMM-REGISTERED, a 5GMM context has been established. Additionally, one or more PDU session(s) may be activated at the UE. The UE may initiate the non-initial registration procedure (including the normal registration update and periodic registration update) and the service request procedure. The UE in the state 5GMM-REGISTERED over non-3GPP access shall not initiate the periodic registration update procedure.

5.1.3.2.1.2.5 5GMM-DEREGISTERED-INITIATED

A UE enters the state 5GMM-DEREGISTERED-INITIATED after it has requested release of the 5GMM context by starting the de-registration procedure and is waiting for a response from the network.

5.1.3.2.1.2.6 5GMM-SERVICE-REQUEST-INITIATED

A UE enters the state 5GMM-SERVICE-REQUEST-INITIATED after it has started the service request procedure and is waiting for a response from the network.

5.1.3.2.1.3 Substates of state 5GMM-DEREGISTERED

5.1.3.2.1.3.1 General

The state 5GMM-DEREGISTERED is subdivided into a number of substates as described in this subclause. The following substates are not applicable to non-3GPP access:

a) 5GMM-DEREGISTERED.LIMITED-SERVICE;

b) 5GMM-DEREGISTERED.PLMN-SEARCH:

c) 5GMM-DEREGISTERED.NO-SUPI;

d) 5GMM-DEREGISTERED.NO-CELL-AVAILABLE; and

e) 5GMM-DEREGISTERED.eCALL-INACTIVE.

Valid subscriber data are available for the UE before it enters the substates, except for the substate 5GMM-DEREGISTERED.NO-SUPI.

5.1.3.2.1.3.2 5GMM-DEREGISTERED.NORMAL-SERVICE

The substate 5GMM-DEREGISTERED.NORMAL-SERVICE is chosen in the UE when a suitable cell has been found and the PLMN or tracking area is not in the forbidden list.

5.1.3.2.1.3.3 5GMM-DEREGISTERED.LIMITED-SERVICE

The substate 5GMM-DEREGISTERED.LIMITED-SERVICE is chosen in the UE, when it is known that a selected cell is unable to provide normal service (e.g. the selected cell is in a forbidden PLMN or is in a forbidden tracking area).

This substate is not applicable to non-3GPP access.

5.1.3.2.1.3.4 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION

The substate 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION is chosen in the UE if the initial registration procedure failed due to a missing response from the network.

Editor's note: Other cases in which this substate is chosen are FFS.

5.1.3.2.1.3.5 5GMM-DEREGISTERED.PLMN-SEARCH

The substate 5GMM-DEREGISTERED.PLMN-SEARCH is chosen in the UE, if the UE is searching for PLMNs. This substate is left either when a cell has been selected (the new substate is NORMAL-SERVICE or LIMITED-SERVICE) or when it has been concluded that no cell is available at the moment (the new substate is NO-CELL-AVAILABLE).

This substate is not applicable to non-3GPP access.

5.1.3.2.1.3.6 5GMM-DEREGISTERED.NO-SUPI

The substate 5GMM-DEREGISTERED.NO-SUPI is chosen in the UE, if the UE has no valid subscriber data available (SIM/USIM not available, the SIM/USIM is considered invalid by the UE) and a cell has been selected.

This substate is not applicable to non-3GPP access.

5.1.3.2.1.3.7 5GMM-DEREGISTERED.NO-CELL-AVAILABLE

No 5G cell can be selected. This substate is entered after a first intensive search failed when in substate 5GMM-DEREGISTERED.PLMN-SEARCH. Cells are searched for at a low rhythm. No 5GS services are offered.

This substate is not applicable to non-3GPP access.

5.1.3.2.1.3.8 5GMM-DEREGISTERED.eCALL-INACTIVE

The substate 5GMM-DEREGISTERED.eCALL-INACTIVE is chosen in the UE when:

a) the UE is configured for eCall only mode as specified in 3GPP TS 31.102 [22];

b) timer T3444 and timer T3445 have expired or are not running;

c) a PLMN has been selected as specified in 3GPP TS 23.122 [5];

d) the UE does not need to perform an eCall over IMS; and

e) the UE does not need to perform a call to a non-emergency MSISDN or URI for test or terminal reconfiguration service.

NOTE: Timers T3444 and T3445 are specified in 3GPP TS 24.301 [15].

In this substate, the UE shall not initiate any signalling towards the network, except to originate an eCall over IMS, or a call to a non-emergency MSISDN or URI for test or terminal reconfiguration service.

Editor's note: Other substates of state 5GMM-DEREGISTERED are FFS, e.g. 5GMM-DEREGISTERED.REGISTRATION-NEEDED.

This substate is not applicable to non-3GPP access.

5.1.3.2.1.4 Substates of state 5GMM-REGISTERED

5.1.3.2.1.4.1 General

The state 5GMM-REGISTERED is subdivided into a number of substates as described in this subclause. The following substates are not applicable to non-3GPP access:

a) 5GMM-REGISTERED.LIMITED-SERVICE;

b) 5GMM-REGISTERED.PLMN-SEARCH:

c) 5GMM-REGISTERED.NON-ALLOWED-SERVICE; and

d) 5GMM-REGISTERED.NO-CELL-AVAILABLE.

5.1.3.2.1.4.2 5GMM-REGISTERED.NORMAL-SERVICE

The substate 5GMM-REGISTERED.NORMAL-SERVICE is chosen by the UE as the primary substate when the UE enters the state 5GMM-REGISTERED, and for 3GPP access, the cell the UE selected is known to be in an allowed area.

5.1.3.2.1.4.3 5GMM-REGISTERED.NON-ALLOWED-SERVICE

The substate 5GMM-REGISTERED.NON-ALLOWED-SERVICE is chosen in the UE, if the cell the UE selected is known to be in a non-allowed area.

This substate is not applicable to non-3GPP access.

5.1.3.2.1.4.4 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE

The substate 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE is chosen by the UE if the registration procedure for mobility and periodic registration update procedure failed due to a missing response from the network. No 5GMM procedure except:

a) mobility and periodic registration update procedure over 3GPP access; and

b) mobility registration procedure over non-3GPP access

shall be initiated by the UE in this substate. No data shall be sent or received.

NOTE: The registration procedure for mobility and periodic registration update over non-3GPP access can be trigger by e.g. the change of UE network capability or renegotiating some parameters.

5.1.3.2.1.4.5 5GMM-REGISTERED.LIMITED-SERVICE

The substate 5GMM-REGISTERED.LIMITED-SERVICE is chosen in the UE, if the cell the UE selected is known not to be able to provide normal service.

This substate is not applicable to non-3GPP access.

5.1.3.2.1.4.6 5GMM-REGISTERED.PLMN-SEARCH

The substate 5GMM-REGISTERED.PLMN-SEARCH is chosen in the UE, while the UE is searching for PLMNs.

This substate is not applicable to non-3GPP access.

5.1.3.2.1.4.7 5GMM-REGISTERED.NO-CELL-AVAILABLE

5G coverage has been lost or MICO mode is active in the UE. If MICO mode is active, the UE can deactivate MICO mode at any time by activating the AS layer when the UE needs to send mobile originated signalling or user data. Otherwise, the UE shall not initiate any 5GMM procedure except for cell and PLMN reselection.

Editor's note: Other substates of state 5GMM-REGISTERED are FFS, e.g. 5GMM-REGISTERED.UPDATE-NEEDED.

This substate is not applicable to non-3GPP access.

5.1.3.2.2 5GS update status in the UE

In order to describe the detailed UE behaviour, the 5GS update (5U) status pertaining to a specific subscriber is defined.

The 5GS 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 .

The 5GS update status value is changed only after the execution of a registration, network-initiated de-registration, 5GS based primary authentication and key agreement, service request or paging procedure.

5U1: UPDATED

The last registration attempt was successful.

5U2: NOT UPDATED

The last registration attempt failed procedurally, e.g. no response or reject message was received from the AMF.

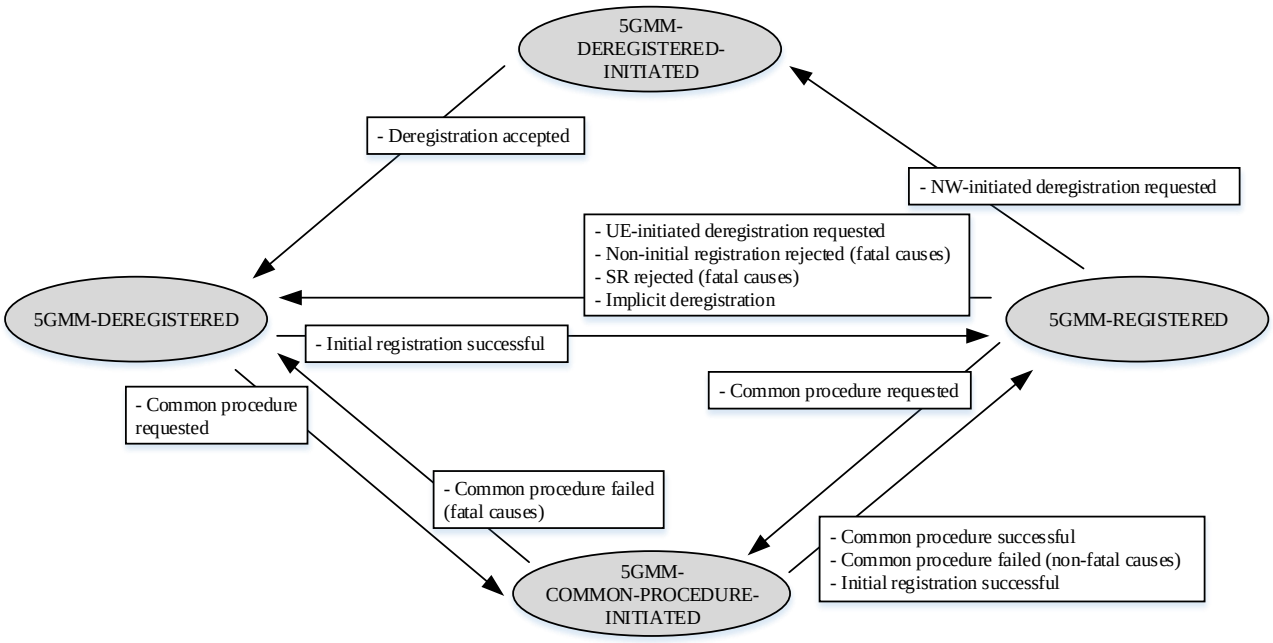
5U3: ROAMING NOT ALLOWED

The last registration, service request, or registration for mobility or periodic registration update attempt was correctly performed, but the answer from the AMF was negative (because of roaming or subscription restrictions).

5.1.3.2.3 5GMM sublayer states in the network side

5.1.3.2.3.1 General

In the following subclauses, the possible 5GMM sublayer states of the network are described and shown in Figure 5.1.3.2.3.1.1.



NOTE: Not all possible transitions are shown in this figure.
Editor's note: The fatal causes and non-fatal causes used in the 5GMM procedures are FFS.

Figure 5.1.3.2.3.1.1: 5GMM main states in the network

5.1.3.2.3.2 5GMM-DEREGISTERED

In the state 5GMM-DEREGISTERED, no 5GMM context has been established or the 5GMM context is marked as deregistered. The UE is deregistered. The network may answer to an initial registration procedure initiated by the UE. The network may also answer to a de-registration procedure initiated by the UE.

5.1.3.2.3.3 5GMM-COMMON-PROCEDURE-INITIATED

The network enters the state 5GMM-COMMON-PROCEDURE-INITIATED, after it has started a common 5GMM procedure and is waiting for a response from the UE.

5.1.3.2.3.4 5GMM-REGISTERED

In the state 5GMM-REGISTERED, a 5GMM context has been established. Additionally, one or more PDU session(s) may be activated at the network.

5.1.3.2.3.5 5GMM-DEREGISTERED-INITIATED

The network enters the state 5GMM-DEREGISTERED-INITIATED after it has started a de-registration procedure and is waiting for a response from the UE.

5.1.4 Coordination between 5GMM and EMM

5.1.4.1 General

If both 5GMM and EMM are enabled, a UE, which is capable of N1 mode and S1 mode and operates in single-registration mode, shall maintain one common registration for 5GMM and EMM.

5.1.4.2 Coordination between 5GMM and EMM with N26 interface

A UE that is not registered shall be in state EMM-DEREGISTERED and state 5GMM-DEREGISTERED.

In N1 mode, upon successful completion of a registration procedure, the UE operating in single-registration mode shall enter substates 5GMM-REGISTERED.NORMAL-SERVICE and EMM-REGISTERED.NO-CELL-AVAILABLE.

At inter-system change from S1 mode to N1 mode, the UE shall enter substates 5GMM-REGISTERED.NORMAL-SERVICE and EMM-REGISTERED.NO-CELL-AVAILABLE and initiate a registration procedure for mobility and peirodic registration update indicating "mobility registration updating" in the 5GS registration type IE of the REGISTRATION REQUEST message (see subclause 5.5.1.3).

In S1 mode, upon successful completion of an attach or tracking area updating procedure, the UE operating in single-registration mode shall enter substates 5GMM-REGISTERED.NO-CELL-AVAILABLE and EMM-REGISTERED.NORMAL-SERVICE.

At inter-system change from N1 mode to S1 mode when there is no active PDU session for which interworking to EPS is supported as specified in subclause 6.1.4.1, and EMM-REGISTERED without PDN connection is not supported by the UE or the MME, the UE shall enter state 5GMM-DEREGISTERED and state EMM-DEREGISTERED and then initiate the EPS attach procedure. If EMM-REGISTERED without PDN connection is supported by the UE and the MME, the UE shall enter substates EMM-REGISTERED.NORMAL-SERVICE and 5GMM-REGISTERED.NO-CELL-AVAILABLE and initiate a tracking area updating procedure.

At inter-system change from N1 mode to S1 mode when there is at least one active PDU session for which interworking to EPS is supported as specified in subclause 6.1.4.1, the UE shall enter substates EMM-REGISTERED.NORMAL-SERVICE and 5GMM-REGISTERED.NO-CELL-AVAILABLE and initiate a tracking area updating procedure (see 3GPP TS 24.301 [15]).

5.1.4.3 Coordination between 5GMM and EMM without N26 interface

A UE operating in the single-registration mode that is not registered shall be in state EMM-DEREGISTERED and in state 5GMM-DEREGISTERED.

In N1 mode, upon successful completion of a registration procedure, the UE operating in the single-registration mode shall enter substates 5GMM-REGISTERED.NORMAL-SERVICE and EMM-REGISTERED.NO-CELL-AVAILABLE.

At inter-system change from N1 mode to S1 mode in 5GMM-IDLE mode, the UE shall behave as specified in subclause 4.8.2.3.

In S1 mode, upon successful completion of an attach or tracking area updating procedure, the UE operating in the single-registration mode shall enter substates 5GMM-REGISTERED.NO-CELL-AVAILABLE and EMM-REGISTERED.NORMAL-SERVICE.

At inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode, the UE operating in the single-registration mode shall enter substates EMM-REGISTERED.NO-CELL-AVAILABLE and 5GMM- REGISTERED.NORMAL-SERVICE and then initiate the registration procedure for mobility and periodic registration update indicating "mobility registration updating" in the 5GS registration type IE of the REGISTRATION REQUEST message (see subclause 5.5.1.3).

5.2 Behaviour of the UE in state 5GMM-DEREGISTERED and state 5GMM-REGISTERED

5.2.1 General

In this subclause, the detailed behaviour of the UE in the states 5GMM-DEREGISTERED and 5GMM-REGISTERED is described.

5.2.2 UE behaviour in state 5GMM-DEREGISTERED

5.2.2.1 General

The state 5GMM-DEREGISTERED is entered in the UE, when:

a) the de-registration is performed either by the UE or by the network (see subclause 5.5.2);

b) the registration request is rejected by the AMF (see subclause 5.5.1.2.5 and 5.5.1.3.5);

c) the service request is rejected by the MME (see subclause 5.6.1); or

d) the UE is switched on.

In state 5GMM-DEREGISTERED, the UE shall behave according to the substate as explained in subclause 5.2.2.1.2.

5.2.2.2 Primary substate selection

5.2.2.2.1 Selection of the substate after power on

For a UE configured for eCall only mode as specified in 3GPP TS 31.102 [22], timers T3444 and T3445 are considered to have expired at 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 [5] for further details.

NOTE: Timers T3444 and T3445 are specified in 3GPP TS 24.301 [15].

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

a) if no cell can be selected, the substate shall be NO-CELL-AVAILABLE;

b) if no USIM is present, the substate shall be NO-SUPI;

c) if a suitable cell has been found and the PLMN or tracking area is not in one of the lists of forbidden tracking areas, then the substate shall be NORMAL-SERVICE;

d) if the selected cell is known not to be able to provide normal service, then the UE shall enter the substate LIMITED-SERVICE;

e) 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

f) if the UE is configured for eCall only mode as specified in 3GPP TS 31.102 [22], the substate shall be eCALL-INACTIVE.

5.2.2.2 Detailed description of UE behaviour in state 5GMM-DEREGISTERED

5.2.2.2.1 NORMAL-SERVICE

The UE shall initiate an initial registration procedure.

5.2.2.2.2 LIMITED-SERVICE

The UE shall initiate an initial registration procedure when entering a cell which provides normal service.

The UE may initiate initial registration for emergency services.

5.2.2.2.3 ATTEMPTING-REGISTRATION

The UE in 3GPP access:

a) shall initiate an initial registration procedure on the expiry of timers T3502, T3511 or T3346;

b) may initiate an initial registration procedure for emergency services even if timer T3346 is running;

c) shall initiate an initial registration procedure when entering a new PLMN, if timer T3346 is running and the new PLMN is not equivalent to the PLMN where the UE started timer T3346, the PLMN identity of the new cell is not in the forbidden PLMN lists and the tracking area is not in one of the lists of forbidden tracking areas; and

d) shall initiate an initial registration procedure when the tracking area of the serving cell has changed, if timer T3346 is not running, the PLMN identity of the new cell is not in one of the forbidden PLMN lists and the tracking area of the new cell is not in one of the lists of forbidden tracking areas.

The UE in non-3GPP access:

a) shall initiate an initial registration procedure on the expiry of timers T3502, T3511 or T3346.

5.2.2.2.4 PLMN-SEARCH

The UE shall perform PLMN selection. If a new PLMN is selected, the UE shall reset the registration attempt counter and initiate the registration procedure for initial registration (see subclause 5.5.1.2.2).

If the selected cell is known not to be able to provide normal service, the UE may initiate the registration procedure for initial registration for emergency services.

5.2.2.2.5 NO-SUPI

The UE shall perform cell selection.

The UE may initiate the registration procedure for initial registration for emergency services.

5.2.2.2.6 NO-CELL-AVAILABLE

The UE shall perform cell selection and choose an appropriate substate when a cell is found.

5.2.2.2.7 eCALL-INACTIVE

The UE camps on a suitable cell or an acceptable cell in a PLMN selected as specified in 3GPP TS 23.122 [5] but initiates no 5GMM signalling with the network and ignores any paging requests.

The UE shall leave substate EMM-DEREGISTERED.eCALL-INACTIVE state only when one of the following events occur:

a) if the USIM is removed, the UE enters substate 5GMM-DEREGISTERED.NO-SUPI;

b) if coverage is lost, the UE enters substate 5GMM-DEREGISTERED.PLMN-SEARCH;

c) if the UE is deactivated (e.g. powered off) by the user, the UE enters state 5GMM-NULL;

d) if the UE receives a request from upper layers to establish an eCall over IMS, the UE enters state 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION. The UE then uses the relevant 5GMM and 5GSM procedures to establish the eCall over IMS at the earliest opportunity; or

e) if the UE receives a request from upper layers to establish a call to an HPLMN designated non-emergency MSISDN or URI for test or terminal reconfiguration service, the UE enters state 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION. Once the registration procedure is completed, the UE uses the relevant 5GMM and 5GSM procedures to establish the non-emergency call.

5.2.2.3 Substate when back to state 5GMM-DEREGISTERED from another 5GMM state

When returning to state 5GMM-DEREGISTERED, the UE shall select a cell as specified in 3GPP TS 38.304 [28].

The substate depends on the result of the cell selection procedure, the outcome of the previously performed 5GMM specific procedures, on the 5GS update status of the UE, on the tracking area data stored in the UE, on the presence of the USIM, on the UE configuration and on the reason for moving to 5GMM-DEREGISTERED:

a) If no cell has been found, the substate is NO-CELL-AVAILABLE, until a cell is found;

b) If no USIM is present or if the inserted USIM is considered invalid by the UE, the substate shall be NO-SUPI;

c) If a suitable cell has been found and the PLMN or tracking area is not in one of the lists of forbidden tracking areas, the substate shall be NORMAL-SERVICE;

d) If a registration shall be performed (e.g. network-requested re-registration), the substate shall be ATTEMPTING-REGISTRATION;

e) If a PLMN reselection (according to 3GPP TS 23.122 [5]) is needed, the substate shall be PLMN-SEARCH;

f) If the selected cell is known not to be able to provide normal service, the substate shall be LIMITED-SERVICE; and

g) If the UE is configured for eCall only mode as specified in 3GPP TS 31.102 [22], T3444 and T3445 have expired or are not running, and substate PLMN-SEARCH is not required, the substate shall be eCALL-INACTIVE.

NOTE: Timers T3444 and T3445 are specified in 3GPP TS 24.301 [15].

5.2.3 UE behaviour in state 5GMM-REGISTERED

5.2.3.1 General

The state 5GMM-REGISTERED is entered at the UE, when:

the initial registration procedure is performed by the UE (see subclause 5.5.1.2.2).

In state 5GMM-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 5GMM-REGISTERED

5.2.3.2.1 NORMAL-SERVICE

The UE:

a) shall initiate the mobility or the periodic registration update procedure (according to conditions given in subclause 5.5.1.3.2), except that the periodic registration update procedure shall not be initiated over non-3GPP access;

b) shall initiate the service request procedure (according to conditions given in subclause 5.6.1);

c) shall respond to paging; and

d) if configured for eCall only mode as specified in 3GPP TS 31.102 [22], shall perform the eCall inactivity procedure at expiry of timer T3444 or timer T3445 (see subclause 5.5.3).

NOTE 1: Paging is not supported over non-3GPP access.

NOTE 2: Timers T3444 and T3445 are specified in 3GPP TS 24.301 [15].

5.2.3.2.2 NON-ALLOWED-SERVICE

The UE shall behave as specified in subclause 5.3.5.

5.2.3.2.3 ATTEMPTING-REGISTRATION-UPDATE

The UE in 3GPP access:

a) shall not send any user data;

b) shall initiate a registration procedure for mobility and periodic registration update on the expiry of timers T3502, T3511 or T3346;

c) shall initiate a registration procedure for mobility and periodic registration update when entering a new PLMN, if timer T3346 is running and the new PLMN is not equivalent to the PLMN where the UE started timer T3346, the

PLMN identity of the new cell is not in the forbidden PLMN lists, and the tracking area is not in one of the lists of forbidden tracking areas;

d) shall initiate a registration procedure for mobility and periodic registration update when the tracking area of the serving cell has changed, if timer T3346 is not running, the PLMN identity of the new cell is not in one of the forbidden PLMN lists and the tracking area is not in one of the lists of forbidden tracking areas;

e) may initiate a registration procedure for mobility and periodic registration update upon request of the upper layers to establish a PDU session for emergency services;

f) may perform de-registration locally and initiate a registration procedure for initial registration for emergency services even if timer T3346 is running;

g) shall initiate registration procedure for mobility and periodic registration update upon reception of paging or NOTIFICATION message with access type indicating 3GPP access; and

h) if configured for eCall only mode as specified in 3GPP TS 31.102 [22], shall perform the eCall inactivity procedure at expiry of timer T3444 or timer T3445 (see subclause 5.5.3).

NOTE: Timers T3444 and T3445 are specified in 3GPP TS 24.301 [15].

The UE in non-3GPP access:

a) shall not send any user data; and

b) shall initiate the registration procedure for mobility and periodic registration update on the expiry of timers T3502, T3511 or T3346.

5.2.3.2.4 LIMITED-SERVICE

The UE:

a) shall perform cell selection/reselection;

b) may initiate registration for emergency services; and

c) if configured for eCall only mode as specified in 3GPP TS 31.102 [22], shall perform the eCall inactivity procedure at expiry of timer T3444 or timer T3445 (see subclause 5.5.3).

NOTE: Timers T3444 and T3445 are specified in 3GPP TS 24.301 [15].

5.2.3.2.5 PLMN-SEARCH

The UE shall perform PLMN selection. If a new PLMN is selected, the UE shall reset the registration attempt counter and initiate the initial registration procedure (see subclause 5.5.1.2).

If the selected cell is known not to be able to provide normal service, the UE may initiate registration for emergency services.

5.2.3.2.6 NO-CELL-AVAILABLE

The UE shall perform cell selection and choose an appropriate substate when a cell is found.

5.3 General on elementary 5GMM procedures

5.3.1 5GMM modes and N1 NAS signalling connection

5.3.1.1 Establishment of the N1 NAS signalling connection

When the UE is in 5GMM-IDLE mode over 3GPP access and needs to transmit an initial NAS message, the UE shall request the lower layer to establish an RRC connection. Upon indication from the lower layers that the RRC connection

has been established, the UE shall consider that the N1 NAS signalling connection over 3GPP access is established and enter 5GMM-CONNECTED mode over 3GPP access.

When the UE is in 5GMM-IDLE mode over non-3GPP access, and the UE receives an indication from the lower layers of access stratum connection establishment, the UE shall consider the N1 NAS signalling connection established enter 5GMM-CONNECTED mode over non-3GPP access and send an initial NAS message.

Initial NAS messages are:

a) REGISTRATION REQUEST message;

b) DEREGISTRATION REQUEST message; and

c) SERVICE REQUEST message.

If the UE is capable of both N1 mode and S1 mode and lower layers provide an indication that the current E-UTRA cell is connected to both EPC and 5GCN, for the routing of the REGISTRATION REQUEST message during the initial registration procedure to the appropriate core network (EPC or 5GCN), the UE NAS provides the lower layers with the selected core network type information.

For the routing of the initial NAS message to the appropriate AMF, if the UE holds a valid 5G-GUTI, the UE NAS provides the lower layers with either the 5G-S-TMSI or the registered GUAMI, or neither the 5G-S-TMSI nor registered GUAMI according to the following rules:

a) if the registration procedure for mobility and periodic update was triggered due to the update of the allowed NSSAI or the configured NSSAI included in the last CONFIGURATION UPDATE COMMAND message, the UE NAS shall not provide the lower layers with the 5G-S-TMSI or the registered GUAMI; or

b) otherwise:

   1) if the tracking area of the current cell is in the registration area, the UE NAS shall provide the lower layers with the 5G-S-TMSI, but shall not provide the registered GUAMI to the lower layers; or

   2) if the tracking area of the current cell is not in the registration area, the UE NAS shall provide the lower layers with the registered GUAMI, but shall not provide the lower layers with the 5G-S-TMSI.

If the UE does not hold a valid 5G-GUTI, the UE NAS does not provide the lower layers with the 5G-S-TMSI or the registered GUAMI.

The UE NAS also provides the lower layers with the identity of the selected PLMN (see 3GPP TS 38.331 [30]). In a shared network, the UE shall choose one of the PLMN identities as specified in 3GPP TS 23.122 [5].

5.3.1.2 Release of the N1 NAS signalling connection

The signalling procedure for the release of the N1 NAS signalling connection is initiated by the network.

In N1 mode, upon indication from lower layers that the access stratum connection has been released, the UE shall enter 5GMM-IDLE mode and consider the N1 NAS signalling connection released.

If the UE is configured for eCall only mode as specified in 3GPP TS 31.102 [22] then:

- if the N1 NAS signalling connection that was released had been established for eCall over IMS, the UE shall start timer T3444; and

- if the N1 NAS signalling connection that was released had been established for a call to an HPLMN designated non-emergency MSISDN or URI for test or terminal reconfiguration service, the UE shall start timer T3445.

NOTE: Timers T3444 and T3445 are specified in 3GPP TS 24.301 [15].

To allow the network to release the N1 NAS signalling connection, the UE:

a) shall start the timer T3540 if the UE receives any of the 5GMM cause values #11, #12, #13 (not applicable to the service request procedure);

b) shall start the timer T3540 if:

1) the UE receives a REGISTRATION ACCEPT message;

2) the UE has not set the "follow-on request pending" indication in the REGISTRATION REQUEST message;

3) the UE has not included the Uplink data status IE in the REGISTRATION REQUEST message;

4) the UE has not included the Allowed PDU session status IE in the REGISTRATION REQUEST message;

5) the registration for mobility and periodic registration update procedure has been initiated in 5GMM-IDLE mode; and

6) the user-plane resources for PDU sessions have not been set up;

c) shall start the timer T3540 if the UE receives a REGISTRATION REJECT message indicating:

the 5GMM cause value #9 or #10;

d) shall start the timer T3540 if the UE receives a SERVICE REJECT message indicating:

the 5GMM cause value #9 or #10; and

e) shall start the timer T3540 if:

1) the UE receives a CONFIGURATION UPDATE COMMAND message indicating registration requested with either new allowed NSSAI information or new configured NSSAI information or both included; and

2) the user-plane resources for PDU sessions have not been set up.

Upon expiry of T3540,

- in cases a) and b), the UE shall locally release the established NAS signalling connection;

- in cases c) and d) the UE shall locally release the established N1 NAS signalling connection and the UE shall initiate the registration procedure as described in subclause 5.5.1.2.2 or 5.5.1.3.2; or

- in case e), the UE shall locally release the established N1 NAS signalling connection and perform a new registration procedure as specified in subclause 5.5.1.3.2.

In case b),

- upon an indication from the lower layers that the user-plane resources for PDU sessions are set up, the UE shall stop timer T3540 and may send uplink signalling via the existing N1 NAS signalling connection or user data via user plane. If the uplink signalling is associated with emergency services fallback or establishing a PDU session for emergency services, the UE shall stop timer T3540 and send the uplink signalling via the existing NAS signalling connection; or

- upon receipt of a DEREGISTRATION REQUEST message, the UE shall stop timer T3540 and respond to the network-initiated de-registration request as specified in subclause 5.5.2.3.

In case c),

- upon an indication from the lower layers that the access stratum connection has been released, the UE shall stop timer T3540 and perform a new registration procedure as specified in subclause 5.5.1.2.2 or 5.5.1.2.3.

- upon receiving a request from upper layers to send NAS signalling associated with emergency services fallback or establishing a PDU session for emergency services, the UE shall stop timer T3540 and shall locally release the NAS signalling connection, before proceeding as specified in subclause 5.5.1.

In case d),

- upon an indication from the lower layers that the RRC connection has been released, the UE shall stop timer T3540 and perform a new registration procedure as specified in subclause 5.5.1.2.2 or 5.5.1.2.3.

- upon receiving a request from upper layers to send NAS signalling associated with emergency services fallback or establishing a PDU session for emergency services, the UE shall stop timer T3540 and shall locally release the NAS signalling connection, before proceeding as specified in subclause 5.5.1.

In case e),

- upon an indication from the lower layers that the RRC connection has been released, the UE shall stop timer T3540 and perform a new registration procedure as specified in subclause 5.5.1.3.2.

5.3.1.3 5GMM-CONNECTED mode with RRC inactive indication

This subclause is only applicable for UE's 5GMM mode over 3GPP access.

The UE is in 5GMM-CONNECTED mode with RRC inactive indication when the UE is in:

a) 5GMM-CONNECTED mode over 3GPP access at the NAS layer; and

b) RRC_INACTIVE state at the AS layer (see 3GPP TS 38.300 [27]).

Unless stated otherwise, the UE behavior in 5GMM-CONNECTED mode with RRC inactive indication follows the UE behavior in 5GMM-CONNECTED over 3GPP access, except that:

a) the UE shall apply the mobility restrictions; and

b) the UE shall perform the PLMN selection procedures

as in 5GMM-IDLE mode over 3GPP access.

The UE shall transition from 5GMM-CONNECTED mode over 3GPP access to 5GMM-CONNECTED mode with RRC inactive indication upon indication from the lower layers that the UE has transitioned to RRC_INACTIVE state.

Upon trigger of a procedure which requires sending of a NAS message, the UE in 5GMM-CONNECTED mode with RRC inactive indication over 3GPP access shall request the lower layers to transition to RRC_CONNECTED state (see 3GPP TS 38.300 [27]).

The UE shall transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-CONNECTED mode over 3GPP access upon receving from the lower layers indication that the UE has transitioned to RRC_CONNECTED state (see 3GPP TS 38.300 [27]).

NOTE: The AMF can be aware of the transition between 5GMM-CONNECTED mode and 5GMM-CONNECTED mode with RRC inactive indication for a UE (see 3GPP TS 23.502 [9]).

The UE shall trigger a transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-IDLE mode upon selection of a PLMN that is not an equivalent PLMN to the registered PLMN.

If the UE requests the lower layers to transition to RRC_CONNECTED state at initiation of a registration procedure, a service request procedure or a de-registration procedure, upon fallback indication from lower layers, the UE shall:

- enter 5GMM-IDLE mode; and

- proceed with the pending procedure.

If the UE requests the lower layers to transition to RRC_CONNECTED state for other reason than initiation of a registration procedure, a service request procedure or a de-registration procedure, upon fallback indication from lower layers, the UE shall:

- enter 5GMM-IDLE mode;

- initiate service request procedure; and

- upon successful service request procedure completion, proceed with any pending procedure.

The UE shall transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-IDLE mode over 3GPP access and initiate the registration procedure for mobility and periodic registration update (i.e. the 5GS registration type IE set to "mobility registration updating" in the REGISTRATION REQUEST message) for NAS signalling connection recovery as specified in subclause 5.5.1.3.2, upon receving from the lower layers:

a) indication that the transition from RRC_INACTIVE state to RRC_CONNECTED state has failed.

The UE shall transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-IDLE mode over 3GPP access upon receving from the lower layers:

a) indication of transition from RRC_INACTIVE to RRC_IDLE;

b) AMF paging indication; or

c) indication of cell selection to E-UTRAN or another RAT that the UE supports.

The UE shall not trigger a transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-IDLE mode upon entering a new PLMN which is in the list of equivalent PLMNs.

5.3.2 Permanent identifiers

A globally unique permanent identity, the 5G subscription permanent identifier (SUPI), is allocated to each subscriber for 5GS-based services. In the current release, the IMSI and the network access identifier (NAI) are valid SUPI types. Though non-IMSI based SUPIs are possible by using NAI, the IMSI can be contained within the NAI for the SUPI. The structure of the SUPI and its derivatives will be specified in 3GPP TS 23.003 [4].

A UE supporting NG-RAN includes a SUCI:

a) in the REGISTRATION REQUEST message when the UE is attempting initial registration procedure and a valid 5G-GUTI is not available; or

b) in the IDENTITY RESPONSE message, if the SUCI is requested by the network during the identification procedure.

The SUCI is a privacy preserving identifier containing the concealed SUPI.

NOTE: If the home network has not provisioned the public key needed to generate a SUCI, the UE uses "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI which equals to the SUPI.

Each UE supporting NG-RAN contains a permanent equipment identifier (PEI) for accessing 5GS-based services. In the current release, the IMEI and the IMEISV are the only PEI format supported by 5GS.The structure of the PEI and its formats will be specified in 3GPP TS 23.003 [4].

A UE supporting NG-RAN includes a PEI:

a) when neither SUPI nor valid 5G-GUTI is available to use for emergency services in the REGISTRATION REQUEST message with 5GS registration type IE set to "emergency registration"; and

b) when the network requests the PEI by using the identification procedure, in the IDENTIFICATION RESPONSE message.

The AMF can request the PEI at any time by using the identification procedure.

5.3.3 Temporary identities

A globally unique temporary user identity for 5GS-based services, the 5G globally unique temporary identity (5G-GUTI), is used for identification within the signalling procedures. The 5G-GUTI is common to both 3GPP and non-3GPP access. In the paging and service request procedures, a shortened form of the 5G-GUTI, the 5G S-temporary mobile subscriber identity (5G-S-TMSI), is used to enable more efficient radio signalling. The purpose of the 5G-GUTI and 5G-S-TMSI is to provide identity confidentiality, i.e., to protect a user from being identified and located by an intruder. The structure of the 5G-GUTI and its derivatives is specified in 3GPP TS 23.003 [4]. The 5G-GUTI has two main components:

a) the globally unique AMF id (GUAMI) that uniquely identifies the AMF that allocated the 5G-GUTI, and

b) the 5G-TMSI that provides for an unambiguous identity of the UE within this AMF.

The 5G-S-TMSI has three main components:

a) the AMF set ID that uniquely identifies the AMF set within the AMF region;

b) the AMF pointer that uniquely identifies the AMF within the AMF set; and

c) the 5G-TMSI.

A UE supporting N1 mode includes a valid 5G-GUTI, if any is available, in the REGISTRATION REQUEST and DEREGISTRATION REQUEST messages. In the SERVICE REQUEST message, the UE includes a valid 5G-S-TMSI as user identity. The AMF may assign a new 5G-GUTI for a particular UE at successful registration and generic UE configuration update procedures.

If a new 5G-GUTI is assigned by the AMF, the UE and the AMF handle the 5G-GUTI as follows:

a) Upon receipt of a 5GMM message containing a new 5G-GUTI the UE considers the new 5G-GUTI as valid and the old 5G-GUTI as invalid, stops timer T3519 if running, and deletes any stored SUCI. The new 5G-GUTI 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.

b) The AMF considers the old 5G-GUTI as invalid as soon as an acknowledgement for a registration or generic UE configuration update procedure is received.

5.3.4 Registration areas

Within the 5GS, the registration area is managed independently per access type, i.e., 3GPP access or non-3GPP access. The AMF assigns a registration area to the UE during the registration procedure. A registration area is defined as a set of tracking areas and each of these tracking areas consists of one or more cells that cover a geographical area. Tracking areas cannot overlap each other. Within the 5GS, the concept of "registration to multiple tracking areas" applies:

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

b) In order to reduce the tracking area update signalling within the 5GS, the AMF can assign several tracking areas to the UE. These tracking areas construct a list of tracking areas which is identified by a TAI list. When generating the TAI list, the AMF shall include only TAIs that are applicable on the access where the TAI list is sent. The AMF shall be able to allocate a TAI List over different NG-RAN access technologies.

c) The UE considers itself registered to a list of tracking areas and does not need to trigger the registration procedure for mobility and periodic registration update (i.e. the 5GS registration type IE set to "mobility registration updating" in the REGISTRATION REQUEST message) as long as the UE stays in one of the tracking areas of the list of tracking areas received from the AMF.

d) The UE will consider the TAI list as valid, until it receives a new TAI list in the next registration procedure for mobility and periodic registration update or generic UE configuration update procedure, or the UE is commanded by the network to delete the TAI list by a reject message or it is deregistered from the 5GS. If the registration request is accepted or the TAI list is reallocated by the AMF, the AMF shall provide at least one entry in the TAI list. If the new and the old TAI list are identical, the AMF does not need to provide the new TAI list to the UE during mobility registration update or periodic registration update.

e) The TAI list can be reallocated by the AMF.

f)- When the UE is deregistered from the 5GS, the TAI list in the UE is invalid.

g) The AMF allocates one 5G-GUTI, which is common between 3GPP access and non-3GPP access, to the UE.

h) The UE includes the last visited registered TAI, if available, to the AMF. The last visited registered TAI 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.

5.3.5 Service area restrictions

Service area restrictions are applicable only to 3GPP access.

The service area restrictions consist of either an allowed area, or a non-allowed area. The allowed area can contain up to 16 tracking areas or include all tracking areas in a PLMN. The non-allowed area can contain up to 16 tracking areas. The network conveys the service area restrictions to the UE by including either an allowed area, or a non-allowed area,

but not both, in the Service area list IE of a REGISTRATION ACCEPT message or a CONFIGURATION UPDATE COMMAND message.

If the network does not convey the service area restrictions to the UE in the Service area list IE of a REGISTRATION ACCEPT message, the UE shall treat all tracking areas in the registered PLMN and its equivalent PLMN(s) as allowed area and delete the stored list of "allowed tracking areas" or the stored list of "non-allowed tracking areas" for the registered PLMN and its equivalent PLMN(s).

When the UE receives a Service area list IE with an allowed area indication during a registration procedure or a generic UE configuration update procedure:

a) if the "Type of list" included in the Service area list IE does not indicate all TAIs belonging to the PLMN are allowed area, the UE shall delete the old list of "allowed tracking areas" and store the tracking areas in the allowed area as the list of "allowed tracking areas". If the UE has a stored list of "non-allowed tracking areas" for the registered PLMN, the UE shall delete that list; or

b) if the "Type of list" included in the Service area list IE indicates all TAIs belonging to the PLMN are allowed area, the UE shall treat all tracking areas in the registered PLMN are allowed area and delete the stored list of "allowed tracking areas" or the stored list of "non-allowed tracking areas" for the registered PLMN.

When the UE receives a Service area list IE with a non-allowed area indication during a registration procedure or a generic UE configuration update procedure, the UE shall delete the old list of "non-allowed tracking areas" and store the tracking areas in the non-allowed area as the list of "non-allowed tracking areas". If the UE has a stored list of "allowed tracking areas" for the registered PLMN, the UE shall delete that list.

If the UE has a stored list of "allowed tracking areas":

a) while camped on a cell whose TAI is in the list of "allowed tracking areas", the UE is allowed to initiate any 5GMM and 5GSM procedures; and

b) while camped on a cell whose TAI is not in the list of "allowed tracking areas":

   1) if the UE is in 5GMM-IDLE mode over 3GPP access, the UE:

      i) shall not perform the registration procedure for mobility and periodic registration update with Uplink data status IE except for emergency services; and

      ii) shall not initiate a service request procedure except for emergency services, high priority access or for responding to core network paging; and

   2) if the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication over 3GPP access, the UE:

      i) shall not perform the registration procedure for mobility and periodic registration update with Uplink data status IE except for emergency services;

      ii) shall not initiate a service request procedure except for emergency services or high priority access; and

      iii) shall not initiate a 5GSM procedure except for emergency services.

If the UE has a stored list of "non-allowed tracking areas":

a) while camped on a cell whose TAI is not in the list of "non-allowed tracking areas", the UE is allowed to initiate any 5GMM and 5GSM procedures; and

b) while camped on a cell whose TAI is in the list of "non-allowed tracking areas":

   1) if the UE is in 5GMM-IDLE mode over 3GPP access, the UE:

      i) shall not perform the registration procedure for mobility and periodic registration update with Uplink data status IE except for emergency services; and

      ii) shall not initiate a service request procedure except for emergency services, high priority access or for responding to core network paging; and

2) if the UE is in 5GMM-CONNECTED mode or 5GMM-CONNECTED mode with RRC inactive indication over 3GPP access, the UE:

   i) shall not perform the registration procedure for mobility and registration update with the Uplink data status IE except for emergency services;

   ii) shall not initiate a service request procedure except for emergency services or high priority access; and

   iii) shall not initiate a 5GSM procedure except for emergency services.

The list of "allowed tracking areas", as well as the list of "non-allowed tracking areas" shall be erased when:

a) the UE is switched off;

b) the UICC containing the USIM is removed; and

c) periodically (with a period in the range 12 to 24 hours).

When the list of "allowed tracking areas" or the list of "non-allowed tracking areas" is erased, the UE performs cell selection procedure.

The UE shall evaluate the information in the list of "5GS forbidden tracking areas for roaming" and in the list of "5GS forbidden tracking areas for regional provision of service" before evaluating the information in the list of "allowed tracking areas" or the list of "non-allowed tracking areas".

5.3.6 Mobile initiated connection only mode

The UE can request the use of mobile initiated connection only (MICO) mode during the registration procedure (see 3GPP TS 23.501 [8] and 3GPP TS 23.502 [9]). The UE shall not request use of MICO mode over non-3GPP access. Furthermore, the UE in 3GPP access shall not request the use of MICO mode during:

a) a registration procedure for initial registration for emergency services (see subclause 5.5.1.2);

b) a registration procedure for mobility and periodic registration update (see subclause 5.5.1.3) for initiating a PDU session for emergency services if the UE is in the state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE; or

c)- a registration procedure for mobility and periodic registration update (see subclause 5.5.1.3) when the UE has a PDU session for emergency services established.

If the UE requests the use of MICO mode, the network can accept the use of MICO mode by providing a MICO indication when accepting the registration procedure. The UE may use MICO mode only if the network has provided the MICO indication IE during the last registration procedure.

If the network accepts the use of MICO mode, the AMF may include an "all PLMN registration area allocated" indication in the MICO indication IE to the UE.

If the network accepts the use of MICO mode, the UE may deactivate the AS layer and activate MICO mode by entering the state 5GMM-REGISTERED.NO-CELL-AVAILABLE if:

a) the UE is in 5GMM-IDLE mode for 3GPP access; and

b) in the 5GMM-REGISTERED.NORMAL-SERVICE state for 3GPP access.

When MICO mode is activated all NAS timers are stopped and associated procedures aborted except for timers T3512, T3346, T3396, T35cd, T35ef, any back-off timers, and the timer T controlling the periodic search for HPLMN or EHPLMN or higher prioritized PLMNs (see 3GPP TS 23.122 [5]).

NOTE: When MICO mode is activated and if the UE is also registered over the non-3GPP access, the AMF will not send a NOTIFICATION message with access type indicating 3GPP access over the non-3GPP access for PDU sessions associated with 3GPP access.

The UE may deactivate MICO mode and activate the AS layer at any time. Upon deactivating MICO mode, the UE may initiate 5GMM procedures (e.g. for the transfer of mobile originated signalling or user data).

When a PDU session for emergency services is successfully established after the MICO mode was enabled, the UE the UE and the AMF shall locally disable MICO mode. The UE and the AMF shall not enable MICO mode until the AMF accepts the use of MICO mode in the next registration procedure. To enable an emergency call back, the UE should wait for a UE implementation-specific duration of time before requesting the use of MICO mode after the release of the emergency PDU session

If the AMF accepts the use of MICO mode, the AMF starts the implicit de-registration timer for 3GPP access when entering 5GMM-IDLE mode for 3GPP access.

Upon successful completion of an attach procedure or tracking area updating procedure after inter-system change from N1 mode to S1 mode (see 3GPP TS 24.301 [15]), the UE operating in single-registration mode shall locally disable MICO mode. After inter-system change from S1 mode to N1 mode, the UE operating in single-registration mode may re-negotiate MICO mode with the network during the registration procedure for mobility and periodic registration update.

5.3.7 Handling of the periodic registration update timer and mobile reachable timer

The periodic registration update procedure is used over 3GPP access to periodically notify the availability of the UE to the network. The procedure is controlled in the UE by the periodic registration update timer, T3512.

If the UE is registered over the 3GPP access, the AMF maintains an implicit de-registration timer to control when the UE is considered implicitly de-registered over the 3GPP access. If the UE is registered over the non-3GPP access, the AMF also maintains a non-3GPP implicit de-registration timer to control when the UE is considered implicitly de-registered over the non-3GPP access. The UE registered over the non-3GPP access maintains a non-3GPP de-registration timer to control when the UE is considered implicitly de-registered for the non-3GPP access.

The AMF shall start a non-3GPP implicit de-registration timer for the UE registered over non-3GPP access when the N1 NAS signalling connection over non-3GPP access is released.

The UE registered over non-3GPP access shall reset and start a non-3GPP de-registration timer when the N1 NAS signalling connection over non-3GPP access is released. The non-3GPP de-registration timer is stopped when the UE enters 5GMM-CONNECTED mode over non-3GPP access or the 5GMM-DEREGISTERED state over non-3GPP access.

The non-3GPP implicit de-registration timer shall be longer than the non-3GPP de-registration timer.

The value of timer T3512 is sent by the network to the UE in the REGISTRATION ACCEPT message. The UE shall apply this value in all tracking areas of the list of tracking areas assigned to the UE until a new value is received. The periodic registration update timer only applies to the UE registered to the 5GS services over 3GPP access.

If timer T3512 received by the UE in a REGISTRATION ACCEPT message contains an indication that the timer is deactivated or the timer value is zero, then timer T3512 is deactivated and the UE shall not perform the periodic registration update procedure.

NOTE: The UE does not perform the periodic registration update procedure for non-3GPP access.

Timer T3512 is reset and started with its initial value, when the UE changes from 5GMM-CONNECTED over 3GPP access to 5GMM-IDLE mode over 3GPP access. Timer T3512 is stopped when the UE enters 5GMM-CONNECTED mode over 3GPP access or the 5GMM-DEREGISTERED state over 3GPP access.

If the UE is registered for emergency services, and timer T3512 expires, the UE shall not initiate a periodic registration update procedure, but shall locally de-register from the network. When the UE is camping on a suitable cell, it may re-register to regain normal service.

When a UE is not registered for emergency services, and timer T3512 expires, the periodic registration update procedure shall be started.

If the UE is not registered for emergency services, and is in a state other than 5GMM-REGISTERED.NORMAL-SERVICE over 3GPP access when timer T3512 expires, the periodic registration update procedure is delayed until the UE returns to 5GMM-REGISTERED.NORMAL-SERVICE over 3GPP access.

The network supervises the periodic registration update procedure of the UE by means of the mobile reachable timer.

If the UE is not registered for emergency services, the mobile reachable timer shall be longer than T3512. In this case, by default, the mobile reachable timer is 4 minutes greater than timer T3512.

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 registered for emergency services, the AMF shall set the mobile reachable timer with a value equal to timer T3512. When the mobile reachable timer expires, the AMF shall locally de-register the UE.

The mobile reachable timer shall be reset and started with the value as indicated above, when the AMF 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 de-registration timer over 3GPP access. The value of the implicit de-registration timer over 3GPP access is network dependent. If MICO is activated, the default value of the implicit de-registration timer over 3GPP access is 4 minutes greater than timer T3512.

If the implicit de-registration timer expires before the UE contacts the network, the network shall implicitly de-register the UE. The implicit de-registration timer shall be stopped when a NAS signalling connection is established for the UE.

If the non-3GPP implicit de-registration timer expires before the UE contacts the network over the non-3GPP access, the network shall implicitly de-register the UE and enter the state 5GMM-DEREGISTERED over non-3GPP access for the UE. The non-3GPP implicit de-registration timer shall be stopped when a NAS signalling connection over non-3GPP access is established for the UE.

If the non-3GPP de-registration timer expires before the UE contacts the network over the non-3GPP access, the UE shall enter the state 5GMM-DEREGISTERED over non-3GPP access. The non-3GPP de-registration timer shall be stopped when a NAS signalling connection over non-3GPP access is established for the UE.

If the AMF provides T3346 value IE in the mobility management messages and T3346 value is greater than timer T3512, the AMF sets the mobile reachable timer and the implicit de-registration timer such that the sum of the timer values is greater than timer T3346 value.

5.3.8 Handling of timer T3502

The value of timer T3502 can be sent by the network to the UE in the REGISTRATION ACCEPT message. The UE shall apply this value in all tracking areas of the registration area assigned to the UE, until a new value is received.

The value of timer T3502 can be sent by the network to the UE in the REGISTRATION REJECT message during the initial registration. If a REGISTRATION REJECT message including timer T3502 value was received integrity protected, the UE shall apply this value until a new value is received with integrity protection or a new PLMN is selected. Otherwise, the default value of this timer is used.

The default value of this timer is also used by the UE in the following cases:

a) REGISTRATION ACCEPT message is received without a value specified;

b) the UE does not have a stored value for this timer; or

c) a new PLMN which is not in the list of equivalent PLMNs has been entered, the registration procedure fails, the registration attempt counter is equal to 5 and no REGISTRATION REJECT message was received from the new PLMN.

5.3.9 Handling of NAS level mobility management congestion control

The AMF may detect 5GMM signalling congestion and perform general NAS level congestion control. Under the 5GMM signalling congestion conditions the AMF may reject 5GMM signalling requests from UEs as specified in 3GPP TS 23.501 [8]. The AMF should not reject the following request:

a) requests for emergency services; and

b) requests from UEs configured for high priority access in selected PLMN.

When general NAS level congestion control is active, the AMF may include a value for the mobility management back-off timer T3346 in the reject messages. The UE starts the timer T3346 with the value received in the 5GMM reject messages. To avoid that large numbers of UEs simultaneously initiate deferred requests, the AMF should select the value for the timer T3346 for the rejected UEs so that timeouts are not synchronised.

If the timer T3346 is running when the UE enters state 5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then the timer T3346 is kept running until it expires or it is stopped.

If the UE is switched off when the timer T3346 is running, the UE shall behave as follows when the UE is switched on and the USIM in the UE remains the same:

> let t1 be the time remaining for T3346 timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

If the UE enters a new PLMN while timer T3346 is running, and the new PLMN is not equivalent to the PLMN where the UE started timer T3346, the UE shall stop timer T3346 when initiating 5GMM procedures in the new PLMN.

If timer T3346 is running or is deactivated, and the UE is a UE configured for high priority access in selected PLMN, or the UE wants to initiate signalling for emergency services or emergency services fallback, then the UE is allowed to initiate 5GMM procedures.

5.3.10 Handling of DNN based congestion control

The AMF may detect and start performing DNN based congestion control when one or more DNN congestion criteria as specified in 3GPP TS 23.501 [8] are met. The AMF may store a DNN congestion back-off timer on a per UE and congested DNN basis. If the UE does not provide a DNN for a non-emergency PDU session, then the AMF uses the selected DNN or the DNN associated with the PDU session corresponding to the 5GSM procedure.

When DNN based congestion control is activated at the AMF, the AMF performs the congestion control as specified in subclause 5.4.5 and the UE performs the congestion control as specified in subclause 5.4.5 and subclause 6.2.7.

5.3.11 Handling of S-NSSAI based congestion control

The AMF may detect and start performing S-NSSAI based congestion control when one or more S-NSSAI congestion criteria as specified in 3GPP TS 23.501 [8] are met. The AMF may store an S-NSSAI congestion back-off timer on a per UE, congested S-NSSAI, and optionally DNN basis. If the UE does not provide a DNN for a non-emergency PDU session, then the AMF uses the selected DNN or the DNN associated with the PDU session corresponding to the 5GSM procedure.

When S-NSSAI based congestion control is activated at the AMF, the AMF performs the congestion control as specified in subclause 5.4.5 and the UE performs the congestion control as specified in subclause 5.4.5 and subclause 6.2.8.

5.3.12 Handling of local emergency numbers

The network may send a Local emergency numbers list or an Extended local emergency numbers list or both, in the REGISTRATION UPDATE ACCEPT message, by including the Emergency number list IE and the Extended emergency number list IE, respectively.

The user equipment shall store the Local emergency numbers list and the Extended local emergency numbers list, as provided by the network. The Local emergency numbers list stored in the user equipment shall be replaced on each receipt of the Emergency number list IE. The Extended local emergency numbers list stored in the user equipment shall be replaced on each receipt of the Extended emergency number list IE.

The emergency number(s) received in the Emergency number list IE and the Extended emergency number list IE are valid only in networks in the same country as the cell on which this IE is received. If no Emergency number list IE or Extended emergency number list IE is contained in the REGISTRATION UPDATE ACCEPT message, then the stored Local emergency numbers list or Extended local emergency numbers list, respectively, in the user equipment shall be kept, except if the user equipment has successfully registered to a PLMN in a country different from that of the PLMN that sent the list.

Editor's note: It is FFS if the Extended local emergency numbers list is deleted if upon a registration update the PLMN provide only the Emergency number list IE.

The Local emergency numbers list and the Extended 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 entries in the Local emergency numbers list and up to twenty entries in the Extended local emergency numbers list, received from the network.

For the use of the Local emergency numbers list and the Extended local emergency numbers list by the UE see 3GPP TS 24.301 [15], subclause 5.3.7.

5.3.13 Lists of 5GS forbidden tracking areas

The UE shall store a list of "5GS forbidden tracking areas for roaming", as well as a list of "5GS forbidden tracking areas for regional provision of service". These lists shall be erased when

a) the UE is switched off or the UICC containing the USIM is removed; and

b) periodically (with a period in the range 12 to 24 hours).

When the lists are erased, the UE performs cell selection according to 3GPP TS 38.304 [28]. A tracking area shall be removed from the list of "5GS forbidden tracking areas for roaming", as well as the list of "5GS forbidden tracking areas for regional provision of service", if the UE receives the tracking area in Service area list of "allowed tracking areas" in REGISTRATION ACCEPT message or a CONFIGURATION UPDATE COMMAND message. The UE shall not remove the tracking area from "5GS forbidden tracking areas for roaming" or "5GS forbidden tracking areas for regional provision of service" if the UE is registered for emergency services.

In N1 mode, the UE shall update the suitable list whenever a REGISTRATION REJECT, SERVICE REJECT or DEREGISTRATION REQUEST message is received with the 5GMM cause #12 "tracking area not allowed" or #13 "roaming not allowed in this 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.

5.3.14 List of equivalent PLMNs

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 5GMM, EMM, GMM and MM (see 3GPP TS 24.301 [15] and 3GPP TS 24.008 [12]).

The UE shall update or delete this list at the end of each registration update 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, the UE 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 registered for emergency services enters the state 5GMM-DEREGISTERED. The UE shall delete the stored list if the USIM is removed or when the UE registered for emergency services enters the state 5GMM-DEREGISTERED. The maximum number of possible entries in the stored list is 16.

5.3.15 Transmission failure abnormal case in the UE

The abnormal case 5GMM uplink message transmission failure indication by lower layers can be identified for 5GMM procedures:

> When it is specified in the relevant procedure that it is up to the UE implementation to re-run the ongoing procedure that triggered that procedure, the procedure can typically be re-initiated using a retransmission mechanism of the uplink message (i.e. the one that has previously failed to be transmitted) with new sequence number and message authentication code information thus avoiding to re-start the whole procedure.

5.4 5GMM common procedures

5.4.1 Primary authentication and key agreement procedure

5.4.1.1 General

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures, as specified in 3GPP TS 33.501 [24].

Two methods are defined:

a) EAP based primary authentication and key agreement procedure.

b) 5G AKA based primary authentication and key agreement procedure.

The UE and the AMF shall support the EAP based primary authentication and key agreement procedure and the 5G AKA based primary authentication and key agreement procedure.

5.4.1.2 EAP based primary authentication and key agreement procedure

5.4.1.2.1 General

The purpose of the EAP based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on a key K_{AMF} (see 3GPP TS 33.501 [24]).

Extensible authentication protocol (EAP) as specified in IETF RFC 3748 [34] enables authentication using various EAP methods.

EAP defines four types of EAP messages:

a) an EAP-request message;

b) an EAP-response message;

c) an EAP-success message; and

d) an EAP-failure message.

Several rounds of exchanges of an EAP-request message and a related EAP-response message can be required to achieve the authentication (see example in figure 5.4.1.2.1.1).

The EAP based primary authentication and key agreement procedure is always initiated and controlled by the network.

The EAP-request message is transported from the network to the UE using the AUTHENTICATION REQUEST message of the EAP message reliable transport procedure.

The EAP-response message is transported from the UE to the network using the AUTHENTICATION RESPONSE message of the EAP message reliable transport procedure.

If the authentication of the UE completes successfully and the serving AMF intends to initiate a security mode control procedure after the EAP based primary authentication and key agreement procedure, then the EAP-success message is transported from the network to the UE using the SECURITY MODE COMMAND message of the security mode control procedure (see subclause 5.4.2).

If the authentication of the UE completes successfully and the serving AMF does not intend to initiate a security mode control procedure after the EAP based primary authentication and key agreement procedure, then the EAP-success message is transported from the network to the UE using the AUTHENTICATION RESULT message of the EAP result message transport procedure.

NOTE 1: The serving AMF will not initiate a security mode control procedure after the EAP based primary authentication and key agreement procedure e.g. in case of AMF relocation during registration procedure.

If the authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE using the AUTHENTICATION RESULT message of the EAP result message transport procedure or in a response of the initial 5GMM procedure as part of which the EAP based primary authentication and key agreement procedure is performed.

The AMF shall set the authenticator retransmission timer specified in IETF RFC 3748 [34] subclause 4.3 to infinite value.

NOTE 2: The EAP message reliable transport procedure provides a reliable transport of EAP messages and therefore retransmissions at the EAP layer do not occur.

The AUSF and the AMF support exchange of EAP messages using N12.

Editor's note: The ngKSI handling at EAP authentication is FFS.

Editor's note: establishment of 5GS security context is FFS.

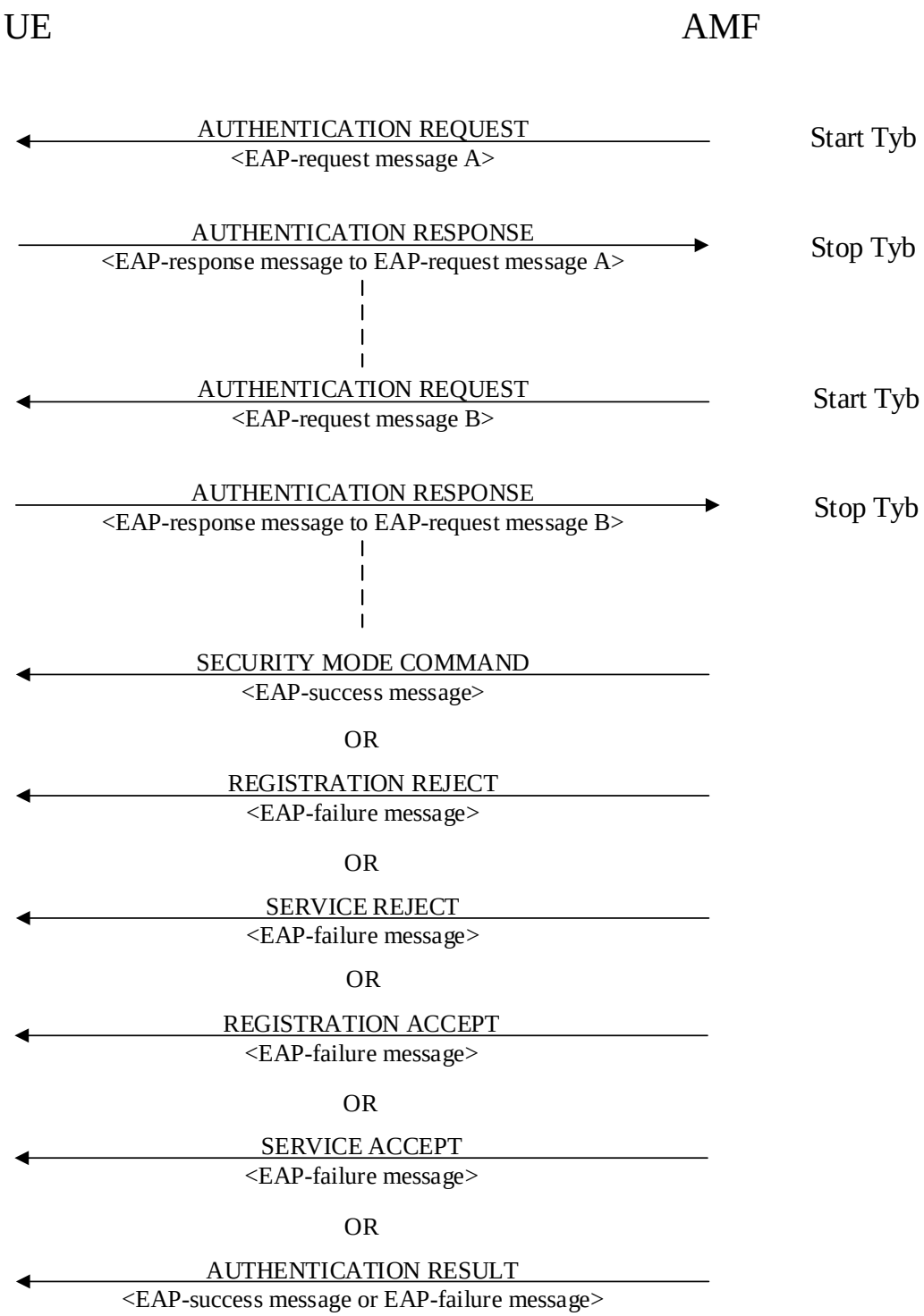


Figure 5.4.1.2.1.1: EAP based primary authentication and key agreement procedure

5.4.1.2.2 EAP-AKA' related procedures

5.4.1.2.2.1 General

The UE shall support acting as EAP-AKA' peer as specified in IETF RFC 5448 [40]. The AUSF may support acting as EAP-AKA' server as specified in IETF RFC 5448 [40].

The EAP-AKA' enables mutual authentication of the UE and the network.

The UE can reject the EAP-request/AKA'-challenge message sent by the network. The UE shall proceed with an EAP-request/AKA'-challenge message only if a USIM is present.

During a successful EAP based primary authentication and key agreement 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_{AMF}. K_{AMF} is stored in the 5GS security contexts (see 3GPP TS 33.501 [24]) of both the network and in the volatile memory of the ME while registered to the network, and is the root for the 5GS integrity protection and ciphering key hierarchy.

5.4.1.2.2.2 Initiation

In order to initiate the EAP based primary authentication and key agreement procedure using EAP-AKA', the AUSF shall send an EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [40]. The AUSF shall set the AT_KDF_INPUT attribute of the EAP-request/AKA'-challenge message to the SNN. The SNN is in format described in subclause 9.9.1. The AUSF may include AT_RESULT_IND attribute in the EAP-request/AKA'-challenge message.

Upon receiving an EAP-request/AKA'-challenge message, the UE shall check whether the UE has a USIM, shall check the key derivation function indicated in AT_KDF attributes as specified in IETF RFC 5448 [40], and if the value of the Key Derivation Function field within the received AT_KDF attribute, is of value 1, shall check:

a) whether the network name field of the AT_KDF_INPUT attribute is the SNN constructed according to subclause 9.9.1; and

b) whether the network name field of the AT_KDF_INPUT attribute matches the PLMN identity saved in the UE.

Editor's Note: It is FFS what the UE should do if the Key Derivation Funtion field is of a value not equal to 1.

The PLMN identity the UE uses for the above network name check is as follows:

a) when the UE moves from 5GMM-IDLE mode to 5GMM-CONNECTED mode, until the first handover, the UE shall use the PLMN identity of the selected PLMN; and

b) after handover or inter-system change to N1 mode in 5GMM-CONNECTED mode:

   1) 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;

   2) if the target cell is a shared network cell and the UE has a valid 5G-GUTI, the UE shall use the PLMN identity that is part of the 5G-GUTI; and

   3) if the target cell is a shared network cell and the UE has a valid 4G-GUTI and TAI, but not a valid 5G-GUTI, the UE shall use the PLMN identity that is part of the TAI.

Editor's Note: In the eventuality that RAN2 decides to use different TAI for 4G and for 5G, the above requirements will need to be revisited.

5.4.1.2.2.3 UE successfully authenticates network

If a USIM is present and the SNN check is successful, the UE shall handle the EAP-request/AKA'-challenge message specified in IETF RFC 5448 [40]. The USIM shall derive CK and IK and compute the authentication response (RES) using the 5G authentication challenge data received from the ME, and pass RES to the ME. The ME shall derive CK' and IK' from CK and IK. Furthermore, the ME shall generate K_{AUSF}, K_{SEAF}, K_{AMF} and MAC as described in 3GPP TS 33.501 [24] and shall send an EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [40].

If the EAP-request/AKA'-challenge message contains AT_RESULT_IND attribute, the UE may include AT_RESULT_IND attribute in the EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [40].

5.4.1.2.2.4 Errors when handling EAP-request/AKA'-challenge message

If a USIM is present, the SNN check fails or the UE does not accept AUTN during handling of the EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [40], the UE shall send an EAP-response/AKA'-authentication-reject message as specified in IETF RFC 5448 [40].

If a USIM is present, the SNN check is successful but the UE detects that the sequence number in AUTN is not correct during handling of the EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [40], the UE shall send an EAP-response/AKA'-synchronization-failure message as specified in IETF RFC 5448 [40].

If a USIM is present, the SNN check is successful, the sequence number in AUTN is correct and the UE detects another error during handling of the EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [40], the UE shall send an EAP-response/AKA'-client-error message as specified in IETF RFC 5448 [40].

If a USIM is not present, the UE shall send an EAP-response/AKA'-client-error message as specified in IETF RFC 5448 [37].

5.4.1.2.2.5 Network successfully authenticates UE

Upon reception of the EAP-response/AKA'-challenge message, if procedures for handling an EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [40] are successful, the AUSF may generate K_{AUSF} and shall generate K_{SEAF} as described in 3GPP TS 33.501 [24] and checks whether the AT_RESULT_IND attribute is included in the EAP-response/AKA'-challenge message and:

a) if the AT_RESULT_IND attribute is included in the EAP-response/AKA'-challenge message, the AUSF shall send an EAP-request/AKA'-notification message as specified in IETF RFC 5448 [40]; and

b) if the AT_RESULT_IND attribute is not included in the EAP-response/AKA'-challenge message, the AUSF shall send an EAP-success message as specified in IETF RFC 5448 [40] along with the K_{SEAF} and shall consider the procedure complete.

NOTE: SEAF generates K_{AMF} based on the received K_{SEAF} immediately following the primary authentication and key agreement procedure and provides K_{AMF} to AMF.

5.4.1.2.2.6 UE handling EAP-AKA' notification

Upon receiving an EAP-request/AKA'-notification message, the UE shall send an EAP-response/AKA'-notification message as specified in IETF RFC 5448 [37].

5.4.1.2.2.7 Network sending EAP-success message

Upon reception of the EAP-response/AKA'-notification message, if earlier procedures for handling an EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [40] were successful, the AUSF shall send an EAP-success message as specified in IETF RFC 5448 [40] along with the K_{SEA} and shall consider the procedure complete.

NOTE: SEAF generates K_{AMF} based on the received K_{SEAF} immediately following the primary authentication and key agreement procedure and provides K_{AMF} to AMF.

5.4.1.2.2.8 UE handling EAP-success message

Upon receiving an EAP-success message, the UE shall consider the procedure complete.

5.4.1.2.2.9 Network not successfully authenticates UE

Upon reception of the EAP-response/AKA'-challenge message, if procedures for handling an EAP-response/AKA'-challenge message as specified in IETF RFC 5448 [40] are not successful, the AUSF shall send an EAP-request/AKA'-notification message that implies failure as specified in IETF RFC 5448 [40].

5.4.1.2.2.10 Network sending EAP-failure message

Upon reception of the EAP-response/AKA'-notification message, if earlier procedures for handling an EAP-request/AKA'-challenge message as specified in IETF RFC 5448 [40] were not successful, the AUSF shall send an EAP-failure message as specified in IETF RFC 5448 [40] and shall consider the procedure complete.

5.4.1.2.2.11 UE handling EAP-success

Upon receiving an EAP-failure message, the UE shall consider the procedure complete.

5.4.1.2.3 EAP-TLS related procedures

5.4.1.2.3.1 General

The UE may support acting as EAP-TLS peer as specified in 3GPP TS 33.501 [24]. The AUSF may support acting as EAP-TLS server as specified in 3GPP TS 33.501 [24].

The EAP-TLS enables mutual authentication of the UE and the network.

When EAP-TLS is used, upon generation of EMSK, the UE shall generate K_{AUSF}, K_{SEAF}, and K_{AMF} as described in 3GPP TS 33.501 [24].

5.4.1.2.4 EAP message reliable transport procedure

5.4.1.2.4.1 General

The purpose of the EAP message reliable transport procedure is to provide a reliable transport of an EAP-request message from the network to the UE and of an EAP-response message from the UE to the network.

The EAP message reliable transport procedure is initiated by an AUTHENTICATION REQUEST message with the EAP message IE.

5.4.1.2.4.2 EAP message reliable transport procedure initiation by the network

In order to initiate the EAP message reliable transport procedure, the AMF shall create an AUTHENTICATION REQUEST message.

The AMF shall set the EAP message IE of the AUTHENTICATION REQUEST message to the EAP-request message to be sent to the UE.

The AMF shall send the AUTHENTICATION REQUEST message to the UE, and the AMF shall start timer T3560 (see example in figure 5.4.1.2.4.2.1).

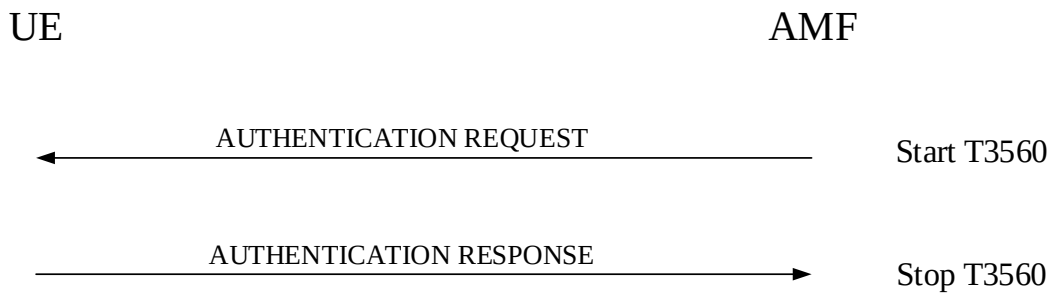


Figure 5.4.1.2.4.2.1: EAP message reliable transport procedure

Upon receipt of an AUTHENTICATION REQUEST message with the EAP message IE, the UE handles the EAP message received in the EAP message IE of the AUTHENTICATION REQUEST message.

5.4.1.2.4.3 EAP message reliable transport procedure accepted by the UE

The UE shall create an AUTHENTICATION RESPONSE message.

If the received EAP message is an EAP-request message, the UE shall set the EAP message IE of the AUTHENTICATION RESPONSE message to the EAP-response message responding to the received EAP-request message.

The UE shall send the AUTHENTICATION RESPONSE message to the AMF.

Upon receipt of an AUTHENTICATION RESPONSE message, the AMF shall stop timer T3560. If the EAP message IE is included in the AUTHENTICATION RESPONSE message, the AMF handles the EAP message received in the EAP message IE of the AUTHENTICATION RESPONSE message.

5.4.1.2.4.4 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3560.

   The AMF shall, on the first expiry of the timer T3560, retransmit the AUTHENTICATION REQUEST message and shall reset and start timer T3560. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3560, the AMF shall abort the EAP based primary authentication and key agreement procedure and any ongoing 5GMM specific procedure, and release the N1 NAS signalling connection.

5.4.1.2.4.5 Abnormal cases in the UE

Editor's note: Abnormal cases are FFS

5.4.1.2.5 EAP result message transport procedure

5.4.1.2.5.1 General

The purpose of the EAP result message transport procedure is to provide an EAP-success message or an EAP-failure message from the network to the UE, when the EAP message cannot be piggybacked by another NAS message.

The EAP result message transport procedure is initiated by an AUTHENTICATION RESULT message with the EAP message IE.

5.4.1.2.5.2 EAP result message transport procedure initiation by the network

In order to initiate the EAP result message transport procedure, the AMF shall create an AUTHENTICATION RESULT message.

The AMF shall set the EAP message IE of the AUTHENTICATION RESULT message to an EAP-success message or an EAP-failure message to be sent to the UE.

The AMF shall send the AUTHENTICATION RESULT message to the UE (see example in figure 5.4.1.2.5.2.1).

Figure 5.4.1.2.5.2.1: EAP result message transport procedure

Upon receipt of an AUTHENTICATION RESULT message with the EAP message IE, the UE handles the EAP message received in the EAP message IE of the AUTHENTICATION RESULT message.

5.4.1.3 5G AKA based primary authentication and key agreement procedure

5.4.1.3.1 General

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on a key K_{AMF} (see 3GPP TS 33.501 [24]). The cases when the 5G AKA based primary authentication and key agreement procedure is used are defined in 3GPP TS 33.501 [24].

The 5G AKA based primary authentication and key agreement procedure is always initiated and controlled by the network. However, the UE can reject the 5G authentication challenge sent by the network.

The UE shall proceed with a 5G authentication challenge only if a USIM is present.

A partial native 5G NAS security context is established in the UE and the network when a 5G authentication is successfully performed. During a successful 5G AKA based primary authentication and key agreement 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_{AMF}. K_{AMF} is stored in the 5G NAS security contexts (see 3GPP TS 33.501 [24]) of both the network and in the volatile memory of the ME while registered to the network, and is the root for the 5GS integrity protection and ciphering key hierarchy.

The 5G AKA based primary authentication and key agreement procedure is initiated by an AUTHENTICATION REQUEST message without the EAP message IE.

5.4.1.3.2 Authentication initiation by the network

The network may initiate a 5G AKA based primary authentication and key agreement procedure for a UE in 5GMM-CONNECTED mode at any time. For restrictions applicable after handover or inter-system change to N1 mode in 5GMM-CONNECTED mode, see subclause 5.4.1.2.3.

The network initiates the 5G AKA based primary authentication and key agreement procedure by sending an AUTHENTICATION REQUEST message to the UE and starting the timer T3560 (see example in figure 5.4.1.3.2.1). The AUTHENTICATION REQUEST message contains the parameters necessary to calculate the authentication response (see 3GPP TS 33.501 [24]).

If an ngKSI is contained in an initial NAS message during a 5GMM procedure, the network shall include a different ngKSI value in the AUTHENTICATION REQUEST message when it initiates a 5G AKA based primary authentication and key agreement procedure.

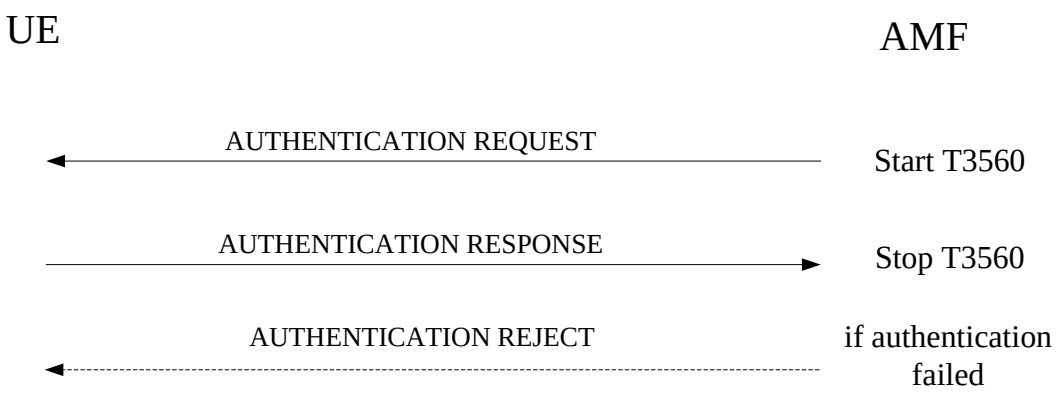


Figure 5.4.1.3.2.1: 5G AKA based primary authentication and key agreement procedure

5.4.1.3.3 Authentication response by the UE

The UE shall respond to an AUTHENTICATION REQUEST message. With the exception of the cases described in subclause 5.4.1.3.5, the UE shall process the 5G authentication challenge data and respond with an AUTHENTICATION RESPONSE message to the network.

Upon a successful 5G authentication challenge, the UE shall determine the PLMN identity to be used for the calculation of the new K_{AMF} from the 5G authentication challenge data according to the following rules:

a) When the UE moves from 5GMM-IDLE mode to 5GMM-CONNECTED mode, until the first handover, the UE shall use the PLMN identity of the selected PLMN; and

b) After handover or inter-system change to N1 mode in 5GMM-CONNECTED mode,

   1) 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;

   2) if the target cell is a shared network cell and the UE has a valid 5G-GUTI, the UE shall use the PLMN identity that is part of the 5G-GUTI; and

   3) if the target cell is a shared network cell and the UE has a valid 4G-GUTI and TAI, but not a valid 5G-GUTI, the UE shall use the PLMN identity that is part of the TAI.

Editor's note: Security context coordination between EPS and 5GS is FFS.

Upon a successful 5G authentication challenge, the new K_{AMF} calculated from the 5G authentication challenge data shall be stored in a new 5G NAS security context in the volatile memory of the ME.

The USIM will compute the authentication response (RES) using the 5G authentication challenge data received from the ME, and pass RES to the ME. From the RES, RES* is then generated according to Annex A of 3GPP TS 33.501 [24].

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*, 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 T3516.

The RAND and RES* values stored in the ME shall be deleted and timer T3516, if running, shall be stopped:

a) upon receipt of a

   1) SECURITY MODE COMMAND message,

2) SERVICE REJECT message,

3) REGISTRATION REJECT message,

4) REGISTRATION ACCEPT message, or

5) AUTHENTICATION REJECT message;

b) upon expiry of timer T3516;

1) if the UE enters the 5GMM state 5GMM-DEREGISTERED or 5GMM-NULL; or

2) if the UE enters 5GMM-IDLE mode.

5.4.1.3.4 Authentication completion by the network

Upon receipt of an AUTHENTICATION RESPONSE message, the network stops the timer T3560 and checks the correctness of RES* (see 3GPP TS 33.501 [24]).

If the 5G AKA based primary authentication and key agreement procedure has been completed successfully and the related ngKSI is stored in the 5G NAS security context of the network, the network shall include a different ngKSI value in the AUTHENTICATION REQUEST message when it initiates a new 5G AKA based primary authentication and key agreement procedure.

Upon receipt of an AUTHENTICATION FAILURE message, the network stops the timer T3560. In the case where the 5GMM cause #21 "synch failure" is received, the core network may renegotiate with the UDM/AUSF and provide the UE with new authentication parameters.

5.4.1.3.5 Authentication not accepted by the network

Editor's note: Authentication not accepted for normal services by the network is FFS.

Depending on local requirements or operator preference for emergency services, if the UE initiates a registration procedure with 5GS registration type IE set to "emergency registration" and the AMF is configured to allow emergency registration without user identity, the AMF needs not follow the procedures specified for the authentication failure in the present subclause. The AMF may continue a current 5GMM specific procedure.

5.4.1.3.6 Authentication not accepted by the UE

In the 5G authentication challenge, the UE shall check the 5G authentication challenge data (RAND, AUTN and ngKSI) received in the AUTHENTICATION REQUEST message to verify authenticity of the 5G core network.

The ME shall check that ngKSI received in the AUTHENTICATION REQUEST message is not already in use. The ME shall forward the RAND and AUTN to the USIM to check.

The UE may reject the core network due to an incorrect, AUTN or ngKSI parameter. If the UE has to reject the 5G authentication challenge, the UE shall return AUTHENTICATION FAILURE message to the network with a cause value indicating the reason for the failure (see 3GPP TS 33.501 [24]).

Incorrect 5G authentication challenge data contains four 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 5GMM cause #20 "MAC failure". The UE shall then follow the procedure described in subclause 5.4.1.3.7, item c.

b) Non-5G authentication unacceptable:

If the UE finds that the "separation bit" in the AMF field of AUTN supplied by the core network is set to 0, the UE shall send an AUTHENTICATION FAILURE message to the network, with the 5GMM cause #26 "non-5G authentication unacceptable" (see subclause 6.1.3 in 3GPP TS 33.501 [24]). The UE shall then follow the procedure described in subclause 5.4.1.3.7, item d.

c) ngKSI already in use:

If the UE detects that ngKSI received in the AUTHENTICATION REQUEST message is already in use in the UE shall send an AUTHENTICATION FAILURE message to the network, with the 5GMM cause #29 "ngKSI already in use". The UE shall then follow the procedure described in subclause 5.4.1.3.7, item e.

d) SQN failure:

If the UE finds the sequence number 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 5GMM cause #21 "synch failure" and a re-synchronization token AUTS provided by the USIM (see 3GPP TS 33.102 [23]). The UE shall then follow the procedure described in subclause 5.4.1.3.7, item f.

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 T3516, if running.

If the UE has a PDU session for emergency services established or is establishing such a PDU session, additional UE requirements are specified in subclause 5.4.1.3.7, under "for items c, d, e and f".

5.4.1.3.7 Abnormal cases

a) Lower layer failure.

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

b) Expiry of timer T3560.

The network shall, on the first expiry of the timer T3560, retransmit the AUTHENTICATION REQUEST message and shall reset and start timer T3560. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3560, the network shall abort the 5G AKA based primary authentication and key agreement procedure and any ongoing 5GMM specific procedure and release the N1 NAS signalling connection.

c) Authentication failure (5GMM cause #20 "MAC failure").

The UE shall send an AUTHENTICATION FAILURE message, with 5GMM cause #20 "MAC failure" according to subclause 5.4.1.3.6, to the network and start timer T3520 (see example in figure 5.4.1.3.7.1). Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3510, T3517 or T3521). Upon the first receipt of an AUTHENTICATION FAILURE message from the UE with 5GMM cause #20 "MAC failure", the network may initiate the identification procedure described in subclause 5.4.3. This is to allow the network to obtain the SUCI from the UE. The network may then check that the 5G-GUTI originally used in the 5G authentication challenge corresponded to the correct SUPI. Upon receipt of the IDENTITY REQUEST message from the network, the UE shall proceed as specified in subclause 5.4.3.3.

NOTE 1: Upon receipt of an AUTHENTICATION FAILURE message from the UE with 5GMM cause #20 "MAC failure", the network may also terminate the 5G AKA based primary authentication and key agreement procedure (see subclause 5.4.1.3.5).

If the mapping of 5G-GUTI to SUPI 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 T3520, if running, and then process the 5G challenge information as normal. If the mapping of 5G-GUTI to SUPI in the network was correct, the network should terminate the 5G AKA based primary authentication and key agreement procedure by sending an AUTHENTICATION REJECT message (see subclause 5.4.1.3.5).

If the network is validated successfully (an AUTHENTICATION REQUEST message 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. T3510, T3517 or T3521) if they were running and stopped when the UE received the first failed AUTHENTICATION REQUEST message.

If the UE receives the second AUTHENTICATION REQUEST message while T3520 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 f.

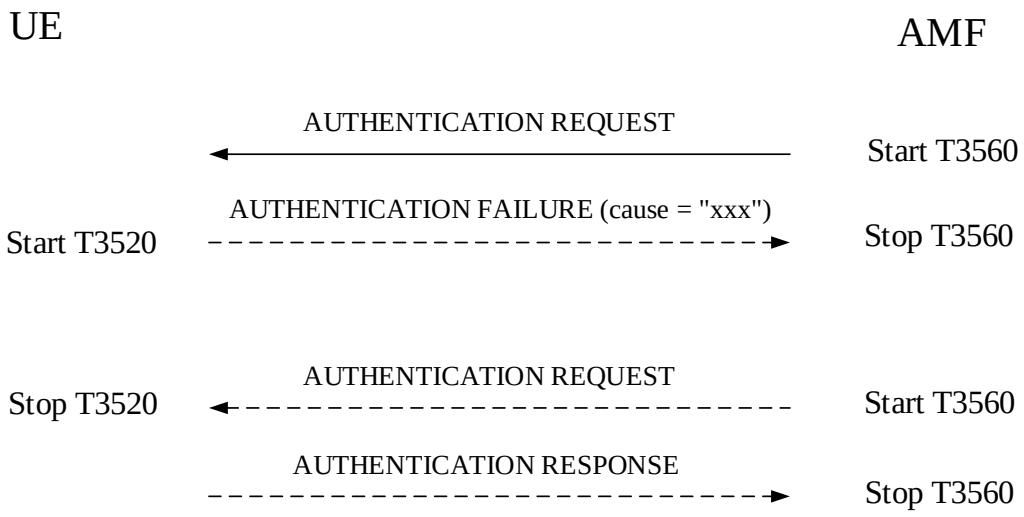


Figure 5.4.1.3.7.1: Authentication failure during 5G AKA based primary authentication and key agreement procedure

d) Authentication failure (5GMM cause #26 "non-5G authentication unacceptable").

The UE shall send an AUTHENTICATION FAILURE message, with 5GMM cause #26 "non-5G authentication unacceptable", to the network and start the timer T3520 (see example in figure 5.4.1.3.7.1). Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3510, T3517 or T3521). Upon the first receipt of an AUTHENTICATION FAILURE message from the UE with 5GMM cause #26 "non-5G authentication unacceptable", the network may initiate the identification procedure described in subclause 5.4.3. This is to allow the network to obtain the SUCI from the UE. The network may then check that the 5G-GUTI originally used in the 5G authentication challenge corresponded to the correct SUPI. Upon receipt of the IDENTITY REQUEST message from the network, the UE shall proceed as specified in subclause 5.4.3.3.

NOTE 2: Upon receipt of an AUTHENTICATION FAILURE message from the UE with 5GMM cause #26 "non-5G authentication unacceptable", the network may also terminate the 5G AKA based primary authentication and key agreement procedure (see subclause 5.4.1.3.5).

If the mapping of 5G-GUTI to SUPI 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 T3520, if running, and then process the 5G challenge information as normal. If the mapping of 5G-GUTI to SUPI in the network was correct, the network should terminate the 5G AKA based primary authentication and key agreement authentication procedure by sending an AUTHENTICATION REJECT message (see subclause 5.4.1.3.5).

e) Authentication failure (5GMM cause #29 "ngKSI already in use").

The UE shall send an AUTHENTICATION FAILURE message, with 5GMM cause #29 "ngKSI already in use", to the network and start the timer T3520 (see example in figure 5.4.1.3.7.1). Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3510, T3517 or T3521). Upon the first receipt of an AUTHENTICATION FAILURE message from the UE with 5GMM cause #29 "ngKSI already in use", the network performs necessary actions to select a new ngKSI and send the same 5G authentication challenge to the UE.

NOTE 3: Upon receipt of an AUTHENTICATION FAILURE message from the UE with 5GMM cause #29 "ngKSI already in use", the network may also re-initiate the 5G AKA based primary authentication and key agreement procedure (see subclause 5.4.1.3.2).

Upon receiving the new AUTHENTICATION REQUEST message from the network, the UE shall stop the timer T3520, if running, and then process the 5G challenge information as normal.

f) Authentication failure (5GMM cause #21 "synch failure").

The UE shall send an AUTHENTICATION FAILURE message, with 5GMM cause #21 "synch failure", to the network and start the timer T3520 (see example in figure 5.4.1.3.7.1). Furthermore, the UE shall stop any of the retransmission timers that are running (e.g. T3510, T3517 or T3521). Upon the first receipt of an AUTHENTICATION FAILURE message from the UE with the 5GMM 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 AMF to delete all unused authentication vectors for that SUPI and obtain new vectors from the UDM/AUSF. When re-synchronisation is complete, the network shall initiate the 5G AKA based primary authentication and key agreement procedure. Upon receipt of the AUTHENTICATION REQUEST message, the UE shall stop the timer T3520, if running.

NOTE 4: Upon receipt of two consecutive AUTHENTICATION FAILURE messages from the UE with 5GMM cause #21 "synch failure", the network may terminate the 5G AKA based primary authentication and key agreement procedure by sending an AUTHENTICATION REJECT message.

If the network is validated successfully (a new AUTHENTICATION REQUEST message is received which contains a valid SQN and MAC) while T3520 is running, the UE shall send the AUTHENTICATION RESPONSE message to the network and shall start any retransmission timers (e.g. T3510, T3517 or T3521), if they were running and stopped when the UE received the first failed AUTHENTICATION REQUEST message.

Upon receipt of an AUTHENTICATION REJECT message, the UE shall perform the actions as specified in subclause 5.4.1.3.5.

g) 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 38.304 [28]). The UE shall start any retransmission timers (e.g. T3510, T3517 or T3521), if they were running and stopped when the UE received the first AUTHENTICATION REQUEST message containing an invalid MAC or SQN or if the new ngKSI was already in use.

Editor's note: It is FFS if the RRC will provide the barring service.

h) Transmission failure of AUTHENTICATION RESPONSE message or AUTHENTICATION FAILURE message indication from lower layers (if the 5G AKA based primary authentication and key agreement procedure is triggered by a registration procedure for mobility and periodic registration update).

The UE shall stop the timer T3520, if running, and re-initiate the registration procedure for mobility and periodic registration update.

i) Transmission failure of AUTHENTICATION RESPONSE message or AUTHENTICATION FAILURE message indication with TAI change from lower layers (if the 5G AKA based primary authentication and key agreement procedure is triggered by a service request procedure).

The UE shall stop the timer T3520, if running.

If the current TAI is not in the TAI list, the 5G AKA based primary authentication and key agreement procedure shall be aborted and a registration procedure for mobility and periodic registration update 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 5G AKA based primary authentication and key agreement procedure.

j) 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).

The UE shall stop the timer T3520, if running. It is up to the UE implementation how to re-run the ongoing procedure that triggered the 5G AKA based primary authentication and key agreement procedure.

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

If the AUTHENTICATION REQUEST message could not be delivered due to an intra AMF handover and the target TA is included in the TAI list, then upon successful completion of the intra AMF handover the AMF shall retransmit the AUTHENTICATION REQUEST message. If a failure of handover procedure is reported by the lower layer and the N1 NAS signalling connection exists, the AMF shall retransmit the AUTHENTICATION REQUEST message.

For items c, d, e, and f whether or not the UE is registered for emergency services:

The UE shall stop timer T3520, if the timer is running and the UE enters 5GMM-IDLE mode, e.g. upon detection of a lower layer failure, release of the N1 NAS signalling connection, or as the result of an inter-system changer in 5GMM-CONNECTED mode from N1 mode to S1 mode.

The UE shall deem that the network has failed the authentication check or assume that the authentication is not genuine and proceed as described in item g above if any of the following occurs:

- the timer T3520 expires;
- the UE detects any combination of the 5G authentication failures: 5GMM causes #20 "MAC failure", #21 "synch failure", #26 "non-5G authentication unacceptable" or #29 “ngKSI already in use”, during three consecutive authentication challenges. The 5G authentication challenges shall be considered as consecutive only, if the 5G authentication challenges causing the second and third 5G authentication failure are received by the UE, while the timer T3520 started after the previous 5G authentication failure is running.

For items c, d, e, and f:

Depending on local requirements or operator preference for emergency services, if the UE has a PDU session for emergency services established or is establishing a PDU session for emergency services, the AMF need not follow the procedures specified for the authentication failure specified in the present subclause. The AMF may respond to the AUTHENTICATION FAILURE message by initiating the security mode control procedure selecting the "null integrity protection algorithm" 5G-IA0, null ciphering algorithm 5G-EA0 or may abort the 5G AKA based primary authentication and key agreement procedure and continue using the current security context, if any. The AMF shall release all non-emergency PDU sessions, if any, by initiating a PDU session release procedure. If there is an ongoing PDU session establishment procedure, the AMF shall release all non-emergency PDU sessions upon completion of the PDU session establishment procedure. The network shall consider the UE to be registered for emergency services.

If a UE has a PDU session for emergency services established or is establishing a PDU session for emergency services and sends an AUTHENTICATION FAILURE message to the AMF with the 5GMM cause appropriate for these cases (#20, #21, #26, or #29 respectively) and receives the SECURITY MODE COMMAND message before the timeout of timer T3520, the UE shall deem that the network has passed the authentication check successfully, stop timer T3520, respectively, and execute the security mode control procedure.

If a UE has a PDU session for emergency services established or is establishing a PDU session for emergency services when timer T3520 expires, the UE shall not deem that the network has failed the authentication check and not behave as described in item g. Instead the UE shall continue using the current security context, if any, release all non-emergency PDU sessions, if any, by initiating UE-requested PDU session release procedure. If there is an ongoing PDU session establishment procedure, the UE shall release all non-emergency PDU sessions upon completion of the PDU session establishment procedure. The UE shall start any retransmission timers (e.g. T3510, T3517 or T3521) if:

- they were running and stopped when the UE received the AUTHENTICATION REQUEST message and detected an authentication failure;
- the procedures associated with these timers have not yet been completed.

The UE shall consider itself to be registered for emergency services.

5.4.2 Security mode control procedure

5.4.2.1 General

The purpose of the NAS security mode control procedure is to take a 5G NAS security context into use, and initialise and start NAS signalling security between the UE and the AMF with the corresponding 5G NAS keys and 5G NAS security algorithms.

Furthermore, the network may also initiate the security mode control procedure in the following cases:

a)- in order to change the 5G NAS security algorithms for a current 5G NAS security context already in use; and

b) in order to change the value of uplink NAS COUNT used in the latest SECURITY MODE COMPLETE message as described in 3GPP TS 33.501 [24], subclause 6.9.4.4.

For restrictions concerning the concurrent running of a security mode control procedure with other security related procedures in the AS or inside the core network see 3GPP TS 33.501 [24], subclause 6.9.5.

5.4.2.2 NAS security mode control initiation by the network

The AMF initiates the NAS security mode control procedure by sending a SECURITY MODE COMMAND message to the UE and starting timer T3560 (see example in figure 5.4.2.2).

The AMF 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:

a) to take into use the security context created after a successful execution of the 5G AKA based primary authentication and key agreement procedure or the EAP based primary authentication and key agreement procedure; or

b) upon receipt of REGISTRATION REQUEST message, if the AMF wants to create a mapped 5G NAS 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 AMF shall send the SECURITY MODE COMMAND message unciphered, but shall integrity protect the message with the 5G NAS integrity key based on K_{AMF} or mapped K'_{AMF} indicated by the ngKSI included in the message. The AMF shall set the security header type of the message to "integrity protected with new 5G NAS security context".

Editor's note: Handling at emergency registration and emergency PDU sessions is FFS.

Upon receipt of a REGISTRATION REQUEST message, if the AMF does not have the valid current 5G NAS security context indicated by the UE, the AMF shall indicate the use of the new mapped 5G NAS 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.

Editor's note: Handling at non-existing 5G NAS security context indicated by the UE when an emergency PDU session exists is FFS.

While having a current mapped 5G NAS security context with the UE, if the AMF wants to take the native 5G NAS security context into use, the AMF shall include the ngKSI that indicates the native 5G NAS security context in the SECURITY MODE COMMAND message.

The AMF 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 and RRC integrity, and other possible target network security capabilities, i.e. E-UTRAN if the UE included them in the message to network) and if the UE included it in the message to the network, the selected 5GS ciphering and integrity algorithms and the ngKSI.

If the UE is connected to the same AMF and the same PLMN through both 3GPP access and non 3GPP access, then after the UE performs the authentication procedure over:

a) the 3GPP access, the AMF may include the ngKSI in the SECURITY MODE COMMAND message identifying the 5GS NAS security context currently used over the non-3GPP access; and

b) the non 3GPP access, the AMF may include the ngKSI in the SECURITY MODE COMMAND message identifying the 5GS NAS security context currently used over the 3GPP access.

The AMF may initiate a SECURITY MODE COMMAND in order to change the 5G security algorithms for a current 5G NAS security context already in use. The AMF re-derives the 5G NAS keys from K_{AMF} with the new 5G algorithm identities as input and provides the new 5GS algorithm identities within the SECURITY MODE COMMAND message. The AMF shall set the security header type of the message to "integrity protected with new 5G NAS security context".

If, during an ongoing registration procedure, the AMF is initiating a SECURITY MODE COMMAND (i.e. after receiving the REGISTRATION REQUEST message, but before sending a response to that message) and the REGISTRATION REQUEST message does not successfully pass the integrity check at the AMF, the AMF shall calculate the $HASH_{AMF}$ of the entire plain REGISTRATION REQUEST message as described in 3GPP TS 33.501 [24] and shall include the $HASH_{AMF}$ in the SECURITY MODE COMMAND message.

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

If the AMF does not support interworking procedures without N26 interface and the UE set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message, the AMF shall select ciphering and integrity algorithms to be used in the EPS and indicate them to the UE via the Selected EPS NAS security algorithms IE in the SECURITY MODE COMMAND message.

NOTE 2: The AS and NAS security capabilities will be the same, i.e. if the UE supports one algorithm for NAS, the same algorithm is also supported for AS.

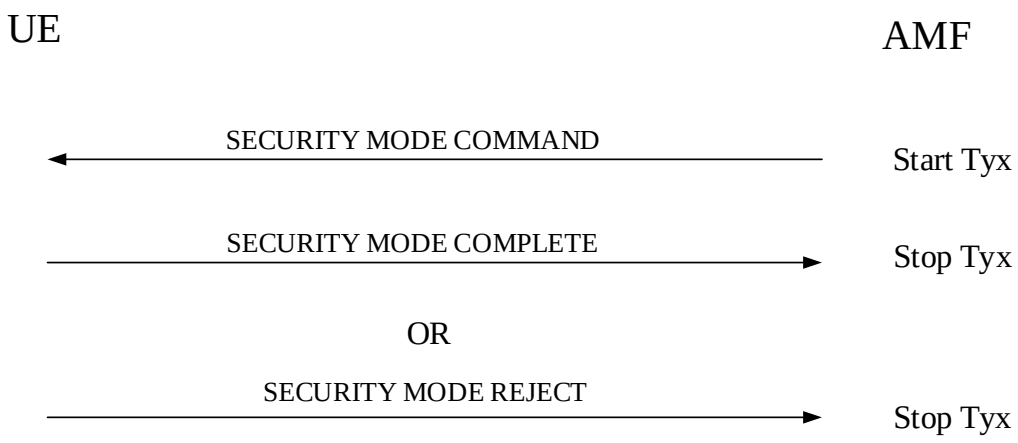


Figure 5.4.2.2: Security mode control procedure

5.4.2.3 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 have not been altered compared to the latest values that the UE sent to the network.

Editor's note: Handling at emergency PDU sessions is FFS.

Editor's note: Handling of "null algorithms" is FFS.

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 5G NAS security context held in the UE while the UE has a mapped 5G NAS security context as the current 5G NAS security context, the UE shall take the non-current native 5G NAS security context into use which then becomes the current native 5G NAS security context and delete the mapped 5G NAS security context.

If the SECURITY MODE COMMAND message can be accepted, the UE shall take the 5G NAS security context indicated in the message into use. The UE shall in addition reset the uplink NAS COUNT counter if:

a) the SECURITY MODE COMMAND message is received in order to take a 5G NAS security context into use created after a successful execution of the 5G AKA based primary authentication and key agreement procedure or the EAP based primary authentication and key agreement procedure; or

b) 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 ngKSI does not match the current 5G NAS security context, if it is a mapped 5G NAS security context.

If the SECURITY MODE COMMAND message can be accepted and a new 5G NAS security context is taken into use and SECURITY MODE COMMAND message does not indicate the "null integrity protection algorithm"5G-IA0 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 to 0, then the UE shall set the downlink NAS COUNT of this new 5G NAS security context to 0;

- otherwise the UE shall set the downlink NAS COUNT of this new 5G NAS 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 5GS integrity algorithm and the 5G NAS integrity key based on the K_{AMF} or mapped K'_{AMF} if the type of security context flag is set to "mapped security context" indicated by the ngKSI. 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, then the UE shall check whether the SECURITY MODE COMMAND message indicates the ngKSI of the current 5GS security context, if it is a mapped 5G NAS security context, in order not to re-generate the K'_{AMF}.

Furthermore, if the SECURITY MODE COMMAND message can be accepted, the UE shall cipher the SECURITY MODE COMPLETE message with the selected 5GS ciphering algorithm and the 5GS NAS ciphering key based on the K_{AMF} or mapped K'_{AMF} indicated by the ngKSI. The UE shall set the security header type of the message to "integrity protected and ciphered with new 5G NAS security context".

From this time onward the UE shall cipher and integrity protect all NAS signalling messages with the selected 5GS integrity and ciphering algorithms.

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

If, during an ongoing registration procedure, the SECURITY MODE COMMAND message includes a $HASH_{AMF}$, the UE shall compare $HASH_{AMF}$ with a hash value locally calculated as described in 3GPP TS 33.501 [24] from the entire plain REGISTRATION REQUEST message that the UE had sent to initiate the procedure. If $HASH_{AMF}$ and the locally calculated hash value are different, the UE shall include the complete REGISTRATION REQUEST message which the UE had previously sent in the Replayed NAS message container IE of the SECURITY MODE COMPLETE message.

If, prior to receiving the SECURITY MODE COMMAND message, the UE had sent an initial NAS message containing a limited set of IEs needed to establish security context, the UE shall include the complete initial message in the NAS SECURITY MODE COMPLETE message.

If the UE operating in the single-registration mode receives the Selected EPS NAS security algorithms IE, the UE shall use the IE according to 3GPP TS 33.501 [24].

5.4.2.4 NAS security mode control completion by the network

The AMF shall, upon receipt of the SECURITY MODE COMPLETE message, stop timer T3560. From this time onward the AMF shall integrity protect and encipher all signalling messages with the selected 5GS integrity and ciphering algorithms.

If the SECURITY MODE COMPLETE message contains a Replayed NAS container message IE with an REGISTRATION REQUEST message, the AMF shall complete the ongoing registration procedure by considering the REGISTRATION REQUEST message contained in the Replayed NAS message container IE as the message that triggered the procedure.

5.4.2.5 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 a 5GMM 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 AMF shall stop timer T3560. The AMF shall also abort the ongoing procedure that triggered the initiation of the NAS security mode control procedure.

Both the UE and the AMF shall apply the 5G NAS 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 subclause 4.4.4 and 4.4.5.

5.4.2.6 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 registration procedure).

The UE shall abort the security mode control procedure and re-initiate the registration 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 registration procedure shall be initiated.

If the current TAI is still part of the TAI list, the security mode control procedure shall be aborted and 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).

The security mode control procedure shall be aborted and it is up to the UE implementation how to re-run the ongoing procedure that triggered the security mode control procedure.

5.4.2.7 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 security mode control procedure.

b) Expiry of timer T3560.

The network shall, on the first expiry of the timer T3560, retransmit the SECURITY MODE COMMAND message and shall reset and start timer T3560. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3560, the procedure shall be aborted.

c) Collision between security mode control procedure and registration, service request or de-registration 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 5GMM 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 AMF handover and the target TA is included in the TAI list, then upon successful completion of the intra AMF handover the AMF shall retransmit the SECURITY MODE COMMAND message. If a failure of the handover procedure is reported by the lower layer and the N1 signalling connection exists, the AMF shall retransmit the SECURITY MODE COMMAND message.

5.4.3 Identification procedure

5.4.3.1 General

The purpose of this procedure is to request a particular UE to provide specific identification parameters, e.g. the SUCI or the IMEI. The SUCI is a privacy preserving identifier containing the concealed SUPI and IMEI is a format of PEI.

5.4.3.2 Identification initiation by the network

The AMF initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and starting timer T3570 (see example in figure 5.4.3.2.1). The IDENTITY REQUEST message specifies the requested identification parameters in the Identity type information element.

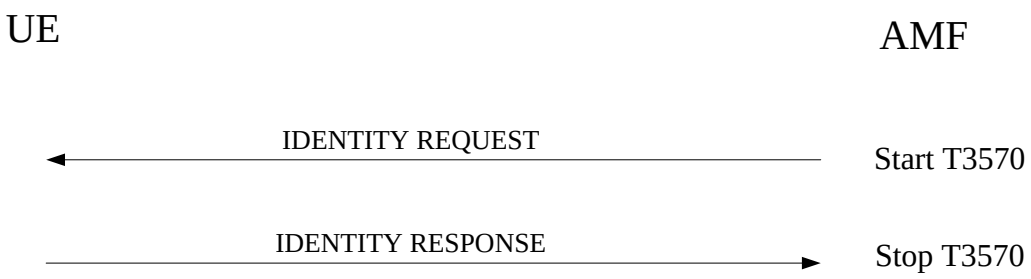


Figure 5.4.3.2.1: Identification procedure

5.4.3.3 Identification response by the UE

A UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in 5GMM-CONNECTED mode.

Upon receipt of the IDENTITY REQUEST message:

a) if the identity type IE in the IDENTITY REQUEST message is not set to "SUCI", 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; and

b) if the identity type IE in the IDENTITY REQUEST message is set to "SUCI", the UE shall:

   1) if timer T3519 is not running, generate a fresh SUCI as specified in 3GPP TS 33.501 [24], send an IDENTITY RESPONSE message with the SUCI, start timer T3519 and store the value of the SUCI sent in the IDENTITY RESPONSE message; and

   2) if timer T3519 is running, send an IDENTITY RESPONSE message with the stored SUCI.

5.4.3.4 Identification completion by the network

Upon receipt of the IDENTITY RESPONSE the network shall stop the timer T3570.

5.4.3.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of the IDENTITY RESPONSE message (if the identification procedure is triggered by a registration procedure).

   The UE shall re-initiate the registration procedure.

b) 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".

5.4.3.6 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 5GMM procedure.

b) Expiry of timer T3570.

The network shall, on the first expiry of the timer T3570, retransmit the IDENTITY REQUEST message and reset and restart the timer T3570. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3570, the network shall abort the identification procedure and any ongoing 5GMM procedure.

c) Collision of an identification procedure with a registration procedure for initial registration.

If the network receives a REGISTRATION REQUEST message indicating either "initial registration" or "5GS emergency registration" in the 5GS registration type IE before the ongoing identification procedure has been completed and no registration procedure is pending on the network (i.e. no REGISTRATION ACCEPT/REJECT message has still to be sent as an answer to a REGISTRATION REQUEST message), the network shall proceed with the registration procedure for initial registration.

d) Collision of an identification procedure with a registration procedure for initial registration when the identification procedure has been caused by a registration procedure for initial registration.

If the network receives a REGISTRATION REQUEST message indicating either "initial registration" or "5GS emergency registration" in the 5GS registration type IE before the ongoing identification procedure has been completed and a registration procedure for initial registration is pending (i.e. a REGISTRATION ACCEPT/REJECT message has to be sent as an answer to an earlier REGISTRATION REQUEST message), then:

- If one or more of the information elements in the REGISTRATION REQUEST message differ from the ones received within the previous REGISTRATION REQUEST message, the network shall proceed with the new registration procedure for initial registration; or

- If the information elements do not differ, then the network shall not treat any further this new REGISTRATION REQUEST message.

e) Collision of an identification procedure with a registration procedure for mobility and periodic registration update.

If the network receives a REGISTRATION REQUEST message indicating either "mobility registration updating" or "mobility registration updating" in the 5GS registration type IE before the ongoing identification procedure has been completed, the network shall progress both procedures.

f) Collision of an identification procedure with a UE initiated de-registration procedure.

If the network receives a DEREGISTRATION REQUEST message with "switch off" indication in the De-registration type IE before the ongoing identification procedure has been completed, the network shall abort the identification procedure and shall progress the UE-initiated de-registration procedure;

Else the network shall complete the identification procedure and shall respond to the UE-initiated de-registration procedure as described in subclause 5.5.2.2.

5.4.4 Generic UE configuration update procedure

5.4.4.1 General

The purpose of this procedure is to:

a) allow the AMF to update the UE configuration for access and mobility management-related parameters decided and provided by the AMF by providing new parameter information within the command; or

b) request the UE to perform a registration procedure for mobility and periodic registration update towards the network to update access and mobility management-related parameters decided and provided by the AMF (see subclause 5.5.1.3).

The procedure may be initiated by the network and can only be used when the UE has an established 5GMM context, and the UE is in 5GMM-CONNECTED mode. The AMF may require a confirmation response in order to ensure that the parameter has been updated by the UE.

The following parameters are supported by the generic UE configuration update procedure without the need for triggering the UE to perform the registration procedure for mobility and periodic registration update:

a) 5G-GUTI;

b) TAI list;

c) Service area list;

d) Network identity and time zone information (Full name for network, short name for network, local time zone, universal time and local time zone, network daylight saving time);

e) LADN information; and

f) Rejected NSSAI.

The following parameters may trigger the UE to perform the registration procedure for mobility and periodic registration update:

a) Allowed NSSAI; or

b) Configured NSSAI.

The following parameter requires triggering the UE to perform the registration procedure for mobility and periodic registration update:

a) MICO.

Editor's note: Other parameters requiring negotiation are FFS.

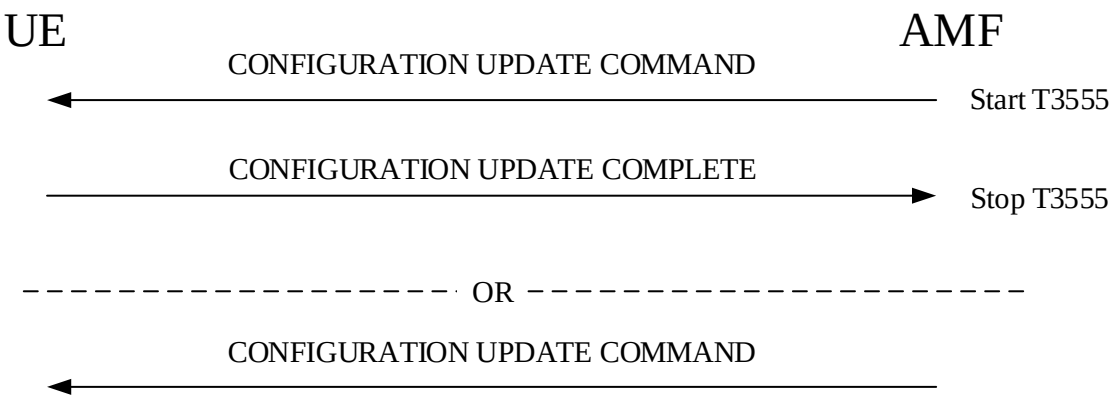


Figure 5.4.4.1.1: Generic UE configuration update procedure

5.4.4.2 Generic UE configuration update procedure initiated by the network

The AMF shall initiate the generic UE configuration procedure by sending the CONFIGURATION UPDATE COMMAND message to the UE.

The AMF shall in the CONFIGURATION UPDATE COMMAND message either:

a) include one or more of 5G-GUTI, TAI list, allowed NSSAI that may include the mapping to the configured NSSAI for the HPLMN, LADN information, service area list, MICO indication NITZ information, configured NSSAI that may include the mapping to the configured NSSAI for the HPLMN, or rejected NSSAI;

b) indicate registration requested; or

c) a combination of both.

If an acknowledgement from the UE is requested, the AMF shall indicate acknowledgement requested in the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message and shall start timer T3555. Acknowledgement shall be requested for all parameters except when only NITZ is included.

To initiate parameter re-negotiation between the UE and network, the AMF shall indicate "registration requested" in the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message. In this case, the acknowledgement shall be requested.

If a new allowed NSSAI information or AMF re-configuration of supported S-NSSAIs requires an AMF relocation, the AMF shall indicate "registration requested" in the Configuration update indication IE and include the Allowed NSSAI IE in the CONFIGURATION UPDATE COMMAND message. In this case, the acknowledgement shall be requested.

If the AMF includes a new configured NSSAI in the CONFIGURATION UPDATE COMMAND message and the new configured NSSAI requires an AMF relocation as specified in 3GPP TS 23.501 [8], the AMF shall indicate "registration requested" in the Configuration update indication IE in the message.

During an established 5GMM context, the network may send none, one, or more CONFIGURATION UPDATE COMMAND messages to the UE. If more than one CONFIGURATION UPDATE COMMAND message is sent, the messages need not have the same content.

5.4.4.3 Generic UE configuration update accepted by the UE

Upon receiving the CONFIGURATION UPDATE COMMAND message, the UE shall use the contents to update appropriate information stored within the UE.

If acknowledgement requested is indicated in the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message and:

a) if all information elements included are successfully accepted by the UE; or

b) if "registration requested" in the Configuration update indication IE is indicated;

the UE shall send a CONFIGURATION UPDATE COMPLETE message.

If the UE receives a new 5G-GUTI in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new 5G-GUTI as valid, the old 5G-GUTI as invalid, stop timer T3519 if running, and delete any stored SUCI; otherwise, the UE shall consider the old 5G-GUTI as valid.

If the UE receives a new TAI list in the CONFIGURATION UPDATE 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.

If the UE receives a new service area list in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new service area list as valid and the old service area list as invalid; otherwise, the UE shall consider the old service area list, if any, as valid.

If the UE receives new NITZ information in the CONFIGURATION UPDATE COMMAND message, the UE considers the new NITZ information as valid and the old NITZ information as invalid; otherwise, the UE shall consider the old NITZ information as valid.

If the UE receives a LADN information IE in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the old LADN information as invalid and the new LADN information as valid, if any; otherwise, the UE shall consider the old LADN information as valid.

If the UE receives a new allowed NSSAI for the associated access type in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new allowed NSSAI as valid for the associated access type, store the allowed NSSAI for the associated access type as specified in subclause 4.6.2.2 and consider the old allowed NSSAI for the associated access type as invalid; otherwise, the UE shall consider the old Allowed NSSAI as valid for the associated access type.

If the UE receives an allowed NSSAI in the CONFIGURATION UPDATE COMMAND message and the UE has one or more PDU sessions associated with S-NSSAI(s) not included in the received allowed NSSAI, the UE shall locally release all such PDU session(s).

If the UE receives a new configured NSSAI in the CONFIGURATION UPDATE COMMAND message, the UE shall consider the new configured NSSAI for the registered PLMN as valid and the old configured NSSAI for the registered

PLMN as invalid; otherwise, the UE shall consider the old configured NSSAI for the registered PLMN as valid The UE shall store the new configured NSSAI as specified in subclause 4.6.2.2.

If the CONFIGURATION UPDATE COMMAND message indicates "registration requested" in the Configuration update indication IE and:

- either a new allowed NSSAI or a new configured NSSAI or both are included, the UE shall, after the completion of the generic UE configuration update procedure, and the release of the existing N1 NAS signalling connection, start a registration procedure for mobility and periodic registration update as specified in subclause 5.5.1.3; or
- an MICO indication is included, the UE shall, after the completion of the generic UE configuration update procedure, start a mobility registration update procedure as specified in subclause 5.5.1.3 to re-negotiate MICO mode with the network.

The UE receiving the rejected NSSAI in the CONFIGURATION UPDATE COMMAND message takes the following actions based on the rejection cause in the rejected NSSAI:

"S-NSSAI not available in the current PLMN"

The UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the current PLMN as specified in subclause 4.6.2.2 and not attempt to use this S-NSSAI in the current PLMN until switching off the UE or the UICC containing the USIM is removed.

"S-NSSAI not available in the current registration area"

The UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the current PLMN and registration area combination as specified in subclause 4.6.2.2 and not attempt to use this S-NSSAI in the current registration area until switching off the UE, the UE moving out of the current registration area or the UICC containing the USIM is removed.

5.4.4.4 Generic UE configuration update completion by the network

Upon receipt of the CONFIGURATION UPDATE COMPLETE message, the AMF shall stop the timer T3555.

If a new 5G-GUTI was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the new 5G-GUTI as valid and the old 5G-GUTI as invalid.

If a new TAI list was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the new TAI list as valid and the old TAI list as invalid.

If a new service area list was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the new service area list as valid and the old service area list as invalid.

If new allowed NSSAI information was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the new Allowed NSSAI information as valid and the old allowed NSSAI information as invalid. In addition, if registration requested was indicated in the CONFIGURATION UPDATE COMMAND message, the AMF shall initiate the release of the N1 NAS signalling connection.

If a LADN information IE was included in the CONFIGURATION UPDATE COMMAND message, the AMF shall consider the old LADN information as invalid and the new LADN information as valid, if any. In this case, if the tracking area identity list received in the new LADN information does not include the current TA, the AMF shall indicate the SMF to release the PDU session for LADN or release the user-plane resources for the PDU session for LADN (see 3GPP TS 23.501 [8] and 3GPP TS 23.502 [9]).

Editor's note: Further details on handling of specific IEs are FFS.

5.4.4.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of the CONFIGURATION UPDATE COMPLETE message with TAI change from lower layers

If the current TAI is not in the TAI list, the generic UE configuration update procedure shall be aborted and a registration procedure for mobility and periodic registration update 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 generic UE configuration update procedure.

b) Transmission failure of CONFIGURATION UPDATE 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 generic UE configuration update procedure.

5.4.4.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3555.

The network shall, on the first expiry of the timer T3555, retransmit the CONFIGURATION UPDATE COMMAND message and shall reset and start timer T3555. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3555, the procedure shall be aborted.

b) Lower layer failure.

If a lower layer failure is detected before the CONFIGURATION UPDATE COMPLETE message is received, the old and the new 5G-GUTI shall be considered as valid until the old 5G-GUTI can be considered as invalid by the AMF. If a new TAI list was provided in the CONFIGURATION UPDATE 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 AMF.

During this period the AMF:

1) may first use the old 5G-S-TMSI from the old 5G-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 5G-GUTI in the CONFIGURATION UPDATE COMMAND message, the new TAI list should also be used for paging. Upon response from the UE, the AMF may re-initiate the CONFIGURATION UPDATE COMMAND. If the response is received from a tracking area within the old and new TAI list, the network shall re-initiate the CONFIGURATION UPDATE COMMAND message. If no response is received to the paging attempts, the network may use the new 5G-S-TMSI from the new 5G-GUTI for paging for an implementation dependent number of paging attempts. In this case, if a new TAI list was provided with new 5G-GUTI in the CONFIGURATION UPDATE COMMAND message, the new TAI list shall be used instead of the old TAI list. Upon response from the UE the AMF shall consider the new 5G-GUTI as valid and the old 5G-GUTI as invalid.

2) shall consider the new 5G-GUTI as valid if it is used by the UE and, additionally, the new TAI list as valid if it was provided with this 5G-GUTI in the CONFIGURATION UPDATE COMMAND message; and

3) may use the identification procedure followed by a new generic UE configuration update procedure if the UE uses the old 5G-GUTI.

5.4.5 NAS transport procedure(s)

5.4.5.1 General

The purpose of the NAS transport procedures is to provide a transport of payload between the UE and the AMF. The type of the payload is identified by the Payload container type IE and includes one of the following:

a) a single 5GSM message;

b) SMS;

c) an LPP message (see 3GPP TS 36.355 [26]);

d) a transparent container; or

e) a UE policy container.

Editor's note: Other types of payload, such as generic application payload, are FFS.

Along with the payload, the NAS transport procedure may transport the associated information (e.g. PDU session information for 5GSM message payload).

5.4.5.2 UE-initiated NAS transport procedure

5.4.5.2.1 General

The purpose of the UE-initiated NAS transport procedure is to provide a transport of:

a) a single 5GSM message as defined in subclause 8.3;

b) SMS (see 3GPP TS 24.011 [13]);

c) an LPP message;

d) a transparent container; or

e) a UE policy container.

and optional associated payload routing information from the UE to the AMF in a 5GMM message.

5.4.5.2.2 UE-initiated NAS transport procedure initiation

In the connected mode, the UE initiates the NAS transport procedure by sending the UL NAS TRANSPORT message, as shown in figure 5.4.5.2.2.1.

In case a) in subclause 5.4.5.2.1, the UE shall:

a) include the PDU session information (PDU session ID, old PDU session ID, S-NSSAI, DNN, request type), if available:

b) set the Payload container type IE to "N1 SM information"; and

c) set the Payload container IE to the 5GSM message.

The UE shall set the PDU session ID IE to the PDU session ID. If an old PDU session ID is to be included, the UE shall set the Old PDU session ID IE to the old PDU session ID.

If an S-NSSAI is to be included, the UE shall set the S-NSSAI IE to the S-NSSAI selected for the PDU session from the allowed NSSAI for the serving PLMN, associated with the mapped configured NSSAI for the HPLMN if available in roaming scenarios.

If a DNN is to be included, the UE shall set the DNN IE to the DNN. 5GSM procedures specified in clause 9 describe conditions for inclusion of the S-NSSAI and the DNN.

If a request type is to be included, the UE shall set the Request type IE to the request type. The request type is not provided along 5GSM messages other than the PDU SESSION ESTABLISHMENT REQUEST message.

The UE shall send the UL NAS TRANSPORT message to the AMF (see example in figure 5.4.5.2.2.1).

In case b) in subclause 5.4.5.2.1, the UE shall:

- set the Payload container type IE to "SMS"; and
- set the Payload container IE to the SMS payload.

Based on the UE preferences regarding access selection for mobile originated (MO) transmission of SMS over NAS as described in 3GPP TS 23.501 [8]:

a) when SMS over NAS is preferred to be sent over 3GPP access: the UE attempts to deliver MO SMS over NAS via the 3GPP access if the UE is registered over both 3GPP access and non-3GPP access;

b) when SMS over NAS is preferred to be sent over non-3GPP access: the UE attempts to deliver MO SMS over NAS via the non-3GPP access if the UE is registered over both 3GPP access and non-3GPP access. If the delivery of SMS over NAS via the non-3GPP access is not available, the UE attempts to deliver MO SMS over NAS via the 3GPP access.

In case c) in subclause 5.4.5.2.1, the UE shall:

- set the Payload container type IE to "LTE Positioning Protocol (LPP) message container";
- set the Payload container IE to the LPP message payload; and
- set the Additional information IE to the routing information provided by the upper layer location services application.

In case d) in subclause 5.4.5.2.1, the UE shall:

- set the Payload container type IE to "transparent container"; and
- set the Payload container IE to the transparent container.

Editor's note: The trigger for the UE to send a transparent container and the encoding of the transparent container are FFS.

In case e) in subclause 5.4.5.2.1, the UE shall:

- set the Payload container type IE to "UE policy container"; and
- set the contents of the Payload container IE as specified in Annex D.

Figure 5.4.5.2.2.1: UE-initiated NAS transport procedure

5.4.5.2.3 UE-initiated NAS transport of messages accepted by the network

Upon reception of a UL NAS TRANSPORT message, if the Payload container type IE is set to:

a) "N1 SM information", the AMF looks up a PDU session routing context for:

1) the UE and the PDU session ID IE in case the Old PDU session ID IE is not included, and:

NOTE 1: If the Old PDU session ID IE is not included in the UL NAS TRANSPORT message and the AMF has received a reallocation requested indication from the SMF, the AMF needs to ignore the reallocation requested indication.

i) if the AMF has a PDU session routing context for the PDU session ID and the UE, and the Request type IE is not included, the AMF shall forward the 5GSM message, and the PDU session ID IE towards the SMF identified by the SMF ID of the PDU session routing context;

ii) if the AMF has a PDU session routing context for the PDU session ID and the UE, the PDU session routing context indicates that the PDU session is not an emergency PDU session, and the Request type IE is included and is set to "existing PDU session", the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type towards the SMF identified by the SMF ID of the PDU session routing context;

iii) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, and the Request type IE is included and is set to "initial request":

A) the AMF shall select an SMF with following handlings:

If the S-NSSAI IE is not included and the user's subscription context obtained from UDM:

- contains one default S-NSSAI, the AMF shall use the default S-NSSAI as the S-NSSAI;
- contains two or more default S-NSSAIs, the AMF shall use one of the default S-NSSAIs selected by operator policy as the S-NSSAI; and
- does not contain a default S-NSSAI, the AMF shall use an S-NSSAI selected based on operator policy as the S-NSSAI.

If the DNN IE is not included or the DNN is not valid, and the user's subscription context obtained from UDM:

- contains the default DNN for the S-NSSAI, the AMF shall use the default DNN as the DNN; and
- does not contain the default DNN for the S-NSSAI, the AMF shall use a locally configured DNN as the DNN; and

If the DNN is a LADN DNN, the AMF shall determine the UE presence in LADN service area.

NOTE 2: SMF selection is out of scope of CT1.

B) if the SMF selection is successful:

- the AMF shall store a PDU session routing context for the PDU session ID and the UE, shall set the SMF ID in the stored PDU session routing context to the SMF ID corresponding to the DNN in the user's subscription context obtained from the UDM; and
- the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received), the request type and UE presence in LADN service area (if DNN received corresponds to an LADN DNN) towards the SMF identified by the SMF ID of the PDU session routing context;

iv) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is included and is set to "existing PDU session", and the user's subscription context obtained from the UDM contains an SMF ID for the PDU session ID such that the SMF ID includes a PLMN identity corresponding to the UE's HPLMN or the current PLMN, then:

A) the AMF shall store a PDU session routing context for the PDU session ID and the UE, shall set the SMF ID in the stored PDU session routing context to the SMF ID contained in the user's subscription context obtained from the UDM; and

B) the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type towards the SMF identified by the SMF ID of the PDU session routing context;

v) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is included and is set to "initial emergency request", and the AMF does not have a PDU session routing context for another PDU session ID of the UE indicating that the PDU session is an emergency PDU session:

A) the AMF shall select an SMF. The AMF shall use the emergency DNN from the AMF emergency configuration data as the DNN, if configured. The AMF shall derive the SMF from the emergency DNN or use the statically configured SMF from the AMF emergency configuration data, if configured; and

B) if the SMF selection is successful:

- the AMF shall store a PDU session routing context for the PDU session ID and the UE, shall set the SMF ID in the stored PDU session routing context to the SMF ID of the selected SMF, and shall store an indication that the PDU session is an emergency PDU session in the stored PDU session routing context; and

- the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if configured in the AMF emergency configuration data), the DNN (if configured in the AMF emergency configuration data), and the request type towards the SMF identified by the SMF ID of the PDU session routing context; and

vi) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is included and is set to "initial emergency request", and the AMF has a PDU session routing context indicating that the PDU session is an emergency PDU session for another PDU session ID of the UE:

A) the AMF shall store a PDU session routing context for the PDU session ID and the UE and shall set the SMF ID in the stored PDU session routing context to the SMF ID of the PDU session routing context for the other PDU session ID of the UE; and

B) the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if configured in the AMF emergency configuration data), the DNN (if configured in the AMF emergency configuration data) and the request type towards the SMF identified by the SMF ID of the PDU session routing context; or

vii)if the AMF has a PDU session routing context for the PDU session ID and the UE, the PDU session routing context indicates that the PDU session is an emergency PDU session, and the Request type IE is included and is set to "existing emergency PDU session", the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if configured in the AMF emergency configuration data), the DNN (if configured in the AMF emergency configuration data), and the request type towards the SMF identified by the SMF ID of the PDU session routing context; and

viii) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is included and is set to "existing emergency PDU session", and the user's subscription context obtained from the UDM contains an SMF ID for the PDU session ID such that the SMF ID includes a PLMN identity corresponding to the current PLMN, then:

A) the AMF shall store a PDU session routing context for the PDU session ID and the UE, shall set the SMF ID in the stored PDU session routing context to the SMF ID contained in the user's subscription context obtained from the UDM; and

B) the AMF shall forward the 5GSM message, the PDU session ID, the S-NSSAI (if configured in the AMF emergency configuration data), the DNN (if configured in the AMF emergency configuration data), and the request type towards the SMF identified by the SMF ID of the PDU session routing context; or

2) the UE and the Old PDU session ID IE in case the Old PDU session ID IE is included, and:

i) the AMF has a PDU session routing context for the old PDU session ID and the UE and does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is included and is set to "initial request", and the AMF received a reallocation requested indication from the SMF indicating that the SMF is to be reused, the AMF shall store a PDU session routing context for the PDU session ID and the UE, set the SMF ID in the stored PDU session routing context to the SMF ID of the PDU session routing context for the old PDU session ID and the UE. If the DNN is a LADN DNN, the AMF shall determine the UE presence in LADN service area. The AMF shall forward the 5GSM message, the PDU session ID, the old PDU session ID, the S-NSSAI (if received), the DNN (if received), the request type and UE presence in LADN service area (if DNN received corresponds to an LADN DNN) towards the SMF identified by the SMF ID of the PDU session routing context;

ii) the AMF has a PDU session routing context for the old PDU session ID and the UE and does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is included and is set to "initial request", the AMF received a reallocation requested indication from the SMF indicating that the SMF is to be reallocated:

A) the AMF shall select an SMF with following handlings;

If the S-NSSAI IE is not included and the user’s subscription context obtained from UDM:

- contains one default S-NSSAI, the AMF shall use the default S-NSSAI as the S-NSSAI;

- contains two or more default S-NSSAIs, the AMF shall use one of the default S-NSSAIs selected by operator policy as the S-NSSAI; and

- does not contain a default S-NSSAI, the AMF shall use an S-NSSAI selected based on operator policy as the S-NSSAI.

If the DNN IE is not included or the DNN is not valid, and the user's subscription context obtained from UDM:

- contains the default DNN for the S-NSSAI, the AMF shall use the default DNN as the DNN; and

- does not contain the default DNN for the S-NSSAI, the AMF shall use a locally configured DNN as the DNN; and

If the DNN is a LADN DNN, the AMF shall determine the UE presence in LADN service area.

B) if the SMF selection is successful:

- the AMF shall store a PDU session routing context for the PDU session ID and the UE and set the SMF ID of the PDU session routing context to the SMF ID of the selected SMF; and

- the AMF shall forward the 5GSM message, the PDU session ID, the old PDU session ID, the S-NSSAI (if received), the DNN (if received), the request type and UE presence in LADN service area (if DNN received corresponds to an LADN DNN) towards the SMF identified by the SMF ID of the PDU session routing context for the PDU session ID and the UE;

b) "SMS", the AMF shall forward the content of the Payload container IE to the SMSF associated with the UE;

c) "LTE Positioning Protocol (LPP) message container", the AMF shall forward the content of the Payload container IE to the LMF associated with the routing information included in the Additional information IE of the UL NAS TRANSPORT message;

d) "transparent container", the AMF shall forward the content of the Payload container IE to the UDM; and

e) "UE policy container", the AMF shall forward the content of the Payload container IE to the PCF.

5.4.5.2.4 UE-initiated NAS transport of messages not accepted by the network

Upon reception of a UL NAS TRANSPORT message, if the Payload container type IE is set to "N1 SM information", the Request type IE is set to "initial request" or "existing PDU session", the UE is not configured for high priority access in selected PLMN and:

a) DNN based congestion control is activated for the DNN included in the UL NAS TRANSPORT message, or DNN based congestion control is activated for the selected DNN in case of no DNN included in the UL NAS TRANSPORT message, e.g. configured by operation and maintenance, the AMF shall send back to the UE the 5GSM message which was not forwarded, a back-off timer value and 5GMM cause #22 "congestion" as specified in subclause 5.4.5.3.1 case f);

b) S-NSSAI and DNN based congestion control is activated for the S-NSSAI and DNN included in the UL NAS TRANSPORT message, or S-NSSAI and DNN based congestion control is activated for the S-NSSAI included in the UL NAS TRANSPORT message and the selected DNN in case of no DNN included in the UL NAS TRANSPORT message, or S-NSSAI and DNN based congestion control is activated for the selected S-NSSAI in case of no S-NSSAI included in the UL NAS TRANSPORT message and the DNN included in the UL NAS TRANSPORT message, or S-NSSAI and DNN based congestion control is activated for the selected S-NSSAI and the selected DNN in case of no S-NSSAI and no DNN included in the UL NAS TRANSPORT message, e.g. configured by operation and maintenance, the AMF shall send back to the UE the 5GSM message which was not forwarded, a back-off timer value and 5GMM cause #67 "insufficient resources for specific slice and DNN" as specified in subclause 5.4.5.3.1 case f); or

c) S-NSSAI only based congestion control is activated for the S-NSSAI included in the UL NAS TRANSPORT message, or S-NSSAI based congestion control is activated for the selected S-NSSAI in case of no S-NSSAI included in the UL NAS TRANSPORT message, e.g. configured by operation and maintenance, the AMF shall send back to the UE the 5GSM message which was not forwarded, a back-off timer value and 5GMM cause #69 "insufficient resources for specific slice" as specified in subclause 5.4.5.3.1 case f).

5.4.5.2.5 Abnormal cases on the network side

The following abnormal cases in AMF are identified:

a) if the Old PDU session ID IE is not included in the UL NAS TRANSPORT message, the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is set to "initial request", and the SMF selection fails then the AMF may send back to the UE the 5GSM message which was not forwarded as specified in subclause 5.4.5.3.1 case e).

b) if the Old PDU session ID IE is included in the UL NAS TRANSPORT message, the AMF has a PDU session routing context for the old PDU session ID and the UE and does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is set to "initial request", the AMF received a reallocation requested indication from the SMF indicating that the SMF is to be reallocated, and the SMF selection fails then the AMF may send back to the UE the 5GSM message which was not forwarded as specified in subclause 5.4.5.3.1 case e).

c) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is set to "existing PDU session", and the user's subscription context obtained from the UDM does not contain an SMF ID for the PDU session ID such that the SMF ID includes a PLMN identity corresponding to the UE's HPLMN or the current PLMN, then the AMF may send back to the UE the 5GSM message which was not forwarded as specified in subclause 5.4.5.3.1 case e).

d) if the Old PDU session ID IE is included in the UL NAS TRANSPORT message, and the AMF has a PDU session routing context for the old PDU session ID and the UE and does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is set to "initial request" and the AMF has not received a reallocation requested indication, the AMF should select an SMF with following handlings:

   If the S-NSSAI IE is not included and the user’s subscription context obtained from UDM:

   1) contains one default S-NSSAI, the AMF shall use the default S-NSSAI as the S-NSSAI;

   2) contains two or more default S-NSSAIs, the AMF shall use one of the default S-NSSAIs selected by operator policy as the S-NSSAI; and

   3) does not contain a default S-NSSAI, the AMF shall use an S-NSSAI selected based on operator policy as the S-NSSAI.

   If the DNN IE is not included or the DNN is not valid, and the user’s subscription context obtained from UDM:

   1) contains the default DNN for the S-NSSAI, the AMF shall use the default DNN as the DNN; and

   2) does not contain the default DNN for the S-NSSAI, the AMF shall use a locally configured DNN as the DNN; and

   If the DNN is a LADN DNN, the AMF shall determine the UE presence in LADN service area.

   If the SMF selection is successful, the AMF should store a PDU session routing context for the PDU session ID and the UE, set the SMF ID in the stored PDU session routing context to the selected SMF ID, and forward the 5GSM message, the PDU session ID, the old PDU session ID, the S-NSSAI (if received), the DNN (if received), the request type and UE presence in LADN service area (if DNN received corresponds to an LADN DNN) towards the SMF ID of the PDU session routing context.

e) if the AMF has a PDU session routing context for the PDU session ID and the UE, the PDU session routing context indicates that the PDU session is an emergency PDU session, the Request type IE is set to "initial emergency request", the AMF should forward the 5GSM message, the PDU session ID, the S-NSSAI (if configured in the AMF emergency configuration data), the DNN (if configured in the AMF emergency configuration data) and the request type towards the SMF ID of the PDU session routing context.

f) if the Request type IE is set to "initial emergency request" and the S-NSSAI or the DNN is received, the AMF ignores the received S-NSSAI or the DNN and uses the emergency DNN from the AMF emergency configuration data, if any.

g) if the AMF does not have a PDU session routing context for the PDU session ID and the UE, and the Request type IE of the UL NAS TRANSPORT message is not provided, then the AMF may send back to the UE the 5GSM message which was not forwarded as specified in subclause 5.4.5.3.1 case e).

h) if the AMF unsuccessfully attempted to forward the 5GSM message, the PDU session ID, the S-NSSAI (if received), the DNN (if received) and the request type (if received) towards a SMF ID, then the AMF may send back to the UE the 5GSM message which was not forwarded as specified in subclause 5.4.5.3.1 case e).

i) the Old PDU session ID IE is included in the UL NAS TRANSPORT message, the AMF does not have a PDU session routing context for the old PDU session ID and the UE, the AMF does not have a PDU session routing context for the PDU session ID and the UE, the Request type IE is set to "initial request", the AMF should select an SMF with following handlings

   If the S-NSSAI IE is not included and the user's subscription context obtained from UDM:

   1) contains one default S-NSSAI, the AMF shall use the default S-NSSAI as the S-NSSAI;

   2) contains two or more default S-NSSAIs, the AMF shall use one of the default S-NSSAIs selected by operator policy as the S-NSSAI; and

   3) does not contain a default S-NSSAI, the AMF shall use an S-NSSAI selected based on operator policy as the S-NSSAI.

   If the DNN IE is not included or the DNN is not valid, and the user's subscription context obtained from UDM:

   1) contains the default DNN for the S-NSSAI, the AMF shall use the default DNN as the DNN; and

   2) does not contain the default DNN for the S-NSSAI, the AMF shall use a locally configured DNN as the DNN; and

   If the DNN is a LADN DNN, the AMF shall determine the UE presence in LADN service area.

   If the SMF selection is successful, the AMF should store a PDU session routing context for the PDU session ID and the UE, set the SMF ID in the stored PDU session routing context to the selected SMF ID, and forward the 5GSM message, the PDU session ID, the old PDU session ID, the S-NSSAI (if received), the DNN (if received), the request type and UE presence in LADN service area (if DNN received corresponds to an LADN DNN) towards the SMF ID of the PDU session routing context. If the SMF selection fails then the AMF may send back to the UE the 5GSM message which was not forwarded as specified in subclause 5.4.5.3.1 case e).

j) if the AMF has a PDU session routing context for the PDU session ID and the UE, the PDU session routing context indicates that the PDU session is not an emergency PDU session, and the Request type IE is included and is set to "existing emergency PDU session", the AMF may send back to the UE the 5GSM message which was not forwarded as specified in subclause 5.4.5.3.1 case e).

k) if the AMF has a PDU session routing context for the PDU session ID and the UE, the PDU session routing context indicates that the PDU session is an emergency PDU session, and the Request type IE is included and is set to "existing PDU session", the AMF may forward the 5GSM message, the PDU session ID, the S-NSSAI (if configured in the AMF emergency configuration data), the DNN (if configured in the AMF emergency configuration data), and the request type towards the SMF identified by the SMF ID of the PDU session routing context.

5.4.5.3 Network-initiated NAS transport procedure

5.4.5.3.1 General

The purpose of the network-initiated NAS transport procedure is to provide a transport of:

a) a single 5GSM message;

b) SMS;

c) an LPP message;

d) a transparent container;

e) a single uplink 5GSM message which was not forwarded due to routing failure;

f) a single uplink 5GSM message which was not forwarded due to congestion control; or

g) a UE policy container.

from the AMF to the UE in a 5GMM message.

5.4.5.3.2 Network-initiated NAS transport procedure initiation

In connected mode, the AMF initiates the NAS transport procedure by sending the DL NAS TRANSPORT message, as shown in figure 5.4.5.3.2.1.

In case a) in subclause 5.4.5.3.1, i.e. upon reception from an SMF of a 5GSM message without an N1 SM delivery skip allowed indication for a UE or a 5GSM message with an N1 SM delivery skip allowed indication for a UE in the 5GMM-CONNECTED mode, the AMF shall:

a) include the PDU session information (PDU session ID) in the PDU session ID IE;

b) set the Payload container type IE to "N1 SM information"; and

c) set the Payload container IE to the 5GSM message.

In case b) in subclause 5.4.5.3.1, i.e. upon reception from an SMSF of an SMS payload, the AMF shall:

a) set the Payload container type IE to "SMS";

b) set the Payload container IE to the SMS payload; and

c) select the access type to deliver the DL NAS TRANSPORT message as follows in case the access type selection is required:

1) if the UE to receive the DL NAS TRANSPORT message is registered to the network via both 3GPP access and non-3GPP access, and the SMS allowed IE in the 5GMM context of the UE is set to "both 3GPP access and non-3GPP access", then the AMF selects non-3GPP access if the UE is in MICO mode and in 5GMM-IDLE state for 3GPP access. Otherwise, the AMF selects either 3GPP access or non-3GPP access; and

2) otherwise, the AMF selects 3GPP access.

NOTE: The AMF selects an access type between 3GPP access and non-3GPP access based on operator policy.

In case c) in subclause 5.4.5.3.1 i.e. upon reception from an LMF of an LPP message payload, the AMF shall:

a) set the Payload container type IE to "LTE Positioning Protocol (LPP) message container";

b) set the Payload container IE to the LPP message payload received from the LMF; and

c) set the Additional information IE to the routing information associated with the LMF from which the LPP message was received.

In case d) in subclause 5.4.5.3.1 i.e. upon reception of a transparent container from the UDM to be forwarded to the UE, the AMF shall:

a) set the Payload container type IE to "transparent container"; and

b) set the Payload container IE to the transparent container received from the UDM.

In case e) in subclause 5.4.5.3.1, i.e. upon sending a single uplink 5GSM message which was not forwarded due to routing failure, the AMF shall:

a) include the PDU session ID in the PDU session ID IE;

b) set the Payload container type IE to "N1 SM information";

c) set the Payload container IE to the 5GSM message which was not forwarded; and

d) set the 5GMM cause IE to the 5GMM cause #90 "payload was not forwarded".

In case f) in subclause 5.4.5.3.1, i.e. upon sending a single uplink 5GSM message which was not forwarded due to congestion control, the AMF shall:

a) include the PDU session ID in the PDU session ID IE;

b) set the Payload container type IE to "N1 SM information";

c) set the Payload container IE to the 5GSM message which was not forwarded;

d) set the 5GMM cause IE to the 5GMM cause #22 "Congestion", the 5GMM cause #67 "insufficient resources for specific slice and DNN" or the 5GMM cause #69 "insufficient resources for specific slice"; and

e) include the Back-off timer value IE.

In case g) in subclause 5.4.5.3.1 i.e. upon reception of a UE policy container from the PCF to be forwarded to the UE, the AMF shall:

a) set the Payload container type IE to "UE policy container"; and

b) set the Payload container IE to the UE policy container received from the PCF.

Figure 5.4.5.3.2.1: Network-initiated NAS transport procedure

5.4.5.3.3 Network-initiated NAS transport of messages

Upon reception of a DL NAS TRANSPORT message, if the Payload container type IE is set to:

a) "N1 SM information" and the 5GMM cause IE set to the 5GMM cause #90 "payload was not forwarded" is not included in the DL NAS TRANSPORT message, the 5GSM message in the Payload container IE and the PDU session ID are handled in the 5GSM procedures specified in clause 9;

b) "SMS", the UE shall forward the content of the Payload container IE to the SMS stack entity;

c) "LTE Positioning Protocol (LPP) message container", the UE shall forward the content of the Payload container IE and the routing information included in the Additional information IE to the upper layer location services application;

d) "transparent container", the UE shall pass the payload to the appropriate entity;

Editor's note: How the UE determines the appropriate entity is FFS and requires input from SA3.

e) "N1 SM information" and the 5GMM cause IE is set to the 5GMM cause #90 "payload was not forwarded" in the DL NAS TRANSPORT message, the UE passes to the 5GSM sublayer an indication that the 5GSM message was not forwarded along with the 5GSM message from the Payload container IE of the DL NAS TRANSPORT message;

f) "N1 SM information" and:

1) the 5GMM cause IE is set to the 5GMM cause #22 "Congestion", the UE passes to the 5GSM sublayer an indication that the 5GSM message was not forwarded due to DNN based congestion control along with the 5GSM message from the Payload container IE of the DL NAS TRANSPORT message, and the time value from the Back-off timer value IE;

2) the 5GMM cause IE is set to the 5GMM cause #67 "insufficient resources for specific slice and DNN", the UE passes to the 5GSM sublayer an indication that the 5GSM message was not forwarded due to S-NSSAI and DNN based congestion control along with the 5GSM message from the Payload container IE of the DL NAS TRANSPORT message, and the time value from the Back-off timer value IE; or

3) the 5GMM cause IE is set to the 5GMM cause #69 "insufficient resources for specific slice", the UE passes to the 5GSM sublayer an indication that the 5GSM message was not forwarded due to S-NSSAI only based congestion control along with the 5GSM message from the Payload container IE of the DL NAS TRANSPORT message, and the time value from the Back-off timer value IE; and

g) "UE policy container", the UE policy container in the Payload container IE is handled in the UE policy delivery procedures specified in Annex D.

5.4.6 5GMM status procedure

5.4.6.1 General

The purpose of the 5GMM STATUS procedure is to report at any time in the 5GMM STATUS message certain error conditions detected upon receipt of 5GMM protocol data in the UE. The 5GMM STATUS message can be sent by both the AMF and the UE (see example in figure 5.4.6.1).

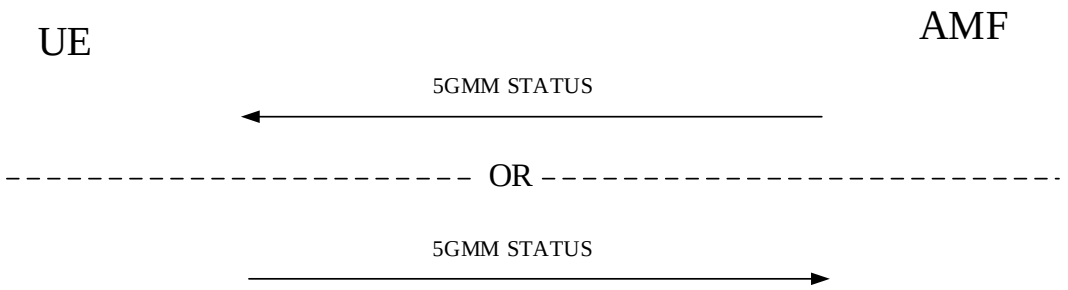


Figure 5.4.6.1: 5GMM status procedure

5.4.6.2 5GMM status received in the UE

On receipt of a 5GMM 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 UE on receipt of a 5GMM STATUS message are implementation dependent.

5.4.6.3 5GMM status received in the network

On receipt of a 5GMM STATUS message in the AMF, 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 AMF on receipt of a 5GMM STATUS message are implementation dependent.

5.5 5GMM specific procedures

5.5.1 Registration procedure

5.5.1.1 General

The registration procedure is always initiated by the UE and used for initial registration as specified in subclause 5.5.1.2.2 or mobility and periodic registration update as specified in subclause 5.5.1.3.2.

When the UE wants to initiate registration over both 3GPP access and non-3GPP access in the same PLMN (e.g. the 3GPP access and the selected N3IWF are located in the same PLMN), the UE:

a) in 5GMM-REGISTERED-INITIATED over 3GPP access shall not initiate registration over non-3GPP access; or

b) in 5GMM-REGISTERED-INITIATED over non-3GPP access shall not initiate registration over 3GPP access.

NOTE: To which access (i.e. 3GPP access or non-3GPP access) the UE initiates registration first is up to UE implementation.

When the UE is registered with a PLMN over a non-3GPP access, the AMF and the UE maintain:

a) registration state and state machine over non-3GPP access;

b) 5G NAS security context;

c) 5G-GUTI;

d) registration area for non-3GPP access, which is associated with a fixed well-known N3GPP TAI; and

e) non-3GPP de-registration timer in the UE and non-3GPP implicit de-registration timer in the AMF.

Editor's note: What information the N3IWF maintains for a registered UE is FFS.

A registration attempt counter is used to limit the number of subsequently rejected registration attempts. The registration attempt counter shall be incremented as specified in subclause 5.5.1.2.7 or subclause 5.5.1.3.6. Depending on the value of the registration attempt counter, specific actions shall be performed. The registration attempt counter shall be reset when:

- the UE is powered on;
- a USIM is inserted;
- a registration procedure is successfully completed; or

Editor's note: Other reasons to reset the registration attempt counter are FFS.

- a new PLMN is selected.

Additionally, the registration attempt counter shall be reset when the UE is in substate 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION and:

- a new registration area is entered;
- timer T3502 expires; or
- timer T3346 is started.

5.5.1.2 Registration procedure for initial registration

5.5.1.2.1 General

This procedure can be used by a UE for initial registration for 5GS services.

When the UE initiates the registration procedure for initial registration, the UE shall indicate "initial registration" in the 5GS registration type IE. When the UE initiates the registration procedure for emergency services, the UE shall indicate "emergency registration" in the 5GS registration type IE.

5.5.1.2.2 Initial registration initiation

The UE in state 5GMM-DEREGISTERED shall initiate the registration procedure for initial registration by sending a REGISTRATION REQUEST message to the AMF,

a) when the UE performs initial registration for 5GS services;

b) when the UE performs initial registration for emergency services;

c) when the UE performs initial registration for SMS over NAS; and

d) when the UE moves from GERAN to NG-RAN coverage or the UE moves from a UTRAN to NG-RAN coverage.

The UE initiates the registration procedure for initial registration by sending a REGISTRATION REQUEST message to the AMF, starting timer T3510. If timer T3502 is currently running, the UE shall stop timer T3502. If timer T3511 is currently running, the UE shall stop timer T3511.

If the UE holds a valid 5G-GUTI, the UE shall indicate the 5G-GUTI in the 5GS mobile identity IE. Otherwise, if a SUCI is available, the UE shall include the SUCI in the 5GS mobile identity IE. If the UE is initiating the registration procedure for emergency services and does not hold a valid 5G-GUTI or SUCI, the PEI shall be included in the 5GS mobile identity IE.

If the UE is operating in the dual-registration mode and it is in EMM state EMM-REGISTERED, the UE shall include the UE status IE with the EMM registration status set to "UE is in EMM-REGISTERED state".

NOTE 1: Inclusion of the UE status IE with this setting corresponds to the indication that the UE is "moving from EPC" as specified in 3GPP TS 23.502 [9].

If the last visited registered TAI is available, the UE shall include the last visited registered TAI in the REGISTRATION REQUEST message.

If the UE requests the use of SMS over NAS, the UE shall include the SMS requested IE in the REGISTRATION REQUEST message and set the SMS requested bit of the SMS requested IE to "SMS over NAS supported".

If the UE supports MICO mode and requests the use of MICO mode, then the UE shall include the MICO indication IE in the REGISTRATION REQUEST message.

If the UE wants to use the UE specific DRX parameters, the UE shall include the Requested DRX parameters IE in the REGISTRATION REQUEST message.

The UE shall include the requested NSSAI containing the S-NSSAI(s) corresponding to the slice(s) to which the UE wants to register and may include the mapping of the requested NSSAI which is the mapping of each S-NSSAI of the requested NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN, if available, in the REGISTRATION REQUEST message. If the UE has allowed NSSAI or configured NSSAI for the current PLMN, the requested NSSAI shall be either:

a) the configured NSSAI for the current PLMN, or a subset thereof as described below, if the UE has no allowed NSSAI for the current PLMN;

b) the allowed NSSAI for the current PLMN, or a subset thereof as described below, if the UE has an allowed NSSAI for the current PLMN; or

c) the allowed NSSAI for the current PLMN, or a subset thereof as described below, plus one or more S-NSSAIs from the configured NSSAI for which no corresponding S-NSSAI is present in the allowed NSSAI and those are neither in the rejected NSSAI for the current PLMN nor in the rejected NSSAI for the current PLMN and registration area combination.

If the UE has neither allowed NSSAI for the current PLMN nor configured NSSAI for the current PLMN and has a configured NSSAI not associated with a PLMN, the UE shall include the S-NSSAI(s) in the Requested NSSAI IE of the REGISTRATION REQUEST message using the configured NSSAI not associated with a PLMN. If the UE has no allowed NSSAI for the current PLMN, no configured NSSAI for the current PLMN, and no configured NSSAI not associated with a PLMN, the UE shall not include a requested NSSAI in the REGISTRATION message.

The subset of configured NSSAI provided in the requested NSSAI consists of one or more S-NSSAIs in the configured NSSAI applicable to the current PLMN, if the S-NSSAI is neither in the rejected NSSAI for the current PLMN nor in the rejected NSSAI for the current PLMN and registration area combination.

The subset of allowed NSSAI provided in the requested NSSAI consists of one or more S-NSSAIs in the allowed NSSAI for the current PLMN, if the rejected S-NSSAI(s) is added by the configuration update procedure and the S-NSSAI is neither in the rejected NSSAI for the current PLMN nor in the rejected NSSAI for the current PLMN and registration area combination.

NOTE 2: How the UE selects the subset of configured NSSAI or allowed NSSAI to be provided in the requested NSSAI is implementation.

NOTE 3: The number of S-NSSAI(s) included in the requested NSSAI cannot exceed eight.

If the UE initiates an initial registration for emergency services or needs to prolong the established NAS signalling connection after the completion of the initial registration procedure (e.g. due to uplink signalling pending), it shall set the "follow-on request pending" indication to 1.

If the UE supports S1 mode, the UE shall:

- set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message;
- include the S1 UE network capability IE in the REGISTRATION REQUEST message; and
- if the UE supports sending an ATTACH REQUEST message containing a PDN CONNECTIVITY REQUEST message with request type set to "handover" to transfer a PDU session from N1 mode to S1 mode, set the HO attach bit to "attach request message containing PDN connectivity request with request type set to handover to transfer PDU session from N1 mode to S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message.

If the UE has one or more stored UE policy sections, the UE shall include the UPSI LIST TRANSPORT message (see annex D) in the Payload container IE of the REGISTRATION REQUEST message.

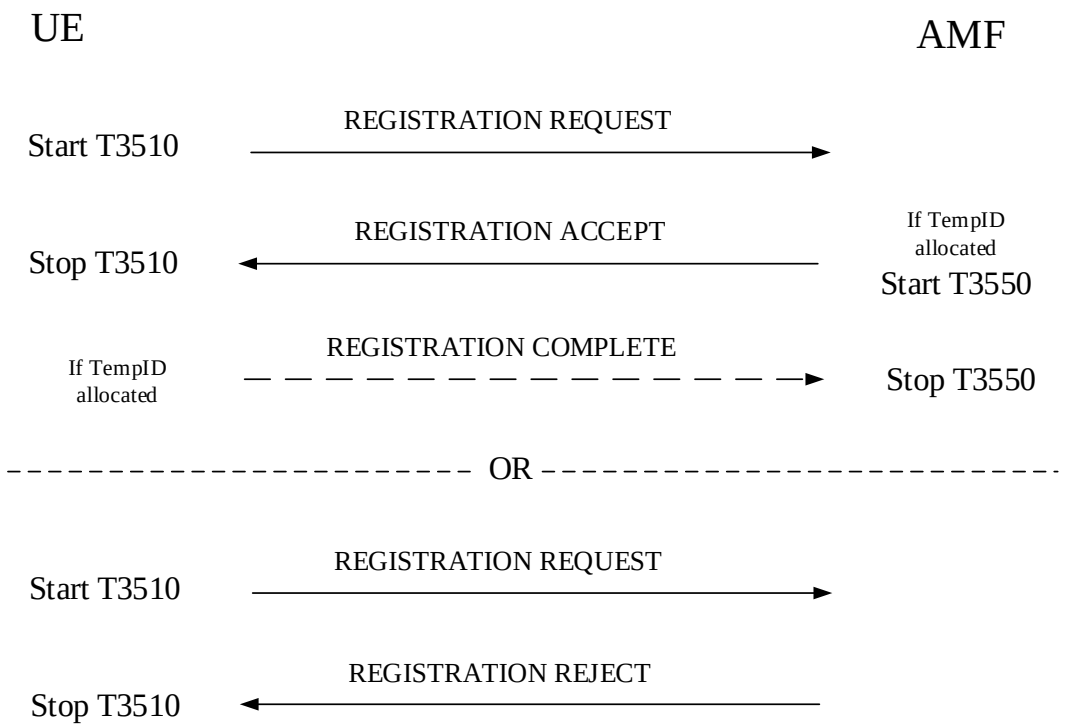


Figure 5.5.1.2.2.1: Registration procedure for initial registration

5.5.1.2.3 5GMM common procedure initiation

The network may initiate 5GMM common procedures, e.g. the identification, authentication and security procedures during the registration procedure, depending on the information received in the REGISTRATION REQUEST message.

During a registration procedure with 5GS registration type IE set to "emergency registration", if the AMF is configured to support emergency registration for unauthenticated SUCIs, the AMF may choose to skip the authentication procedure even if no 5G NAS security context is available and proceed directly to the execution of the security mode control procedure.

5.5.1.2.4 Initial registration accepted by the network

During a registration procedure with 5GS registration type IE set to "emergency registration", the AMF shall not check for mobility and access restrictions, regional restrictions or subscription restrictions, when processing the REGISTRATION REQUEST message.

If the initial registration request is accepted by the network, the AMF shall send a REGISTRATION ACCEPT message to the UE.

The AMF shall assign and include a TAI list as a registration area the UE is registered to in the REGISTRATION ACCEPT message. The UE, upon receiving a REGISTRATION ACCEPT message, shall delete its old TAI list and store the received TAI list. If the REGISTRATION REQUEST message was received over non-3GPP access, the AMF shall include only the N3GPP TAI in the TAI list.

NOTE: The N3GPP TAI is operator-specific.

The AMF may include service area restrictions in the Service area list IE in the REGISTRATION ACCEPT message. The UE, upon receiving a REGISTRATION ACCEPT message with the service area restrictions shall act as described in subclause 5.3.5.

If the Service area list IE is not included in the REGISTRATION ACCEPT message, any tracking area in the registered PLMN and its equivalent PLMN(s) is considered as an allowed tracking area as described in subclause 5.3.5.

The AMF shall include the LADN information in the LADN information IE of the REGISTRATION ACCEPT message, if there are valid LADN service area(s) for the subscribed DNN(s) of the UE in the current registration area. The UE, upon receiving the REGISTRATION ACCEPT message with the LADN information, shall store the received LADN information.

The 5G-GUTI reallocation may be part of the initial registration procedure. When the REGISTRATION REQUEST message includes the SUCI or PEI, or the AMF considers the 5G-GUTI provided by the UE is invalid, or the 5G-GUTI provided by the UE was assigned by another AMF, the AMF shall allocate a new 5G-GUTI to the UE. The AMF shall include in the REGISTRATION ACCEPT message the new assigned 5G-GUTI together with the assigned TAI list. In this case the AMF shall start timer T3550 and enter state 5GMM-COMMON-PROCEDURE-INITIATED as described in subclause 5.1.3.2.3.3.

The AMF shall include the MICO indication IE in the REGISTRATION ACCEPT message only if the MICO indication IE was included in the REGISTRATION REQUEST message, the AMF supports and accepts the use of MICO mode. If the AMF supports and accepts the use of MICO mode, the AMF may indicate "all PLMN registration area allocated" in the MICO indication IE in the REGISTRATION ACCEPT message. If "all PLMN registration area allocated" is indicated in the MICO indication IE, the AMF shall not assign and include the TAI list in the REGISTRATION ACCEPT message. If the REGISTRATION ACCEPT message included an MICO indication IE indicating "all PLMN registration area allocated", the UE shall treat all TAIs in the current PLMN as a registration area and delete its old TAI list.

The AMF shall include the T3512 value IE in the REGISTRATION ACCEPT message only if the REGISTRATION REQUEST message was sent over the 3GPP access.

The AMF shall include the non-3GPP de-registration timer value IE in the REGISTRATION ACCEPT message only if the REGISTRATION REQUEST message was sent for the non-3GPP access.

If the REGISTRATION ACCEPT message included a T3512 value IE, the UE shall use the value in the T3512 value IE as periodic registration update timer (T3512).

If the REGISTRATION ACCEPT message included a non-3GPP de-registration timer value IE, the UE shall use the value in non-3GPP de-registration timer value IE as non-3GPP de-registration timer.

If the REGISTRATION ACCEPT message contained a 5G-GUTI, the UE shall return a REGISTRATION COMPLETE message to the AMF to acknowledge the received 5G-GUTI, stop timer T3519 if running, and delete any stored SUCI.

Upon receiving a REGISTRATION COMPLETE message, the AMF shall stop timer T3550 and change to state 5GMM-REGISTERED. The 5G-GUTI, if sent in the REGISTRATION ACCEPT message, shall be considered as valid.

If the REGISTRATION REQUEST message contained the SMS requested IE with the SMS requested bit set to "SMS over NAS supported", and SMSF selection is successful, then the AMF shall send the REGISTRATION ACCEPT

message after the SMSF has confirmed that the activation of the SMS service was successful. When sending the REGISTRATION ACCEPT message, the AMF shall:

a) include the SMS allowed IE in the REGISTRATION ACCEPT message with the SMS allowed bit of the SMS allowed IE set to "SMS over NAS allowed" if the UE has set the SMS requested bit of the SMS requested IE to "SMS over NAS supported" and the network allows the SMS delivery over NAS; and

b) store the SMSF address and the contents of the SMS allowed IE in the UE 5GMM context, and consider the UE available for SMS.

If SMSF selection in the AMF or SMS activation via the SMSF is not successful, then the AMF shall not include the SMS allowed IE in the REGISTRATION ACCEPT message. If the AMF does not allow the use of SMS over NAS, then the AMF shall not include the SMS allowed IE in the REGISTRATION ACCEPT message.

If the AMF includes an SMS allowed IE in the REGISTRATION ACCEPT message and the UE is also registered over another access to the same PLMN, the UE considers the new value indicated by the SMS allowed IE as applicable for both accesses over which the UE is registered.

The AMF shall include the allowed NSSAI for the current PLMN and may include the mapping of each S-NSSAI of the allowed NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN contained in the requested NSSAI from the UE if available, in the REGISTRATION ACCEPT message if the UE included the requested NSSAI in the REGISTRATION REQUEST message and the AMF allows one or more S-NSSAIs in the requested NSSAI. The AMF may also include rejected NSSAI in the REGISTRATION ACCEPT message. Rejected NSSAI contains S-NSSAI(s) which was included in the requested NSSAI but rejected by the network associated with rejection cause(s).

The AMF may include a new configured NSSAI for the current PLMN in the REGISTRATION ACCEPT message if the REGISTRATION REQUEST message did not include the requested NSSAI, or the REGISTRATION REQUEST message included the requested NSSAI containing an S-NSSAI that is not valid in the serving PLMN. If a new configured NSSAI for the current PLMN is included, the AMF may also include the mapping of the configured NSSAI for the current PLMN to the configured NSSAI for the HPLMN in the REGISTRATION ACCEPT message.

The UE receiving the rejected NSSAI in the REGISTRATION ACCEPT message takes the following actions based on the rejection cause in the rejected NSSAI:

"S-NSSAI not available in the current PLMN"

The UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the current PLMN as specified in subclause 4.6.2.2 and not attempt to use this S-NSSAI in the current PLMN until switching off the UE or the UICC containing the USIM is removed.

"S-NSSAI not available in the current registration area"

The UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the current PLMN and registration area combination as specified in subclause 4.6.2.2 and not attempt to use this S-NSSAI in the current registration area until switching off the UE, the UE moving out of the current registration area or the UICC containing the USIM is removed.

If the UE did not include the requested NSSAI in the REGISTRATION REQUEST message or none of the requested NSSAI are present in the subscribed S-NSSAIs, and one or more subscribed S-NSSAIs (containing one or more S-NSSAIs each of which may be associated with a new S-NSSAI) marked as default are available, the AMF shall put the subscribed S-NSSAIs marked as default in the allowed NSSAI of the REGISTRATION ACCEPT message. The AMF shall determine a registration area such that all S-NSSAIs of the allowed NSSAI are available in the registration area.

If the REGISTRATION ACCEPT message contains the allowed NSSAI, then the UE shall store the included allowed NSSAI together with the PLMN identity of the registered PLMN and the registration area as specified in subclause 4.6.2.2.

If the REGISTRATION ACCEPT message contains a configured NSSAI IE with a new configured NSSAI for the current PLMN and optionally the mapping of the configured NSSAI for the current PLMN to the configured NSSAI for the HPLMN, the UE shall store the contents of the configured NSSAI IE as specified in subclause 4.6.2.2.

If the UE included S1 mode supported indication in the REGISTRATION REQUEST message, the AMF supporting inter-system change with EPS shall set the IWK N26 bit to either:

a) "interworking without N26 not supported" if the AMF does not support interworking procedures without N26 interface; or

b) "interworking without N26 supported" if the AMF supports interworking procedures without N26 interface

in the 5GS network feature support IE in the REGISTRATION ACCEPT message.

The UE supporting S1 mode shall operate in the mode for inter-system interworking with EPS as follows:

a) if the IWK N26 bit in the 5GS network feature support IE is set to "interworking without N26 not supported", the UE shall operate in single-registration mode;

b) if the IWK N26 bit in the 5GS network feature support IE is set to "interworking without N26 supported" and the UE supports dual-registration mode, the UE may operate in dual-registration mode; or

NOTE: The registration mode used by the UE is implementation dependent.

c) if the IWK N26 bit in the 5GS network feature support IE is set to "interworking without N26 supported" and the UE only supports single-registration mode, the UE shall operate in single-registration mode.

The UE shall treat the received interworking without N26 supported indication for inter-system change with EPS as valid in the entire PLMN and its equivalent PLMN(s).

The network informs the UE about the support of specific features, such as IMS voice over PS session, emergency services or emergency services fallback, in the 5GS network feature support information element. In a UE with IMS voice over PS session capability, the IMS voice over PS session indicator, the emergency service support indicator, and the emergency services fallback indicator shall be provided to the upper layers. The upper layers take the IMS voice over PS session indicator into account when selecting the access domain for voice sessions or calls. When initiating an emergency call, the upper layers also take the IMS voice over PS session indicator, the emergency service support indicator, and the emergency services fallback indicator into account for the access domain selection.

The AMF shall set the EMF bit in the 5GS network feature support IE to:

a) "Emergency services fallback supported in NR connected to 5GCN and E-UTRA connected to 5GCN" if the network supports the emergency services fallback procedure when the UE is in an NR cell connected to 5GCN or an E-UTRA cell connected to 5GCN;

b) "Emergency services fallback supported in NR connected to 5GCN only" if the network supports the emergency services fallback procedure when the UE is in an NR cell connected to 5GCN and does not support the emergency services fallback procedure when the UE is in an E-UTRA cell connected to 5GCN;

c) "Emergency services fallback supported in E-UTRA connected to 5GCN only" if the network supports the emergency services fallback procedure when the UE is in an E-UTRA cell connected to 5GCN and does not support the emergency services fallback procedure when the UE is in an NR cell connected to 5GCN; or

d) "Emergency services fallback not supported" if network does not support the emergency services fallback procedure when the UE is in any cell connected to 5GCN.

The network informs the UE that the use of access identity 1 is valid in the RPLMN or equivalent PLMN by setting the MPS indicator bit of the 5GS network feature support IE to "Access identity 1 valid in RPLMN or equivalent PLMN", in the REGISTRATION ACCEPT message. Based on operator policy, the AMF sets the MPS indicator bit in the REGISTRATION ACCEPT message based on the MPS priority information in the user’s subscription context obtained from the UDM.

Upon receiving a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 valid in RPLMN or equivalent PLMN", if the UE is not in the country of its HPLMN, the UE shall act as a UE with access identity 1 configured for MPS as described in subclause 4.5.2, in all NG-RAN TAs of the registered PLMN and its equivalent PLMNs. The MPS indicator bit in the 5GS network feature support IE provided in the REGISTRATION ACCEPT message is valid until the UE receives a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 not valid in RPLMN or equivalent PLMN" or until the UE selects a non-equivalent PLMN. Access identity 1 is only applicable while the UE is in N1 mode.

If the UE has indicated "follow-on request pending" in REGISTRATION REQUEST message, or the network has downlink signalling pending, the AMF shall not immediately release the NAS signalling connection after the completion of the registration procedure.

If the Requested DRX Parameters IE was included in the REGISTRATION REQUEST message, the AMF shall include the UE specific DRX parameters IE in the REGISTRATION ACCEPT message. The AMF may set the UE specific DRX parameters IE based on the received Requested DRX Parameters IE and operator policy if available.

If:

a) the UE's USIM is configured with indication that the UE is to receive the Transparent container IE, the Transparent container IE is not included in the REGISTRATION ACCEPT message or the Transparent container IE does not successfully pass the integrity check (see 3GPP TS 33.501 [24]); and

b) if the UE attempts obtaining service on another PLMNs as specified in 3GPP TS 23.122 [5] annex C;

then the UE shall locally release the established N1 NAS signalling connection.

If the REGISTRATION ACCEPT message includes the Transparent container IE and the Transparent container IE successfully passes the integrity check (see 3GPP TS 33.501 [24]):

a) the UE shall proceed with the behavior as specified in 3GPP TS 23.122 [5] annex C; and

b) if the UE attempts obtaining service on another PLMNs as specified in 3GPP TS 23.122 [5] annex C, then the UE may locally release the established N1 NAS signalling connection, otherwise the UE shall send a REGISTRATION COMPLETE message. If an acknowledgement is requested in the Transparent container IE of the REGISTRATION ACCEPT message, the UE acknowledgement is included in the Transparent container IE of the REGISTRATION COMPLETE message.

5.5.1.2.5 Initial registration not accepted by the network

If the initial registration request cannot be accepted by the network, the AMF shall send a REGISTRATION REJECT message to the UE including an appropriate 5GMM cause value.

If the initial registration request is rejected due to general NAS level mobility management congestion control, the network shall set the 5GMM cause value to #22 "congestion" and assign a back-off timer T3346.

The UE shall take the following actions depending on the 5GMM cause value received in the REGISTRATION REJECT message.

#3 (Illegal UE);

#6 (Illegal ME); or

#7 (5GS services not allowed).

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall consider the USIM as invalid for 5GS services until switching off or the UICC containing the USIM is removed. The UE shall enter the state 5GMM-DEREGISTERED.

If the UE is operating in single-registration mode, the UE shall handle 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the attach request procedure is rejected with the EMM 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.

#11 (PLMN not allowed).

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall delete the list of equivalent PLMNs and reset the registration attempt counter and store the PLMN identity in the "forbidden PLMN list". The UE shall perform a PLMN selection according to 3GPP TS 23.122 [5].

If the UE is operating in single-registration mode, the UE shall in addition delete any 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the attach request procedure is rejected with the EMM cause with the same value.

#12 (Tracking area not allowed).

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. Additionally, the UE shall reset the registration attempt counter.

The UE shall store the current TAI in the list of "5GS forbidden tracking areas for regional provision of service" and enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE.

If the UE is operating in single-registration mode, the UE shall handle 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the attach request procedure is rejected with the EMM cause with the same value.

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

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. Additionally, the UE shall delete the list of equivalent PLMNs and reset the registration attempt counter.

The UE shall store the current TAI in the list of "5GS forbidden tracking areas for roaming" and enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE or optionally 5GMM-DEREGISTERED.PLMN-SEARCH. The UE shall perform a PLMN selection according to 3GPP TS 23.122 [5].

If the UE is operating in single-registration mode, the UE shall handle 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the attach request procedure is rejected with the EMM cause with the same value.

#22 (Congestion).

If the T3346 value IE is present in the REGISTRATION REJECT message and the value indicates that this timer is neither zero nor deactivated, the UE shall proceed as described below; otherwise it shall be considered as an abnormal case and the behaviour of the UE for this case is specified in subclause 5.5.1.2.7.

The UE shall abort the initial registration procedure, set the 5GS update status to 5U2 NOT UPDATED and enter state 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION.

The UE shall stop timer T3346 if it is running.

If the REGISTRATION REJECT message is integrity protected, the UE shall start timer T3346 with the value provided in the T3346 value IE.

If the REGISTRATION REJECT message is not integrity protected, the UE shall start timer T3346 with a random value from the default range specified in 3GPP TS 24.008 [12].

The UE stays in the current serving cell and applies the normal cell reselection process. The initial registration procedure is started if still needed when timer T3346 expires or is stopped.

#27 (N1 mode not allowed).

The UE capable of S1 mode shall disable the N1 mode capability for both 3GPP access and non-3GPP access (see subclause 4.9).

Other values are considered as abnormal cases. The behaviour of the UE in those cases is specified in subclause 5.5.1.2.7.

5.5.1.2.6 Initial registration for emergency services not accepted by the network

Upon receiving the REGISTRATION REJECT message including 5GMM cause #5 "PEI not accepted", the UE shall enter the state 5GMM-DEREGISTERED.NO-SUPI.

Upon receiving the REGISTRATION REJECT message including 5GMM cause value which is not #5 "PEI not accepted", the UE shall perform the actions as described in subclause 5.5.1.2.5 with the following addition: the UE shall inform the upper layers of the failure of the procedure.

NOTE 1: This can result in the upper layers requesting implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [14] can result in the emergency call being attempted to another IP-CAN.

If the initial registration request for emergency services fails due to abnormal cases, the UE shall perform the actions as described in subclause 5.5.1.2.7 and inform the upper layers of the failure to access the network or the failure of the procedure.

NOTE 2: This can result in the upper layers requesting other implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [14] can result in the emergency call being attempted to another IP-CAN.

In a shared network, upon receiving the REGISTRATION REJECT message, the UE shall perform the actions as described in subclause 5.5.1.2.5, and shall:

a) inform the upper layers of the failure of the procedure; or

NOTE 3: The upper layers may request implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [14] that can result in the emergency call being attempted to another IP-CAN.

b) attempt to perform a PLMN selection in the shared network and initiate an initial registration for emergency services to the selected PLMN.

In a shared network, if the initial registration request for emergency services fails due to abnormal cases, the UE shall perform the actions as described in subclause 5.5.1.2.7 and shall:

a) inform the upper layers of the failure of the procedure; or

NOTE 4: The upper layers may request implementation specific mechanisms, e.g. procedures specified in 3GPP TS 24.229 [14] that can result in the emergency call being attempted to another IP-CAN.

b) attempt the initial registration for emergency services to another PLMN in the shared network.

5.5.1.2.7 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Timer T3346 is running.

The UE shall not start the registration procedure for initial registration unless:

1) the UE is a UE configured for high priority access in selected PLMN; or

2) the UE needs to perform the registration procedure for initial registration for emergency services.

The UE stays in the current serving cell and applies the normal cell reselection process.

NOTE 1: It is considered an abnormal case if the UE needs to initiate a registration procedure for initial registration while timer T3346 is running independent on whether timer T3346 was started due to an abnormal case or a non-successful case.

b) The lower layers indicate that the access attempt is barred.

The UE shall not start the initial registration procedure. The UE stays in the current serving cell and applies the normal cell reselection process.

The initial registration procedure is started, if still needed, when the lower layers indicate that the barring is alleviated for the access category with which the access attempt was associated.

Editor's note: Abnormal case handling for N1 NAS signalling connection establishment rejected by the network with "Extended wait time" received from lower layers is FFS.

c) T3510 timeout

The UE shall abort the registration procedure for initial registration and the NAS signalling connection, if any, shall be released locally if the initial registration request is not for emergency services, the registration attempt counter shall be incremented, unless it was already set to 5.

d) REGISTRATION REJECT message, other 5GMM cause values than those treated in subclause 5.5.1.2.5, and cases of 5GMM cause value #22, if considered as abnormal cases according to subclause 5.5.1.2.5.

If the registration request is not an initial registration request for emergency services, upon reception of the 5GMM causes #95, #96, #97, #99 and #111 the UE should set the registration attempt counter to 5.

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

If the registration attempt counter is less than 5:

- if the initial registration request is not for emergency services, timer T3511 is started and the state is changed to 5GMM-DEREGISTERED.ATEMPTING-REGISTRATION. When timer T3511 expires the registration procedure for initial registration shall be restarted, if still required.

If the registration attempt counter is equal to 5

- the UE shall delete 5G-GUTI, TAI list, last visited TAI, list of equivalent PLMNs and ngKSI, start timer T3502 and shall set the 5GS update status to 5U2 NOT UPDATED. The state is changed to 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION or optionally to 5GMM-DEREGISTERED.PLMN-SEARCH in order to perform a PLMN selection according to 3GPP TS 23.122 [5].

- if the UE is operating in single registration mode:

- the UE shall in addition handle the EPS update status, EMM parameters, EMM state as specified in 3GPP TS 24.301 [15] for the abnormal cases when an EPS attach procedure fails and the tracking area attempt counter is equal to 5; and

- the UE shall attempt to select E-UTRAN radio access technology and proceed with appropriate EMM specific procedures. Additionally, The UE may disable N1 mode capability as specified in subclause 4.9.

5.5.1.2.8 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 REGISTRATION COMPLETE message has been received from the UE, the AMF shall locally abort the registration procedure for initial registration, enter state 5GMM-DEREGISTERED and shall not resend the REGISTRATION ACCEPT message. If a new 5G-GUTI was assigned to the UE in the registration procedure for initial registration, the AMF shall consider both the old and the new 5G-GUTI as valid until the old 5G-GUTI can be considered as invalid by the AMF or the 5GMM context which has been marked as deregistered in the AMF is released.

If the old 5G-GUTI was allocated by an AMF other than the current AMF, the current AMF does not need to retain the old 5G-GUTI. If the old 5G-GUTI is used by the UE in a subsequent REGISTRATION REQUEST message, the network may use the identification procedure to request the UE's SUPI.

b) Protocol error

If the REGISTRATION REQUEST message is received with a protocol error, the AMF shall return a REGISTRATION REJECT message with one of the following 5GMM cause values:

#96 invalid mandatory information;

#99 information element non-existent or not implemented;

#100 conditional IE error; or

#111 protocol error, unspecified.

c) T3550 time-out

On the first expiry of the timer, the AMF shall retransmit the REGISTRATION ACCEPT message and shall reset and restart timer T3550.

This retransmission is repeated four times, i.e. on the fifth expiry of timer T3550, the registration procedure for initial registration shall be aborted and the AMF enters state 5GMM-DEREGISTERED. If a new 5G-GUTI was allocated in the REGISTRATION ACCEPT message, the AMF shall consider both the old and the new 5G-GUTI as valid until the old 5G-GUTI can be considered as invalid by the AMF or the 5GMM context which has

been marked as de-registered in the AMF is released. If the old 5G-GUTI was allocated by an AMF other than the current AMF, the current AMF does not need to retain the old 5G-GUTI.

If the old 5G-GUTI is used by the UE in a subsequent REGISTRATION REQUEST message, the AMF acts as specified for case a above.

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

1) If one or more of the information elements in the REGISTRATION REQUEST message differ from the ones received within the previous REGISTRATION REQUEST message, the previously initiated the registration procedure for initial registration shall be aborted if the REGISTRATION COMPLETE message has not been received and the new registration procedure for initial registration shall be progressed; or

2) if the information elements do not differ, then the REGISTRATION ACCEPT message shall be resent and the timer T3550 shall be restarted if an REGISTRATION COMPLETE message is expected. In that case, the retransmission counter related to T3550 is not incremented.

e) More than one REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration" received and no REGISTRATION ACCEPT or REGISTRATION REJECT message has been sent.

1) If one or more of the information elements in the REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration" differs from the ones received within the previous REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration", the previously initiated the registration procedure for initial registration shall be aborted and the new the registration procedure for initial registration shall be executed;

2) if the information elements do not differ, then the network shall continue with the previous the registration procedure for initial registration and shall ignore the second REGISTRATION REQUEST message.

f) REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration" received in state 5GMM-REGISTERED.

If an REGISTRATION REQUEST message with 5GS registration type IE set to "initial registration" is received in state 5GMM-REGISTERED the network may initiate the 5GMM common procedures; if it turned out that the REGISTRATION REQUEST message was sent by a UE that has already been registered, the 5GMM context, if any, are deleted and the new REGISTRATION REQUEST is progressed.

g) REGISTRATION REQUEST message with 5GS registration type IE set to "mobility registration updating" or "periodic registration updating" received before REGISTRATION COMPLETE message.

Timer T3550 shall be stopped. The allocated 5G-GUTI in the registration procedure for initial registration shall be considered as valid and the registration procedure for mobility and periodic update shall be rejected with the 5GMM cause #10 "implicitly de-registered" as described in subclause 5.5.1.3.5.

h) DEREGISTRATION REQUEST message received before REGISTRATION COMPLETE message.

The AMF shall abort the registration procedure for initial registration and shall progress the de-registration procedure as described in subclause 5.5.2.2.

5.5.1.3 Registration procedure for mobility and periodic registration update

5.5.1.3.1 General

This procedure is used by a UE for mobility and periodic registration update of 5GS services. This procedure, when used for periodic registration update of 5GS service, is performed only in 3GPP access.

The periodic registration update procedure of 5GS services is controlled in the UE by timer T3512. When timer T3512 expires, the registration procedure for mobility and periodic registration area updating is started. Start and reset of timer T3512 is described in subclause 10.2.

5.5.1.3.2 Mobility and periodic registration update initiation

The UE in state 5GMM-REGISTERED shall initiate the registration procedure for mobility and periodic registration update by sending a REGISTRATION REQUEST message to the AMF,

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 AMF;

b) when the periodic registration updating timer T3512 expires;

c) when requested by the CONFIGURATION UPDATE COMMAND message;

d) when the UE in state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE either receives a paging or the UE receives a NOTIFICATION message with access type indicating 3GPP access over the non-3GPP access for PDU sessions associated with 3GPP access;

e) upon inter-system change from S1 mode to N1 mode;

f) 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);

g) when the UE changes the 5GMM capability or the S1 UE network capability or both;

h) when the UE's usage setting changes;

i) when the UE needs to change the slice(s) it is currently registered to;

j) when the UE changes the UE specific DRX parameters;

k) when the UE in state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE receives a request from the upper layers to establish a PDU session for emergency services; or

l) when the UE needs to register for SMS over NAS, indicate a change in the requirements to use SMS over NAS, or de-register from SMS over NAS.

If item b) is the only reason for initiating the registration procedure for mobility and periodic registration update, the UE shall indicate "periodic registration updating" in the 5GS registration type IE; otherwise the UE shall indicate "mobility registration updating".

If the UE indicates "mobility registration updating" in the 5GS registration type IE and the UE supports S1 mode, the UE shall:

- set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message;

- include the S1 UE network capability IE in the REGISTRATION REQUEST message; and

- if the UE supports sending an ATTACH REQUEST message containing a PDN CONNECTIVITY REQUEST message with request type set to "handover" to transfer a PDU session from N1 mode to S1 mode, set the HO attach bit to "attach request message containing PDN connectivity request with request type set to handover to transfer PDU session from N1 mode to S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message.

If the UE operating in the single-registration mode performs inter-system change from S1 mode to N1 mode and has one or more stored UE policy sections, the UE shall include the UPSI LIST TRANSPORT message (see annex D) in the Payload container IE of the REGISTRATION REQUEST message.

The UE in state 5GMM-REGISTERED shall initiate the registration procedure for mobility and periodic update by sending a REGISTRATION REQUEST message to the AMF when the UE needs to request the use of SMS over NAS transport or the current requirements to use SMS over NAS transport change in the UE. The UE shall include the SMS requested IE in the REGISTRATION REQUEST message as specified in subclause 5.5.1.2.2.

When initiating a registration procedure for mobility and periodic registration update for periodic registration update of 5GS services (i.e. the 5GS registration type IE is set to "periodic registration updating") and the requirements to use SMS over NAS have not changed in the UE, the UE shall not include the SMS requested IE in the REGISTRATION REQUEST message.

If the UE no longer requires the use of SMS over NAS, then the UE shall include the SMS requested IE in the REGISTRATION REQUEST message with the SMS requested bit set to "SMS over NAS not supported".

After sending the REGISTRATION REQUEST message to the AMF the UE shall start timer T3510. If timer T3502 is currently running, the UE shall stop timer T3502. If timer T3511 is currently running, the UE shall stop timer T3511.

If the last visited registered TAI is available, the UE shall include the last visited registered TAI in the REGISTRATION REQUEST message.

The UE shall handle the 5GS mobility identity IE in the REGISTRATION REQUEST message as follows:

a) if the UE is operating in the single-registration mode, performs inter-system change from S1 mode to N1 mode, and the UE holds a valid 4G-GUTI, the UE shall include the 5G-GUTI mapped from the 4G-GUTI as specified in 3GPP TS 23.003 [4] in the 5GS mobility identity IE. Additionally, if the UE holds a valid 5G-GUTI, the UE shall include the 5G-GUTI in the Additional GUTI IE in the REGISTRATION REQUEST message; and

b) for all other cases, if the UE holds a valid 5G-GUTI, the UE shall indicate the 5G-GUTI in the 5GS mobile identity IE.

If the UE supports MICO mode and requests the use of MICO mode, then the UE shall include the MICO indication IE in the REGISTRATION REQUEST message.

If the UE wants to change the UE specific DRX parameters, the UE shall include the Requested DRX parameters IE in the REGISTRATION REQUEST message.

If the UE is initiating the registration procedure for mobility and periodic registration update, the UE may include the Uplink data status IE to indicate which PDU session(s) have pending user data to be sent. If the UE has one or more active always-on PDU sessions and the user-plane resources for these PDU sessions are not established, the UE shall include the Uplink data status IE and indicate that the UE has pending user data to be sent for those PDU sessions. If the UE is located outside the LADN service area, the UE shall not include the PDU session for LADN in the Uplink data status IE.

When the registration procedure for mobility and periodic registration update is initiated in 5GMM-IDLE mode, the UE may include a PDU session status IE in the REGISTRATION REQUEST message, indicating which PDU sessions associated with the access type the REGISTRATION REQUEST message is sent over are active in the UE.

If the UE received a paging message with the access type indicating non-3GPP access, the UE shall include the Allowed PDU session status IE in the REGISTRATION REQUEST message indicating the PDU session(s) that the UE allows to re-establish over 3GPP access.

If the UE operating in the single-registration mode performs inter-system change from S1 mode to N1 mode, the UE:

a) shall include the UE status IE with the EMM registration status set to "UE is in EMM-REGISTERED state" in the REGISTRATION REQUEST message;

NOTE 1: Inclusion of the UE status IE with this setting corresponds to the indication that the UE is "moving from EPC" as specified in 3GPP TS 23.502 [9], subclause 4.11.1.3.3 and 4.11.2.3.

b) may include the PDU session status IE in the REGISTRATION REQUEST message indicating the status of the PDU session(s) mapped during the inter-system change from S1 mode to N1 mode from the PDN connection(s) for which the EPS indicated that interworking to 5GS is supported, if any (see subclause 6.1.4.1); and

c) shall include a TRACKING AREA UPDATE REQUEST message as specified in 3GPP TS 24.301 [15] in the EPS NAS message container IE in the REGISTRATION REQUEST message.

If the UE operating in the single-registration mode performs inter-system change from S1 mode to N1 mode and the UE has at least one PDN connection with active EPS bearer context(s) for which interworking to 5GS is supported as specified in subclause 6.1.4.1, the UE shall include the S-NSSAI(s) associated with the established PDN connection(s) for which interworking to 5GS is supported in the Requested NSSAI IE of the REGISTRATION REQUEST message.

The UE shall include the requested NSSAI containing the S-NSSAI(s) corresponding to the slices to which the UE wants to register and may include the mapping of requested NSSAI which is the mapping of each S-NSSAI of the requested NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN, if available, in the REGISTRATION REQUEST message. If the UE has allowed NSSAI or configured NSSAI for the current PLMN, the requested NSSAI shall be either:

a) the configured NSSAI for the current PLMN, or a subset thereof as described below, if the UE has no allowed NSSAI for the current PLMN;

b) the allowed NSSAI for the current PLMN, or a subset thereof as described below, if the UE has an allowed NSSAI for the current PLMN; or

c) the allowed NSSAI for the current PLMN, or a subset thereof as described below, plus one or more S-NSSAIs from the configured NSSAI for which no corresponding S-NSSAI is present in the allowed NSSAI and those are neither in the rejected NSSAI for the current PLMN nor in the rejected NSSAI for the current PLMN and registration area combination.

If the UE has neither allowed NSSAI for the current PLMN nor configured NSSAI for the current PLMN and has a configured NSSAI not associated with a PLMN, the UE shall include the S-NSSAI(s) in the Requested NSSAI IE of the REGISTRATION REQUEST message using the configured NSSAI not associated with a PLMN. If the UE has no allowed NSSAI for the current PLMN, no configured NSSAI for the current PLMN, and no configured NSSAI not associated with a PLMN, the UE shall not include a requested NSSAI in the REGISTRATION REQUEST message.

The subset of configured NSSAI provided in the requested NSSAI consists of one or more S-NSSAIs in the configured NSSAI applicable to this PLMN, if the S-NSSAI is neither in the rejected NSSAIs for the current PLMN nor in the rejected NSSAI for the current PLMN and registration area combination.

The subset of allowed NSSAI provided in the requested NSSAI consists of one or more S-NSSAIs in the allowed NSSAI for this PLMN, if the rejected S-NSSAI(s) is added by the configuration update procedure and the S-NSSAI is neither in the rejected NSSAI for the current PLMN nor in the rejected NSSAI for the current PLMN and registration area combination.

NOTE 2: How the UE selects the subset of configured NSSAI or allowed NSSAI to be provided in the requested NSSAI is implementation.

NOTE 3: The number of S-NSSAI(s) included in the requested NSSAI cannot exceed eight.

If the UE initiates the mobility and periodic registration updating procedure upon request of the upper layers to establish a PDU session for emergency services or needs to prolong the established NAS signalling connection after the completion of the registration procedure for mobility and periodic registration update (e.g. due to uplink signalling pending but no user data pending), it shall set the "follow-on request pending" indication to 1.

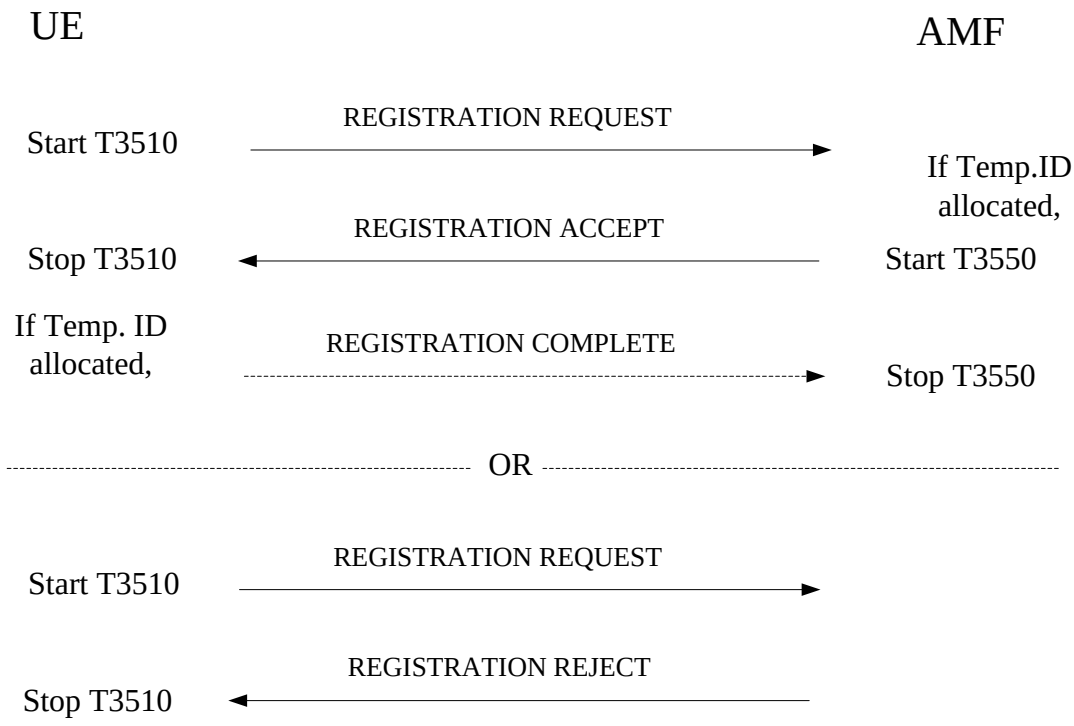


Figure 5.5.1.3.2.1: Registration procedure for mobility and periodic registration update

5.5.1.3.3 5GMM common procedure initiation

The AMF may initiate 5GMM common procedures, e.g. the identification, authentication and security procedures during the registration procedure, depending on the information received in the REGISTRATION REQUEST message.

5.5.1.3.4 Mobility and periodic registration update accepted by the network

If the registration update request has been accepted by the network, the AMF shall send a REGISTRATION ACCEPT message to the UE. If the AMF assigns a new 5G-GUTI for the UE, a 5G-GUTI shall be included in the REGISTRATION ACCEPT message or if the transparent container IE is included in the REGISTRATION ACCEPT message, the AMF shall start timer T3550 and enter state 5GMM-COMMON-PROCEDURE-INITIATED as described in subclause 5.1.3.2.3.3.

If timer T3513 is running in the AMF, the AMF shall stop timer T3513 if a paging request was sent with the access type indicating non-3GPP and the REGISTRATION REQUEST message includes the Allowed PDU session status IE.

If timer T3565 is running in the AMF, the AMF shall stop timer T3565 when a REGISTRATION REQUEST message is received.

The AMF may include a new TAI list for the UE in the REGISTRATION ACCEPT message. The UE, upon receiving a REGISTRATION ACCEPT message, shall delete its old TAI list and store the received TAI list. If there is no TAI list received, the UE shall consider the old TAI list as valid.

The AMF may include new service area restrictions in the Service area list IE in the REGISTRATION ACCEPT message. The UE, upon receiving a REGISTRATION ACCEPT message with new service area restrictions shall act as described in subclause 5.3.5.

If the Service area list IE is not included in the REGISTRATION ACCEPT message, any tracking area in the registered PLMN and its equivalent PLMN(s) is considered as an allowed tracking area as described in subclause 5.3.5.

The AMF shall include the MICO indication IE in the REGISTRATION ACCEPT only if the MICO indication IE was included in the REGISTRATION REQUEST message, the AMF supports and accepts the use of MICO mode. If the AMF supports and accepts the use of MICO mode, the AMF may indicate "all PLMN registration area allocated" in the MICO indication IE in the REGISTRATION ACCEPT message. If "all PLMN registration area allocated" is indicated in the MICO indication IE, the AMF shall not assign and include the TAI list in the REGISTRATION ACCEPT message. If the REGISTRATION ACCEPT message includes an MICO indication IE indicating "all PLMN registration area allocated", the UE shall treat all TAIs in the current PLMN as a registration area and delete its old TAI list.

The AMF may include the T3512 value IE in the REGISTRATION ACCEPT message only if the REGISTRATION REQUEST message was sent over the 3GPP access.

The AMF may include the non-3GPP de-registration timer value IE in the REGISTRATION ACCEPT message only if the REGISTRATION REQUEST message was sent for the non-3GPP access.

If the REGISTRATION ACCEPT message includes an MICO indication IE indicating "all PLMN registration area allocated", the UE shall treat all TAIs in the current PLMN as a registration area and delete its old TAI list.

If the REGISTRATION ACCEPT message included a T3512 value IE, the UE shall use the value in T3512 value IE as periodic registration update timer (T3512). If the T3512 value IE is not included, the UE shall use the value currently stored, e.g. from a prior REGISTRATION ACCEPT message.

If the REGISTRATION ACCEPT message included a non-3GPP de-registration timer value IE, the UE shall use the value in non-3GPP de-registration timer value IE as non-3GPP de-registration timer. If non-3GPP de-registration timer value IE is not included, the UE shall use the value currently stored, e.g. from a prior REGISTRATION ACCEPT message.

If the REGISTRATION ACCEPT message contains a 5G-GUTI, the UE shall return a REGISTRATION COMPLETE message to the AMF to acknowledge the received 5G-GUTI, stop timer T3519 if running, and delete any stored SUCI.

Upon receiving a REGISTRATION COMPLETE message, the AMF shall stop timer T3550 and change to state 5GMM-REGISTERED. The 5G-GUTI, if sent in the REGISTRATION ACCEPT message, shall be considered as valid.

If the REGISTRATION REQUEST message contained the SMS requested bit indicating that the UE supports SMS delivery over NAS and:

a) the SMSF address is stored in the UE 5GMM context and:

   1) the UE is considered available for SMS; or

   2) the UE is considered not available for SMS and the SMSF has confirmed that the activation of the SMS service is successful; or

b) the SMSF address is not stored in the UE 5GMM context, the SMSF selection is successful and the SMSF has confirmed that the activation of the SMS service is successful;

then the AMF shall include the SMS allowed IE in the REGISTRATION ACCEPT message as specified in subclause 5.5.1.2.4. If the UE 5GMM context does not contain an SMSF address or the UE is not considered available for SMS, then the AMF shall:

a) store the SMSF address in the UE 5GMM context if not stored already; and

b) store the contents of the SMS allowed IE in the UE 5GMM context and consider the UE available for SMS.

If SMSF selection in the AMF or SMS activation via the SMSF is not successful, then the AMF shall not include the SMS allowed IE in the REGISTRATION ACCEPT message. If the AMF does not allow the use of SMS over NAS, then the AMF shall not include the SMS allowed IE in the REGISTRATION ACCEPT message.

If the REGISTRATION REQUEST message contained the SMS requested bit set to "SMS over NAS not supported", then the AMF shall:

a) mark the 5GMM context to indicate that the UE is not available for SMS over NAS; and

NOTE: The AMF can notify the SMSF that the UE is deregistered from SMS over NAS based on local configuration.

b) not include the SMS allowed IE in the REGISTRATION ACCEPT message.

If the AMF includes an SMS allowed IE in the REGISTRATION ACCEPT message and the UE is also registered over another access to the same PLMN, the UE considers the new value indicated by the SMS allowed IE as applicable for both accesses over which the UE is registered.

The AMF shall include the allowed NSSAI for the current PLMN and may include the mapping of each S-NSSAI of the allowed NSSAI to the S-NSSAI(s) of the configured NSSAI for the HPLMN contained in the requested NSSAI from the UE if available, in the REGISTRATION ACCEPT message if the UE included the requested NSSAI in the REGISTRATION REQUEST message and the AMF allows one or more S-NSSAIs in the requested NSSAI. The AMF may also include rejected NSSAI in the REGISTRATION ACCEPT message. Rejected NSSAI contains S-NSSAI(s) which was included in the requested NSSAI but rejected by the network associated with rejection cause(s).

The AMF may include a new configured NSSAI for the current PLMN in the REGISTRATION ACCEPT message if the REGISTRATION REQUEST message did not include the requested NSSAI, or the REGISTRATION REQUEST message included the requested NSSAI containing an S-NSSAI that is not valid in the serving PLMN. If a new configured NSSAI for the current PLMN is included, the AMF may also include the mapping of the configured NSSAI for the current PLMN to the configured NSSAI for the HPLMN in the REGISTRATION ACCEPT message.

If the S-NSSAI(s) associated with the existing PDU session(s) of the UE is not included in the requested NSSAI of the REGISTRATION REQUEST message, the AMF shall release the PDU session(s) associated with the S-NSSAI(s) locally and shall request the SMF to release those PDU session(s) locally, without peer-to-peer signalling between the SMF and the UE.

The UE receiving the rejected NSSAI in the REGISTRATION ACCEPT message takes the following actions based on the rejection cause in the rejected NSSAI:

"S-NSSAI not available in the current PLMN"

The UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the current PLMN as specified in subclause 4.6.2.2 and not attempt to use this S-NSSAI in the current PLMN until switching off the UE or the UICC containing the USIM is removed.

"S-NSSAI not available in the current registration area"

The UE shall add the rejected S-NSSAI(s) in the rejected NSSAI for the current PLMN and registration area combination as specified in subclause 4.6.2.2 and not attempt to use this S-NSSAI in the current registration area until switching off the UE, the UE moving out of the current registration area or the UICC containing the USIM is removed.

If the UE did not include the requested NSSAI in the REGISTRATION REQUEST message or none of the requested NSSAI are present in the subscribed S-NSSAIs, and one or more subscribed S-NSSAIs marked as default are available, the AMF shall put the subscribed S-NSSAIs marked as default in the allowed NSSAI of the REGISTRATION ACCEPT message. The AMF shall determine a registration area such that all S-NSSAIs of the allowed NSSAI are available in the registration area.

If the REGISTRATION ACCEPT message contains the allowed NSSAI, then the UE shall store the included allowed NSSAI together with the PLMN identity of the registered PLMN and the registration area as specified in subclause 4.6.2.2. If the UE has one or more PDU sessions associated with S-NSSAI(s) not included in the received allowed NSSAI, the UE shall locally release all such PDU session(s).

If the REGISTRATION ACCEPT message contains a configured NSSAI IE with a new configured NSSAI for the current PLMN and optionally the mapping of the configured NSSAI for the current PLMN to the configured NSSAI for the HPLMN, the UE shall store the contents of the configured NSSAI IE as specified in subclause 4.6.2.2.

If the Uplink data status IE is included in the REGISTRATION REQUEST message, the AMF shall:

a) indicate the SMF to re-establish the user-plane resources for the corresponding PDU session; and

b) include PDU session reactivation result IE in the REGISTRATION ACCEPT message to indicate the user-plane resources reactivation result of the PDU sessions the UE requested to re-establish.

If the Uplink data status IE is not included in the REGISTRATION REQUEST message and the REGISTRATION REQUEST message is sent for the trigger d) in subclause 5.5.1.3.2, the AMF may indicate the SMF to re-establish the user-plane resources for the PDU sessions.

If a PDU session status IE is included in the REGISTRATION REQUEST message, the AMF shall:

a) release all those PDU session locally (without peer-to-peer signalling between the SMF and the UE) which are in 5GSM state PDU SESSION ACTIVE on the AMF side associated with the access type the REGISTRATION REQUEST message is sent over, but are indicated by the UE as being in 5GSM state PDU SESSION INACTIVE; and

b) include a PDU session status IE in the REGISTRATION ACCEPT message to indicate which PDU sessions associated with the access type the REGISTRATION REQUEST message is sent over are active in the AMF.

If the Allowed PDU session status IE is included in the REGISTRATION REQUEST message, the AMF shall:

a) indicate the SMF to re-establish the user-plane resources for the corresponding PDU sessions allowed to be re-established over 3GPP access and have indicated pending downlink data if there is at least one PDU session indicated in the Allowed PDU session status IE that can be re-established over 3GPP access;

b) notify the SMF that have indicated pending downlink data, that reactivation of the user-plane resources for the corresponding PDU sessions cannot be performed if not allowed to be re-established over 3GPP access, if any; and

c) include the PDU session reactivation result IE in the REGISTRATION ACCEPT message to indicate the successfully re-established user-plane resources for the corresponding PDU sessions, if any.

If the AMF has included the PDU session reactivation result IE in the REGISTRATION ACCEPT message and there exist one or more PDU sessions for which the user-plane resources cannot be re-established, then the AMF may include the PDU session reactivation result error cause IE to indicate the cause of failure to re-establish the user-plane resources.

If the AMF needs to initiate PDU session status synchronization the AMF shall include a PDU session status IE in the REGISTRATION ACCEPT message to indicate the UE which PDU sessions are active in the AMF.

The AMF may include the LADN information in the REGISTRATION ACCEPT message as described in subclause 5.5.1.2.4. The UE, upon receiving the REGISTRATION ACCEPT message with the LADN information, shall delete its old LADN information (if any) and store the received new LADN information.

If the AMF does not include the LADN information in the REGISTATION ACCEPT message during registration procedure for mobility and registration update, the UE shall delete its old LADN information.

If the PDU session status IE is included in the REGISTRATION ACCEPT message, the UE shall release all those PDU sessions locally (without peer-to-peer signalling between the SMF and the UE) which are in 5GSM state PDU SESSION ACTIVE on the UE side, but are indicated by the AMF as being in 5GSM state PDU SESSION INACTIVE.

The network informs the UE about the support of specific features, such as IMS voice over PS session, emergency services or emergency services fallback, in the 5GS network feature support information element. In a UE with IMS voice over PS session capability, the IMS voice over PS session indicator, emergency services and emergency services fallback indicator shall be provided to the upper layers. The upper layers take the IMS voice over PS session indicator into account when selecting the access domain for voice sessions or calls. When initiating an emergency call, the upper layers take the IMS voice over PS session indicator, emergency services indicator and emergency services fallback indicator into account for the access domain selection. When the UE determines via the IMS voice over PS session indicator that the network does not support IMS voice over PS sessions in N1 mode, then the UE shall not locally release any persistent PDU session. When the UE determines via the emergency service support indicator that the network does not support emergency services in N1 mode, then the UE shall not locally release any emergency PDU session if there is a radio bearer associated with that context.

The AMF shall set the EMF bit in the 5GS network feature support IE to:

a) "Emergency services fallback supported in NR connected to 5GCN and E-UTRA connected to 5GCN" if the network supports the emergency services fallback procedure when the UE is in an NR cell connected to 5GCN or an E-UTRA cell connected to 5GCN;

b) "Emergency services fallback supported in NR connected to 5GCN only" if the network supports the emergency services fallback procedure when the UE is in an NR cell connected to 5GCN and does not support the emergency services fallback procedure when the UE is in an E-UTRA cell connected to 5GCN;

c) "Emergency services fallback supported in E-UTRA connected to 5GCN only" if the network supports the emergency services fallback procedure when the UE is in an E-UTRA cell connected to 5GCN and does not support the emergency services fallback procedure when the UE is in an NR cell connected to 5GCN; or

d) "Emergency services fallback not supported" if network does not support the emergency services fallback procedure when the UE is in any cell connected to 5GCN.

The network informs the UE that the use of access identity 1 is valid in the RPLMN or equivalent PLMN by setting the MPS indicator bit of the 5GS network feature support IE to "Access identity 1 valid in RPLMN or equivalent PLMN", in the REGISTRATION ACCEPT message. Based on operator policy, the AMF sets the MPS indicator bit in the REGISTRATION ACCEPT message based on the MPS priority information in the user’s subscription context obtained from the UDM.

Upon receiving a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 valid in RPLMN or equivalent PLMN", if the UE is not in the country of its HPLMN, the UE shall act as a UE with access identity 1 configured for MPS as described in subclause 4.5.2, in all NG-RAN TAs of the registered PLMN and its equivalent PLMNs. The MPS indicator bit in the 5GS network feature support IE provided in the REGISTRATION ACCEPT message is valid until the UE receives a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 not valid in RPLMN or equivalent PLMN" or until the UE selects a non-equivalent PLMN. Access identity 1 is only applicable while the UE is in N1 mode.

During ongoing active PDU sessions that were set up relying on the MPS indicator bit being set to "Access identity 1 valid in RPLMN or equivalent PLMN", if the network indicates in a registration update that the MPS indicator bit is reset to "Access identity 1 not valid in RPLMN or equivalent PLMN", then the UE shall no longer act as a UE with access identity 1 configured for MPS as described in subclause 4.5.2 unless the USIM contains a valid configuration for access identity 1 in RPLMN or equivalent PLMN. In the UE, the ongoing active PDU sessions are not affected by the change of the MPS indicator bit.

If the UE has indicated "follow-on request pending" in REGISTRATION REQUEST message, or the network has downlink signalling pending, the AMF shall not immediately release the NAS signalling connection after the completion of the registration procedure.

If the Requested DRX Parameters IE was included in the REGISTRATION REQUEST message, the AMF shall include the UE specific DRX parameters IE in the REGISTRATION ACCEPT message. The AMF may set the UE specific DRX parameters IE based on the received Requested DRX Parameters IE and operator policy if available.

If the UE included in the REGISTRATION REQUEST message the UE status information IE with the EMM registration status set to "UE in EMM-REGISTERED state" and the AMF does not support N26 interface, the AMF shall operate as described in subclause 5.5.1.2.4.

If due to regional subscription restrictions or access restrictions the UE is not allowed to access the TA, but the UE has a PDU session for emergency services established, the AMF may accept the REGISTRATION REQUEST message and indicate to the SMF to release all non-emergency PDU sessions when the registration procedure is initiated in 5GMM-CONNECTED mode. When the registration procedure is initiated in 5GMM-IDLE mode, the AMF indicates to the SMF to release all non-emergency PDU sessions and informs the UE via the PDU session status IE in the REGISTRATION ACCEPT message. The AMF shall not indicate to the SMF to release the emergency PDU session. The network shall consider the UE to be registered for emergency service.

If the REGISTRATION ACCEPT message includes the transparent container IE and:

a) the transparent container IE does not successfully pass the integrity check (see 3GPP TS 33.501 [24]); and

b) if the UE attempts obtaining service on another PLMNs as specified in 3GPP TS 23.122 [5] annex C;

then the UE shall locally release the established NAS signalling connection.

If the REGISTRATION ACCEPT message includes the transparent container IE and the transparent container IE successfully passes the integrity check (see 3GPP TS 33.501 [24]):

a) the UE shall proceed with the behavior as specified in 3GPP TS 23.122 [5] annex C; and

b) if the UE attempts obtaining service on another PLMNs as specified in 3GPP TS 23.122 [5] annex C then the UE may locally release the established NAS signalling connection, otherwise the UE shall send a REGISTRATION COMPLETE message. If an acknowledgement is requested in the transparent container IE of the REGISTRATION ACCEPT message, the UE acknowledgement is included in the transparent container IE of the REGISTRATION COMPLETE message.

5.5.1.3.5 Mobility and periodic registration update not accepted by the network

If the mobility and periodic registration update request cannot be accepted by the network, the AMF shall send a REGISTRATION REJECT message to the UE including an appropriate 5GMM cause value.

The UE shall take the following actions depending on the 5GMM cause value received in the REGISTRATION REJECT message.

#3 (Illegal UE);

#6 (Illegal ME); or

#7 (5GS services not allowed).

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall consider the USIM as invalid for 5GS services until switching off or the UICC containing the USIM is removed. The UE shall delete the list of equivalent PLMNs and shall move to 5GMM-DEREGISTERED state.

If the UE is operating in single-registration mode, the UE shall handle 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the normal tracking area updating procedure is rejected with the EMM 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. If the UE is in EMM-REGISTERED state, the UE shall move to EMM-DEREGISTERED state.

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

The UE shall set the 5GS update status to 5U2 NOT UPDATED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall enter the state 5GMM-DEREGISTERED.

If the rejected request was not for initiating a PDU session for emergency services, the UE shall subsequently, automatically initiate the initial registration procedure.

NOTE 1: User interaction is necessary in some cases when the UE cannot re-establish the PDU session(s) automatically.

If the UE is operating in single-registration mode, the UE shall handle 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the normal tracking area updating procedure is rejected with the EMM cause with the same value.

#10 (implicitly de-registered).

The UE shall enter the state 5GMM-DEREGISTERED.NORMAL-SERVICE. The UE shall delete any mapped 5G security context or partial native 5G security context.

If the registration rejected request was not for initiating a PDU session for emergency bearer services, the UE shall perform a new registration procedure for initial registration.

NOTE 2: User interaction is necessary in some cases when the UE cannot re-establish the PDU session(s) automatically.

If the UE is operating in single-registration mode and the UE is in EMM-REGISTERED state, the UE shall move to EMM-DEREGISTERED state.

#11 (PLMN not allowed).

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall store the PLMN identity in the "forbidden PLMN list", delete the list of equivalent PLMNs, reset the registration attempt counter and enter the state 5GMM-DEREGISTERED.PLMN-SEARCH. The UE shall perform a PLMN selection according to 3GPP TS 23.122 [5].

If the UE is operating in single-registration mode, the UE shall in addition delete any 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the normal tracking area updating procedure is rejected with the EMM cause with the same value. The UE shall move to EMM-DEREGISTERED state.

#12 (Tracking area not allowed).

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. Additionally, the UE shall reset the registration attempt counter.

The UE shall store the current TAI in the list of "5GS forbidden tracking areas for regional provision of service" and enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE.

If the UE is operating in single-registration mode, the UE shall handle 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the normal tracking area updating procedure is rejected with the EMM cause with the same value.

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

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. Additionally, the UE shall delete the list of equivalent PLMNs and reset the registration attempt counter.

The UE shall store the current TAI in the list of "5GS forbidden tracking areas for roaming" and enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE or optionally 5GMM-DEREGISTERED.PLMN-SEARCH. The UE shall perform a PLMN selection according to 3GPP TS 23.122 [5].

If the UE is operating in single-registration mode, the UE shall handle 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the normal tracking area updating procedure is rejected with the EMM cause with the same value.

#22 (Congestion).

If the T3346 value IE is present in the REGISTRATION REJECT message and the value indicates that this timer is neither zero nor deactivated, the UE shall proceed as described below, otherwise it shall be considered as an abnormal case and the behaviour of the UE for this case is specified in subclause 5.5.1.3.6.

The UE shall abort the registration procedure for mobility and periodic registration update. If the rejected request was not for initiating a PDU session for emergency services, the UE shall set the 5GS update status to 5U2 NOT UPDATED and change to state 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE.

The UE shall stop timer T3346 if it is running.

If the REGISTRATION REJECT message is integrity protected, the UE shall start timer T3346 with the value provided in the T3346 value IE.

If the REGISTRATION REJECT message is not integrity protected, the UE shall start timer T3346 with a random value from the default range specified in 3GPP TS 24.008 [12].

The UE stays in the current serving cell and applies the normal cell reselection process. The registration procedure for mobility and periodic registration update is started, if still necessary, when timer T3346 expires or is stopped.

#27 (N1 mode not allowed).

The UE capable of S1 mode shall disable the N1 mode capability for both 3GPP access and non-3GPP access (see subclause 4.9).

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 following abnormal cases can be identified:

a) Timer T3346 is running.

The UE shall not start the registration procedure for mobility and periodic registration update unless:

1) the UE is in 5GMM-CONNECTED mode;

2) the UE received a paging;

3) the UE receives a NOTIFICATION message over non-3GPP access when the UE is in 5GMM-CONNECTED mode over non-3GPP access and in 5GMM-IDLE mode over 3GPP access;

4) the UE is a UE configured for high priority access in selected PLMN; or

5) the UE has a PDU session for emergency services established or is establishing a PDU session for emergency services

The UE stays in the current serving cell and applies the normal cell reselection process.

NOTE: It is considered an abnormal case if the UE needs to initiate a registration procedure for mobility and periodic registration update while timer T3346 is running independent on whether timer T3346 was started due to an abnormal case or a non-successful case.

b) The lower layers indicate that the access attempt is barred.

The UE shall not start the registration procedure for mobility and periodic registration update. The UE stays in the current serving cell and applies the normal cell reselection process.

The registration procedure for mobility and periodic registration update is started, if still needed, when the lower layers indicate that the barring is alleviated for the access category with which the access attempt was associated.

Editor's note: Abnormal case handling for N1 NAS signalling connection establishment rejected by the network with "Extended wait time" received from lower layers is FFS.

c) T3510 timeout.

The UE shall abort the registration update procedure and the NAS signalling connection, if any, shall be released locally, the registration attempt counter shall be incremented, unless it was already set to 5.

d) REGISTRATION REJECT message, other 5GMM cause values than those treated in subclause 5.5.1.3.5, and cases of 5GMM cause value #22, if considered as abnormal cases according to subclause 5.5.1.3.5.

upon reception of the 5GMM causes #95, #96, #97, #99 and #111 the UE should set the registration attempt counter to 5.

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

If the registration attempt counter is less than 5:

- if the TAI of the current serving cell is not included in the TAI list or the 5GS update status is different to 5U1 UPDATED, the UE shall start timer T3511, shall set the 5GS update status to 5GU2 NOT UPDATED and change to state 5GMM-REGISTERED.ATTEMPTING-TO-UPDATE. When timer T3511 expires the registration update procedure is triggered again.

- if the TAI of the current serving cell is included in the TAI list and the 5GS update status is equal to 5U1 UPDATED, the UE shall keep the 5GS update status to 5GU1 UPDATED and enter statue 5GMM-REGISTERED.NORMAL-SERVICE. The UE shall start timer T3511.

- If the UE is operating in single registration mode, the UE shall in addition handle the EPS update status as specified in 3GPP TS 24.301 [15] for the abnormal cases when a normal or periodic tracking area updating procedure fails and the tracking area attempt counter is less than 5 and the EPS update status is different from EU1 UPDATED

If the registration attempt counter is equal to 5

- the UE shall start timer T3502, shall set the 5GS update status to 5U2 NOT UPDATED.

- the UE shall delete the list of equivalent PLMNs and shall change to state 5GMM-REGISTERED.ATTEMPTING-TO-UPDATE or optionally to 5GMM-REGISTERED.PLMN-SEARCH in order to perform a PLMN selection according to 3GPP TS 23.122 [5].

- if the UE is operating in single registration mode:

- the UE shall in addition handle the EPS update status as specified in 3GPP TS 24.301 [15] for the abnormal cases when a normal or periodic tracking area updating procedure fails and the tracking area attempt counter is equal to 5; and

- if the UE does not change to state 5GMM-REGISTERED.PLMN-SEARCH, the UE shall attempt to select E-UTRAN radio access technology. The UE may disable N1 mode capability as specified in subclause 4.9.

5.5.1.3.7 Abnormal cases on the network side

Editor's note: Abnormal cases in the network are FFS.

5.5.2 De-registration procedure

5.5.2.1 General

The de-registration procedure is used:

a) by the UE to de-register for 5GS services over 3GPP access when the UE is registered over 3GPP access;;

b) by the UE to de-register for 5GS services over 3GPP access, non-3GPP access, or both when the UE is registered in the same PLMN over both accesses;

c) by the network to inform the UE that it is deregistered for 5GS services over 3GPP access when the UE is registered over 3GPP access;

d) by the network to inform the UE that it is deregistered for 5GS services over 3GPP access, non-3GPP access, or both when the UE is registered in the same PLMN over both accesses; and

e) by the network to inform the UE to re-register to the network.

The de-registration procedure with appropriate de-registration type shall be invoked by the UE:

a) if the UE is switched off; and

b) as part of the eCall inactivity procedure defined in subclause 5.5.3.

The de-registration procedure with appropriate de-registration type shall be invoked by the network:

a) if the network informs whether the UE should re-register to the network.

The de-registration procedure with appropriate access type shall be invoked by the UE:

a) if the UE wants to de-register for 5GS services over 3GPP access when the UE is registered over 3GPP access; or

b) the UE wants to de-register for 5GS services over 3GPP access, non-3GPP access, or both when the UE is registered in the same PLMN over both accesses.

If the de-registration procedure is triggered due to USIM removal, the UE shall indicate "switch off" in the de-registration type IE.

If the de-registration procedure is requested by the UDM for a UE that has PDU sessions for emergency services, the AMF shall not send a DEREGISTRATION REQUEST message to the UE.

If the de-registration procedure for 5GS services is performed, the PDU sessions, if any, for this particular UE are released locally without peer-to-peer signalling between the UE and the network.

The UE is allowed to initiate the de-registration procedure even if the timer T3346 is running.

NOTE: When the UE has no PDU sessions over non-3GPP access, or the UE moves all the PDU sessions over a non-3GPP access to a 3GPP access, the UE and the AMF need not initiate de-registration over the non-3GPP access.

The AMF shall provide the UE with a non-3GPP de-registration timer.

5.5.2.2 UE-initiated de-registration procedure

5.5.2.2.1 UE-initiated de-registration procedure initiation

The de-registration procedure is initiated by the UE by sending a DEREGISTRATION REQUEST message (see example in figure 5.5.2.2.1). The De-registration type IE included in the message indicates whether the de-registration procedure is due to a "switch off" or not. The access type included in the message indicates whether the de-registration procedure is:

a) for 5GS services over 3GPP access when the UE is registered over 3GPP access only;

b) for 5GS services over non-3GPP access when the UE is registered over non-3GPP access only; or

c) for 5GS services over 3GPP access, non-3GPP access or both 3GPP access and non-3GPP access when the UE is registered in the same PLMN over both accesses.

If the UE has a valid 5G-GUTI, the UE shall populate the 5GS mobile identity IE with the valid 5G-GUTI. If the UE does not have a valid 5G-GUTI, the UE shall populate the 5GS mobile identity IE with its SUCI.

If the UE does not have a valid 5G-GUTI and it does not have a valid SUCI, then the UE shall populate the5GSmobile identity IE with its PEI.

If the de-registration request is not due to switch off and the UE is in the state 5GMM-REGISTERED or 5GMM-REGISTERED-INITIATED, timer T3521 shall be started in the UE after the DEREGISTRATION REQUEST message has been sent. The UE shall enter the state 5GMM-DEREGISTERED-INITIATED.

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

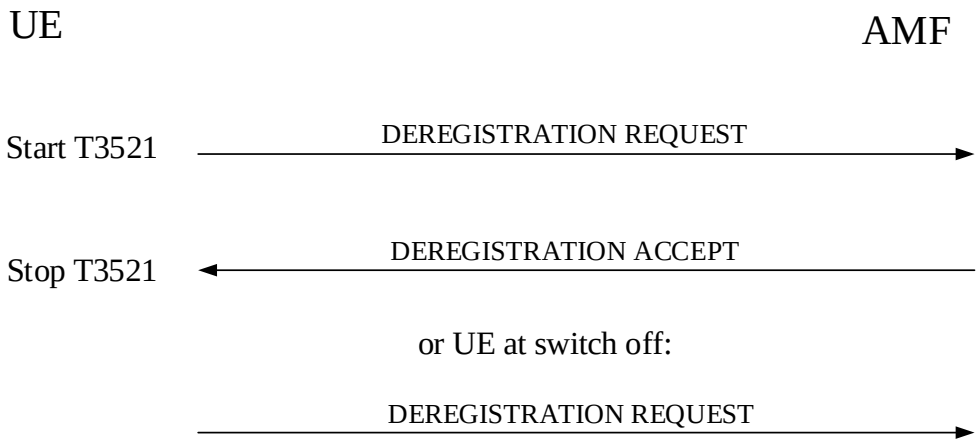


Figure 5.5.2.2.1.1: UE-initiated de-registration procedure

5.5.2.2.2 UE-initiated de-registration procedure completion - common procedure

When the DEREGISTRATION REQUEST message is received by the AMF, the AMF shall send a DEREGISTRATION ACCEPT message to the UE, if the De-registration type IE does not indicate "switch off". Otherwise, the procedure is completed when the AMF receives the DEREGISTRATION REQUEST message.

The UE, when receiving the DEREGISTRATION ACCEPT message, shall stop timer T3521.

5.5.2.2.3 UE-initiated de-registration procedure completion for 5GS services over 3GPP access

If the access type in the DEREGISTRATION REQUEST message indicates that the de-registration procedure is for 3GPP access, the AMF shall trigger the SMF to release the PDU session context(s) established over 3GPP access, if any, locally for this UE without peer-to-peer signalling between the UE and the SMF. The UE shall release the PDU session context(s) established over 3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE is marked as inactive in the AMF for 5GS services for 3GPP access. The AMF shall enter the state 5GMM-DEREGISTERED for 3GPP access.

If the UE supports N1 mode only then:

a) if the de-registration procedure was performed due to disabling of 5GS services, then the UE shall enter the 5GMM-NULL state for 3GPP access;

b) otherwise, the UE shall enter the 5GMM-DEREGISTERED state for 3GPP access.

5.5.2.2.4 UE-initiated de-registration procedure completion for 5GS services non-3GPP access

If the access type in the DEREGISTRATION REQUEST indicates that the de-registration procedure is for non-3GPP access, the AMF shall trigger SMF to release the PDU session context(s) established over non-3GPP access, if any, locally for this UE without peer-to-peer signalling between the UE and the SMF. The UE shall release the PDU session context(s) established over non-3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE is marked as inactive in the AMF for 5GS services for non-3GPP access. The AMF shall enter the state 5GMM-DEREGISTERED over non-3GPP access.

The UE shall:

- if the de-registration procedure was performed due to disabling of 5GS services, enter the 5GMM-NULL state for non-3GPP access;

- otherwise, enter the 5GMM-DEREGISTERED state for non-3GPP access.

5.5.2.2.5 UE-initiated de-registration procedure completion for 5GS services over both 3GPP access and non-3GPP access

If the access type in the DEREGISTRATION REQUEST indicates that the de-registration procedure is for both 3GPP access and non-3GPP access when the UE is registered in the same PLMN over both accesses, the descriptions for UE-initiated de-registration procedure completion for 5GS services over 3GPP access and over non-3GPP access, as specified in subclauses 5.5.2.2.3 and 5.5.2.2.4, shall be followed.

5.5.2.2.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Lower layer failure or release of the N1 NAS signalling connection before reception of DEREGISTRATION ACCEPT message.

The de-registration procedure shall be aborted and the UE proceeds as follows:

1) if the de-registration procedure was performed due to disabling of 5GS services, the UE shall enter the 5GMM-NULL state; or

2) if the de-registration type "normal de-registration" was requested for reasons other than disabling of 5GS services, the UE shall enter the 5GMM-DEREGISTERED state.

b) The lower layers indicate that the access attempt is barred.

The UE shall not start the de-registration procedure. The UE stays in the current serving cell and applies the normal cell reselection process.

The UE may perform a local de-registration either immediately or after an implementation-dependent time.

The de-registration procedure is started, if still needed, when the lower layers indicate that the barring is alleviated for the access category with which the access attempt was associated.

Editor's note: Abnormal case handling for N1 NAS signalling connection establishment rejected by the network with "Extended wait time" received from lower layers is FFS.

c) T3521 timeout.

On the first four expiries of the timer, the UE shall retransmit the DEREGISTRATION REQUEST message and shall reset and restart timer T3521. On the fifth expiry of timer T3521, the detach procedure shall be aborted and the UE proceeds as follows:

1) if the de-registration procedure was performed due to disabling of 5GS services, the UE shall enter the 5GMM-NULL state; or

2) if the de-registration type "normal de-registration" was requested for reasons other than disabling of 5GS services, the UE shall enter the 5GMM-DEREGISTERED state.

d) De-registration procedure collision.

De-registration containing de-registration type "switch off":

- If the UE receives a DEREGISTRATION REQUEST message before the UE-initiated de-registration procedure has been completed, this message shall be ignored and the UE-initiated de-registration procedure shall continue.

Otherwise:

- If the UE receives a DEREGISTRATION REQUEST message before the UE-initiated de-registration procedure has been completed, it shall treat the message as specified in subclause 5.5.2.3.2 with the following modification:

  - If the DEREGISTRATION REQUEST message received by the UE contains de-registration type "re-registration required", and the UE-initiated de-registration procedure is with de-registration type "normal de-registration", the UE need not initiate the registration procedure for initial registration.

e) De-registration and 5GMM common procedure collision.

De-registration containing de-registration type "switch off":

- If the UE receives a message used in a 5GMM common procedure before the de-registration procedure has been completed, this message shall be ignored and the de-registration procedure shall continue.

Otherwise:

- If the UE receives a message used in a 5GMM common procedure before the de-registration procedure has been completed, both the 5GMM common procedure and the de-registration 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 de-registration procedure is completed, the de-registration procedure shall be aborted and re-initiated after successfully performing a registration procedure for mobility or periodic update. If the de-registration procedure was initiated due to removal of the USIM or the UE is to be switched off, the UE shall abort the de-registration procedure and enter the state 5GMM-DEREGISTERED.

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

If the current TAI is not in the TAI list, the de-registration procedure shall be aborted and re-initiated after successfully performing a registration procedure for mobility or periodic update. If the detach procedure was initiated due to removal of the USIM or the UE is to be switched off, the UE shall abort the de-registration procedure and enter the state 5GMM-DEREGISTERED.

If the current TAI is still part of the TAI list, the UE shall restart the de-registration procedure.

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

The UE shall restart the de-registration procedure.

5.5.2.2.7 Abnormal cases in the network side

Apart from the case described in subclauses 5.5.2.2.2 and 5.5.2.2.3, no abnormal cases have been identified.

5.5.2.3 Network-initiated de-registration procedure

5.5.2.3.1 Network-initiated de-registration procedure initiation

The network initiates the de-registration procedure by sending a DEREGISTRATION REQUEST message to the UE (see example in figure 5.5.2.3.1.1).

NOTE: If the AMF performs a local de-registration, it will inform the UE with a 5GMM messages (e.g. SERVICE REJECT message or REGISTRATION REJECT message) with 5GMM cause #10 "implicitly de-registered" only when the UE initiates a 5GMM procedure.

The network may include a 5GMM cause IE to specify the reason for the DEREGISTRATION REQUEST message. The network shall start timer T3522. The network shall indicate whether re-registration is needed or not in the De-registration type IE. The network shall also indicate via the access type whether the de-registration procedure is:

a) for 3GPP access; or

b) for 3GPP access, non-3GPP access or both when the UE is registered in the same PLMN for both accesses.

The AMF shall trigger the SMF to release the PDU session context(s) over the indicated access(es), if any, for the UE locally and enter state 5GMM-DEREGISTERED-INITIATED.

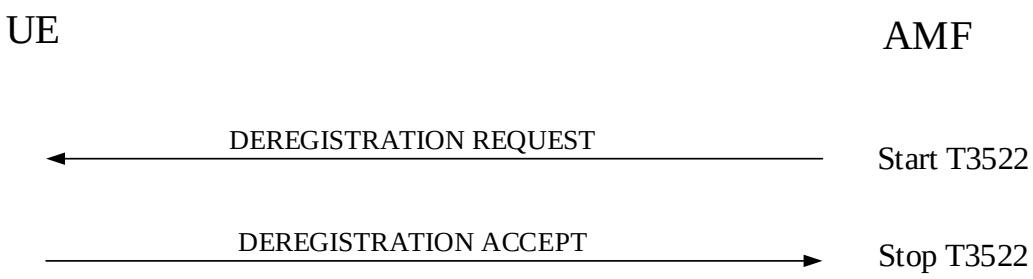


Figure 5.5.2.3.1.1: Network-initiated de-registration procedure

5.5.2.3.2 Network-initiated de-registration procedure completion by the UE

Upon receiving the DEREGISTRATION REQUEST message, and the DEREGISTRATION REQUEST message indicates "re-registration required" and the de-registration request is for 3GPP access, the UE shall release the PDU sessions over 3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE shall stop the timer(s) T3346, T3396, T35cd and T35ef, if any is running. The UE shall ignore the 5GMM cause IE if received. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for 3GPP access. Furthermore, the UE shall, after the completion of the de-registration procedure, and the release of the existing NAS signalling connection, initiate an initial registration. The UE should also re-establish any previously established PDU sessions.

Editor's note: It is FFS to use which timer for T35cd.

Editor's note: It is FFS to use which timer for T35ef.

Upon receiving the DEREGISTRATION REQUEST message and the DEREGISTRATION REQUEST message indicates "re-registration required" and the de-registration request is for non-3GPP access, the UE shall release the PDU sessions over non-3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE shall stop the timer(s) T3346, T3396, T35cd and T35ef, if any is running. The UE shall ignore the 5GMM cause IE if received. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for non-3GPP access. Furthermore, the UE shall, after the completion of the de-registration procedure, and the release of the existing NAS signalling connection, initiate an initial registration over non-3GPP. The UE should also re-establish any previously established PDU sessions.

Upon receiving the DEREGISTRATION REQUEST message and the DEREGISTRATION REQUEST message indicates "re-registration required" and the de-registration request is for both 3GPP access and non-3GPP access when the UE is registered in the same PLMN for both accesses, the UE shall release the PDU sessions over both 3GPP access and non-3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE shall stop the timer(s) T3346, T3396, T35cd and T35ef, if any is running. The UE shall ignore the 5GMM cause IE if received. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for both 3GPP access and non-3GPP access. Furthermore, the UE shall, after the completion of the de-registration procedure, and the release of the existing NAS signalling connection, initiate an initial registration over both 3GPP access and non-3GPP access. The UE should also re-establish any previously established PDU sessions.

NOTE 1: When the de-registration type indicates "re-registration required", user interaction is necessary in some cases when the UE cannot re-establish the PDU session (s), if any, automatically.

Upon receiving the DEREGISTRATION REQUEST message and the DEREGISTRATION REQUEST message indicates "re-registration not required" and the de-registration request is for 3GPP access, the UE shall release the PDU sessions over 3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for 3GPP access.

Upon receiving the DEREGISTRATION REQUEST message and the DEREGISTRATION REQUEST message indicates "re-registration not required" and the de-registration request is for non-3GPP access, the UE shall release the PDU sessions over non-3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for non-3GPP access.

Upon receiving the DEREGISTRATION REQUEST message and the DEREGISTRATION REQUEST message indicates "re-registration not required" and the de-registration request is for both 3GPP access and non-3GPP access when the UE is registered in the same PLMN for both accesses, the UE shall release the PDU sessions over both 3GPP access and non-3GPP access, if any, locally without peer-to-peer signalling between the UE and the SMF. The UE shall send a DEREGISTRATION ACCEPT message to the network and enter the state 5GMM-DEREGISTERED for both 3GPP access and non-3GPP access.

Upon sending a DEREGISTRATION ACCEPT message, the UE shall delete the rejected NSSAI as specified in subclause 4.6.2.2.

If the de-registration type indicates "re-registration required", then the UE shall ignore the 5GMM cause IE if received.

If the de-registration type indicates "re-registration not required", the UE shall take the actions depending on the received 5GMM cause value:

#3 (Illegal UE);

#6 (Illegal ME); or

#7 (5GS services not allowed).

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall consider the USIM as invalid for 5GS 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 5GMM-DEREGISTERED.

A UE operating in single-registration mode shall handle the EMM parameters, EMM state, 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when a DETACH REQUEST is received with the EMM cause with the same value and with detach type set to "re-attach not required".

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.

#11 (PLMN not allowed).

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall delete the list of equivalent PLMNs, shall reset the registration attempt counter and enter the state 5GMM-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 [5].

A UE operating in single-registration mode shall handle the EMM parameters, EMM state, 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when a DETACH REQUEST is received with the EMM 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 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall reset the registration attempt counter and shall enter the state 5GMM-DEREGISTERED.LIMITED-SERVICE.

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

A UE operating in single-registration mode shall handle the EMM parameters, EMM state, 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when a DETACH REQUEST is received with the EMM 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 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall reset the registration attempt counter and shall change to state 5GMM-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 [5]

A UE operating in single-registration mode the UE shall handle the EMM parameters, EMM state, 4G-GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when a DETACH REQUEST is received with the EMM cause with the same value and with detach type set to "re-attach not required".

#27 (N1 mode not allowed).

The UE capable of S1 mode shall disable the N1 mode capability for both 3GPP access and non-3GPP access (see subclause 4.9).

5.5.2.3.3 Network-initiated de-registration procedure completion by the network

The network shall stop timer T3522 upon receipt of the DEREGISTRATION ACCEPT message. The network shall enter state 5GMM-DEREGISTERED for 3GPP access if the de-registration request is for 3GPP access. The network shall enter state 5GMM-DEREGISTERED for non-3GPP access if the de-registration request is for non-3GPP access. The network shall enter state 5GMM-DEREGISTERED for both 3GPP access and non-3GPP access if the de-registration request is for both 3GPP access and non-3GPP access.

5.5.2.3.4 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Transmission failure of DEREGISTRATION ACCEPT message indication from lower layers.

The de-registration procedure shall be progressed and the UE shall send the DEREGISTRATION ACCEPT message.

b) DEREGISTRATION REQUEST, other 5GMM cause values than those treated in subclause 5.5.2.3.2 or no 5GMM cause IE is included, and the De-registration type IE indicates "re-registration not required".

The UE shall delete 5G-GUTI, TAI list, last visited registered TAI, list of equivalent PLMNs, ngKSI, shall set the 5GS update status to 5U2 NOT UPDATED and shall start timer T3502.

A UE not supporting S1 mode may enter the state 5GMM-DEREGISTERED.PLMN-SEARCH in order to perform a PLMN selection according to 3GPP TS 23.122 [5]; otherwise the UE shall enter the state 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION.

A UE operating in single-registration mode shall set the EPS update status to EU2 NOT UPDATED and shall delete the EMM parameters 4G-GUTI, last visited registered TAI, TAI list and eKSI and shall enter the state EMM-DEREGISTERED.

5.5.2.3.5 Abnormal cases in the network side

The following abnormal cases can be identified:

a) T3522 time-out

On the first expiry of the timer, the network shall retransmit the DEREGISTRATION REQUEST message and shall start timer T3522. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3522, the de-registration procedure shall be aborted.

b) Lower layer failure

The de-registration procedure is aborted.

c) De-registration procedure collision

If the network receives a DEREGISTRATION REQUEST message with "switch off" indication, before the network-initiated de-registration procedure has been completed, both procedures shall be considered completed.

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

d) De-registration and registration procedure for initial registration collision

If the network receives a REGISTRATION REQUEST message indicating either "initial registration" or "5GS emergency registration" in the 5GS registration type IE before the network-initiated de-registration procedure with de-registration type "re-registration required" has been completed, the network shall aborted the de-registration procedure and the registration procedure shall be progressed after the PDU sessions associated with the access type the REGISTRATION REQUEST message is sent over have been deleted.

e) De-registration and registration procedure for mobility and periodic registration update collision

If the network sent a DEREGISTRATION REQUEST message indicating "re-registration required" in the De-registration type IE and the network receives a REGISTRATION REQUEST message indicating either "mobility registration updating" or "mobility registration updating" in the 5GS registration type IE before the network-initiated de-registration procedure has been completed, the de-registration procedure shall be progressed, i.e. the REGISTRATION REQUEST message shall be ignored.

f) De-registration and service request procedure collision

If the network receives a SERVICE REQUEST message before the network-initiated de-registration procedure has been completed (e.g. the DEREGISTRATION REQUEST message is pending to be sent to the UE) and the DEREGISTRATION REQUEST contains de-registration type "re-registration required", the network shall progress the de-registration procedure.

5.5.3 eCall inactivity procedure

The eCall inactivity procedure is applicable only to a UE configured for eCall only mode as specified in 3GPP TS 31.102 [22]. The procedure shall be started when:

a) the UE is in any 5GMM-REGISTERED substate except substates 5GMM-REGISTERED.PLMN-SEARCH or 5GMM-REGISTERED.NO-CELL-AVAILABLE;

b) the UE is in 5GMM-IDLE mode; and

c) one of the following conditions applies:

1) timer T3444 expires or is found to have already expired and timer T3445 is not running;

2) timer T3445 expires or is found to have already expired and timer T3444 is not running; or

3) timers T3444 and T3445 expire or are found to have already expired.

NOTE: Timers T3444 and T3445 are specified in 3GPP TS 24.301 [15].

The UE shall then perform the following actions:

a) stop other running timers (e.g. T3511, T3512);

b) if the UE is currently registered to the network for 5GS services, perform a de-registration procedure;

c) delete any 5G-GUTI, TAI list, last visited registered TAI, list of equivalent PLMNs, and ngKSI; and

d) enter 5GMM-DEREGISTERED.eCALL-INACTIVE state.

5.6 5GMM connection management procedures

5.6.1 Service request procedure

5.6.1.1 General

The purpose of the service request procedure is to change the 5GMM mode from 5GMM-IDLE to 5GMM-CONNECTED mode, and/or to request the establishment of user-plane resources for PDU sessions which are activated without user-plane resources. In latter case, the 5GMM mode can be the 5GMM-IDLE mode or the 5GMM-CONNECTED mode if the UE requires to activate user-plane resources for PDU sessions. This procedure is used when:

- the network has downlink signalling pending over 3GPP access and the UE is in 5GMM-IDLE mode over 3GPP access;
- the network has downlink signalling pending over non-3GPP access, the UE is in 5GMM-IDLE mode over non-3GPP access and in 5GMM-IDLE or 5GMM-CONNECTED mode over 3GPP access;
- the UE has uplink signalling pending over 3GPP access and the UE is in 5GMM-IDLE mode over 3GPP access;
- the network has downlink user data pending over 3GPP access and the UE is in 5GMM-IDLE mode over 3GPP access;
- the network has downlink user data pending over non-3GPP access, the UE is in 5GMM-IDLE mode over non-3GPP access and in 5GMM-IDLE or 5GMM-CONNECTED mode over 3GPP access;
- the UE has user data pending over 3GPP access and the UE is in 5GMM-IDLE or 5GMM-CONNECTED mode over 3GPP access;
- the UE has user data pending over non-3GPP access and the UE is in 5GMM-CONNECTED mode over non-3GPP access;
- the UE in 5GMM-IDLE mode over non-3GPP access, receives an indication from the lower layers of non-3GPP access, that the access stratum connection is established between UE and network; or
- the UE in 5GMM-IDLE or 5GMM-CONNECTED mode over 3GPP access receives a request for emergency service from the upper layer and performs emergency services fallback as specified in subclause 4.13.4.2 of 3GPP TS 23.502 [9].

This procedure shall not be used for initiating user data transfer or PDU session related signalling related to a PDU session for LADN when the UE is located outside the LADN service area.

The service request procedure is initiated by the UE, however, it can be triggered by the network by means of:

- the paging procedure (see subclause 5.6.2) for the transfer of downlink signalling or user data pending over 3GPP access to a UE in 5GMM-IDLE mode over 3GPP access;
- the paging procedure (see subclause 5.6.2) for the transfer of downlink signalling or user data pending over non-3GPP access to a UE in 5GMM-IDLE mode over 3GPP access and in 5GMM-IDLE mode over non-3GPP access;
- the notification procedure (see subclause 5.6.3) for the transfer of downlink signalling or user data pending over non-3GPP access to a UE in 5GMM-CONNECTED mode over3GPP access and in 5GMM-IDLE mode over non-3GPP access; or
- the notification procedure (see subclause 5.6.3) for the transfer of downlink signalling or user data pending over 3GPP access to a UE in 5GMM-IDLE mode over 3GPP access and in 5GMM-CONNECTED mode over non-3GPP access.

NOTE: In case the UE is in 5GMM-IDLE mode over 3GPP access and in 5GMM-CONNECTED mode over non-3GPP access and downlink signalling or user data pending over 3GPP access needs to be transferred, the AMF can trigger either the notification procedure or the paging procedure based on implementation.

The UE shall invoke the service request procedure when:

a) the UE, in 5GMM-IDLE mode over 3GPP access, receives a paging request from the network;

b) the UE, in 5GMM-CONNECTED mode over 3GPP access, receives a notification from the network with access type indicating non-3GPP access;

c) the UE, in 5GMM-IDLE mode over 3GPP access, has uplink signalling pending;

d) the UE, in 5GMM-IDLE mode over 3GPP access, has uplink user data pending;

e) the UE, in 5GMM-CONNECTED mode, has user data pending due to no user-plane resources established for PDU session(s) used for user data transport;

f) the UE in 5GMM-IDLE mode over non-3GPP access, receives an indication from the lower layers of non-3GPP access, that the access stratum connection is established between UE and network;

g) the UE, in 5GMM-IDLE mode over 3GPP access, receives a notification from the network with access type indicating 3GPP access when the UE is in 5GMM-CONNECTED mode over non-3GPP access; or

h) the UE in 5GMM-IDLE or 5GMM-CONNECTED mode over 3GPP access receives a request for emergency service from the upper layer and performs emergency services fallback as specified in subclause 4.13.4.2 of 3GPP TS 23.502 [9].

The UE shall not invoke the service request procedure when the UE is in the state 5GMM-SERVICE-REQUEST-INITIATED.

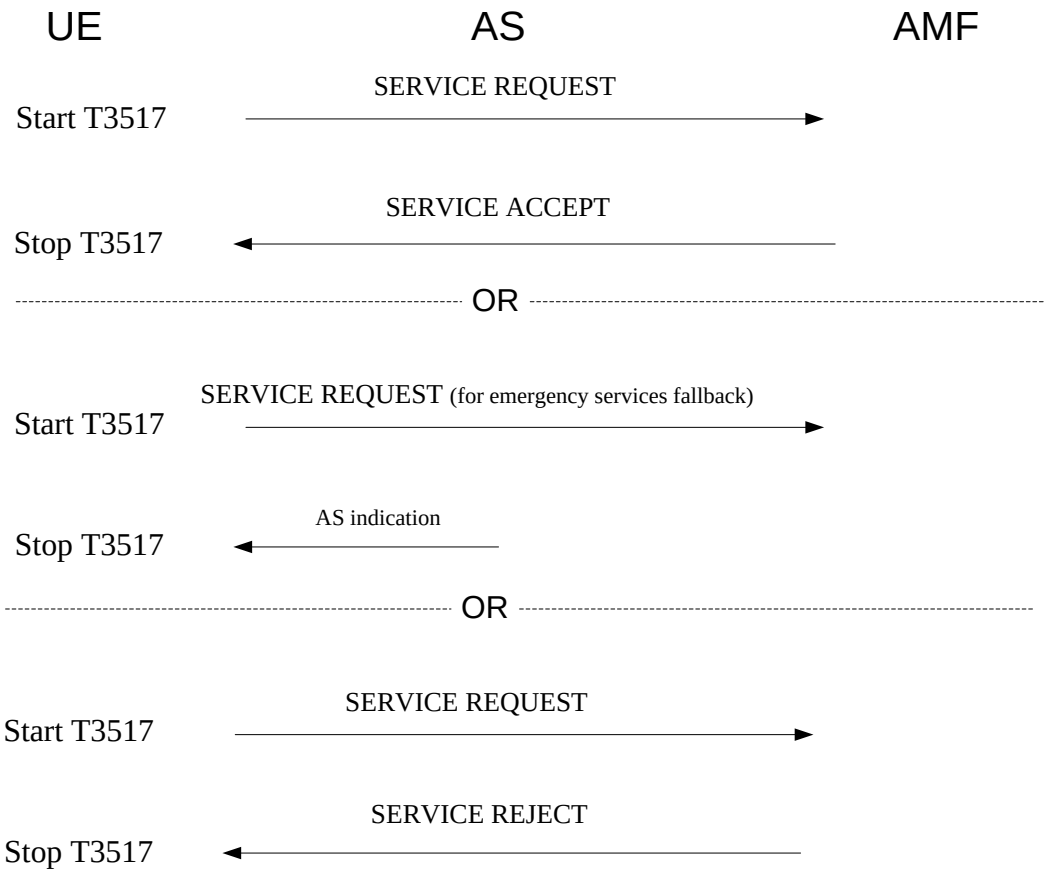


Figure 5.6.1.1.1: Service Request procedure

5.6.1.2 Service request procedure initiation

The UE initiates the service request procedure by sending a SERVICE REQUEST message to the AMF and starts timer T3517.

For case a), b) and g) in subclause 5.6.1.1, the service type IE in the SERVICE REQUEST message shall be set to "mobile terminated services".

For case c), d), e) and f) in subclause 5.6.1.1, if the UE is a UE configured for high priority access in selected PLMN, the service type IE in the SERVICE REQUEST message shall be set to "high priority access".

For case a) in subclause 5.6.1.1:

a) if the paging request includes an indication for non-3GPP access type, the Allowed PDU session status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) for which the UE allows the user-plane resources to be re-establish over 3GPP access or if there is no PDU session(s) for which the UE allows the user-plane resources to be re-established over 3GPP access;

b) if the UE has uplink user data pending to be sent, the Uplink data status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) for which the UE has pending user data to be sent; or

c) otherwise, the Uplink data status IE shall not be included in the SERVICE REQUEST message.

For case b) in subclause 5.6.1.1, the Allowed PDU session status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) for which the UE allows the user-plane resources to be re-established over 3GPP access or if there is no PDU session(s) for which the UE allows the user-plane resources to be re-established over 3GPP access.

For case c) in subclause 5.6.1.1, the Uplink data status IE shall not be included in the SERVICE REQUEST message except if the UE has one or more active always-on PDU sessions. The UE shall set the service type IE in the SERVICE REQUEST message to "emergency services", if the SERVICE REQUEST message is triggered by a request for emergency services from the upper layer and both the UE and the network support emergency services in N1 mode. Otherwise, if the UE is not a UE configured for high priority access in selected PLMN, the UE shall set the service type IE to "signalling".

For cases d) and e) in subclause 5.6.1.1, the Uplink data status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) the UE has pending user data to be sent. If the UE is not a UE configured for high priority access in selected PLMN, the service type IE in the SERVICE REQUEST message shall be set to "data".

For case f) in subclause 5.6.1.1:

a) if the UE has uplink user data pending to be sent, the Uplink data status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) the UE has pending user data to be sent. If the UE is not a UE configured for high priority access in selected PLMN, the service type IE in the SERVICE REQUEST message shall be set to "data";

b) otherwise, if the UE is not a UE configured for high priority access in selected PLMN, the service type IE in the SERVICE REQUEST message shall be set to "signalling".

For case g) in subclause 5.6.1.1, if the UE has uplink user data pending to be sent, the Uplink data status IE shall be included in the SERVICE REQUEST message to indicate the PDU session(s) the UE has pending user data to be sent.

For case h) in subclause 5.6.1.1, if the UE receives a request for emergency service from the upper layer and performs emergency services fallback as specified in subclause 4.13.4.2 of 3GPP TS 23.502 [9], the UE shall send a SERVICE REQUEST message with service type set to "emergency services fallback".

The UE shall include a valid 5G-S-TMSI in the 5G-S-TMSI IE of the SERVICE REQUEST message.

If the UE has one or more active always-on PDU sessions and the user-plane resources for these PDU sessions are not established, the UE shall include the Uplink data status IE in the SERVICE REQUEST message and indicate that the UE has pending user data to be sent for those PDU sessions.

The PDU session status information element may be included in the SERVICE REQUEST message to indicate the PDU session(s) available in the UE associated with the access type the SERVICE REQUEST message is sent over. If the PDU session status information element is included in the SERVICE REQUEST message, then the AMF shall release all those PDU sessions locally (without peer-to-peer signalling between the UE and the network) which are in active on the AMF side associated with the access type the SERVICE REQUEST message is sent over, but are indicated by the UE as being inactive, and shall request the SMF to release all those PDU sessions locally.

5.6.1.3 Common procedure initiation

Upon receipt of the SERVICE REQUEST message, the AMF may initiate the common procedures e.g. the 5G AKA based primary authentication and key agreement procedure or the EAP based primary authentication and key agreement procedure.

5.6.1.4 Service request procedure accepted by the network

For cases a), b), c), d), e), f) and g) in subclause 5.6.1.1, the UE shall treat the reception of the SERVICE ACCEPT message as successful completion of the procedure and stop timer T3517 and enter the state 5GMM-REGISTERED.

For case h) in subclause 5.6.1.1, the UE shall treat the indication from the lower layers when the UE has changed to S1 mode or E-UTRA connected to 5GCN (see 3GPP TS 23.502 [9]) as successful completion of the procedure and stop timer T3517.

If the AMF needs to initiate PDU session status synchronization or a PDU session status IE was included in the SERVICE REQUEST message, the AMF shall include a PDU session status IE in the SERVICE ACCEPT message to indicate which PDU sessions associated with the access type the SERVICE ACCEPT message is sent over are active in the AMF. If the PDU session status information element is included in the SERVICE ACCEPT message, then the UE shall release all those PDU sessions locally (without peer-to-peer signalling between the network and the UE) which are in active on the UE side associated with the access type the SERVICE ACCEPT message is sent over, but are indicated by the AMF as being inactive.

If the Uplink data status IE is included in the SERVICE REQUEST message, the AMF shall:

a) indicate the SMF to re-establish the user-plane resources for the corresponding PDU sessions;

b) include the PDU session reactivation result IE in the SERVICE ACCEPT message to indicate the user-plane resources reactivation result of the PDU sessions the UE requested to re-establish ;

c) determine the UE presence in LADN service area and forward the UE presence in LADN service area towards the SMF, if the corresponding PDU session is a PDU session for LADN; and

d) include a cause #43 "LADN not available" to indicate the user-plane resources of the PDU session is not activated in the PDU session reactivation result error cause IE of the SERVICE ACCEPT message, if the corresponding PDU session is a PDU session for LADN and the SMF indicated to the AMF that the UE is located outside the LADN service area.

If the Allowed PDU session status IE is included in the SERVICE REQUEST message, the AMF shall:

a) indicate the SMF to re-establish the user-plane resources for the corresponding PDU sessions allowed to be re-established over 3GPP access and have indicated pending downlink data if there is at least one PDU session that indicated in the Allowed PDU session status IE can be re-established over 3GPP access;

b) notify the SMF that have indicated pending downlink data, that reactivation of the user-plane resources for the corresponding PDU sessions cannot be performed if not allowed to be re-established over 3GPP access; and

c) include the PDU session reactivation result IE in the SERVICE ACCEPT message to indicate the successfully reactivated user-plane resources for the corresponding PDU sessions, if any.

If the AMF has included the PDU session reactivation result IE in the SERVICE ACCEPT message and there exist one or more PDU sessions for which the user-plane resources cannot be re-established, then the AMF may include the PDU session reactivation result error cause IE to indicate the cause of failure to re-establish the user-plane resources.

If the SERVICE REQUEST message is for emergency services fallback, the AMF triggers the emergency services fallback procedure as specified in subclause 4.13.4.2 of 3GPP TS 23.502 [9].

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 5GMM cause value and stop timer T3517.

If the AMF needs to initiate PDU session status synchronisation or a PDU session status IE was included in the SERVICE REQUEST message, the AMF shall include a PDU session status IE in the SERVICE REJECT message to

indicate which PDU sessions associated with the access type the SERVICE REJECT message is sent over are active in the AMF. If the PDU session status IE is included in the SERVICE REJECT message, then the UE shall release all those PDU sessions locally (without peer-to-peer signalling between the network and the UE) which are active on the UE side associated with the access type the SERVICE REJECT message is sent over, but are indicated by the AMF as being inactive.

On receipt of the SERVICE REJECT message, if the message is integrity protected, the UE shall stop timer T3517 if running.

If the service request for mobile originated services is rejected due to general NAS level mobility management congestion control, the network shall set the 5GMM cause value to #22 "congestion" and assign a value for back-off timer T3346.

If the AMF determines that the UE is in a non-allowed area or is not in an allowed area as specified in subclause 5.3.5, then:

a) if the service type IE in the SERVICE REQUEST message is set to "signalling" or "data", the AMF shall send a SERVICE REJECT message with the 5GMM cause value set to #28 "Restricted service area";

b) otherwise, if the service type IE in the SERVICE REQUEST message is set to "mobile terminated services", "emergency services", "emergency services fallback" or "high priority access", the AMF shall continue the process as specified in subclause 5.6.1.4 unless for other reasons the service request cannot be accepted.

The UE shall take the following actions depending on the 5GMM cause value received in the SERVICE REJECT message.

#3 (Illegal UE);

#6 (Illegal ME); or

#7 (5GS services not allowed).

The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.2.2) and shall delete any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall consider the USIM as invalid for 5GS services until switching off or the UICC containing the USIM is removed. The UE shall enter the state 5GMM-DEREGISTERED.

If S1 mode is supported by the UE, the UE shall handle the EMM parameters EMM state, GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the service request procedure is rejected with the EMM 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.

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

The UE shall set the 5GS update status to 5U2 NOT UPDATED (and shall store it according to subclause 5.1.3.2.2) and shall delate any 5G-GUTI, last visited registered TAI, TAI list and ngKSI. The UE shall enter the state 5GMM-DEREGISTERED.

If the service request was initiated for emergency services fallback, the UE shall attempt to select an E-UTRA cell connected to EPC or 5GCN according to the emergency services support indicator. If the UE finds a suitable E-UTRA cell, it then proceeds with the appropriate EMM or 5GMM procedures.

If the service request was initiated for any reason other than emergency services fallback or initiating a PDU session for emergency services, the UE shall perform a new initial registration procedure.

NOTE 2: User interaction is necessary in some cases when the UE cannot re-activate the PDU session(s) automatically.

If the UE is operating in the single-registration mode, the UE shall handle the EMM parameters EMM state, GUTI, last visited registered TAI, TAI list and eKSI as specified in 3GPP TS 24.301 [15] for the case when the service request procedure is rejected with the EMM cause with the same value.

#10 (Implicitly de-registered).

The UE shall enter the state 5GMM-DEREGISTERED.NORMAL-SERVICE. The UE shall delete any mapped 5G NAS security context or partial native 5G NAS security context.

If the rejected request was not for initiating a PDU session for emergency services, the UE shall perform a new initial registration procedure.

NOTE 3: User interaction is necessary in some cases when the UE cannot re-establish the PDU session(s) automatically.

If S1 mode is supported by the UE, the UE shall handle the EMM state as specified in 3GPP TS 24.301 [15] for the case when the service request procedure is rejected with the EMM cause with the same value.

#22 (Congestion).

If the T3346 value IE is present in the SERVICE REJECT message and the value indicates that this timer is neither zero nor deactivated, the UE shall proceed as described below, otherwise it shall be considered as an abnormal case and the behaviour of the UE for this case is specified in subclause 5.6.1.6.

If the rejected request was not for initiating a PDU session for emergency services, the UE shall abort the service request procedure and enter state 5GMM-REGISTERED, and stop timer T3517 if still running.

The UE shall stop timer T3346 if it is running.

If the SERVICE REJECT message is integrity protected, the UE shall start timer T3346 with the value provided in the T3346 value IE.

If the SERVICE REJECT message is not integrity protected, the UE shall start timer T3346 with a random value from the default range specified in 3GPP TS 24.008 [12].

For all other cases the UE stays in the current serving cell and applies normal cell reselection process. The service request procedure is started, if still necessary, when timer T3346 expires or is stopped.

#27 (N1 mode not allowed).

The UE capable of S1 mode shall disable the N1 mode capability for both 3GPP access and non-3GPP access (see subclause 4.9).

#28 (Restricted service area).

The UE shall perform the registration procedure for mobility and periodic registration update (see subclause 5.5.1.3).

5.6.1.6 Service request procedure for initiating a PDU session for emergency services not accepted by the network

If the service request for initiating a PDU session for emergency 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 of the failure of the procedure; or

NOTE 1: This can result in the upper layers requesting another emergency call attempt using domain selection as specified in 3GPP TS 23.167 [6].

b) de-register locally, if not de-registered already, attempt initial registration for emergency services.

If the service request for initiating a PDU session for emergency services fails due to abnormal cases a) in subclause 5.6.1.7, 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 message was attempted, the UE shall:

a) inform the upper layers of the failure of the procedure; or

NOTE 2: This can result in the upper layers requesting another emergency call attempt using domain selection as specified in 3GPP TS 23.167 [6] and 3GPP TS 24.229 [14].

b) de-register locally, if not de-registered already, attempt initial registration for emergency services.

5.6.1.7 Abnormal cases in the UE

The following abnormal cases can be identified:

a) T3517 expired.

The UE shall enter the state 5GMM-REGISTERED.

If the UE triggered the service request procedure in 5GMM-IDLE mode, then the 5GMM sublayer shall abort the procedure and release locally any resources allocated for the service request procedure.

If the UE triggered the service request procedure in 5MM-CONNECTED mode, the 5GMM sublayer shall abort the procedure, and stay in 5GMM-CONNECTED mode.

b) The lower layers indicate that the access attempt is barred.

The UE shall not start the service request procedure. The UE stays in the current serving cell and applies the normal cell reselection process.

If the event which triggered the access attempt was an MO-MMTEL-voice-call-started indication, an MO-MMTEL-video-call-started indication or an MO-SMSoIP-attempt-started indication and:

1) if the UE in 5GMM-IDLE mode is operating in the single-registration mode and the UE's usage setting is "voice centric", the UE may attempt to select an E-UTRA cell connected to EPC. If the UE finds a suitable E-UTRA cell connected to EPC, it then proceeds with the service request procedure as described in 3GPP TS 24.301 [15];

Editor's note: It is FFS whether the UE is recommended to attempt to select E-UTRA cell connected to EPC in this case.

2) if the UE is operating in the dual-registration mode, the UE may proceed with the service request procedure as described in 3GPP TS 24.301 [15]; or

3) otherwise, the UE NAS layer shall notify the upper layers that the access attempt is barred. In this case, upon receiving an indication from the lower layers that the barring is alleviated for the access category with which the access attempt was associated, the NAS shall notify the upper layers that the barring is alleviated for the access category. Otherwise, the service request procedure is started, if still needed, when the lower layers indicate that the barring is alleviated for the access category with which the access attempt was associated.

Editor's note: Abnormal case handling for N1 NAS signalling connection establishment rejected by the network with "Extended wait time" received from lower layers is FFS.

c) Timer T3346 is running.

The UE shall not start the service request procedure unless:

1) the UE receives a paging;

2) the UE receives a NOTIFICATION message over non-3GPP access when the UE is in 5GMM-CONNECTED mode over non-3GPP access and in 5GMM-IDLE mode over 3GPP access;

3) the UE receives a NOTIFICATION message over 3GPP access when the UE is in 5GMM-CONNECTED mode over 3GPP access and in 5GMM-IDLE mode over non-3GPP access;

4) the UE is a UE configured for high priority access in selected PLMN; or

5) the UE has a PDU session for emergency services established or is establishing a PDU session for emergency services;

If the UE is in 5GMM-IDLE mode, the UE stays in the current serving cell and applies normal cell reselection process. The service request procedure is started, if still necessary, when timer T3346 expires or is stopped.

d) Registration procedure for mobility and periodic registration update is triggered.

The UE shall abort the service request procedure, stop timer T3517, if running and perform the registration procedure for mobility and periodic registration update. The "follow-on request pending" indication shall be set in the REGISTRATION REQUEST message.

e) Switch off.

If the UE is in state 5GMM-SERVICE-REQUEST-INITIATED at switch off, the de-registration procedure shall be performed.

f) De-registration procedure collision.

If the UE receives a DEREGISTRATION REQUEST message from the network in state 5GMM-SERVICE-REQUEST-INITIATED, the UE shall progress the DEREGISTRATION REQUEST message and the service request procedure shall be aborted.

5.6.1.8 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure.

If a lower layer failure occurs before a SERVICE REJECT message has been sent to the UE or the service request procedure has been completed by the AMF, the AMF enters/stays in 5GMM-IDLE.

b) Protocol error.

If the SERVICE REQUEST message is received with a protocol error, the AMF shall return a SERVICE REJECT message with one of the following 5GMM cause values:

#96 invalid mandatory information;

#99 information element non-existent or not implemented;

#100 conditional IE error; or

#111 protocol error, unspecified.

The AMF stays in the current 5GMM mode.

c) More than one SERVICE REQUEST message received before the procedure has been completed (i.e., before SERVICE REJECT message has been sent or service request procedure has 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 AMF shall continue with the previous service request procedure and shall not treat any further this SERVICE REQUEST message.

d) REGISTRATION REQUEST message received with "initial registration" or "emergency registration" in the 5GS registration type IE before a SERVICE REJECT message has been sent or the service request procedure has been completed.

If a REGISTRATION REQUEST message with "initial registration" or "emergency registration" in the 5GS registration type IE is received and the service request procedure has not been completed or a SERVICE REJECT message has not been sent, the AMF may initiate the 5GMM common procedures, e.g. the primary authentication and key agreement procedure. The AMF may e.g. after a successful primary authentication and key agreement procedure execution, abort the service request procedure, delete the 5GMM context, indicate towards the SMF that the 5GMM context has been deleted and progress the new REGISTRATION REQUEST message.

e) REGISTRATION REQUEST message received with "mobility registration updating" or "periodic registration updating" in the 5GS registration type IE received before the service request procedure has been completed or a SERVICE REJECT message has been sent.

If a REGISTRATION REQUEST message with "mobility registration updating" or "periodic registration updating" in the 5GS registration type IE is received and the service request procedure has not been completed or a SERVICE REJECT message has not been sent, the AMF may initiate the 5GMM common procedures, e.g. the primary authentication and key agreement procedure. The AMF may e.g. after a successful primary authentication and key agreement procedure execution, abort the service request procedure and progress the new REGISTRATION REQUEST message.

5.6.2 Paging procedure

5.6.2.1 General

The paging procedure is performed only in 3GPP access and used by the network to request the establishment of an NAS signalling connection to the UE. The paging procedure is also used by the network to request the UE to re-establish the user-plane resources of PDU sessions for downlink user data transport. Another purpose of the paging procedure is to request the UE to re-establish the user-plane resources of PDU session(s) associated with non-3GPP access over 3GPP access.

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

5.6.2.2 Paging for 5GS services

5.6.2.2.1 General

The network shall initiate the paging procedure for 5GS services when NAS signalling messages or user data is pending to be sent to the UE in 5GMM-IDLE mode (see example in figure 5.6.2.2.1).

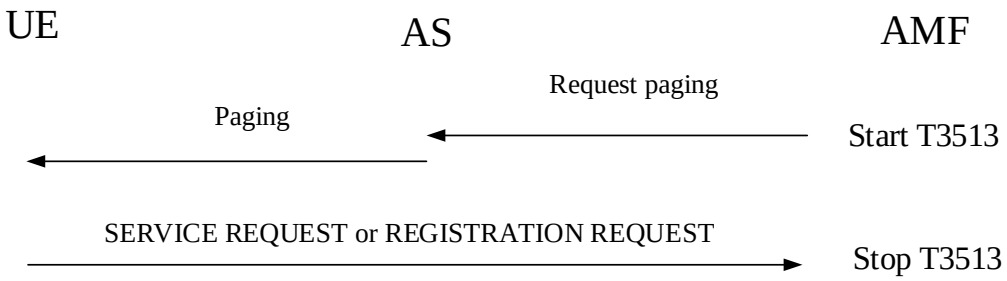


Figure 5.6.2.2.1.1: Paging procedure

To initiate the procedure the 5GMM entity in the AMF requests the lower layer to start paging and shall start timer T3513. Upon reception of a paging indication, the UE shall initiate a service request procedure to respond to the paging (see 3GPP TS 23.502 [9]).

If downlink signalling or user data is pending to be sent over non-3GPP access, the 5GMM entity in the AMF shall indicate the lower layer that the paging is due to signalling or user data associated to non-3GPP access.

Upon reception of a paging indication, the UE shall stop the timer T3346, if running, and shall initiate:

- a service request procedure over 3GPP access to respond to the paging as specified in subclauses 5.6.1; or
- a registration procedure for mobility and periodic registration update over 3GPP access to respond to the paging as specified in subclauses 5.5.1.3.

The network shall stop timer T3513 for the paging procedure when an integrity-protected response is received from the UE and successfully integrity checked by the network. If the response received is not integrity protected, or the integrity check is unsuccessful, timer T3513 for the paging procedure shall be kept running.

Upon expiry of timer T3513, the network may reinitiate paging.

If the network, while waiting for a response to the paging sent without paging priority, receives downlink signalling or downlink data associated with priority user-plane resources for PDU sessions, the network shall stop the timer for the paging procedure (i.e. either timer T3413), and then initiate the paging procedure with paging priority.

5.6.2.2.2 Abnormal cases on the network side

The following abnormal case can be identified:

a) REGISTRATION REQUEST message indicating either "initial registration" or "5GS emergency registration" in the 5GS registration type IE is received when paging procedure is ongoing.

   If an integrity-protected REGISTRATION REQUEST message is received from the UE and successfully integrity checked by the network, the network shall abort the paging procedure. If the REGISTRATION REQUEST message received is not integrity protected, or the integrity check is unsuccessful, the paging procedure shall be progressed. The paging procedure shall be aborted when the primary authentication and key agreement procedure performed during the registration procedure for initial registration is completed successfully.

5.6.2.2.3 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Paging message received with access type set to non-3GPP access while the UE is in 5GMM-CONNECTED mode over non-3GPP access.

   The UE shall not respond to paging message.

5.6.3 Notification procedure

5.6.3.1 General

The notification procedure is used by the network:

a) to request the UE, by sending the NOTIFICATION message over 3GPP access, to re-establish the user-plane resources of PDU session(s) associated with non-3GPP access over 3GPP access when the UE is in 5GMM-IDLE mode over non-3GPP access and in 5GMM-CONNECTED mode over 3GPP access; or

b) to request the UE, by sending the NOTIFICATION message over non-3GPP access, to re-establish user-plane resources of the PDU session(s) associated with 3GPP access over 3GPP access when the UE is in 5GMM-CONNECTED mode over non-3GPP access and in 5GMM-IDLE mode over 3GPP access when the UE is not in MICO mode.

5.6.3.2 Notification procedure initiation

The network shall initiate the notification procedure by sending the NOTIFICATION message to the UE and start timer T3565 (see example in figure 5.6.3.2.1).

For case a) in subclause 5.6.3.1, the NOTIFICATION message is sent from the network to the UE via 3GPP access with access type indicating non-3GPP access.

For case b) in subclause 5.6.3.1, the NOTIFICATION message is sent from the network to the UE via non-3GPP access with access type indicating 3GPP access when the UE is not in MICO mode.

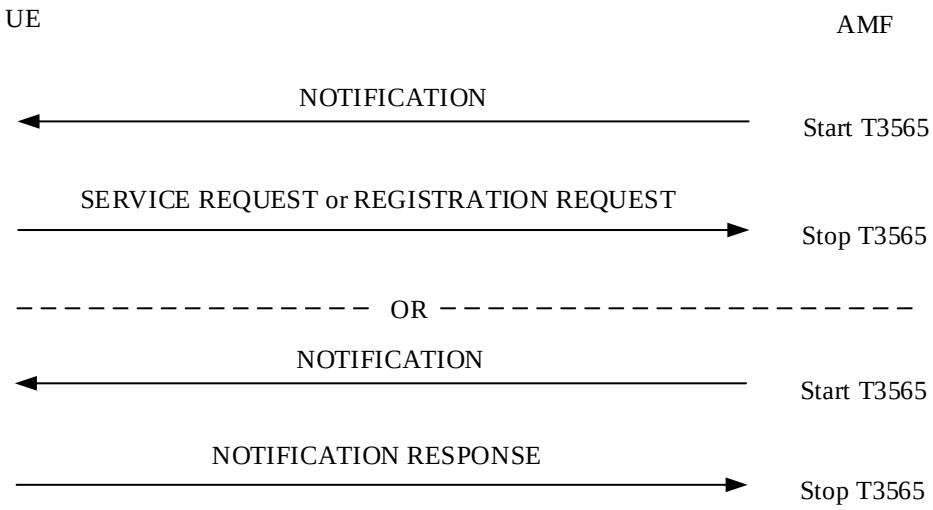


Figure 5.6.3.2.1: Notification procedure

For case a) in subclause 5.6.3.1, upon reception of NOTIFICATION message, the UE shall initiate a service request procedure over 3GPP access as specified in subclauses 5.6.1.

For case b) in subclause 5.6.3.1, upon reception of NOTIFICATION message:

a) if the UE is in 5GMM-REGISTERED.NORMAL-SERVICE state, the UE shall initiate a service request procedure over 3GPP access as specified in subclauses 5.6.1;

b) if the UE is in 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE state, the UE shall initiate a registration procedure for mobility and periodic registration update over 3GPP access as specified in subclauses 5.5.1.3; or

c) if the UE is in 5GMM-REGISTERED.NO-CELL-AVAILABLE state or 5GMM-REGISTERED.PLMN-SEARCH state, the UE shall respond with NOTIFICATION RESPONSE message indicating failure to re-establish the user plane resources of PDU sessions.

Upon reception of NOTIFICATION message:

For case b) in subclause 5.6.3.1, if the UE is in 5GMM-REGISTERED.NO-CELL-AVAILABLE state or 5GMM-REGISTERED.PLMN-SEARCH state and the PDU sessions associated with the 3GPP access are locally released in the UE;

then the UE shall respond with NOTIFICATION RESPONSE message indicating with the PDU session status information element that its PDU sessions are locally released.

Upon reception of a NOTIFICATION message, the UE shall stop the timer T3346, if running.

5.6.3.3 Notification procedure completion

Upon reception of SERVICE REQUEST message or REGISTRATION REQUEST message, the AMF shall stop T3565 and proceed service request procedure as specified in subclauses 5.6.3.1 or registration procedure for mobility and periodic registration update as specified in subclauses 5.5.1.3. If no user-plane resources of PDU session(s) need to be re-established, the AMF should notify the SMF that the UE was reachable but did not accept to re-establish the user-plane resources of PDU session(s).

Upon reception of NOTIFICATION RESPONSE message, the AMF shall stop T3565 and should notify the SMF that the UE is unreachable, and:

- For case b) in subclause 5.6.3.1, if the NOTIFICATION RESPONSE message includes the PDU session status information element indicating that the PDU sessions associated with the 3GPP access are inactive in the UE, then the AMF shall release all those PDU sessions locally (without peer-to-peer signalling between the UE and

the network) which are active on the AMF side associated with 3GPP access, but are indicated by the UE as being inactive, and shall request the SMF to release all those PDU sessions locally.

5.6.3.4 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3565.

The network shall, on the first expiry of the timer T3565, retransmit the NOTIFICATION message and shall reset and start timer T3565. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3565, the procedure shall be aborted. In addition, upon the fifth expiry of timer T3565:

For case a) in subclause 5.6.3.1, the AMF should notify the SMF that the UE is unreachable. The AMF may enter 5GMM-IDLE mode over 3GPP access.

For case b) in subclause 5.6.3.1, the AMF may either:

1) perform the paging procedure over the 3GPP access; or

2) notify the SMF that the UE is unreachable.

NOTE: Whether the AMF performs the paging procedure or notifies the SMF is up to operator′s policies.

b) REGISTRATION REQUEST message indicating either "initial registration" or "5GS emergency registration" received over 3GPP access when notification procedure is ongoing over non-3GPP access; or

REGISTRATION REQUEST message indicating either "initial registration" or "5GS emergency registration" received over non-3GPP access when notification procedure is ongoing over 3GPP access.

If an integrity-protected REGISTRATION REQUEST message is received from the UE and successfully integrity checked by the network, the network shall abort the notification procedure. If the REGISTRATION REQUEST message received is not integrity protected, or the integrity check is unsuccessful, the notification procedure shall be progressed. The notification procedure shall be aborted when the primary authentication and key agreement procedure performed during registration procedure for initial registration is completed successfully.

6 Elementary procedures for 5GS session management

6.1 Overview

6.1.1 General

This clause describes the procedures used for 5GS session management (5GSM) performed over an N1 NAS signalling connection.

The main function of the 5GSM sublayer is to support the PDU session handling in the UE and in the SMF (transferred via the AMF).

The 5GSM comprises procedures for:

- the authentication and authorization, establishment, modification and release of PDU sessions; and
- request for performing handover of an existing PDU session between 3GPP access and non-3GPP access, or to transfer an existing PDN connection in the EPS to the 5GS.

Each PDU session represents a PDU session established between the UE and an SMF. PDU sessions can remain established even if the radio and network resources constituting the corresponding PDU session between the UE and the SMF are temporarily released.

5GSM procedures can be performed only if a 5GMM context has been established between the UE and the AMF, and the secure exchange of NAS messages has been initiated by the AMF by use of the 5GMM procedures described in clause 5. Once the UE is successfully registered to a PLMN, a PDU session can be established. If no 5GMM context has been established, the 5GMM sublayer has to initiate the establishment of a 5GMM context by use of the 5GMM procedures as described in clause 5.

The UE can request the network to modify or release PDU sessions. The network can fulfil such a request from the UE by modifying a PDU session or releasing a PDU session using network-requested procedures (see subclause 6.3).

6.1.2 Types of 5GSM procedures

Three types of 5GSM procedures can be distinguished:

a) Procedures related to PDU sessions:

These procedures are initiated by the network and are used for authentication and authorization or manipulation of PDU sessions:

a) PDU authentication and authorization;

b) network-initiated PDU session modification; and

c) network-initiated PDU session release.

This procedure is initiated by the UE and to request for establishment of PDU sessions or to perform handover of an existing PDU session between 3GPP access and non-3GPP access, or to transfer an existing PDN connection in the EPS to the 5GS:

- UE-requested PDU session establishment.

b) Transaction related procedures:

These procedures are initiated by the UE to request for handling of PDU sessions, i.e. to modify a PDU session, or to release a PDU session:

a) UE-requested PDU session modification; and

b) UE-requested PDU session release.

A successful transaction related procedure initiated by the UE triggers the network to execute one of the following procedures related to PDU session; network-initiated PDU session modification procedure or network-initiated PDU session release procedure. The UE treats the start of the procedure related to the PDU session as completion of the transaction related procedure.

c) Common procedure:

The following 5GSM procedure can be related to a PDU session or to a procedure transaction:

5GSM status procedure.

6.1.3 5GSM sublayer states

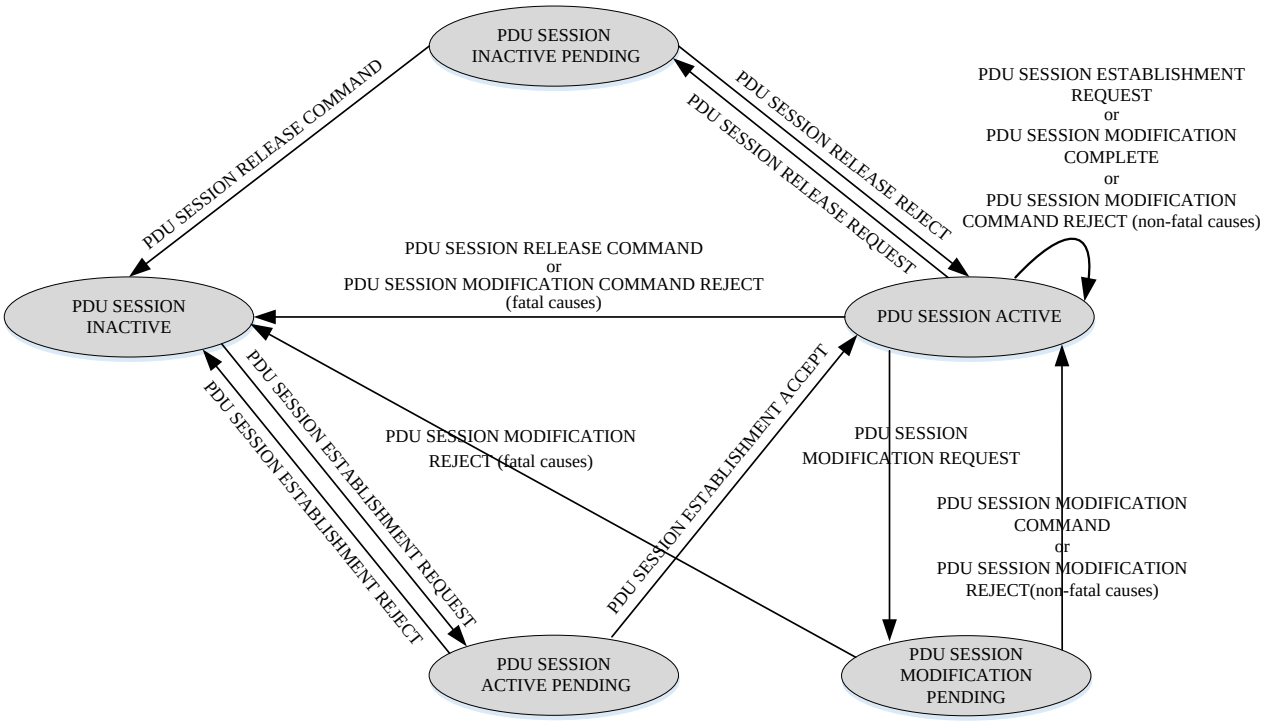
6.1.3.1 General

In the following subclauses, the possible states of a PDU session in the UE and the network side are described.

6.1.3.2 5GSM sublayer states in the UE

6.1.3.2.1 Overview

In the following subclauses, the possible 5GSM sublayer states of the UE are described and shown in figure 6.1.3.2.1.1.



NOTE: Not all possible transitions are shown in this figure.
Editor's note: The fatal causes and non-fatal causes used in the 5GSM procedure are FFS.

Figure 6.1.3.2.1.1: The 5GSM sublayer states for PDU session handling in the UE (overview)

6.1.3.2.2 PDU SESSION INACTIVE

No PDU session exists.

6.1.3.2.3 PDU SESSION ACTIVE PENDING

The UE has initiated a PDU session establishment procedure towards the network and is waiting for a response from the network.

6.1.3.2.4 PDU SESSION ACTIVE

The PDU session is active in the UE.

6.1.3.2.5 PDU SESSION INACTIVE PENDING

The UE has initiated a PDU session release procedure towards the network and is waiting for a response from the network.

6.1.3.2.6 PDU SESSION MODIFICATION PENDING

The UE has initiated a PDU session modification procedure towards the network and is waiting for a response from the network.

6.1.3.2.7 PROCEDURE TRANSACTION INACTIVE

No procedure transaction exists.

6.1.3.2.8 PROCEDURE TRANSACTION PENDING

The UE has initiated a procedure transaction towards the network.

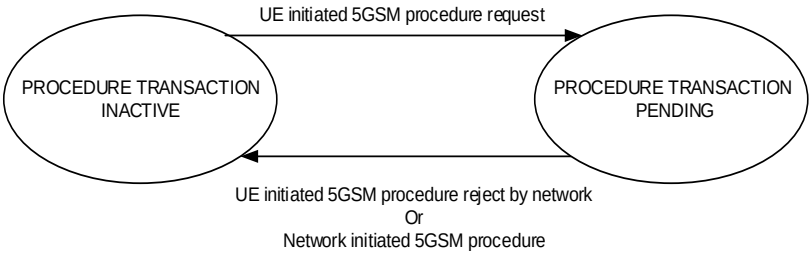
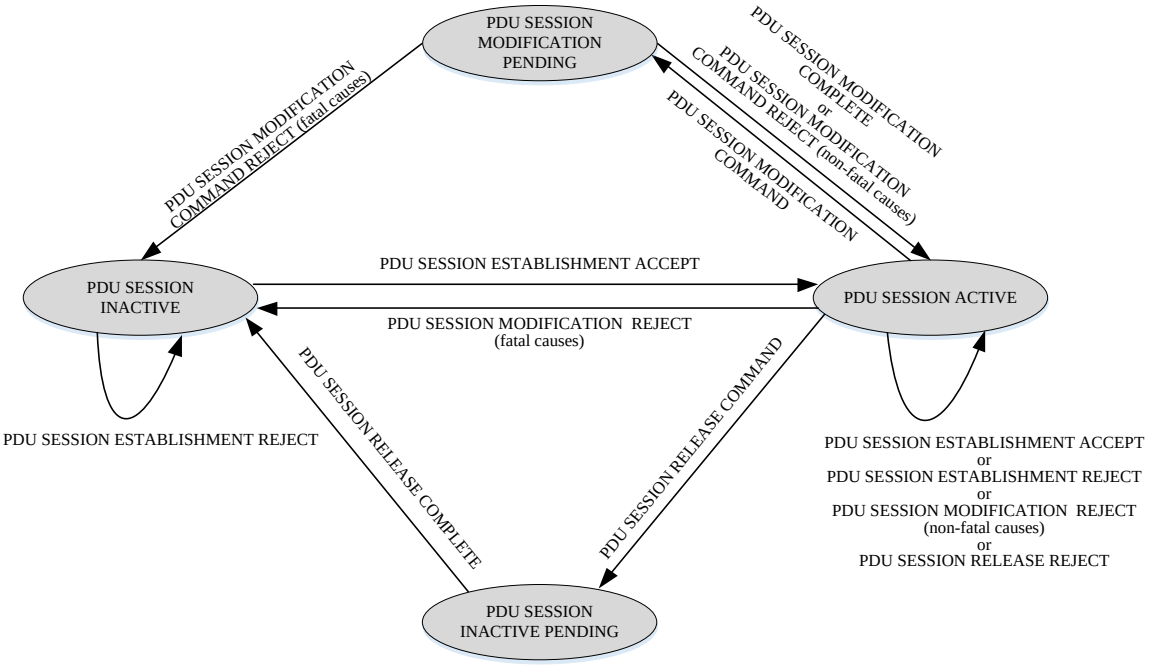


Figure 6.1.3.2.8.1: The procedure transaction states in the UE (overview)

6.1.3.3 5GSM sublayer states in the network side

6.1.3.3.1 Overview

In the following subclauses, the possible 5GSM sublayer states of the network are described and shown in Figure 6.1.3.3.1.1.



NOTE: Not all possible transitions are shown in this figure.
Editor's note: The fatal causes and non-fatal causes used in the 5GSM procedure are FFS.

Figure 6.1.3.3.1.1: The 5GSM sublayer states for PDU session handling in the network (overview)

6.1.3.3.2 PDU SESSION INACTIVE

No PDU session exists.

6.1.3.3.3 PDU SESSION ACTIVE

The PDU session is active in the network.

6.1.3.3.4 PDU SESSION INACTIVE PENDING

The network has initiated a PDU session release procedure towards the UE and is waiting for a response from the UE.

6.1.3.3.5 PDU SESSION MODIFICATION PENDING

The network has initiated a PDU session modification procedure towards the UE and is waiting for a response from the UE.

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.

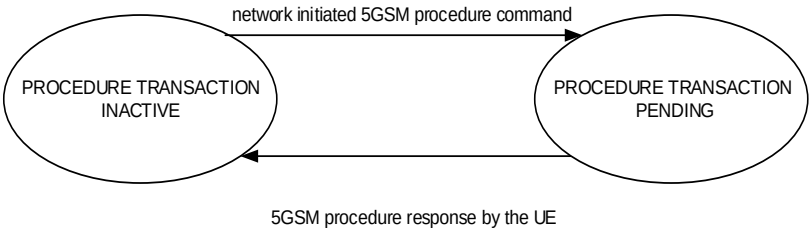


Figure 6.1.3.3.7.1: The procedure transaction states in the network (overview)

6.1.4 Coordination between 5GSM and ESM

6.1.4.1 Coordination between 5GSM and ESM with N26 interface

Interworking to EPS is supported for a PDU session, if the context includes the mapped EPS bearer. The SMF shall not include any mapped EPS bearer contexts associated with a PDU session for LADN. See coding of the Mapped EPS bearer contexts IE in subclause 9.10.4.5.

Upon inter-system change from N1 mode to S1 mode in EMM-IDLE mode, the UE shall create the default EPS bearer context and the dedicated EPS bearer context(s) based on the parameters of mapped EPS bearer contexts in the PDU session context, if available. The UE uses the parameters from each PDU session for which interworking to EPS is supported to create corresponding default EPS bearer context and optionally dedicated EPS bearer context(s) as follows:

a) the PDU session type of the PDU session shall be mapped to the PDN type of the default EPS bearer context as follows:

   1) the PDN type shall be set to "non-IP" if the PDU session type is "Ethernet" or "Unstructured";

   2) the PDN type shall be set to "IPv4" if the PDU session type is "IPv4";

   3) the PDN type shall be set to "IPv6" if the PDU session type is "IPv6"; and

   4) the PDN type shall be set to "IPv4v6" if the PDU session type is "IPv4v6";

b) the PDU address of the PDU session shall be mapped to the PDN address of the default EPS bearer context as follows:

   1) the PDN address of the default EPS bearer context is set to the PDU address of the PDU session, if the PDU session type is "IPv4", "IPv6" or "IPv4v6"; and

2) the PDN address of the default EPS bearer context is set to zero, if the PDU session type is "Ethernet" or "Unstructured";

c) the DNN of the PDU session shall be mapped to the APN of the default EPS bearer context;

d) the APN-AMBR and extended APN-AMBR received in the parameters of the default EPS bearer context of the mapped EPS bearer contexts shall be mapped to the APN-AMBR and extended APN-AMBR of the default EPS bearer context;

e) for each PDU session of a PDU session in state PDU SESSION ACTIVE or PDU SESSION MODIFICATION PENDING the UE shall set the state of the mapped EPS bearer context(s) to BEARER CONTEXT ACTIVE; and

f) for any other PDU session of a PDU session the UE shall set the state of the mapped EPS bearer context(s) to BEARER CONTEXT INACTIVE.

Additionally, for each mapped EPS bearer context in the PDU session:

a) the EPS bearer identity shall be set to the EPS bearer identity received in the mapped EPS bearer context, or the EPS bearer identity associated with the QoS flow;

b) the EPS QoS parameters shall be set to the mapped EPS QoS parameters of the EPS bearer received in the mapped EPS bearer context, or the EPS QoS parameters associated with the QoS flow;

c) the extended EPS QoS parameters shall be set to the mapped extended EPS QoS parameters of the EPS bearer received in the mapped EPS bearer context, or the extended EPS QoS parameters associated with the QoS flow; and

d) the traffic flow template shall be set to the mapped traffic flow template of the EPS bearer received in the mapped EPS bearer context, or the stored traffic flow template associated with the QoS flow, if available.

After inter-system change from N1 mode to S1 mode, the UE shall associate the PDU session identity, the S-NSSAI, and the session-AMBR with the default EPS bearer context, and for each EPS bearer context mapped from one or more QoS flows, associate the QoS rule(s) for the QoS flow(s) with the EPS bearer context.

After inter-system change from N1 mode to S1 mode, the UE and the SMF shall maintain the PDU session type of the PDU session context if the UE supports non-IP PDN type and the PDU session type is "Ethernet" or "Unstructured".

When the UE is provided with a new S-NSSAI, a new session-AMBR, one or more new QoS rules in the Protocol configuration options IE or Extended protocol configuration options IE in the MODIFY EPS BEARER CONTEXT REQUEST message, the UE shall discard the corresponding association(s) and associate the new value(s) with the EPS bearer context.

Upon successful completion of an attach procedure or tracking area updating procedure after inter-system change from N1 mode to S1 mode (see 3GPP TS 24.301 [15]), the UE shall delete any UE derived QoS rules.

Interworking to 5GS is supported for a PDN connection, if the corresponding default EPS bearer context includes a PDU session identity, session AMBR and one or more QoS rules (see 3GPP TS 24.301 [15]).

Upon inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode, the UE uses the parameters from the default EPS bearer context of each PDN connection for which interworking to 5GS is supported to create a corresponding PDU session as follows:

a) the PDN type of the default EPS bearer context shall be mapped to the PDU session type of the PDU session context as follows:

1) if the PDN type is "non-IP", the PDU session type is set to the locally available information associated with the PDN connection (either "Ethernet" or "Unstructured"), if available;

2) if the PDN type is "IPv4" the PDU session type is set to "IPv4";

3) if the PDN type is "IPv6", the PDU session type is set to "IPv6"; and

4) the PDN type shall be set to "IPv4v6" if the PDU session type is "IPv4v6";

b) the PDN address of the default EPS bearer context shall be mapped to PDU address of the PDU session, if the PDN type is "IPv4", "IPv6" or "IPv4v6";

c) the APN of the default EPS bearer context shall be mapped to the DNN of the PDU session;

d) for each default EPS bearer context in state BEARER CONTEXT ACTIVE the UE shall set the state of the mapped PDU session to PDU SESSION ACTIVE; and

e) for any other default EPS bearer context the UE shall set the state of the mapped PDU session to PDU SESSION INACTIVE.

Additionally, the UE shall set:

a) the PDU session identity of the PDU session to the PDU session identity included by the UE in the Protocol configuration options IE or Extended protocol configuration options IE in the PDN CONNECTIVITY REQUEST message, or the PDU session identity associated with the default EPS bearer context;

b) the S-NSSAI of the PDU session to the S-NSSAI included by the network in the Protocol configuration options IE or Extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER REQUEST message, or the S-NSSAI associated with the default EPS bearer context;

c) the session-AMBR of the PDU session to the session-AMBR included by the network in the Protocol configuration options IE or Extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER REQUEST message, or the session-AMBR associated with the default EPS bearer context; and

d) the SSC mode of the PDU session to "SSC mode 1".

For each EPS bearer context of the PDN connection, the UE shall create QoS flow(s) each of which is associated with the QoS rule(s) received in the Protocol configuration options IE or Extended protocol configuration options IE in the ACTIVATE DEFAULT EPS BEARER REQUEST message, ACTIVATE DEDICATED EPS BEARER REQUEST message, and/or MODIFY EPS BEARER REQUEST message (see 3GPP TS 24.301 [15]), or the QoS rules(s) associated with EPS bearer context.

After inter-system change from S1 mode to N1 mode, for each QoS flow mapped from a EPS bearer context the UE shall associate the EPS bearer ID, the EPS QoS parameters, the extended EPS QoS parameters, and the traffic flow template, if available, of the EPS bearer context with the QoS flow.

When the UE is provided with a new EPS bearer ID, a new EPS QoS parameters, a new extended EPS QoS parameters, or a new traffic flow template in the Mapped EPS bearer context IE of the PDU SESSION MODIFICATION COMMAND message for a QoS flow, the UE shall discard the corresponding association(s) and associate the new value(s) with the QoS flow.

When a QoS flow is deleted, all the associated EPS bearer context information that are mapped from the deleted QoS flow shall be deleted from the UE and the network. When an EPS bearer is released, all the associated QoS flow context information that are mapped from the released EPS bearer shall be deleted from the UE and the network.

NOTE: If T35cd is running or deactivated for an [S-NSSAI, DNN] combination, or if T35ef is running or deactivated for an S-NSSAI, the UE is allowed to initate ESM procedures in EPS for the APN corresponding to that DNN, and if the APN is congested in EPS, the MME can send a back-off timer for the APN to the UE as specified in 3GPP TS 24.301 [15].

6.1.4.2 Coordination between 5GSM and ESM without N26 interface

When interworking without N26 is supported, the SMF does not provide the UE with the mapped EPS bearer context for a PDU session context.

NOTE 1: Since the SMF does not provide the UE with the mapped EPS bearer context for a PDU session context, the UE does not know whether interworking to EPS is supported for a PDU session before attempting to transfer the PDU session context from N1 mode to S1 mode.

Upon inter-system change from N1 mode to S1 mode in EMM-IDLE mode, the UE shall use the parameters from each PDU session context which the UE intends to transfer to EPS to create the contents of a PDN CONNECTIVITY REQUEST message as follows:

a) if the PDU session is a PDU session for emergency services, the request type shall be set to "handover of emergency bearer services". Otherwise the request type shall be set to "handover";

b) the PDU session type of the PDU session context shall be mapped to the PDN type of the default EPS bearer context as follows:

   1) the PDN type shall be set to "non-IP" if the PDU session type is "Ethernet" or "Unstructured";

   2) the PDN type shall be set to "IPv4" if the PDU session type is "IPv4";

   3) the PDN type shall be set to "IPv6" if the PDU session type is "IPv6"; and

   4) the PDN type shall be set to "IPv4v6" if the PDU session type is "IPv4v6";

c) the DNN of the PDU session shall be mapped to the APN of the default EPS bearer context; and

d) the PDU session ID parameter in the PCO IE shall be set to the PDU session identity of the PDU session.

After inter-system change from N1 mode to S1 mode, the UE shall associate the PDU session identity with the default EPS bearer context.

Upon successful completion of an attach procedure after inter-system change from N1 mode to S1 mode (see 3GPP TS 24.301 [15]), the UE shall delete any UE derived QoS rules

When interworking without N26 is supported, the MME does not provide the UE with the mapped PDU session context for a PDN connection. When establishing a new PDN connection in S1 mode, if the UE wants to be able to attempt to transfer the PDN connection from S1 mode to N1 mode in case of inter-system change, the UE shall allocate a PDU session identity, indicate the allocated PDU session identity in the PDU session ID parameter in the PCO IE of the PDN CONNECTIVITY REQUEST and associate the allocated PDU session identity with the default EPS bearer context of the PDN connection.

NOTE 2: Since the MME does not provide the UE with the mapped PDU session context for a PDN connection, the UE does not know whether interworking to 5GS is supported for a PDN connection for which the UE assigned a PDU Session identity before attempting to transfer the PDN connection from S1 mode to N1 mode.

Upon inter-system change from S1 mode to N1 mode in 5GMM-IDLE mode, the UE uses the parameters from the default EPS bearer context of each PDN connection which the UE intends to transfer to 5GS and for which the UE has allocated a PDU session identity to create a PDU SESSION ESTABLISHMENT REQUEST message as follows:

a) if the PDN connection is for emergency bearer services, the request type shall be set to "existing emergency PDU session". Otherwise the request type shall be set to "existing PDU session";

b) the PDN type of the default EPS bearer context shall be mapped to the PDU session type of the PDU session context as follows:

   1) if the PDN type is "non-IP", the PDU session type is set to the locally available information associated with the PDN connection (either "Ethernet" or "Unstructured"), if available;

   2) if the PDN type is "IPv4" the PDU session type is set to "IPv4";

   3) if the PDN type is "IPv6", the PDU session type is set to "IPv6"; and

   4) the PDN type shall be set to "IPv4v6" if the PDU session type is "IPv4v6";

c) the APN of the default EPS bearer context shall be mapped to the DNN of the PDU session context; and

d) the PDU session ID shall be set to the PDU session ID associated with the default EPS bearer context.

6.2 General on elementary 5GSM procedures

6.2.1 Principles of PTI handling for 5GSM procedures

When the UE or the network initiates a transaction related procedure (i.e. a procedure consisting of more than one message and the messages are related), it shall include a valid PTI value in the message header of the request message or of the command message.

If a response message is sent as result of a received request message or a received command message, the sending entity shall include in the response message the PTI value received within the request message or within the command message (see examples in figure 6.2.1.1, figure 6.2.1.2, figure 6.2.1.3, and figure 6.2.1.4).

If a command message is sent as result of a received request message, the sending entity shall include in the command message the PTI value received with the request message (see examples in figure 6.2.1.3).

If a command message is not sent as result of a received request message, the sending entity shall include in the command message the PTI value set to "no procedure transaction identity assigned" (see examples in figure 6.2.1.3).

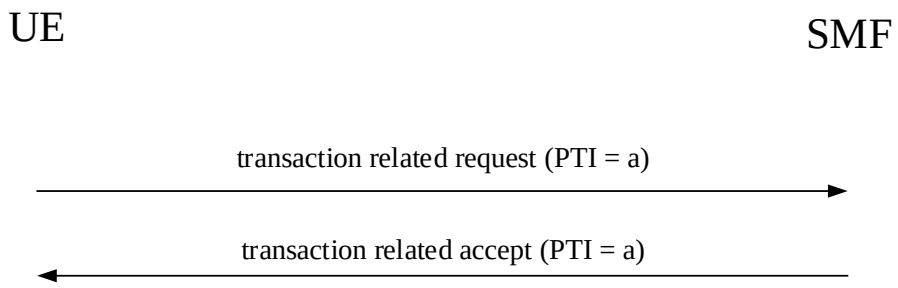


Figure 6.2.1.1: UE-requested transaction related procedure accepted by the network

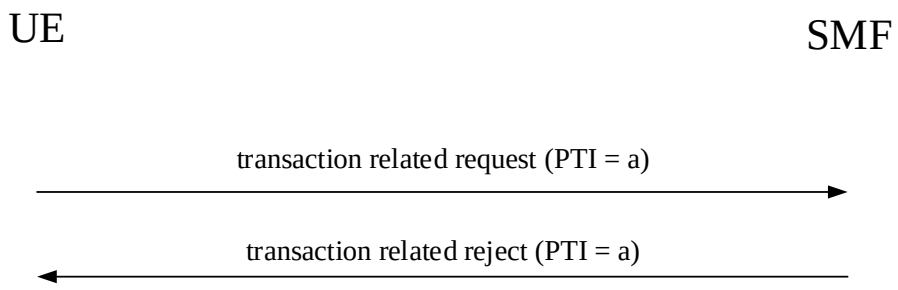


Figure 6.2.1.2: UE-requested transaction related procedure rejected by the network

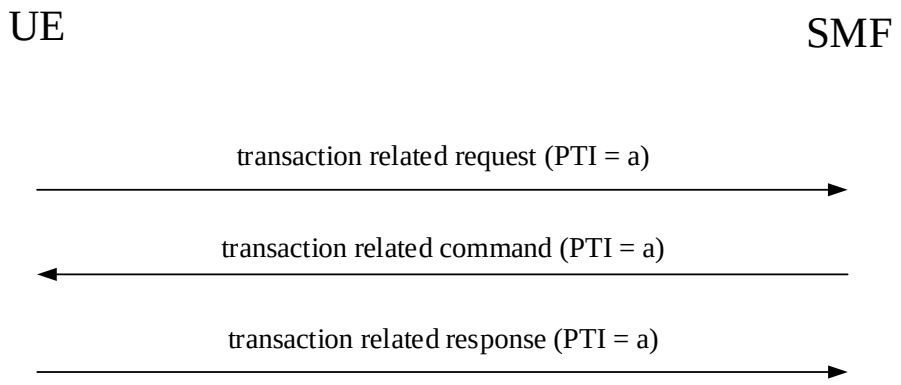


Figure 6.2.1.3: UE-requested transaction related procedure triggering a network-requested transaction related procedure

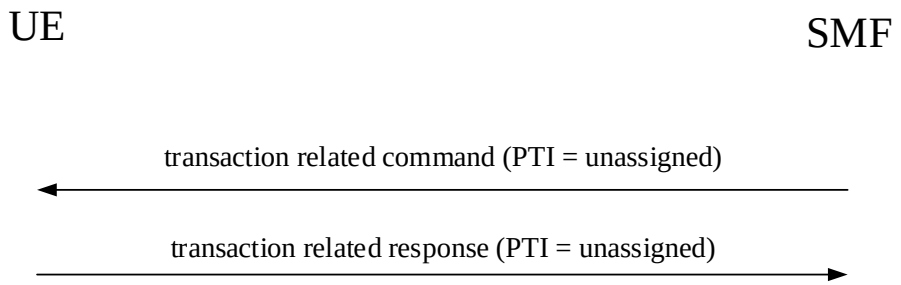


Figure 6.2.1.4: network-requested transaction related procedure not triggered by a UE-requested transaction related procedure

6.2.2 PDU session types

The following PDU Session types are supported:

a) IPv4;

b) IPv6;

c) IPv4v6;

d) Ethernet (EtherType as defined in IEEE 802.3); and

e) Unstructured.

IP address allocation for IPv4, IPv6 and IPv4v6 PDU session types is described in subclause 6.2.4.

Neither a MAC nor an IP address is allocated by the 5GCN to the UE for Ethernet PDU session type.

6.2.3 PDU session management

The SMF is responsible for the session management functions to provide the PDU connectivity service to the UE via the SM signalling between UE and SMF. The session management procedures includes:

a) the UE-requested PDU session establishment procedure;

b) the PDU session establishment authentication and authorization procedure;

c) the UE-requested PDU session modification procedure;

d) the network-requested PDU session modification procedure;

e) the UE-requested PDU session release procedure; and

f) the network-requested PDU session release procedure.

A UE may establish multiple PDU sessions, to the same data network or to different data networks, via 3GPP and via and Non-3GPP access networks at the same time.

The session management messages between UE and SMF are transferred via AMF as specified in subclause 8.3.

6.2.4 IP address allocation

6.2.4.1 General

This clause specifies IP address allocation for the PDU session.

In this release of specification, PDU session can be initiated with one IP version, i.e. IPv4 PDU session type or IPv6 PDU session type, or with both IP versions, i.e. IPv4v6 PDU session type.

IP address allocation to the UE shall be performed by SMF based on one or both the selected IP versions and operator policies. If IPv4 PDU session type is selected, an IPv4 address is allocated to the UE. If IPv6 PDU session type is selected, an IPv6 prefix and an interface identifier for the IPv6 link local address are allocated to the UE. If IPv4v6 PDU session type is selected, an IPv4 address, an IPv6 prefix and an interface identifier for the IPv6 link local address are allocated to the UE.

For IPv4 PDU session type and for IPv4v6 PDU session type, the UE:

a) shall obtain an IPv4 address via:

   1) NAS signalling as specified in subclause 6.2.4.2; or

   2) DHCPv4; and

b) may obtain IPv4 configuration parameters (e.g. DNS server address) via DHCPv4.

For IPv6 PDU session type and for IPv4v6 PDU session type, the UE:

a) shall build an IPv6 link local address based on the allocated interface identifier for the IPv6 link local address;

b) shall obtain /64 IPv6 prefix via IPv6 stateless address autoconfiguration as specified in 3GPP TS 23.501 [8] and IETF RFC 4862 [39]; and

c) may obtain IPv6 configuration parameters via stateless DHCPv6 as specified in IETF RFC 3736 [35].

The UE capable of IPv6 shall support acting as a type C host as specified in IETF RFC 4191 [36].

6.2.4.2 IP address allocation via NAS signalling

The UE shall set the PDU session type IE in the PDU SESSION ESTABLISHMENT REQUEST message, based on its IP stack capabilities if the UE requests IP connectivity as follows:

a) A UE:

   1) which is IPv6 and IPv4 capable, shall set the PDU session type IE to IPv4, IPv6 or IPv4v6 according to UE configuration or received policy.

   2) which is only IPv6 capable, shall set the PDU session type IE to IPv6.

   3) which is only IPv4 capable, shall set the PDN type IE to IPv4.

b) 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 PDU session type IE to IPv4v6.

If the UE wants to use DHCPv4 for IPv4 address assignment, it shall indicate that to the network within the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT REQUEST.

On receipt of the PDU SESSION ESTABLISHMENT REQUEST message sent by the UE, the network when allocating an IP address shall take into account the PDU session type IE, the operator's policies of the network, and the user's subscription data and:

a) if the UE requests the PDU session type IPv4v6, but the subscription or SMF configuration is limited to IPv4 only or IPv6 only for the requested DNN, the network shall set the PDU session type IE to either "IPv4" or "IPv6" and the 5GSM cause value to #50 "PDU session type IPv4 only allowed", or #51 "PDU session type IPv6 only allowed" in the PDU SESSION ESTABLISHMENT ACCEPT message, respectively. The UE shall not subsequently initiate another UE requested PDU session establishment procedure to the same DNN (or no DNN, if no DNN was indicated by the UE) and the same S-NSSAI (or no S-NSSAI, if no S-NSSAI was indicated by the UE) to obtain a PDU session type different from the one allowed by the network;

b) if the network sets the PDU session type IE to IPv4, the network shall include an IPv4 address in the PDU address IE;

c) if the network sets the PDU session type IE to IPv6, the network shall include an interface identifier for the IPv6 link local address in the PDU address IE; and

d) if the network sets the PDU session type IE to IPv4v6, the network shall include an IPv4 address and an interface identifier for the IPv6 link local address in the PDU address IE.

6.2.5 Quality of service

6.2.5.1 General

6.2.5.1.1 QoS rules

6.2.5.1.1.1 General

In a PDU session of IPv4, IPv6, IPv4v6 and Ethernet PDU session type, the NAS protocol enables different forwarding treatments of UL user data packets in one or more QoS flows based on signalled QoS rules, derived QoS rules or any combination of them.

In a PDU session of Unstructured PDU session type, all UL user data packets are associated with the same QoS flow.

6.2.5.1.1.2 Signalled QoS rules

The NAS protocol enables the network to provide the UE with signalled QoS rules associated with a PDU session.

The network can provide the UE with one or more signalled QoS rules associated with a PDU session at the PDU session establishment or at QoS flow establishment.

Each signalled QoS rule contains:

a) an indication of whether the QoS rule is the default QoS rule;

b) a QoS rule identifier (QRI);

c) a QoS flow identifier (QFI);

d) optionally, a set of packet filters;

e) a precedence value;

f) if the flow is a GBR QoS flow:

1) Guaranteed flow bit rate (GFBR) for UL;

2) Guaranteed flow bit rate (GFBR) for DL;

3) Maximum flow bit rate (MFBR) for UL;

4) Maximum flow bit rate (MFBR) for DL; and

5) optionally averaging window, applicable for both UL and DL;

g) 5QI, if the QFI is not the same as the 5QI of the QoS flow identified by the QFI;

h) optionally, an EPS bearer identity (EBI) if the QoS flow can be mapped to an EPS bearer as specified in subclause 4.11.2 of 3GPP TS 23.502 [9].

For case d) above:

1) If the QoS rule is the default rule of a PDU session of IPv4, IPv6, IPv4v6 or Ethernet PDU session type, the set of packet filters contains zero or more packet filters for DL direction, and may additionaly contain one of the following:

   A) a match-all packet filter for UL direction;

   B) a match-all packet filter for UL and DL directions;

   C) zero or more packet filters for UL direction (other than the match-all packet filter for UL direction);

   D) zero or more packet filters for UL and DL directions (other than the match-all packet filter for UL and DL directions); or

   E) one or more packet filters for UL direction (other than the match-all packet filter for UL direction) and one or more packet filters for UL and DL directions (other than the match-all packet filter for UL and DL directions).

   The set of packet filters for the default rule shall not be. If the default QoS rule contains a match-all packet filter, then the highest precedence value shall be used for the default QoS rule.

2) If the QoS rule is a QoS rule of a PDU session of IPv4, IPv6, IPv4v6 or Ethernet PDU session type and is not the default QoS rule, the set of packet filters contains zero or more packet filters for the DL direction, and may additionally contain one of the following:

   A) zero or more packet filters for UL direction (other than the match-all packet filter for UL direction); and

   B) zero or more packet filters for both UL and DL directions (other than the match-all packet filter for UL and DL directions).

3) For PDU session of unstructured PDU session type, there is only one QoS rule associated with it and the set of packet filters of that QoS rule is empty.

If the UE requests a new QoS flow, it shall assign a precedence value for the signalled QoS rule which is not in the range from 70 to 99 (decimal).

If the averaging window is not included in a QoS rule for a GBR QoS flow with a 5QI indicated in 3GPP TS 23.501 [8] table 5.7.4-1, the averaging window associated with the 5QI in 3GPP TS 23.501 [8] table 5.7.4-1 applies for the averaging window.

If the averaging window is not included in a QoS rule for a GBR QoS flow with a 5QI not indicated in 3GPP TS 23.501 [8] table 5.7.4-1, the standardized value of two seconds is used as the averaging window.

Within a PDU session:

a) each signalled QoS rule has a unique QRI;

b) there is at least one signalled QoS rule;

c) one signalled QoS rule is the default QoS rule; and

d) there can be zero, one or more signalled QoS rules associated with a given QFI.

6.2.5.1.1.3 Derived QoS rules

Derived QoS rules are applicable only for PDU session of IPv4, IPv6, IPv4v6 or Ethernet PDU session type.

The reflective QoS in the UE creates derived QoS rules associated with a PDU session based on DL user data packets received via the PDU session.

Each derived QoS rule contains:

a) a QoS flow identifier (QFI);

b) a packet filter for UL direction; and

c) a precedence value of 80 (decimal).

NOTE: On the network side, the corresponding QoS rule can be associated with a different precedence value in the range from 70 to 99 (decimal).

Within a PDU session:

a) there can be zero, one or more derived QoS rules associated with a given QFI; and

b) there can be up to one derived QoS rule associated with a given packet filter for UL direction.

In the UE, a timer T3583 runs for each derived QoS rule.

6.2.5.1.2 Session-AMBR

The NAS protocol enables the network to provide the UE with the session-AMBR associated with a PDU session.

The standardized value of two seconds is used as the averaging window for the UE's enforcement of the UL rate limitation indicated by the session-AMBR.

6.2.5.1.3 UL user data packet matching

For PDU session of IPv4, IPv6, IPv4v6 or Ethernet PDU session type, upon receiving an UL user data packet from the upper layers for transmission via a PDU session, the UE shall attempt to associate the UL user data packet with:

a) the QFI of a signalled QoS rule associated with the PDU session which has a set of packet filters containing a packet filter for UL direction matching the UL user data packet or containing a packet filter for both UL and DL directions matching the UL user data packet; or

b) the QFI of a derived QoS rule associated with the PDU session which has the packet filter for UL direction matching the UL user data packet;

by evaluating the QoS rules in increasing order of their precedence values until the UL user data packet is associated with a QFI or all QoS rules are evaluated.

For PDU session of unstructured PDU session type, upon receiving an UL user data packet from the upper layers for transmission via a PDU session, the UE shall associate the UL user data packet with the QFI of the default QoS rule associated with the PDU session.

If the UL user data packet is associated with a QFI, the UE shall pass the QFI along the UL user data packet to the lower layers for transmission.

NOTE: Marking of the UL user data packet with the QFI is performed by the lower layers.

If all QoS rules are evaluated and the UL user data packet is not associated with a QFI, the UE shall discard the UL user data packet.

6.2.5.1.4 Reflective QoS

6.2.5.1.4.1 General

The UE may support reflective QoS.

If the UE supports the reflective QoS, the UE shall support the procedures in the following subclauses.

The reflective QoS is applicable in a PDU session of IPv4, IPv6, IPv4v6 and Ethernet PDU session type. The reflective QoS is not applicable in a PDU session of Unstructured PDU session type.

The UE may request to revoke the usage of reflective QoS for an existing PDU session for which the UE had previously indicated support for reflective QoS.

6.2.5.1.4.2 Derivation of packet filter for UL direction from DL user data packet

If the UE needs to derive a packet filter for UL direction from the DL user data packet (see subclause 6.2.5.1.4.3 and 6.2.5.1.4.4), the UE shall proceed as follows:

a) if the received DL user data packet belongs to a PDU session of IPv4 or IPv4v6 PDU session type and is an IPv4 packet and:

   1) the protocol field of the received DL user data packet indicates TCP as specified in IETF RFC 793 [33];

   2) the protocol field of the received DL user data packet indicates UDP as specified in IETF RFC 768 [32]; or

   3) the protocol field of the received DL user data packet indicates ESP as specified in IETF RFC 4303 [38] and an uplink IPSec SA corresponding to a downlink IPSec SA indicated in the security parameters index field of the received DL user data packet exists;

   then the packet filter for UL direction contains the following packet filter components:

   1) an IPv4 remote address component set to the value of the source address field of the received DL user data packet;

   2) an IPv4 local address component set to the value of the destination address field of the received DL user data packet;

   3) a protocol identifier/next header type component set to the value of the protocol field of the received DL user data packet;

   4) if the protocol field of the received DL user data packet indicates TCP as specified in IETF RFC 793 [33] or UDP as specified in IETF RFC 768 [32]:

      i) a single local port type component set to the value of the destination port field of the received DL user data packet; and

      ii) a single remote port type component set to the value of the source port field of the received DL user data packet; and

   5) if the protocol field of the received DL user data packet indicates ESP as specified in IETF RFC 4303 [38]:

      i) a security parameter index type component set to the security parameters index of the uplink IPSec SA corresponding to the downlink IPSec SA indicated in the security parameters index field of the received DL user data packet;

   otherwise it is not possible to derive a packet filter for UL direction from the DL user data packet;

b) if the received DL user data packet belongs to a PDU session of IPv6 or IPv4v6 PDU session type and is an IPv6 packet and:

   1) the last next header field of the received DL user data packet indicates TCP as specified in IETF RFC 793 [33];

2) the last next header field of the received DL user data packet indicates UDP as specified in IETF RFC 768 [32]; or

3) the last next header field of the received DL user data packet indicates ESP as specified in IETF RFC 4303 [38] and an uplink IPSec SA corresponding to a downlink IPSec SA indicated in the security parameters index field of the received DL user data packet exists;

then the packet filter for UL direction contains the following packet filter components:

1) an IPv6 remote address/prefix length component set to the value of the source address field of the received DL user data packet;

2) an IPv6 local address/prefix length component set to the value of the destination address field of the received DL user data packet;

3) a protocol identifier/next header type component set to the value of the last next header field of the received DL user data packet;

4) if the last next header field of the received DL user data packet indicates TCP as specified in IETF RFC 793 [33] or UDP as specified in IETF RFC 768 [32]:

   i) a single local port type component set to the value of the destination port field of the received DL user data packet; and

   ii) a single remote port type component set to the value of the source port field of the received DL user data packet; and

5) if the last next header field of the received DL user data packet indicates ESP as specified in IETF RFC 4303 [38]:

   i) a security parameter index type component set to the security parameters index of the uplink IPSec SA corresponding to the downlink IPSec SA indicated in the security parameters index field of the received DL user data packet;

otherwise it is not possible to derive a packet filter for UL direction from the DL user data packet;

c) if the received DL user data packet belongs to a PDU session of Ethernet PDU session type, the packet filter for UL direction contains the following packet filter components:

1) a destination MAC address component set to the source MAC address of the received DL user data packet;

2) a source MAC address component set to the destination MAC address of the received DL user data packet;

3) if an 802.1Q C-TAG is included in the received DL user data packet, an 802.1Q C-TAG VID component set to the 802.1Q C-TAG VID of the received DL user data packet and an 802.1Q C-TAG PCP/DEI component set to the 802.1Q C-TAG PCP/DEI of the received DL user data packet;

4) if an 802.1Q S-TAG is included in the received DL user data packet, an 802.1Q S-TAG VID component set to the 802.1Q S-TAG VID of the received DL user data packet and an 802.1Q S-TAG PCP/DEI component set to the 802.1Q S-TAG PCP/DEI of the received DL user data packet;

5) If the Ethertype field of the received DL user data packet is set to a value of 1536 or above, an Ethertype component set to the Ethertype of the received DL user data packet;

6) if the Ethertype field of the Ethernet frame header indicates that the data carried in the Ethernet frame is IPv4 data, the UE shall also add to the packet filter for UL direction the IP-specific components based on the contents of the IP header of the received DL user data packet as described in bullet a) above; and

7) if the Ethertype field of the Ethernet frame header indicates that the data carried in the Ethernet frame is IPv6 data, the UE shall also add to the packet filter for UL direction the IP-specific components based on the contents of the IP header of the received DL user data packet as described in bullet b) above; and

d) if the received DL user data packet belongs to a PDU session of PDU session type other than Ethernet, IPv4, IPv6 and IPv4v6, it is not possible to derive a packet filter for UL direction from the DL user data packet.

6.2.5.1.4.3 Creating a derived QoS rule by reflective QoS in the UE

If the UE receives a DL user data packet marked with a QFI and an RQI, the DL user data packet belongs to a PDU session of IPv4, IPv6, IPv4v6 or Ethernet PDU session type, and the UE does not have a derived QoS rule with the same packet filter for UL direction as the packet filter for UL direction derived from the DL user data packet as specified in subclause 6.2.5.1.4.2, then the UE shall create a new derived QoS rule as follows:

a) the QFI of the derived QoS rule is set to the received QFI;

b) the precedence value of the derived QoS rule is set to 80 (decimal); and

c) the packet filter for UL direction of the derived QoS rule is set to the derived packet filter for UL direction;

and the UE shall start the timer T3583 associated with the derived QoS rule with the RQ timer value last received during the UE-requested PDU session establishment procedure of the PDU session (see subclause 6.4.1) or the network-requested PDU session modification procedure of the PDU session (see subclause 6.4.2). If the RQ timer value was received neither in the UE-requested PDU session establishment procedure of the PDU session nor in any network-requested PDU session modification procedure of the PDU session, the default standardized RQ timer value is used.

6.2.5.1.4.4 Updating a derived QoS rule by reflective QoS in the UE

If the UE receives a DL user data packet associated with a QFI and an RQI, the DL user data packet belongs to a PDU session of IPv4, IPv6, IPv4v6 or Ethernet PDU session type, and the UE has a derived QoS rule with the same packet filter for UL direction as the packet filter for UL direction derived from the DL user data packet as specified in subclause 6.2.5.1.4.2:

a) the UE shall re-start the timer T3583 associated with the derived QoS rule with the RQ timer value last received during the UE-requested PDU session establishment procedure of the PDU session (see subclause 6.4.1) or the network-requested PDU session modification procedure of the PDU session (see subclause 6.4.2). If the RQ timer value was received neither in the UE-requested PDU session establishment procedure of the PDU session nor in any network-requested PDU session modification procedure of the PDU session, the default standardized RQ timer value is used; and

b) if the QFI value associated with the DL user data packet is different from the QFI value stored for the derived QoS rule, the UE shall replace the QFI value stored for the derived QoS rule with the new QFI value for the derived QoS rule.

6.2.5.1.4.5 Deleting a derived QoS rule in the UE

Upon expiration of timer T3583 associated with a derived QoS rule, the UE shall remove the derived QoS rule.

Upon release of the PDU session, the UE shall remove the derived QoS rule(s) associated with the PDU session.

If the network accepts the request from the UE to revoke the usage of reflective QoS and sets the value of the RQ timer to "deactivated" or zero, the UE shall remove the derived QoS rule(s) associated with the PDU session.

When a derived QoS rule is deleted, the timer T3583 associated with the derived QoS rule shall be stopped.

6.2.5.1.4.6 Ignoring RQI in the UE

If the UE receives a DL user data packet marked with a QFI and an RQI and it is not possible to derive a packet filter for UL direction from the DL user data packet as specified in subclause 6.2.5.1.4.2, the UE shall ignore the RQI and shall handle the received DL user data packet.

6.2.6 Local area data network (LADN)

The UE can receive the local area data network (LADN) information consisting of LADN DNNs and LADN service area (a set of tracking areas that belong to the current registration area) information based on the UE location during the registration procedure or the generic UE configuration update procedure (see subclause 5.5.1 and subclause 5.4.4).

The UE may request a PDU session establishment and modification or initiate the service request to re-establish the PDU session for LADN when the UE is located in the LADN service area. If the UE has moved out of the LADN service area, the SMF shall:

a) release the PDU session for LADN; or

b) release the user-plane resources for the PDU session for LADN;

according to operator's policy.

In case b):

- if the UE has returned to the LADN service area, and the network has downlink user data pending, the network re-establishes the user-plane resources for the PDU session for LADN; and.
- if the UE has not returned to the LADN service area after a period of time according to operator's policy, the SMF may release the PDU session for LADN.

When the UE moves to 5GMM-DEREGISTERED state, the UE shall delete the stored LADN information, if any.

NOTE: In this release, LADNs apply only to 3GPP access.

6.2.7 Handling of DNN based congestion control

The network may detect and start performing DNN based congestion control when one or more DNN congestion criteria as specified in 3GPP TS 23.501 [8] are met. The network may store a DNN congestion back-off timer on a per UE and congested DNN basis. If the UE does not provide a DNN for a non-emergency PDU session, then the network uses the selected DNN.

In the UE, 5GS session management timers T3396 for DNN based congestion control are started and stopped on a per DNN basis.

In case the timer T3396 is provided during the PDU session establishment procedure, the DNN associated with T3396 is the DNN provided by the UE during the PDU session establishment. If no DNN is provided by the UE along the PDU SESSION ESTABLISHMENT REQUEST, then T3396 is associated with no DNN. For this purpose the UE shall memorize the DNN provided to the network during the PDU session establishment. The timer T3396 associated with no DNN will never be started due to any 5GSM procedure related to an emergency PDU session. If the timer T3396 associated with no DNN is running, it does not affect the ability of the UE to request an emergency PDU session.

In case the timer T3396 is provided during the UE-requested PDU session modification procedure or the network-requested PDU session release procedure, the DNN associated with T3396 is the DNN associated with the PDU session corresponding to the 5GSM procedure.

If T3396 is running or is deactivated, and the UE is a UE configured for high priority access in selected PLMN, then the UE is allowed to initiate 5GSM procedures for the respective DNN or without a DNN.

6.2.8 Handling of S-NSSAI based congestion control

The network may detect and start performing S-NSSAI based congestion control when one or more S-NSSAI congestion criteria as specified in 3GPP TS 23.501 [8] are met. The network may store an S-NSSAI congestion back-off timer on a per UE, S-NSSAI, and optionally DNN basis. If the UE does not provide a DNN for a non-emergency PDU session, then the network uses the selected DNN.

In the UE, 5GS session management timers T35cd for the S-NSSAI based congestion control are started and stopped on a per S-NSSAI and DNN basis.

In the UE, 5GS session management timers T35ef for the S-NSSAI based congestion control are started and stopped on a per S-NSSAI basis.

In case the timer T35cd is provided during the PDU session establishment procedure, the S-NSSAI associated with T35cd is the S-NSSAI provided by the UE during the PDU session establishment. The DNN associated with T35cd is the DNN provided by the UE during the PDU session establishment. If no S-NSSAI but DNN is provided by the UE along the PDU SESSION ESTABLISHMENT REQUEST message, then T35cd is associated with no S-NSSAI and a DNN provided to the network during the PDU session establishment. If no DNN but S-NSSAI is provided by the UE along the PDU SESSION ESTABLISHMENT REQUEST message, then T35cd is associated with no DNN and an S-NSSAI provided to the network during the PDU session establishment. If no DNN and no S-NSSAI is provided by the UE along the PDU SESSION ESTABLISHMENT REQUEST message, then T35cd is associated with no DNN and no

S-NSSAI. For this purpose the UE shall memorize the DNN and S-NSSAI provided to the network during the PDU session establishment. The timer T35cd associated with no DNN and an S-NSSAI will never be started due to any 5GSM procedure related to an emergency PDU session. If the timer T35cd associated with no DNN and an S-NSSAI is running, it does not affect the ability of the UE to request an emergency PDU session.

In case the timer T35ef is provided during the PDU session establishment procedure, the S-NSSAI associated with T35ef is the S-NSSAI provided by the UE during the PDU session establishment. If no S-NSSAI is provided by the UE along the PDU SESSION ESTABLISHMENT REQUEST message, then T35ef is associated with no S-NSSAI.

In case the timer T35cd is provided during the UE-requested PDU session modification procedure or the network-requested PDU session release procedure, the S-NSSAI and DNN associated with T35cd are the S-NSSAI and DNN associated with the PDU session corresponding to the 5GSM procedure.

In case the timer T35ef is provided during the UE-requested PDU session modification procedure or the network-requested PDU session release procedure, the S-NSSAI associated with T35ef is the S-NSSAI associated with the PDU session corresponding to the 5GSM procedure.

If T35cd is running or is deactivated, and the UE is a UE configured for high priority access in selected PLMN, then the UE is allowed to initiate 5GSM procedures for the respective S-NSSAI or [S-NSSAI, DNN] combination.

If T35ef is running or is deactivated, and the UE is configured for high priority access in selected PLMN, then the UE is allowed to initiate 5GSM procedure for the respective S-NSSAI.

6.2.9 Interaction with upper layers

6.2.9.1 General

A 5GSM entity may interact with upper layers. Subclause 6.2.9.2 describes how the 5GSM entity interacts with upper layers with respect to the URSP.

6.2.9.2 URSP

The URSP requires interaction between upper layers and the 5GSM entities in the UE (see 3GPP TS 24.5xx [19] for further details). Each of the 5GSM entities in the UE shall indicate attributes (e.g. PDU session identity, SSC mode, S-NSSAI, DNN, PDU session type, access type, PDU address) of a newly established PDU session to the upper layers. If a PDU session is released, the 5GSM entity handling the PDU session shall inform the PDU session identity of the released PDU session to the upper layers. The upper layers may request a 5GSM entity to establish a PDU session indicating one or more PDU session attributes and to release an existing PDU session.

6.2.10 Handling of 3GPP PS data off

A UE, which supports 3GPP PS data off (see 3GPP TS 23.501 [8]), can be configured with up to two lists of 3GPP PS data off exempt services as specified in 3GPP TS 24.368 [17] or in the $EF_{3GPPPSDATAOFF}$ USIM file as specified in 3GPP TS 31.102 [22]:

a) a list of 3GPP PS data off exempt services to be used in the HPLMN or EHPLMN; and

b) a list of 3GPP PS data off exempt services to be used in the VPLMN.

If only the list of 3GPP PS data off exempt services to be used in the HPLMN or EHPLMN is configured at the UE, this list shall be also used in the VPLMN.

If the UE supports 3GPP PS data off, the UE shall provide the 3GPP PS data off UE status in the extended protocol configuration options IE during UE-requested PDU session establishment procedure, and UE-requested PDU session modification procedure (see subclause 6.4.1 and subclause 6.4.2).

The network shall support of 3GPP PS data off.

The UE shall indicate change of the 3GPP PS data off UE status for the PDU session by using the UE-requested PDU session modification procedure as specified in subclause 6.4.2.

When the 3GPP PS data off UE status is "activated", the UE does not send uplink IP packets via 3GPP access except:

a) for those services indicated in the list of 3GPP PS data off exempt services to be used in the HPLMN or EHPLMN as specified in 3GPP TS 24.368 [17] when the UE is in its HPLMN or EHPLMN;

b) for those services indicated in the list of 3GPP PS data off exempt services to be used in the HPLMN or EHPLMN when the UE is in the VPLMN, if only the list of 3GPP PS data off exempt services to be used in the HPLMN or EHPLMN is configured to the UE as specified in 3GPP TS 24.368 [17];

c) for those services indicated in the list of 3GPP PS data off exempt services to be used in the VPLMN when the UE is in the VPLMN, if the list of 3GPP PS data off exempt services to be used in the VPLMN is configured to the UE as specified in 3GPP TS 24.368 [17];

d) for those services indicated in the $EF_{3GPPPSDATAOFF}$ USIM file as specified in 3GPP TS 31.102 [22];

e) any uplink traffic due to procedures specified in 3GPP TS 24.229 [14]; and

f) any uplink traffic due to procedures specified in 3GPP TS 24.623 [20].

Otherwise the UE sends uplink IP packets without restriction.

NOTE: If the UE supports 3GPP PS data off, uplink IP packets are filtered as specified in 3GPP TS 24.229 [14] in U.3.1.5.

3GPP PS data off does not restrict sending of uplink IP packets via non-3GPP access.

3GPP PS data off does not restrict sending of uplink user data packets via a PDU session of Ethernet or Unstructured PDU session type.

6.3 Network-requested 5GSM procedures

6.3.1 PDU session authentication and authorization procedure

6.3.1.1 General

The purpose of the PDU session authentication and authorization procedure is to enable the DN:

a) to authenticate the upper layers of the UE, when establishing the PDU session;

b) to authorize the upper layers of the UE, when establishing the PDU session;

c) both of the above; or

d) to re-authenticate the upper layers of the UE after establishment of the PDU session.

The PDU session authentication and authorization procedure can be performed only during or after the UE-requested PDU session procedure establishing a non-emergency PDU session. The PDU session establishment authentication and authorization procedure shall not be performed during or after the UE-requested PDU session establishment procedure establishing an emergency PDU session.

The network authenticates the UE using the Extensible Authentication Protocol (EAP) as specified in IETF RFC 3748 [32].

EAP has defined four types of EAP messages:

a) an EAP-request message;

b) an EAP-response message;

c) an EAP-success message; and

d) an EAP-failure message.

The EAP-request message is transported from the network to the UE using the PDU SESSION AUTHENTICATION COMMAND message of the PDU EAP message reliable transport procedure.

The EAP-response message to the EAP-request message is transported from the UE to the network using the PDU SESSION AUTHENTICATION COMPLETE message of the PDU EAP message reliable transport procedure.

If the PDU session authentication and authorization procedure is performed during the UE-requested PDU session establishment procedure:

a) and the DN authentication of the UE completes successfully, the EAP-success message is transported from the network to the UE as part of the UE-requested PDU session establishment procedure in the PDU SESSION ESTABLISHMENT ACCEPT message.

b) and the DN authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE as part of the UE-requested PDU session establishment procedure in the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU session authentication and authorization procedure is performed after the UE-requested PDU session establishment procedure:

a) and the DN authentication of the UE completes successfully, the EAP-success message is transported from the network to the UE using the PDU SESSION AUTHENTICATION RESULT message of the PDU EAP result message transport procedure.

b) and the DN authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE using the PDU SESSION RELEASE COMMAND message of the network-requested PDU session release procedure.

There can be several rounds of exchange of an EAP-request message and a related EAP-response message for the DN to complete the authentication and authorization of the request for a PDU session (see example in figure 6.3.1.1).

The SMF shall set the authenticator retransmission timer specified in IETF RFC 3748 [34] subclause 4.3 to infinite value.

NOTE: The PDU session authentication and authorization procedure provides a reliable transport of EAP messages and therefore retransmissions at the EAP layer of the SMF do not occur.

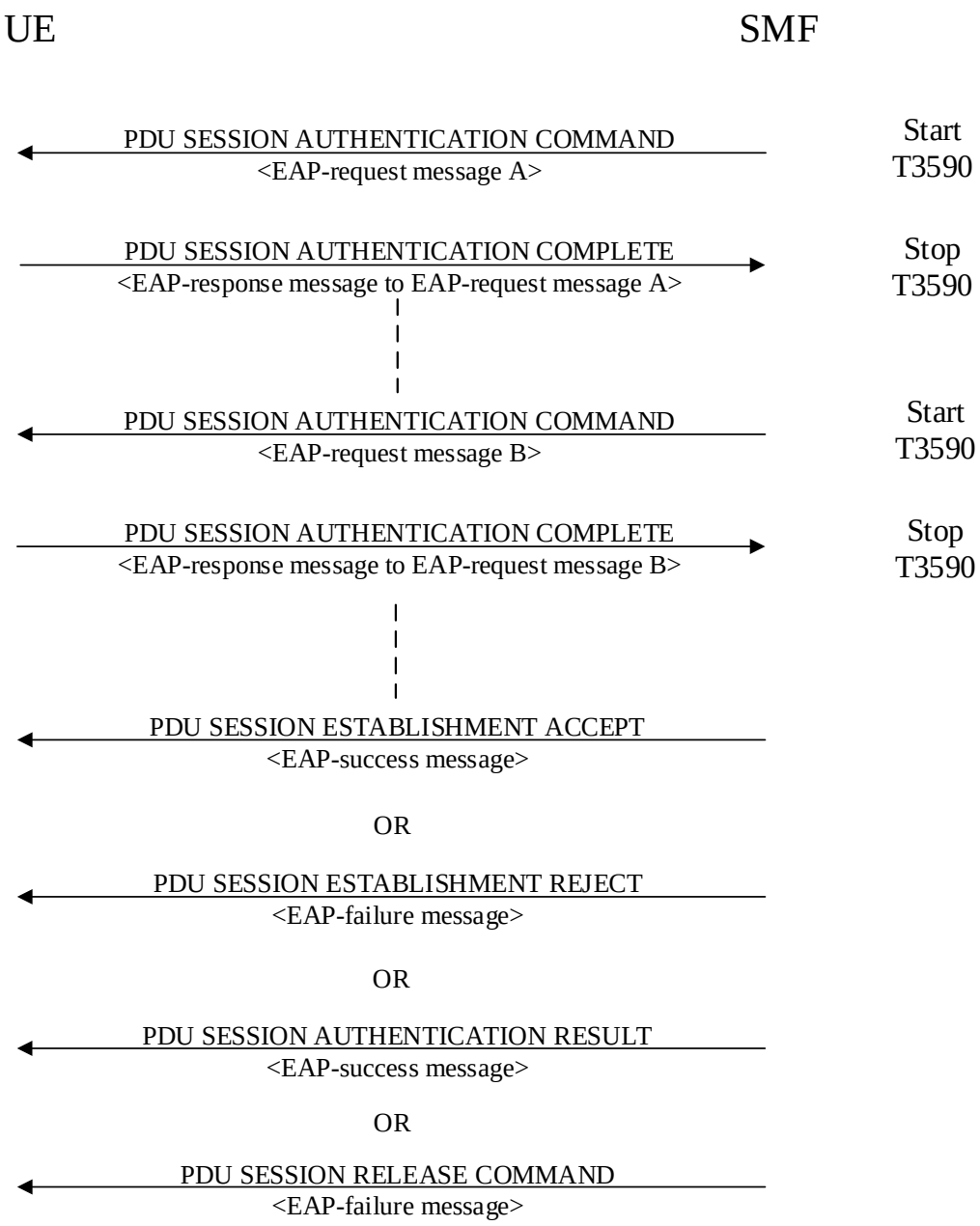


Figure 6.3.1.1: PDU session authentication and authorization procedure

6.3.1.2 PDU EAP message reliable transport procedure

6.3.1.2.1 PDU EAP message reliable transport procedure initiation

In order to initiate the PDU EAP message reliable transport procedure, the SMF shall create a PDU SESSION AUTHENTICATION COMMAND message.

The SMF shall set the PTI IE of the PDU SESSION AUTHENTICATION COMMAND message to "No procedure transaction identity assigned".

The SMF shall set the EAP message IE of the PDU SESSION AUTHENTICATION COMMAND message to the EAP-request message provided by the DN or generated locally.

The SMF shall send the PDU SESSION AUTHENTICATION COMMAND message, and the SMF shall start timer T3590 (see example in figure 6.3.1.1).

Upon receipt of a PDU SESSION AUTHENTICATION COMMAND message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, the UE passes to the upper layers the EAP message received in the EAP message IE of the PDU SESSION AUTHENTICATION COMMAND message. Apart from this action, the authentication and authorization procedure initiated by the DN is transparent to the 5GSM layer of the UE.

6.3.1.2.2 PDU EAP message reliable transport procedure accepted by the UE

When the upper layers provide an EAP-response message responding to the received EAP-request message, the UE shall create a PDU SESSION AUTHENTICATION COMPLETE message.

The UE shall set the EAP message IE of the PDU SESSION AUTHENTICATION COMPLETE message to the EAP-response message.

The UE shall transport the PDU SESSION AUTHENTICATION COMPLETE message and the PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5. Apart from this action, the authentication and authorization procedure initiated by the DN is transparent to the 5GSM layer of the UE.

Upon receipt of a PDU SESSION AUTHENTICATION COMPLETE message, the SMF shall stop timer T3590 and provides the EAP message received in the EAP message IE of the PDU SESSION AUTHENTICATION COMPLETE message to the DN or handles it locally.

6.3.1.2.3 Abnormal cases on the network side

The following abnormal cases can be identified:

a) T3590 expired.

   The SMF shall, on the first expiry of the timer T3590, retransmit the PDU SESSION AUTHENTICATION COMMAND message and shall reset and start timer T3590. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3590, the SMF shall abort the procedure.

Editor's note: Further abnormal cases are FFS

6.3.1.2.4 Abnormal cases in the UE

Editor's note: Abnormal cases are FFS

6.3.1.3 PDU EAP result message transport procedure

6.3.1.3.1 PDU EAP result message transport procedure initiation

In order to initiate the PDU EAP result message transport procedure, the SMF shall create a PDU SESSION AUTHENTICATION RESULT message.

The SMF shall set the PTI IE of the PDU SESSION AUTHENTICATION RESULT message to "No procedure transaction identity assigned".

The SMF shall set the EAP message IE of the PDU SESSION AUTHENTICATION RESULT message to the EAP-success message provided by the DN.

The SMF shall send the PDU SESSION AUTHENTICATION RESULT message.

Upon receipt of a PDU SESSION AUTHENTICATION RESULT message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, the UE passes to the upper layers the EAP message received in the EAP message IE of the PDU SESSION AUTHENTICATION RESULT message. Apart from this action, the authentication and authorization procedure initiated by the DN is transparent to the 5GSM layer of the UE.

6.3.2 Network-requested PDU session modification procedure

6.3.2.1 General

The purpose of the network-requested PDU session modification procedure is to enable the network to modify a PDU session.

6.3.2.2 Network-requested PDU session modification procedure initiation

In order to initiate the network-requested PDU session modification procedure, the SMF shall create a PDU SESSION MODIFICATION COMMAND message.

If the authorized QoS rules of the PDU session is modified, the SMF shall set the authorized QoS rules IE of the PDU SESSION MODIFICATION COMMAND message to the authorized QoS rules of the PDU session.

If the session-AMBR of the PDU session is modified, the SMF shall set the selected Session-AMBR IE of the PDU SESSION MODIFICATION COMMAND message to the session-AMBR of the PDU session.

If interworking to EPS is supported for the PDU session and if the mapped EPS bearer contexts of the PDU session is modified, the SMF shall set the mapped EPS bearer contexts IE of the PDU SESSION MODIFICATION COMMAND message to the mapped EPS bearer contexts of the PDU session. If the association between a QoS flow and the mapped EPS bearer context is changed, the SMF shall set the EPS bearer identity parameter in QoS rules IE of the PDU SESSION MODIFICATION COMMAND message to the new EPS bearer identity associated with the QoS flow.

If the network-requested PDU session modification procedure is triggered by a UE-requested PDU session modification procedure and the PDU SESSION MODIFICATION REQUEST message includes a 5GSM capability IE with the RQoS bit set to "Reflective QoS supported", the SMF shall consider that reflective QoS is supported for QoS flows belonging to this PDU session and may include the RQ timer IE set to an RQ timer value in the PDU SESSION MODIFICATION COMMAND message.

If the network-requested PDU session modification procedure is triggered by a UE-requested PDU session modification procedure and the PDU SESSION MODIFICATION REQUEST message includes a 5GSM capability IE with the MH6-PDU bit to "Multi-homed IPv6 PDU session supported", the SMF shall consider that this PDU session is supported to use multiple IPv6 prefixes.

If the network-requested PDU session modification procedure is triggered by a UE-requested PDU session modification procedure, the PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet" and the PDU SESSION MODIFICATION REQUEST message includes a Maximum number of supported packet filters IE, the SMF shall consider this number as the maximum number of packet filters that can be supported by the UE for this PDU session. Otherwise the SMF considers that the UE supports 16 packet filters for this PDU session.

If the value of the RQ timer is set to "deactivated" or has a value of zero, the UE considers that RQoS is not applied for this PDU session.

If the network-requested PDU session modification procedure is triggered by a UE-requested PDU session modification procedure, the SMF shall set the PTI IE of the PDU SESSION MODIFICATION COMMAND message to the PTI of the PDU SESSION MODIFICATION REQUEST message received as part of the UE-requested PDU session modification procedure.

If the network-requested PDU session modification procedure is not triggered by a UE-requested PDU session modification procedure, the SMF shall set the PTI IE of the PDU SESSION MODIFICATION COMMAND message to "No procedure transaction identity assigned".

If the selected SSC mode of the PDU session is "SSC mode 3" and the SMF requests the relocation of SSC mode 3 PDU session anchor with multiple PDU sessions as specified in 3GPP TS 23.502 [9], the SMF shall include 5GSM cause #39 "reactivation requested" , in the PDU SESSION MODIFICATION COMMAND message, and may include the PDU session address lifetime in a PDU session address lifetime PCO parameter in the Extended protocol configuration options IE of the PDU SESSION MODIFICATION COMMAND message.

The SMF shall send the PDU SESSION MODIFICATION COMMAND message, and the SMF shall start timer T3591 (see example in figure 6.3.2.2.1).

NOTE: If the SMF requests the relocation of SSC mode 3 PDU session anchor with multiple PDU sessions as specified in 3GPP TS 23.502 [9], the reallocation requested indication indicating whether the SMF is to be reallocated or the SMF is to be reused is provided to the AMF.

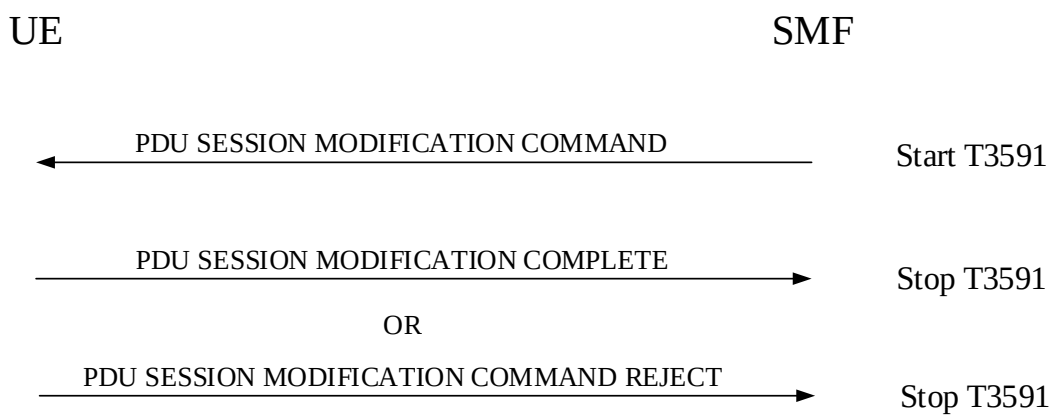


Figure 6.3.2.2.1: Network-requested PDU session modification procedure

6.3.2.3 Network-requested PDU session modification procedure accepted by the UE

Upon receipt of the PDU SESSION MODIFICATION COMMAND message, if the UE provided a DNN for the establishment of the PDU session, the UE shall stop timer T3396, if it is running for the DNN provided by the UE. If the UE did not provide a DNN for the establishment of the PDU session and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop the timer T3396 associated with no DNN if it is running. If the PDU SESSION MODIFICATION COMMAND message was received for an emergency PDU session, the UE shall not stop the timer T3396 associated with no DNN if it is running.

Upon receipt of the PDU SESSION MODIFICATION COMMAND message, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is established, if it is running.

Upon receipt of the PDU SESSION MODIFICATION COMMAND message, if the UE provided an S-NSSAI for the establishment of the PDU session, the UE shall stop timer T35ef, if it is running for the S-NSSAI provided by the UE. If the UE did not provide an S-NSSAI for the establishment of the PDU session and the request type was different from "initial emergency request", the UE shall stop the timer T35ef associated with no S-NSSAI if it is running. If the MODIFY EPS BEARER CONTEXT REQUEST message was received for an emergency PDU session, the UE shall not stop the timer T35ef associated with no S-NSSAI if it is running.

Editor's note: it is FFS whether to stop the timer T35ef in the procedures above.

The UE shall replace the stored authorized QoS rules, session-AMBR and mapped EPS bearer contexts of the PDU session with the received value(s), if any, in the PDU SESSION MODIFICATION COMMAND message. And if a new EPS bearer identity parameter in QoS rules IE is received for a QoS flow which can be transferred to EPS, the UE shall update the association between the QoS flow and the mapped EPS bearer context, based on the new EPS bearer identity and the mapped EPS bearer contexts. If the "Delete existing EPS bearer" operation code in the Mapped EPS bearer contexts IE was received, the UE shall discard the association between the QoS flow and the corresponding mapped EPS bearer context.

Upon receipt of a PDU SESSION MODIFICATION COMMAND message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, if the UE accepts the PDU SESSION MODIFICATION COMMAND message, the UE considers the PDU session as modified and the UE shall create a PDU SESSION MODIFICATION COMPLETE message.

If the PDU SESSION MODIFICATION COMMAND message contains the PTI value allocated in the UE-requested PDU session modification procedure, the UE shall stop the timer T3581. The UE should ensure that the PTI value assigned to this procedure is not released immediately.

NOTE 1: The way to achieve this is implementation dependent. For example, the UE can ensure that the PTI value assigned to this procedure is not released during the time equal to or greater than the default value of timer T3591.

While the PTI value is not released, the UE regards any received PDU SESSION MODIFICATION COMMAND message with the same PTI value as a network retransmission (see subclause 7.3.1).

If the selected SSC mode of the PDU session is "SSC mode 3" and the PDU SESSION MODIFICATION COMMAND message includes 5GSM cause #39 "reactivation requested", the UE can provide to the upper layers the PDU session address lifetime if received in the PDU session address lifetime PCO parameter of the Extended protocol configuration options IE of the PDU SESSION MODIFICATION COMMAND message, and the UE should re-initiate the UE-requested PDU session establishment procedure with a new PDU session ID as specified in subclause 6.4.1 for the PDU session type, the SSC mode, the DNN, and the S-NSSAI if provided in the UE-requested PDU session establishment procedure of the present PDU session, after the completion of the network-requested PDU session modification procedure. The UE shall include the PDU session ID of the old PDU session which is about to get released in the old PDU session ID IE of the UL NAS TRANSPORT message that transports the PDU SESSION ESTABLISHMENT REQUEST message.

NOTE 2: The UE is expected to maintain the PDU session for which the PDU SESSION MODIFICATION COMMAND message including 5GSM cause #39 "reactivation requested" is received during the time indicated by the PDU session address lifetime value or until receiving an indication from upper layers (e.g. that the old PDU session is no more needed).

If the selected PDU session type of the PDU session is "Unstructured" or "Ethernet", the UE supports inter-system change from N1 mode to S1 mode, the UE does not support establishment of a PDN connection for the PDN type set to "non-IP" in S1 mode, and the parameters list field of one or more QoS rules received in the QoS rules IE of the PDU SESSION MODIFICATION COMMAND message contains an EPS bearer identity (EBI) then the UE shall locally remove the EPS bearer identity (EBI) from the parameters list field of such one or more QoS rules.

The UE shall transport the PDU SESSION MODIFICATION COMPLETE message and the PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5.

Upon receipt of a PDU SESSION MODIFICATION COMPLETE message, the SMF shall stop timer T3591 and shall consider the PDU session as modified. If the selected SSC mode of the PDU session is "SSC mode 3" and the PDU SESSION MODIFICATION COMMAND message included 5GSM cause #39 "reactivation requested", the SMF shall start timer T3593. If the PDU Session Address Lifetime value is sent to the UE in the PDU SESSION MODIFICATION COMMAND message then timer T3593 shall be started with the same value, otherwise it shall use a default value.

6.3.2.4 Network-requested PDU session modification procedure not accepted by the UE

Upon receipt of a PDU SESSION MODIFICATION COMMAND message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, if the UE rejects the PDU SESSION MODIFICATION COMMAND message, the UE considers the PDU session as not modified and the UE shall create a PDU SESSION MODIFICATION COMMAND REJECT message.

If the PDU SESSION MODIFICATION COMMAND message contains the PTI value allocated in the UE-requested PDU session modification procedure, the UE shall release the PTI indicated by the PTI IE and shall stop the timer T3581.

The UE shall set the 5GSM cause IE of the PDU SESSION MODIFICATION COMMAND REJECT message to indicate the reason for rejecting the PDU session modification.

If the selected SSC mode of the PDU session is "SSC mode 3" and the PDU SESSION MODIFICATION COMMAND messages includes 5GSM cause #39 "reactivation requested", while the UE does not have sufficient resources for initiating the PDU session establishment procedure as specified in subclause 6.4.1 then the UE shall set cause IE to #26 "insufficient resources".

If the PDU SESSION MODIFICATION COMMAND message includes a request to add a new QoS rule, and the UE decides to reject the addition of the new QoS rule due to e.g. the supported number of QoS rules or number of packet filters associated with a PDU session having reached the maximum number, then the UE shall set the 5GSM cause IE to #26 "insufficient resources".

NOTE: The maximum number of supported QoS rules or packet filters associated with a PDU session is implementation specific.

The 5GSM cause IE typically indicates one of the following 5GSM cause values:

#26 insufficient resources; or

#43 Invalid PDU session identity.

Editor's note: Other 5GSM causes are FFS.

The UE shall transport the PDU SESSION MODIFICATION COMMAND REJECT message and the PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5.

Upon receipt of a PDU SESSION MODIFICATION COMMAND REJECT message, the SMF shall stop timer T3591 and shall consider the PDU session as not modified.

6.3.2.5 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3591.

On the first expiry of the timer T3591, the SMF shall resend the PDU SESSION MODIFICATION COMMAND message and shall reset and restart timer T3591. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3591, the SMF shall abort the procedure and enter the state PDU SESSION ACTIVE.

The SMF may continue to use the previous configuration of the PDU session or initiate the network-requested PDU session release procedure.

b) Invalid PDU session identity.

Upon receipt of the PDU SESSION MODIFICATION COMMAND REJECT message including 5GSM cause #43 "invalid PDU session identity", the SMF shall release the existing PDU session locally without peer-to-peer signalling between the SMF and the UE.

c) Collision of UE-requested PDU session release procedure and network-requested PDU session modification procedure.

If the SMF receives a PDU SESSION RELEASE REQUEST message during the network-requested PDU session modification procedure, and the PDU session indicated in the PDU SESSION RELEASE REQUEST message is the PDU session that the SMF wants to modify, the SMF shall abort the PDU session modification procedure and proceed with the UE-requested PDU session release procedure.

6.3.2.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) No PDU session active for the received PDU session ID.

If the PDU session ID in the PDU SESSION MODIFICATION COMMAND message does not belong to any PDU session in state PDU SESSION ACTIVE in the UE, the UE shall set the 5GSM cause IE to #43 "Invalid PDU session identity" in the PDU SESSION MODIFICATION COMMAND REJECT message.

6.3.3 Network-requested PDU session release procedure

6.3.3.1 General

The purpose of the network-requested PDU session release procedure is to enable the network to release a PDU session.

6.3.3.2 Network-requested PDU session release procedure initiation

In order to initiate the network-requested PDU session release procedure, the SMF shall create a PDU SESSION RELEASE COMMAND message.

The SMF shall set the SM cause IE of the PDU SESSION RELEASE COMMAND message to indicate the reason for releasing the PDU session.

The SM cause IE typically indicates one of the following SM cause values:

#26 insufficient resources;

#29 user authentication or authorization failed;

#36 regular deactivation;

#39 reactivation requested;

#67 insufficient resources for specific slice and DNN; or

#69 insufficient resources for specific slice.

Editor's note: Further 5GSM causes are FFS.

If the selected SSC mode of the PDU session is "SSC mode 2" and the SMF requests the relocation of SSC mode 2 PDU session anchor with different PDU sessions as specified in 3GPP TS 23.502 [9], the SMF shall include 5GSM cause #39 "reactivation requested".

If the network-requested PDU session release procedure is triggered by a UE-requested PDU session release procedure, the SMF shall set the PTI IE of the PDU SESSION RELEASE COMMAND message to the PTI of the PDU SESSION RELEASE REQUEST message received as part of the UE-requested PDU session release procedure.

If the network-requested PDU session release procedure is not triggered by a UE-requested PDU session release procedure, the SMF shall set the PTI IE of the PDU SESSION RELEASE COMMAND message to "No procedure transaction identity assigned".

The SMF may include a Back-off timer value IE in the PDU SESSION RELEASE COMMAND message when the 5GSM cause value #26 "insufficient resources" is included in the PDU SESSION RELEASE COMMAND message. If the 5GSM cause value is #26 "insufficient resources" and the PDU SESSION RELEASE COMMAND message is sent to a UE configured for high priority access in selected PLMN or the request type was set to "initial emergency request" or "existing emergency PDU session" for the establishment of the PDU session, the network shall not include a Back-off timer value IE.

The SMF may include a Back-off timer value IE in the PDU SESSION RELEASE COMMAND message when the 5GSM cause value #67 "insufficient resources for specific slice and DNN" is included in the PDU SESSION RELEASE COMMAND message. If the 5GSM cause value is #67 "insufficient resources for specific slice and DNN" and the PDU SESSION RELEASE COMMAND message is sent to a UE configured for high priority access in selected PLMN or the request type was set to "initial emergency request" or "existing emergency PDU session" for the establishment of the PDU session, the network shall not include a Back-off timer value IE.

The SMF may include a Back-off timer value IE in the PDU SESSION RELEASE COMMAND message when the 5GSM cause #69 "insufficient resources for specific slice" is included in the PDU SESSION RELEASE COMMAND message. If the 5GSM cause value is #69 "insufficient resources for specific slice" and the PDU SESSION RELEASE COMMAND message is sent to a UE configured for high priority access in selected PLMN or the request type was set to "initial emergency request" or "existing emergency PDU session" for the establishment of the PDU session, the network shall not include a Back-off timer value IE.

The SMF shall send:

a) the PDU SESSION RELEASE COMMAND message; and

b) if the SMF allows the AMF to skip sending of the N1 SM container to the UE and the 5GSM cause IE is not set to #39 "reactivation requested", the N1 SM delivery skip allowed indication;

towards the AMF, and the SMF shall start timer T3592 (see example in figure 6.3.3.2.1).

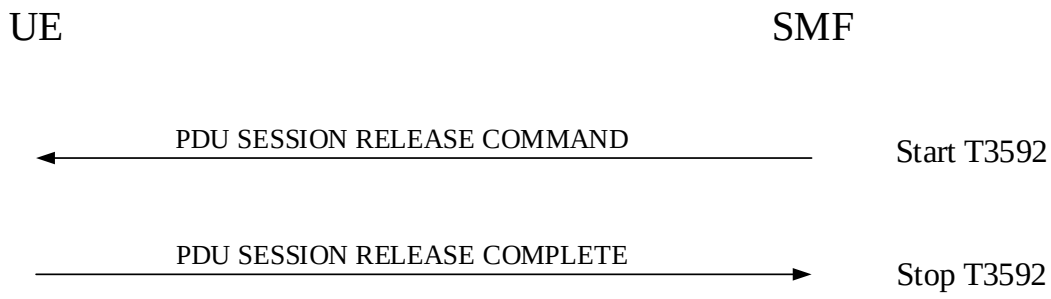


Figure 6.3.3.2.1: Network-requested PDU session release procedure

6.3.3.3 Network-requested PDU session release procedure accepted by the UE

Upon receipt of a PDU SESSION RELEASE COMMAND message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, the UE considers the PDU session as released and the UE shall create an PDU SESSION RELEASE COMPLETE message.

If the PDU SESSION RELEASE COMMAND message contains the PTI value allocated in the UE-requested PDU session release procedure, the UE shall stop the timer T3582. The UE should ensure that the PTI value assigned to this procedure is not released immediately.

NOTE 1: The way to achieve this is implementation dependent. For example, the UE can ensure that the PTI value assigned to this procedure is not released during the time equal to or greater than the default value of timer T3592.

While the PTI value is not released, the UE regards any received PDU SESSION RELEASE COMMAND message with the same PTI value as a network retransmission (see subclause 7.3.1).

If the PDU SESSION RELEASE COMMAND message includes 5GSM cause #39 "reactivation requested", the UE should re-initiate the UE-requested PDU session establishment procedure as specified in subclause 6.4.1 for the PDU session type, the SSC mode, the DNN, and the S-NSSAI as provided in the UE-requested PDU session establishment procedure of the released PDU session, after completion of the network-requested PDU session release procedure.

If the PDU SESSION RELEASE COMMAND message includes 5GSM cause #39 "reactivation requested" and the UE provided an S-NSSAI for the establishment of the PDU session, the UE shall stop timer T35ef if it is running for the S-NSSAI provided by the UE. The UE should then re-initiate the UE requested PDU session establishment procedure for the same S-NSSAI. If the UE did not provide an S-NSSAI for the establishment of the PDU session and the request type was different from "initial emergency request", the UE shall stop the timer T35ef associated with no S-NSSAI if it is running, and should re-initiate the UE requested PDU session establishment procedure without including an S-NSSAI. If the PDU SESSION RELEASE COMMAND message was received for an emergency PDU session, the UE shall not stop the timer T35ef associated with no S-NSSAI if it is running.

If the PDU SESSION RELEASE COMMAND message includes 5GSM cause #39 "reactivation requested" and the UE provided a DNN for the establishment of the PDU session, the UE shall stop timer T3396 if it is running for the DNN provided by the UE. The UE should then re-initiate the UE requested PDU session establishment procedure for the same DNN. If the UE did not provide a DNN for the establishment of the PDU session and the request type was

different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop the timer T3396 associated with no DNN if it is running, and should re-initiate the UE requested PDU session establishment procedure without including a DNN. If the PDU SESSION RELEASE COMMAND message was received for an emergency PDU session, the UE shall not stop the timer T35cd associated with no DNN if it is running.

If the PDU SESSION RELEASE COMMAND message includes 5GSM cause #39 "reactivation requested", the UE shall stop timer T35cd if it is running for the same [S-NSSAI, DNN] combination provided by the UE. The UE should then re-initiate the UE requested PDU session establishment procedure for the same [S-NSSAI, DNN] combination. If the UE did not provide a DNN for the establishment of the PDU session and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop the timer T35cd associated with [S-NSSAI, no DNN] if it is running, and should re-initiate the UE requested PDU session establishment procedure with the same S-NSSAI but without a DNN. If the PDU SESSION RELEASE COMMAND message was received for an emergency PDU session, the UE shall not stop the timer T35cd associated with [S-NSSAI, no DNN] if it is running.

NOTE 2: User interaction is necessary in some cases when the UE cannot re-initiate the UE-requested PDU session establishment procedure automatically.

If the PDU SESSION RELEASE COMMAND message includes 5GSM cause #26 "insufficient resources" and the Back-off timer value IE, the UE shall take different actions depending on the timer value received for timer T3396 in the Back-off timer value:

a) If the timer value indicates neither zero nor deactivated and a DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message, the UE shall stop timer T3396 associated with the corresponding DNN, if it is running. If the timer value indicates neither zero nor deactivated and no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop timer T3396 associated with no DNN if it is running. The UE shall then start timer T3396 with the value provided in the Back-off timer value IE and:

   1) shall not send a PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same DNN that was sent by the UE, until timer T3396 expires or timer T3396 is stopped; and

   2) shall not send a PDU SESSION ESTABLISHMENT REQUEST message without an DNN and with request type different from "initial emergency request" and different from "existing emergency PDU session", or a PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an DNN provided by the UE, if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", until timer T3396 expires or timer T3396 is stopped.

   The UE shall not stop timer T3396 upon a PLMN change or inter-system change;

b) if the timer value indicates that this timer is deactivated and a DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message, the UE shall stop timer T3396 associated with the corresponding DNN, if it is running. If the timer value indicates that this timer is deactivated and no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop timer T3396 associated with no DNN if it is running. The UE:

   1) shall not send a PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST for the same DNN until the UE is switched off or the USIM is removed, or the UE receives an PDU SESSION MODIFICATION REQUEST message for the same DNN from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same DNN from the network; and

   2) shall not send a PDU SESSION ESTABLISHMENT REQUEST message without an DNN and with request type different from "initial emergency request" and different from "existing emergency PDU session", or a PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an DNN provided by the UE, if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", until the UE is switched off or the USIM is removed, or the UE receives an PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an DNN provided by the UE, or a PDU SESSION RELEASE COMMAND messages including

5GSM cause IE set to 5GSM cause #39 "reactivation requested" for a non-emergency PDU session established without an DNN provided by the UE.

The timer T3396 remains deactivated upon a PLMN change or inter-system change; and

c) if the timer value indicates zero, the UE:

1) shall stop timer T3396 associated with the corresponding DNN, if running, and may send a PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same DNN; and

2) if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop timer T3396 associated with no DNN, if running, and may send a PDU SESSION ESTABLISHMENT REQUEST message without a DNN, or a PDU SESSION MODIFICATION REQUEST message without an DNN provided by the UE.

If the PDU SESSION RELEASE COMMAND message includes 5GSM cause #26 "insufficient resources" and the Back-off timer value IE is not included, then the UE may send a PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same DNN or without a DNN.

When the timer T3396 is running or the timer is deactivated, the UE is allowed to initiate a PDU session establishment procedure for emergency services.

If the timer T3396 is running when the UE enters state 5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T3396 is kept running until it expires or it is stopped.

If the UE is switched off when the timer T3396 is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

let t1 be the time remaining for T3396 timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

If the 5GSM cause value is #67 "insufficient resources for specific slice and DNN" and the Back-off timer value IE is included, the UE shall take different actions depending on the timer value received for timer T35cd in the Back-off timer value:

a) If the timer value indicates neither zero nor deactivated, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is established, if it is running. The UE shall then start timer T35cd with the value provided in the Back-off timer value IE. The UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message with request type different from "initial emergency request" and different from "existing emergency PDU session", or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination that was sent by the UE, until timer T35cd expires or timer T35cd is stopped;

The UE shall not stop timer T35cd upon a PLMN change or inter-system change;

b) if the timer value indicates that this timer is deactivated, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is established, if it is running. The UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message with request type different from "initial emergency request" and different from "existing emergency PDU session", or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination that was sent by the UE, until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same [S-NSSAI, DNN] combination from the network; and

The timer T35cd remains deactivated upon a PLMN change or inter-system change; and

c) if the timer value indicates zero, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination that was sent by the UE, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

If the Back-off timer value IE is not included, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST message or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

When the timer T35cd is running or the timer is deactivated, the UE is allowed to initiate a PDU session establishment procedure for emergency services.

If the timer T35cd is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T35cd is kept running until it expires or it is stopped.

If the UE is switched off when the timer T35cd is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

let t1 be the time remaining for T35cd timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

NOTE 3: As described in this subclause, upon PLMN change or inter-system change, the UE does not stop the timer T35cd or T35ef. This means the timer T35cd or T35ef can still be running or be deactivated for the given 5GSM procedure, the PLMN, the S-NSSAI and optionally the DNN combination when the UE returns to the PLMN or when it performs inter-system change back from S1 mode to N1 mode. Thus the UE can still be prevented from sending another PDU SESSION ESTABLISHMENT REQUEST message in the PLMN for the same S-NSSAI and optionally the same DNN.

Upon PLMN change, if T35cd is running or is deactivated for a S-NSSAI, a DNN, and old PLMN, but T35cd is not running and is not deactivated for the S-NSSAI, the DNN, and new PLMN, then the UE is allowed to send a PDU SESSION ESTABLISHMENT REQUEST message for the same S-NSSAI and the same DNN in the new PLMN.

Upon PLMN change, if T35ef is running or is deactivated for a S-NSSAI and old PLMN, but T35cd is not running and is not deactivated for the S-NSSAI and new PLMN, then the UE is allowed to send a PDU SESSION ESTABLISHMENT REQUEST message for the same S-NSSAI in the new PLMN.

The UE shall transport the PDU SESSION RELEASE COMPLETE message and the PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5.

Upon receipt of a PDU SESSION RELEASE COMPLETE message, the SMF shall stop timer T3592 and shall consider the PDU session as released.

6.3.3.4 N1 SM delivery skipped

If the PDU SESSION RELEASE COMMAND message was sent along the N1 SM delivery skip allowed indication towards AMF, then upon receipt of an indication that N1 SM delivery was skipped, the SMF shall stop timer T3592 and shall consider the PDU session as released.

6.3.3.5 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Expiry of timer T3592.

The SMF shall, on the first expiry of the timer T3592, retransmit the PDU SESSION RELEASE COMMAND message and shall reset and start timer T3592. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3592, the SMF shall abort the procedure.

b) Collision of network-requested PDU session release procedure and UE-requested PDU session modification procedure.

When the SMF receives a PDU SESSION MODIFICATION REQUEST message during the network-requested PDU session release procedure, and the PDU session indicated in PDU SESSION MODIFICATION REQUEST message is the PDU session that the SMF wants to release, the SMF shall ignore the PDU SESSION MODIFICATION REQUEST message and proceed with the PDU session release procedure.

c) Collision of network-requested PDU session release procedure and UE-requested PDU session release procedure.

If the SMF receives a PDU SESSION RELEASE REQUEST message after sending a PDU SESSION RELEASE COMMAND message to the UE, and the PDU session ID in the PDU SESSION RELEASE REQUEST message is the same as the PDU session ID in the PDU SESSION RELEASE COMMAND message, the SMF shall ignore the PDU SESSION RELEASE REQUEST message and proceed with the network-requested PDU session release procedure.

6.3.3.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) No PDU session active for the received PDU session ID.

If the PDU session ID in the PDU SESSION RELEASE COMMAND message does not belong to any PDU session in state PDU SESSION ACTIVE in the UE, the UE shall include the 5GSM cause #43 "Invalid PDU session identity" in the extended protocol configuration options IE of the PDU SESSION RELEASE COMPLETE message, and transport the message and the received PDU session ID using the NAS transport procedure as specified in subclause 5.4.5.

6.4 UE-requested 5GSM procedures

6.4.1 UE-requested PDU session establishment procedure

6.4.1.1 General

The purpose of the UE-requested PDU session establishment procedure is to establish a new PDU session with a DN or to perform handover of an existing PDU session between 3GPP access and non-3GPP access or to transfer an existing PDN connection in the EPS to the 5GS. If accepted by the network, the PDU session enables exchange of PDUs between the UE and the DN. The UE shall not request a PDU session establishment for an LADN when the UE is located outside the LADN service area.

6.4.1.2 UE-requested PDU session establishment procedure initiation

In order to initiate the UE-requested PDU session establishment procedure, the UE shall create a PDU SESSION ESTABLISHMENT REQUEST message.

NOTE 1: When IMS voice is available over either 3GPP access or non-3GPP access, the "voice centric" UE in 5GMM-REGISTERED state will receive a request from upper layers to establish the PDU session for IMS signalling, if the conditions for performing an initial registration with IMS indicated in 3GPP TS 24.229 [14] subclause U.3.1.2 are satisfied.

The UE shall allocate a PDU session ID which is not currently being used by another PDU session over either 3GPP access or non-3GPP access.

The UE shall allocate a PTI value currently not used and shall set the PTI IE of the PDU SESSION ESTABLISHMENT REQUEST message to the allocated PTI value.

If the UE requests to establish a new non-emergency PDU session with a DN and requests a PDU session type, the UE shall set the PDU session type IE of the PDU SESSION ESTABLISHMENT REQUEST message to one of the following values: the IP version capability as specified in subclause 6.2.4.2, "Ethernet" or "Unstructured".

NOTE 2: When the UE initiates the UE-requested PDU session establishment procedure to transfer an existing non-IP PDN connection in the EPS to the 5GS, the UE can use locally available information associated with the PDN connection to select the PDU session type between "Ethernet" and "Unstructured".

If the UE requests to establish a new non-emergency PDU session with a DN and the UE requests an SSC mode, the UE shall set the SSC mode IE of the PDU SESSION ESTABLISHMENT REQUEST message to the SSC mode. If the UE requests to establish a PDU session of "IPv4", "IPv6" or "IPv4v6" PDU session type, the UE shall either omit the SSC mode IE or set the SSC mode IE to "SSC mode 1", "SSC mode 2", or "SSC mode 3". If the UE requests to establish a

PDU session of "Ethernet" or "Unstructured" PDU session type, the UE shall either omit the SSC mode IE or set the SSC mode IE to "SSC mode 1" or "SSC mode 2". If the UE requests transfer of an existing PDN connection in the EPS to the 5GS, the UE shall set the SSC mode IE to "SSC mode 1".

If the UE requests to establish a new emergency PDU session, the UE shall set the SSC mode IE of the PDU SESSION ESTABLISHMENT REQUEST message to "SSC mode 1".

If the UE requests to establish a new PDU session with a DN, the UE may include the SM PDU DN request container with a DN-specific identity of the UE complying with network access identifier (NAI) format as specified in IETF RFC 4282 [37].

If the UE requests to establish a new PDU session of "IPv4", "IPv6", "IPv4v6" or "Ethernet" PDU session type and the UE supports reflective QoS, the UE should set the RQoS bit to "Reflective QoS supported" in the 5GSM capability IE of the PDU SESSION ESTABLISHMENT REQUEST message.

NOTE 3: The determination to not request the usage of reflective QoS by the UE for a PDU session is implementation dependent.

If the UE requests to establish a new PDU session of "IPv4", "IPv6", "IPv4v6", or "Ethernet" PDU session type, and the UE can support more than 16 packet filters for this PDU session, the UE shall indicate the maximum number of packet filters that can be supported for the PDU session in the Maximum number of supported packet filters IE of the PDU SESSION ESTABLISHMENT REQUEST message.

If the UE requests to establish a new PDU session of "IPv6" or "IPv4v6" PDU session type and the UE supports acting as a type C host as specified in IETF RFC 4191 [36], the UE shall set the MH6-PDU bit to "Multi-homed IPv6 PDU session supported" in the 5GSM capability IE of the PDU SESSION ESTABLISHMENT REQUEST message.

If the UE has an emergency PDU session, the UE shall not perform the UE-requested PDU session establishment procedure to establish another emergency PDU session. The UE may perform the UE-requested PDU session establishment procedure to transfer an existing emergency PDU session or an existing PDN connection for emergency bearer services.

If the UE operating in the single-registration mode performs mobility from S1 mode to N1 mode and the UE wants to establish a PDU session corresponding to an existing PDN connection in EPS for which interworking to 5GS is supported, the UE shall:

a) set the PDU session ID in the PDU SESSION ESTABLISHMENT REQUEST message and in the UL NAS TRANSPORT message to the stored PDU session ID corresponding to the PDN connection; and

b) set the S-NSSAI in the UL NAS TRANSPORT message to the stored S-NSSAI associated with the PDU session ID only if the S-NSSAI is included in the allowed NSSAI.

If the UE supports 3GPP PS data off, the UE shall include the extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT REQUEST message and include the 3GPP PS data off UE status. The UE behaves as described in subclause 6.2.10.

The UE shall transport:

a) the PDU SESSION ESTABLISHMENT REQUEST message;

b) the PDU session ID of the PDU session being established;

c) if the request type is set to:

1) "initial request" and the UE determined to establish a new PDU session based on a URSP rule including one or more S-NSSAIs in the URSP (see subclause 6.2.9):

i) in case of a non-roaming scenario, an S-NSSAI in the allowed NSSAI which corresponds to one of the S-NSSAI(s) in the URSP rule, if any; or

ii) in case of a roaming scenario:

A) one of the mapped configured S-NSSAI(s) for the HPLMN which corresponds to one of the S-NSSAI(s) in the URSP rule, if any; and

B) the S-NSSAI in the allowed NSSAI associated with the S-NSSAI in A);

2) "existing PDU session", an S-NSSAI, which is an S-NSSAI associated with the PDU session and, if available in roaming scenarios, a mapped configured S-NSSAI from the configured NSSAI for the HPLMN;

d) the requested DNN, if the request type is set to "initial request" or "existing PDU session", and the UE requests a connectivity to a DNN other than the default DNN;

e) the request type which is set to:

1) "initial request", if the UE is not registered for emergency services and the UE requests to establish a new non-emergency PDU session;

2) "existing PDU session", if the UE is not registered for emergency services and the UE requests:

i) handover of an existing non-emergency PDU session between 3GPP access and non-3GPP access; or

ii) transfer of an existing PDN connection for non-emergency bearer services in the EPS to the 5GS;

3) "initial emergency request", if the UE requests to establish a new emergency PDU session; and

4) "existing emergency PDU session", if the UE requests:

i) handover of an existing emergency PDU session between 3GPP access and non-3GPP access; or

ii) transfer of an existing PDN connection for emergency bearer services in the EPS to the 5GS; and

f) the old PDU session ID which is the PDU session ID of the existing PDU session, if the UE initiates the UE-requested PDU session establishment procedure upon receiving the PDU SESSION MODIFICATION COMMAND messages with the 5GSM cause IE set to #39 "reactivation requested";

using the NAS transport procedure as specified in subclause 5.4.5, and the UE shall start timer T3580 (see example in figure 6.4.1.2.1).

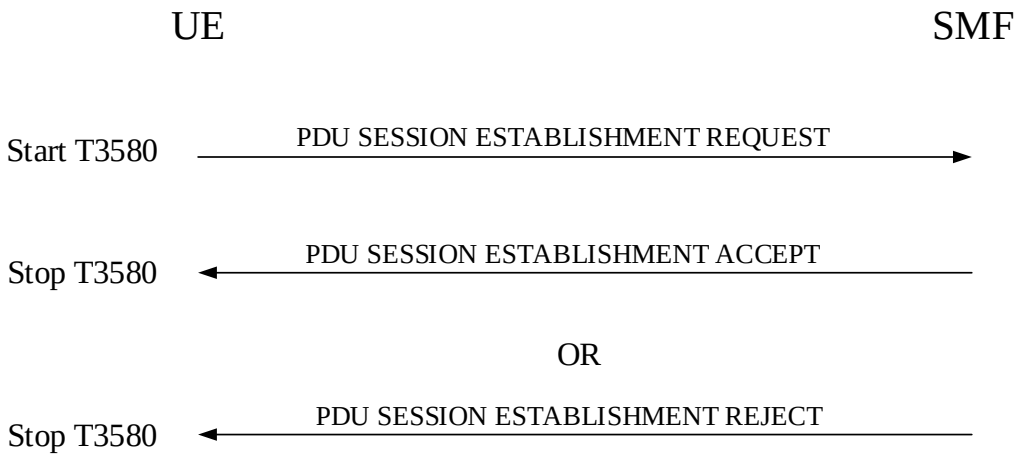


Figure 6.4.1.2.1: UE-requested PDU session establishment procedure

Upon receipt of a PDU SESSION ESTABLISHMENT REQUEST message, a PDU session ID, optionally a S-NSSAI, optionally a DNN, the request type, and optionally an old PDU session ID, the SMF checks whether connectivity with the requested DN can be established. If the requested DNN is not included, the SMF shall use the default DNN.

If the PDU session being established is a non-emergency PDU session, the request type is not set to "existing PDU session" and the PDU session authentication and authorization by the external DN is required due to local policy, the SMF shall check whether the PDU SESSION ESTABLISHMENT REQUEST message includes the PDU DN request container.

If the PDU session being established is a non-emergency PDU session, the request type is not set to "existing PDU session", the PDU DN request container is included in the PDU SESSION ESTABLISHMENT REQUEST message

and the PDU session authentication and authorization by the external DN is required due to local policy and user's subscription data, the SMF shall:

a) if the information for the PDU session authentication and authorization by the external DN in PDU DN request container is compliant with the local policy and user's subscription data, proceed with the EAP Authentication procedure specified in 3GPP TS 33.501 [24] and refrain from accepting or rejecting the PDU SESSION ESTABLISHMENT REQUEST message until the EAP Authentication procedure finalizes; and

b) if the information for the PDU session authentication and authorization by the external DN in PDU DN request container is not compliant with the local policy, reject the PDU session establishment request including the 5GSM cause #29 "user authentication failed", in the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU session being established is a non-emergency PDU session, the request type is not set to "existing PDU session", the PDU DN request container is not included in the PDU SESSION ESTABLISHMENT REQUEST message and the PDU session authentication and authorization by the external DN is required due to local policy and user's subscription data, the SMF shall proceed with the EAP Authentication procedure specified in 3GPP TS 33.501 [24] and refrain from accepting or rejecting the PDU SESSION ESTABLISHMENT REQUEST message until the EAP Authentication procedure finalizes.

If the SMF receives the old PDU session ID from the AMF and a PDU session exists for the old PDU session ID, the SMF shall consider that the request for the relocation of SSC mode 3 PDU session anchor with multiple PDU sessions as specified in 3GPP TS 23.502 [9] is accepted by the UE.

6.4.1.3 UE-requested PDU session establishment procedure accepted by the network

If the connectivity with the requested DN is accepted by the network, the SMF shall create a PDU SESSION ESTABLISHMENT ACCEPT message.

The SMF shall set the authorized QoS rules IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the authorized QoS rules of the PDU session. If the received request type is "initial emergency request", the SMF shall set the authorized QoS rules IE according to the initial QoS parameters used for establishing emergency services configured in the SMF emergency configuration data.

If interworking to EPS is supported for the PDU session, the SMF shall set in the PDU SESSION ESTABLISHMENT ACCEPT message:

a) the Mapped EPS bearer contexts IE to the EPS bearer contexts mapped from one or more QoS flows of the PDU session context; and

b) the EPS bearer identity parameter in the QoS rules IE to the EPS bearer identity corresponding to the QoS flow, for each QoS flow which can be transferred to EPS.

Furthermore, the SMF shall store the association between the QoS flow and the mapped EPS bearer context, for each QoS flow which can be transferred to EPS.

The SMF shall set the selected SSC mode IE of the PDU SESSION ESTABLISHMENT ACCEPT message to:

a) the received SSC mode in the SSC mode IE included in the PDU SESSION ESTABLISHMENT REQUEST message based on the subscription, the SMF configuration, or both.;

b) either the default SSC mode for the data network listed in the subscription or the SSC mode associated with the SMF configuration, if the SSC mode IE is not included in the PDU SESSION ESTABLISHMENT REQUEST message.

If the PDU session is an emergency PDU session, the SMF shall set the Selected SSC mode IE of the PDU SESSION ESTABLISHMENT ACCEPT message to "SSC mode 1". If the PDU session is a non-emergency PDU session of "Ethernet" or "Unstructured" PDU session type, the SMF shall set the Selected SSC mode IE to "SSC mode 1" or "SSC mode 2". If the PDU session is a non-emergency PDU session of "IPv4", "IPv6" or "IPv4v6" PDU session type, the SMF shall set the selected SSC mode IE to "SSC mode 1", "SSC mode 2", or "SSC mode 3".

If the PDU session is a non-emergency PDU session, the SMF shall set the S-NSSAI IE of the PDU SESSION ESTABLISHMENT ACCEPT message to:

a) the S-NSSAI of the PDU session; and

b) the mapped configured S-NSSAI for the HPLMN, if available, in roaming scenarios.

The SMF shall set the selected PDU session type IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the PDU session type of the PDU session.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IPv4v6", the SMF shall select "IPv4", "IPv6" or "IPv4v6" as the selected PDU session type IE of the PDU session. If the subscription, the SMF configuration, or both, are limited to IPv4 only or IPv6 only for the requested DNN, the SMF shall include the 5GSM cause value #50 "PDU session type IPv4 only allowed", or #51 "PDU session type IPv6 only allowed", respectively, in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT ACCEPT message.

If the selected PDU session type is "IPv4", the SMF shall include the PDU address IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the PDU address IE to an IPv4 address is allocated to the UE in the PDU session.

If the selected PDU session type is "IPv6", the SMF shall include the PDU address IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the PDU address IE to an interface identifier for the IPv6 link local address allocated to the UE in the PDU session.

If the selected PDU session type is "IPv4v6", the SMF shall include the PDU address IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the PDU address IE to an IPv4 address and an interface identifier for the IPv6 link local address, allocated to the UE in the PDU session.

The SMF shall set the DNN IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the DNN of the PDU session.

The SMF shall set the Session-AMBR IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the Session-AMBR of the PDU session.

If the selected PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet" and if the PDU SESSION ESTABLISHMENT REQUEST message includes a 5GSM capability IE with the RQoS bit set to "Reflective QoS supported", the SMF shall consider that reflective QoS is supported for QoS flows belonging to this PDU session and may include the RQ timer IE set to an RQ timer value in the PDU SESSION ESTABLISHMENT ACCEPT message.

If the selected PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet" and if the PDU SESSION ESTABLISHMENT REQUEST message includes a Maximum number of supported packet filters IE, the SMF shall consider this number as the maximum number of packet filters that can be supported by the UE for this PDU session. Otherwise the SMF considers that the UE supports 16 packet filters for this PDU session.

If the value of the RQ timer is set to "deactivated" or has a value of zero, the UE considers that RQoS is not applied for this PDU session.

NOTE: If the 5G core network determines that reflective QoS is to be used for a QoS flow, the SMF sends reflective QoS indication (RQI) to UPF to activate reflective QoS. If the QoS flow is established over 3GPP access, the SMF also includes reflective QoS Attribute (RQA) in QoS profile of the QoS flow during QoS flow establishment.

If the selected PDU session type is "IPv6" or "IPv4v6" and if the PDU SESSION ESTABLISHMENT REQUEST message includes a 5GSM capability IE with the MH6-PDU bit set to "Multi-homed IPv6 PDU session supported", the SMF shall consider that this PDU session is supported to use multiple IPv6 prefixes.

If the DN authentication of the UE was performed and completed successfully, the SMF shall set the EAP message IE of the PDU SESSION ESTABLISHMENT ACCEPT message to an EAP-success message as specified in IETF RFC 3748 [34], provided by the DN.

The SMF shall send the PDU SESSION ESTABLISHMENT ACCEPT message.

Upon receipt of a PDU SESSION ESTABLISHMENT ACCEPT message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, the UE shall stop timer T3580, shall release the allocated PTI value and shall consider that the PDU session was established.

The UE shall store the authorized QoS rules and session-AMBR received in the PDU SESSION ESTABLISHMENT ACCEPT message for the PDU session.

The UE shall store the mapped EPS bearer contexts, if received in the PDU SESSION ESTABLISHMENT ACCEPT message. Furthermore, the UE shall also store the association between the QoS flow and the mapped EPS bearer context, for each QoS flow which can be transferred to EPS, based on the received EPS bearer identity parameter in QoS rules IE and the mapped EPS bearer contexts.

If the UE requests the PDU session type "IPv4v6" and:

a) the UE receives the selected PDU session type set to "IPv4" and does not receive the 5GSM cause value #50 "PDU session type IPv4 only allowed"; or

b) the UE receives the selected PDU session type set to "IPv6" and does not receive the 5GSM cause value #51 "PDU session type IPv6 only allowed";

the UE may subsequently request another PDU session for the other IP version using the UE-requested PDU session establishment procedure to the same DNN (or no DNN, if no DNN was indicated by the UE) and the same S-NSSAI (or no S-NSSAI, if no S-NSSAI was indicated by the UE) with a single address PDN type (IPv4 or IPv6) other than the one already activated.

If the UE requests the PDU session type "IPv4v6", receives the selected PDU session type set to "IPv4" and the 5GSM cause value #50 "PDU session type IPv4 only allowed", the UE shall not subsequently request another PDU session for "IPv6" using the UE-requested PDU session establishment procedure to the same DNN (or no DNN, if no DNN was indicated by the UE) and the same S-NSSAI (or no S-NSSAI, if no S-NSSAI was indicated by the UE) and the PDU session type "IPv6" until the PDU session is released.

If the UE requests the PDU session type "IPv4v6", receives the selected PDU session type set to "IPv6" and the 5GSM cause value #51 "PDU session type IPv6 only allowed", the UE shall not subsequently request another PDU session for "IPv4" using the UE-requested PDU session establishment procedure to the same DNN (or no DNN, if no DNN was indicated by the UE) and the same S-NSSAI (or no S-NSSAI, if no S-NSSAI was indicated by the UE) and the PDU session type "IPv4" until the PDU session is released.

If the selected PDU session type of the PDU session is "Unstructured" or "Ethernet", the UE supports inter-system change from N1 mode to S1 mode, the UE does not support establishment of a PDN connection for the PDN type set to "non-IP" in S1 mode, and the parameters list field of one or more QoS rules received in the QoS rules IE of the PDU SESSION ESTABLISHMENT ACCEPT message contains an EPS bearer identity (EBI) then the UE shall locally remove the EPS bearer identity (EBI) from the parameters list field of such one or more QoS rules.

6.4.1.4 UE requested PDU session establishment procedure not accepted by the network

6.4.1.4.1 General

If the connectivity with the requested DN is rejected by the network, the SMF shall create a SM PDU SESSION ESTABLISHMENT REJECT message.

If the UE requests a PDU session establishment for an LADN when the UE is located outside the LADN service area, the SMF shall reject the request.

The SMF shall set the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message to indicate the reason for rejecting the PDU session establishment.

The 5GSM cause IE typically indicates one of the following SM cause values:

#26 insufficient resources;

#27 missing or unknown DNN;

#28 unknown PDU session type;

#29 user authentication failed;

#31 request rejected, unspecified;

#34 service option temporarily out of order;

#35 PTI already in use;

#50 PDU session type IPv4 only allowed;

#51 PDU session type IPv6 only allowed;

#54 PDU session does not exist;

#67 insufficient resources for specific slice and DNN;

#68 not supported SSC mode;

#69 insufficient resources for specific slice; or

#70 missing or unknown DNN in a slice.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IPv6", and the subscription, the SMF configuration, or both, are limited to IPv4 only for the requested DNN, the SMF shall include the 5GSM cause value #50 "PDU session type IPv4 only allowed" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IPv6", and the subscription, the SMF configuration, or both, support none of "IPv4" and "IPv6" PDU session types for the requested DNN, the SMF shall include the 5GSM cause value #28 "unknown PDU session type" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IPv4", and the subscription, the SMF configuration, or both, are limited to IPv6 only for the requested DNN, the SMF shall include the 5GSM cause value #51 "PDU session type IPv6 only allowed" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IPv4", and the subscription, the SMF configuration, or both, support none of "IPv4" and "IPv6" PDU session types for the requested DNN, the SMF shall include the 5GSM cause value #28 "unknown PDU session type" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IPv4v6", and the subscription, the SMF configuration, or both, support none of "IPv4v6", "IPv4" and "IPv6" PDU session types for the requested DNN, the SMF shall include the 5GSM cause value #28 "unknown PDU session type" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "Unstructured" or "Ethernet", and the subscription, the SMF configuration, or both, do not support the PDU session type for the requested DNN, the SMF shall include the 5GSM cause value #28 "unknown PDU session type" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU SESSION ESTABLISHMENT REQUEST message contains the SSC mode IE indicating an SSC mode not supported by the subscription, the SMF configuration, or both of them, and the SMF decides to rejects the PDU session establishment, the SMF shall include the 5GSM cause value #68 "not supported SSC mode" in the 5GSM cause IE and the SSC modes allowed by SMF in the Allowed SSC mode IE of the PDU SESSION ESTABLISHMENT REJECT message.

The SMF may include a Back-off timer value IE in the PDU SESSION ESTABLISHMENT REJECT message when the 5GSM cause value #26"insufficient resources" is included in the PDU SESSION ESTABLISHMENT REJECT message. If the 5GSM cause value is #26"insufficient resources" and the PDU SESSION ESTABLISHMENT REQUEST message was received from a UE configured for high priority access in selected PLMN or the request type in the PDU SESSION ESTABLISHMENT REQUEST message is set to "initial emergency request" or "existing emergency PDU session", the network shall not include a Back-off timer value IE.

The SMF may include a Back-off timer value IE in the PDU SESSION ESTABLISHMENT REJECT message when the 5GSM cause value #67 "insufficient resources for specific slice and DNN" is included in the PDU SESSION ESTABLISHMENT REJECT message. If the 5GSM cause value is #67 "insufficient resources for specific slice and DNN" and the PDU SESSION ESTABLISHMENT REQUEST message was received from a UE configured for high priority access in selected PLMN or the request type is "initial emergency request" or "existing emergency PDU

session" in the PDU SESSION ESTABLISHMENT REQUEST message, the network shall not include a Back-off timer value IE.

Editor's note: Whether the SMF knows that the UE is a UE configured for high priority access so as not to include the Back-off timer is FFS.

The SMF may include a Back-off timer value IE in the PDU SESSION ESTABLISHMENT REJECT message when the 5GSM cause #69 "insufficient resources for specific slice" is included in the PDU SESSION ESTABLISHMENT REJECT message. If the 5GSM cause value is #69 "insufficient resources for specific slice" and the PDU SESSION ESTABLISHMENT REQUEST message was received from a UE configured for high priority access in selected PLMN or the request type is "initial emergency request" or "existing emergency PDU session" in the PDU SESSION ESTABLISHMENT REQUEST message, the network shall not include a Back-off timer value IE.

The SMF shall send the SM PDU SESSION ESTABLISHMENT REJECT message.

Upon receipt of a PDU SESSION ESTABLISHMENT REJECT message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, the UE shall stop timer T3580 shall release the allocated PTI value and shall consider that the PDU session was not established.

If the DN authentication of the UE was performed and completed unsuccessfully, the SMF shall include the 5GSM cause value #29 "user authentication failed" in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT REJECT message and shall set the EAP message IE of the PDU SESSION ESTABLISHMENT REJECT message to an EAP-failure message as specified in IETF RFC 3748 [34], provided by the DN.

If:

- the 5GSM cause value #26 "insufficient resources" and the Back-off timer value IE are included in the PDU SESSION ESTABLISHMENT REJECT message; or

- an indication that the 5GSM message was not forwarded due to DNN based congestion control is received along a Back-off timer value and a PDU SESSION ESTABLISHMENT REQUEST message with the PDU session ID IE set to the PDU session ID of the PDU session;

the UE shall take different actions depending on the timer value received for timer T3396 in the Back-off timer value:

a) If the timer value indicates neither zero nor deactivated and a DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message, the UE shall stop timer T3396 associated with the corresponding DNN, if it is running. If the timer value indicates neither zero nor deactivated and no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop timer T3396 associated with no DNN if it is running. The UE shall then start timer T3396 with the value provided in the Back-off timer value IE and:

   1) shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same DNN that was sent by the UE, until timer T3396 expires or timer T3396 is stopped; and

   2) shall not send another PDU SESSION ESTABLISHMENT REQUEST message without a DNN and with request type different from "initial emergency request" and different from "existing emergency PDU session", or another PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without a DNN provided by the UE, if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", until timer T3396 expires or timer T3396 is stopped.

   The UE shall not stop timer T3396 upon a PLMN change or inter-system change;

b) if the timer value indicates that this timer is deactivated and a DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message, the UE shall stop timer T3396 associated with the corresponding DNN, if it is running. If the timer value indicates that this timer is deactivated and no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop timer T3396 associated with no DNN if it is running. The UE:

   1) shall not send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST for the same DNN until the UE is switched off or the USIM is removed, or the

UE receives a PDU SESSION MODIFICATION REQUEST message for the same DNN from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same DNN from the network; and

2) shall not send another PDU SESSION ESTABLISHMENT REQUEST message without a DNN and with request type different from "initial emergency request" and different from "existing emergency PDU session", or another PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without a DNN provided by the UE, if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without a DNN provided by the UE, or a PDU SESSION RELEASE COMMAND messages including 5GSM cause IE set to 5GSM cause #39 "reactivation requested" for a non-emergency PDU session established without a DNN provided by the UE.

The timer T3396 remains deactivated upon a PLMN change or inter-system change; and

c) if the timer value indicates zero, the UE:

1) shall stop timer T3396 associated with the corresponding DNN, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same DNN; and

2) if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop timer T3396 associated with no DNN, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST message without a DNN, or another PDU SESSION MODIFICATION REQUEST message without a DNN provided by the UE.

If the Back-off timer value IE is not included or no Back-off timer value is received from the 5GMM sublayer, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same DNN or without a DNN.

When the timer T3396 is running or the timer is deactivated, the UE is allowed to initiate a PDU session establishment procedure for emergency services.

If the timer T3396 is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T3396 is kept running until it expires or it is stopped.

If the UE is switched off when the timer T3396 is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

let t1 be the time remaining for T3396 timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

If:

- the 5GSM cause value #67 "insufficient resources for specific slice and DNN" and the Back-off timer value IE are included in the PDU SESSION ESTABLISHMENT REJECT message; or

- an indication that the 5GSM message was not forwarded due to S-NSSAI and DNN based congestion control is received along a Back-off timer value and a PDU SESSION ESTABLISHMENT REQUEST message with the PDU session ID IE set to the PDU session ID of the PDU session;

the UE shall take different actions depending on the timer value received for timer T35cd in the Back-off timer value:

a) If the timer value indicates neither zero nor deactivated, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided during the PDU session establishment, if it is running. If the timer value indicates neither zero nor deactivated and no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop timer T35cd associated with [S-NSSAI, no DNN] combination if it is running. The UE shall then start timer T35cd with the value provided in the Back-off timer value IE and:

1) shall not send another PDU SESSION ESTABLISHMENT REQUEST message with request type different from "initial emergency request" and different from "existing emergency PDU session", or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination that was sent by the UE, until timer T35cd expires or timer T35cd is stopped; and

2) shall not send another PDU SESSION ESTABLISHMENT REQUEST message with request type different from "initial emergency request" and different from "existing emergency PDU session", or another PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, no DNN] combination that was sent by the UE, if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message, until timer T35cd expires or timer T35cd is stopped.

The UE shall not stop timer T35cd upon a PLMN change or inter-system change;

b) if the timer value indicates that this timer is deactivated, the UE:

1) shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided during the PDU session establishment, if it is running. The UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message with request type different from "initial emergency request" and different from "existing emergency PDU session", or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination that was sent by the UE, until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same [S-NSSAI, DNN] combination from the network; and

2) shall not send a PDU SESSION ESTABLISHMENT REQUEST message with request type different from "initial emergency request" and different from "existing emergency PDU session", or a PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, no DNN] combination that was sent by the UE, if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message, until the UE is switched off or the USIM is removed, or the UE receives an PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, no DNN] combination from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same [S-NSSAI, no DNN] combination from the network.

The timer T35cd remains deactivated upon a PLMN change or inter-system change; and

c) if the timer value indicates zero, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination that was sent by the UE, if running. The UE:

1) may send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

2) may send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, no DNN] combination if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session".

If the Back-off timer value IE is not included or no Back-off timer value is received from the 5GMM sublayer, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST message or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

When the timer T35cd is running or the timer is deactivated, the UE is allowed to initiate a PDU session establishment procedure for emergency services.

If the timer T35cd is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T35cd is kept running until it expires or it is stopped.

If the UE is switched off when the timer T35cd is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

let t1 be the time remaining for T35cd timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

If:

- the 5GSM cause value #69 "insufficient resources for specific slice" and the Back-off timer value IE are included in the PDU SESSION ESTABLISHMENT REJECT message; or

- an indication that the 5GSM message was not forwarded due to S-NSSAI only based congestion control is received along a Back-off timer value and a PDU SESSION ESTABLISHMENT REQUEST message with the PDU session ID IE set to the PDU session ID of the PDU session;

the UE shall take different actions depending on the timer value received for timer T35ef in the Back-off timer value:

a) If the timer value indicates neither zero nor deactivated and an S-NSSAI was included in the PDU SESSION ESTABLISHMENT REQUEST message, the UE shall stop timer T35ef associated with the corresponding S-NSSAI, if it is running. If the timer value indicates neither zero nor deactivated and no S-NSSAI was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request", the UE shall stop timer T35ef associated with no S-NSSAI if it is running. The UE shall then start timer T35ef with the value provided in the Back-off timer value IE and:

   1) shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same S-NSSAI that was sent by the UE, until timer T35ef expires or timer T35ef is stopped; and

   2) shall not send another PDU SESSION ESTABLISHMENT REQUEST message without an S-NSSAI and with request type different from "initial emergency request", or another PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an S-NSSAI provided by the UE, if no S-NSSAI was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request", until timer T35ef expires or timer T35ef is stopped.

   The UE shall not stop timer T35ef upon a PLMN change or inter-system change;

b) if the timer value indicates that this timer is deactivated and an S-NSSAI was included in the PDU SESSION ESTABLISHMENT REQUEST message, the UE shall stop timer T35ef associated with the corresponding S-NSSAI, if it is running. If the timer value indicates that this timer is deactivated and no S-NSSAI was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request", the UE shall stop timer T35ef associated with no S-NSSAI if it is running. The UE:

   1) shall not send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST for the same S-NSSAI until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for the same S-NSSAI from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same S-NSSAI from the network; and

   2) shall not send another PDU SESSION ESTABLISHMENT REQUEST message without an S-NSSAI and with request type different from "initial emergency request", or another PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an S-NSSAI provided by the UE, if no S-NSSAI was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request", until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an S-NSSAI provided by the UE, or a PDU SESSION RELEASE COMMAND messages including 5GSM cause IE set to 5GSM cause #39 "reactivation requested" for a non-emergency PDU session established without an S-NSSAI provided by the UE.

   The timer T35ef remains deactivated upon a PLMN change or inter-system change; and

c) if the timer value indicates zero, the UE:

   1) shall stop timer T35ef associated with the corresponding S-NSSAI, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same S-NSSAI; and

   2) if no S-NSSAI was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request ", the UE shall stop timer T35ef associated with no S-NSSAI, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST message without

an S-NSSAI, or another PDU SESSION MODIFICATION REQUEST message without an S-NSSAI provided by the UE.

If the Back-off timer value IE is not included or no Back-off timer value is received from the 5GMM sublayer, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same S-NSSAI or without an S-NSSAI.

When the timer T35ef is running or the timer is deactivated, the UE is allowed to initiate a PDU session establishment procedure for emergency services.

If the timer T35ef is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T35ef is kept running until it expires or it is stopped.

If the UE is switched off when the timer T35ef is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

let t1 be the time remaining for T35ef timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

NOTE: As described in this subclause, upon PLMN change or inter-system change, the UE does not stop the timer T35cd or T35ef. This means the timer T35cd or T35ef can still be running or be deactivated for the given 5GSM procedure, the PLMN, the S-NSSAI and optionally the DNN combination when the UE returns to the PLMN or when it performs inter-system change back from S1 mode to N1 mode. Thus the UE can still be prevented from sending another PDU SESSION ESTABLISHMENT REQUEST message in the PLMN for the same S-NSSAI and optionally the same DNN.

Upon PLMN change, if T35cd is running or is deactivated for a S-NSSAI, a DNN, and old PLMN, but T35cd is not running and is not deactivated for the S-NSSAI, the DNN, and new PLMN, then the UE is allowed to send a PDU SESSION ESTABLISHMENT REQUEST message for the same S-NSSAI and the same DNN in the new PLMN.

Upon PLMN change, if T35ef is running or is deactivated for a S-NSSAI and old PLMN, but T35cd is not running and is not deactivated for the S-NSSAI and new PLMN, then the UE is allowed to send a PDU SESSION ESTABLISHMENT REQUEST message for the same S-NSSAI in the new PLMN.

6.4.1.4.2 Handling of network rejection due to 5GSM cause #26

Editor's note: Handling of network rejection due to 5GSM cause #26 is FFS.

6.4.1.4.3 Handling of network rejection due to 5GSM cause other than 5GSM cause #26

If the 5GSM cause value is #27 "missing or unknown DNN", the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message in the PLMN for the same DNN that was sent by the UE, until the UE is switched off, the USIM is removed, or the DNN is included in the LADN information and the network updates the LADN information during the registration procedure or the generic UE configuration update procedure.

If the 5GSM cause value is #28 "unknown PDU session type" and the PDU SESSION ESTABLISHMENT REQUEST message contained a PDU session type IE indicating a PDU session type, the UE may send another PDU SESSION ESTABLISHMENT REQUEST with the PDU session type IE indicating another PDU session type or without the PDU session type IE.

If the 5GSM cause value is #68 "not supported SSC mode", UE may send PDU SESSION ESTABLISHMENT REQUEST with the SSC mode included in the Allowed SSC mode IE of the PDU SESSION ESTABLISHMENT REJECT message or evaluate other URSP rules if available as specified in subclause 6.2.9.

If the 5GSM cause value is #70 "missing or unknown DNN in a slice", the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message in the PLMN for the same DNN and the same S-NSSAI that were sent by the UE (or for the same DNN and no S-NSSAI, if S-NSSAI that was not sent by the UE), until the UE is switched off, the USIM is removed, or the DNN is included in the LADN information and the network updates the LADN information during the registration procedure or the generic UE configuration update procedure.

6.4.1.5 Handling the maximum number of established PDU sessions

If the maximum number of established PDU sessions is reached at the UE and the upper layers of the UE request connectivity to a DNN the UE shall not send a PDU SESSION ESTABLISHMENT message unless an established PDU session is released. If the UE needs to release an established PDU session, choosing which PDU session to release is implementation specific, however the UE shall not release the PDU session for emergency.

If the UE needs to release a PDU session in order to request an emergency PDU session, it shall either release a PDU session locally or via explicit signalling. If the UE performs local release, the UE shall perform a registration procedure for mobility and periodic registration update to indicate PDU session status to the network.

Editor's note: How does the UE determine the maximum number of established PDU sessions is FFS.

6.4.1.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Expiry of timer T3580

The UE shall, on the first expiry of the timer T3580, retransmit the PDU SESSION ESTABLISHMENT REQUEST message and shall reset and start timer T3580. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3580, the UE shall abort the procedure.

b) Upon receiving an indication that the 5GSM message was not forwarded along with a PDU SESSION ESTABLISHMENT REQUEST message with the PDU session ID IE set to the PDU session ID of the PDU session, the UE shall stop timer T3580 and shall abort the procedure.

6.4.1.7 Abnormal cases on the network side

Editor's note: Further abnormal cases in the network side are FFS.

The following abnormal cases can be identified:

a) If the received request type is "initial emergency request" and there is already another emergency PDU session for the UE, the SMF shall reject the PDU SESSION ESTABLISHMENT REQUEST message with 5GSM cause #31 "request rejected, unspecified" or release the existing emergency PDU session locally without notification to the UE and proceed the new PDU SESSION ESTABLISHMENT REQUEST message

b) The information for the PDU session authentication and authorization by the external DN in PDU DN request container is not compliant with local policy and user's subscription data

If the PDU session being established is a non-emergency PDU session, the PDU session authentication and authorization by the external DN is required due to local policy and user's subscription data and the information for the PDU session authentication and authorization by the external DN in PDU DN request container is not compliant with local policy and user's subscription data, the SMF shall reject the PDU session establishment request including the 5GSM cause #29 "user authentication failed", in the PDU SESSION ESTABLISHMENT REJECT message.

c) UE-requested PDU session establishment with request type set to "initial request" or "initial emergency request" for an existing PDU session:

If the SMF receives a PDU SESSION ESTABLISHMENT REQUEST message with a PDU session ID identical to the PDU session ID of an existing PDU session and with request type set to "initial request" or "initial emergency request", the SMF shall release the existing PDU session locally without notification to the UE and proceed with the PDU session establishment procedure.

d) UE-requested PDU session establishment with request type "existing PDU session" or "existing emergency PDU session" for a PDU session that does not exist:

If the SMF receives a PDU SESSION ESTABLISHMENT REQUEST message with request type set to "existing PDU session" or "existing emergency PDU session", and the SMF does not have any information about that PDU session, then the SMF shall reject the PDU session establishment procedure with the 5GSM cause set to #54 "PDU session does not exist" in the PDU SESSION ESTABLISHMENT REJECT message.

6.4.2 UE-requested PDU session modification procedure

6.4.2.1 General

The purpose of the UE-requested PDU session modification procedure is to enable the UE to request modification of a PDU session or to indicate a change of 3GPP PS data off UE status for a PDU session. The UE shall not request a PDU session modification for an LADN when the UE is located outside the LADN service area. If the UE supports reflective QoS, the UE shall initiate this procedure as follows:

a) the UE is operating in single-registration mode with N26 interface supported in the network and the UE needs to indicate the support of reflective QoS after an inter-system change from S1 mode to N1 mode; or

b) to revoke the previously indicated support for reflective QoS.

If the UE supports acting as a type C host as specified in IETF RFC 4191 [36], and the UE is operating in single-registration mode with N26 interface supported in the network, the UE shall initiate the UE-requested PDU session modification procedure to indicate the support of multi-homed IPv6 PDU session after an inter-system change from S1 mode to N1 mode.

If the UE can support more than 16 packet filters for a PDU session of "IPv4", "IPv6", "IPv4v6", or "Ethernet" PDU session type, the UE shall initiate the UE-requested PDU session modification procedure to indicate the maximum number of packet filters that can be supported for the PDU session after an inter-system change from S1 mode to N1 mode.

6.4.2.2 UE-requested PDU session modification procedure initiation

In order to initiate the UE-requested PDU session modification procedure, the UE shall create a PDU SESSION MODIFICATION REQUEST message.

The UE shall allocate a PTI value currently not used and shall set the PTI IE of the PDU SESSION MODIFICATION REQUEST message to the allocated PTI value.

The UE shall not perform the UE-requested PDU session modification procedure for an emergency PDU session.

The UE shall not perform the UE-requested PDU session modification procedure for a PDU session for LADN when the UE is located outside the LADN service area.

If the UE requests a specific QoS handling, the UE shall include the requested QoS rules IE indicating requested QoS rules for the specific QoS handling.

If the UE is performing the PDU session modification procedure to indicate the support of reflective QoS after an inter-system change from S1 mode to N1 mode, the UE should set the RQoS bit to "Reflective QoS supported" in the 5GSM capability IE of the PDU SESSION MODIFICATION REQUEST message.

If the UE is performing the PDU session modification procedure to revoke the previously indicated support of reflective QoS, the UE shall set the RQoS bit to "Reflective QoS not supported" in the 5GSM capability IE of the PDU SESSION MODIFICATION REQUEST message. The UE shall not indicate support for reflective QoS for this PDU Session for the remaining lifetime of the PDU Session.

NOTE: The determination to revoke the usage of reflective QoS by the UE for a PDU session is implementation dependent.

If the UE is performing the PDU session modification procedure to indicate the support of Multi-homed IPv6 PDU session after an inter-system change from S1 mode to N1 mode, the UE shall set the MH6-PDU bit to "Multi-homed IPv6 PDU session supported" in the 5GSM capability IE of the PDU SESSION MODIFICATION REQUEST message.

If the UE is performing the PDU session modification procedure to indicate that the UE can support more than 16 packet filters for this PDU session, the UE shall indicate the maximum number of packet filters that can be supported for the PDU session in the Maximum number of supported packet filters IE of the PDU SESSION MODIFICATION REQUEST message.

To indicate a change of 3GPP PS data off UE status associated to a PDU session, the UE shall include the extended protocol configuration options IE in the PDU SESSION MODIFICATION REQUEST message and set the 3GPP PS data off UE status.

The UE shall transport the PDU SESSION MODIFICATION REQUEST message and the PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, and the UE shall start timer T3581 (see example in figure 6.4.2.2.1).

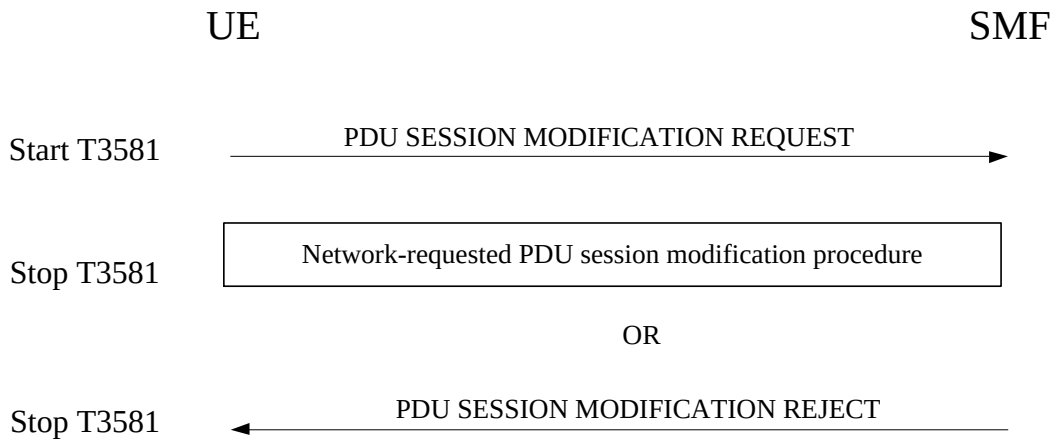


Figure 6.4.2.2.1: UE-requested PDU session modification procedure

6.4.2.3 UE-requested PDU session modification procedure accepted by the network

Upon receipt of a PDU SESSION MODIFICATION REQUEST message, if the SMF accepts the request to modify the PDU session, the SMF shall perform the network-requested PDU session modification procedure as specified in subclause 6.3.2.

6.4.2.4 UE-requested PDU session modification procedure not accepted by the network

Upon receipt of a PDU SESSION MODIFICATION REQUEST message, if the SMF does not accepts the request to modify the PDU session, the SMF shall create a PDU SESSION MODIFICATION REJECT message.

If the UE requests a PDU session modification for an LADN when the UE is located outside the LADN service area, the SMF shall reject the request.

The SMF shall set the 5GSM cause IE of the PDU SESSION MODIFICATION REJECT message to indicate the reason for rejecting the PDU session modification.

The 5GSM cause IE typically indicates one of the following SM cause values:

#26 insufficient resources;

#31 request rejected, unspecified;

#34 service option temporarily out of order;

#35 PTI already in use;

#43 Invalid PDU session identity;

#67 insufficient resources for specific slice and DNN; or

#69 insufficient resources for specific slice.

The SMF may include a Back-off timer value IE in the PDU SESSION MODIFICATION REJECT message when the 5GSM cause value #26 "insufficient resources" is included in the PDU SESSION MODIFICATION REJECT message. If the 5GSM cause value is #26 "insufficient resources" and the PDU SESSION MODIFICATION REQUEST message was received from a UE configured for high priority access in selected PLMN or the request type was set to "initial emergency request" or "existing emergency PDU session" for the establishment of the PDU session, the network shall not include a Back-off timer value IE.

Editor's note: Whether the SMF knows that the UE is a UE configured for high priority access so as not to include the Back-off timer is FFS.

The SMF may include a Back-off timer value IE in the PDU SESSION MODIFICATION REJECT message when the 5GSM cause value #67 "insufficient resources for specific slice and DNN" is included in the PDU SESSION MODIFICATION REJECT message. If the 5GSM cause value is #67 "insufficient resources for specific slice and DNN" and the PDU SESSION MODIFICATION REQUEST message was received from a UE configured for high priority access in selected PLMN or the request type was set to "initial emergency request" or "existing emergency PDU session" for the establishment of the PDU session, the network shall not include a Back-off timer value IE.

Editor's note: Whether the SMF knows that the UE is a UE configured for high priority access so as not to include the Back-off timer is FFS.

The SMF may include a Back-off timer value IE in the PDU SESSION MODIFICATION REJECT message when the 5GSM cause #69 "insufficient resources for specific slice" is included in the PDU SESSION MODIFICATION REJECT message. If the 5GSM cause value is #69 "insufficient resources for specific slice" and the PDU SESSION MODIFICATION REQUEST message was received from a UE configured for high priority access in selected PLMN or the request type is set to "initial emergency request" for the establishment of the PDU session, the network shall not include a Back-off timer value IE.

The SMF shall send the PDU SESSION MODIFICATION REJECT message.

Upon receipt of a PDU SESSION MODIFICATION REJECT message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, the UE shall stop timer T3581, shall release the allocated PTI value and shall consider that the PDU session is not modified.

If the 5GSM cause value is #26 "insufficient resources" and the Back-off timer value IE is included, the UE shall take different actions depending on the timer value received for timer T3396 in the Back-off timer value:

a) If the timer value indicates neither zero nor deactivated, the UE shall stop timer T3396 associated with the corresponding DNN, if it is running. The UE shall then start timer T3396 with the value provided in the Back-off timer value IE and shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same DNN that was sent by the UE, until timer T3396 expires or timer T3396 is stopped.

   If the UE did not provide a DNN for the establishment of the PDU session and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop the timer T3396 associated with no DNN if it is running. The UE shall start timer T3396 with the received value and not send another PDU SESSION ESTABLISHMENT REQUEST message without a DNN and with request type different from "initial emergency request" and different from "existing emergency PDU session", or another PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without a DNN provided by the UE, until timer T3396 expires or timer T3396 is stopped.

   The UE shall not stop timer T3396 upon a PLMN change or inter-system change.

b) if the timer value indicates that this timer is deactivated, the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same DNN until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for the same DNN from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same DNN from the network.

   If the UE did not provide a DNN for the establishment of the PDU session and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message without a DNN and with request type different from "initial emergency request" and different from "existing emergency PDU session", or another PDU SESSION MODIFICATION REQUEST for a non-emergency PDU session established without DNN provided by the UE, until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION

MODIFICATION REQUEST message for a non-emergency PDU session established without a DNN provided by the UE, or the UE receives a PDU SESSION RELEASE COMMAND messages including 5GSM cause IE set to 5GSM cause #39 "reactivation requested" for a non-emergency PDU session established without a DNN provided by the UE.

The timer T3396 remains deactivated upon a PLMN change or inter-system change.

c) if the timer value indicates zero, the UE shall stop timer T3396 associated with the corresponding DNN, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same DNN.

if the UE did not provide a DNN for the establishment of the PDU session and the request type was different from "initial emergency request" and different from "existing emergency PDU session", the UE shall stop timer T3396 associated with no DNN, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST message without a DNN, or another PDU SESSION MODIFICATION REQUEST message established without a DNN provided by the UE.

If the Back-off timer value IE is not included, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same DNN or without DNN.

If the timer T3396 is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T3396 is kept running until it expires or it is stopped.

If the UE is switched off when the timer T3396 is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

let t1 be the time remaining for T3396 timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

If the 5GSM cause value is #67 "insufficient resources for specific slice and DNN" and the Back-off timer value IE is included, the UE shall take different actions depending on the timer value received for timer T35cd in the Back-off timer value:

a) If the timer value indicates neither zero nor deactivated, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is established, if it is running. If the timer value indicates neither zero nor deactivated, the UE shall stop timer T35cd associated with the same [S-NSSAI, no DNN] combination as that the UE provided when the PDU session is established, if it is running. The UE shall then start timer T35cd with the value provided in the Back-off timer value IE, and:

1) shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination that was sent by the UE, until timer T35cd expires or timer T35cd is stopped.

2) shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, no DNN] combination that was sent by the UE, until timer T35cd expires or timer T35cd is stopped.

The UE shall not stop timer T35cd upon a PLMN change or inter-system change.

b) if the timer value indicates that this timer is deactivated, the UE:

1) shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination as that the UE provided when the PDU session is established, if it is running. the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST for the same [S-NSSAI, DNN] combination until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same [S-NSSAI, DNN] combination from the network; and

2) shall stop timer T35cd associated with the same [S-NSSAI, no DNN] combination as that the UE provided when the PDU session is established, if it is running. The UE shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST for the same [S-NSSAI, no DNN] combination if no DNN was included in the PDU SESSION ESTABLISHMENT

REQUEST message until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, no DNN] combination from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same [S-NSSAI, no DNN] combination from the network.

The timer T35cd remains deactivated upon a PLMN change or inter-system change.

c) if the timer value indicates zero, the UE shall stop timer T35cd associated with the same [S-NSSAI, DNN] combination, if running. The UE:

1) may send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

2) may send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, no DNN] combination if no DNN was included in the PDU SESSION ESTABLISHMENT REQUEST message and the request type was different from "initial emergency request" and different from "existing emergency PDU session".

If the Back-off timer value IE is not included, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same [S-NSSAI, DNN] combination.

When the timer T35cd is running or the timer is deactivated, the UE is allowed to initiate a PDU session establishment procedure for emergency services.

If the timer T35cd is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T35cd is kept running until it expires or it is stopped.

If the UE is switched off when the timer T35cd is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

let t1 be the time remaining for T35cd timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

If the 5GSM cause value is #69 "insufficient resources for specific S-NSSAI" and the Back-off timer value IE is included, the UE shall take different actions depending on the timer value received for timer T35ef in the Back-off timer value:

a) If the timer value indicates neither zero nor deactivated, the UE shall stop timer T35ef associated with the corresponding S-NSSAI, if it is running. The UE shall then start timer T35ef with the value provided in the Back-off timer value IE and shall not send another PDU SESSION ESTABLISHMENT REQUEST message, or PDU SESSION MODIFICATION REQUEST message for the same S-NSSAI that was sent by the UE, until timer T35ef expires or timer T35ef is stopped.

If the UE did not provide an S-NSSAI for the establishment of the PDU session and the request type was different from "initial emergency request", the UE shall stop the timer T35ef associated with no S-NSSAI if it is running. The UE shall start timer T35ef with the received value and not send another PDU SESSION ESTABLISHMENT REQUEST message without an S-NSSAI and with request type different from "initial emergency request", or another PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an S-NSSAI provided by the UE, until timer T35ef expires or timer T35ef is stopped.

The UE shall not stop timer T35ef upon a PLMN change or inter-system change.

b) if the timer value indicates that this timer is deactivated, the UE shall not send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same S-NSSAI until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for the same S-NSSAI from the network or a PDU SESSION RELEASE COMMAND message including 5GSM cause #39 "reactivation requested" for the same S-NSSAI from the network.

If the UE did not provide an S-NSSAI for the establishment of the PDU session and the request type was different from "initial emergency request", the UE shall not send another PDU SESSION ESTABLISHMENT

REQUEST message without an S-NSSAI and with request type different from "initial emergency request", or another PDU SESSION MODIFICATION REQUEST for a non-emergency PDU session established without S-NSSAI provided by the UE, until the UE is switched off or the USIM is removed, or the UE receives a PDU SESSION MODIFICATION REQUEST message for a non-emergency PDU session established without an S-NSSAI provided by the UE, or the UE receives a PDU SESSION RELEASE COMMAND messages including 5GSM cause IE set to 5GSM cause #39 "reactivation requested" for a non-emergency PDU session established without an S-NSSAI provided by the UE.

The timer T35ef remains deactivated upon a PLMN change or inter-system change.

c) if the timer value indicates zero, the UE shall stop timer T35ef associated with the corresponding S-NSSAI, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST message for the same S-NSSAI.

if the UE did not provide an S-NSSAI for the establishment of the PDU session and the request type was different from " initial emergency request ", the UE shall stop timer T35ef associated with no S-NSSAI, if running, and may send another PDU SESSION ESTABLISHMENT REQUEST message without an S-NSSAI, or another PDU SESSION MODIFICATION REQUEST message established without an S-NSSAI provided by the UE.

If the Back-off timer value IE is not included, then the UE may send another PDU SESSION ESTABLISHMENT REQUEST or PDU SESSION MODIFICATION REQUEST message for the same S-NSSAI or without S-NSSAI.

If the timer T35ef is running when the UE enters state5GMM-DEREGISTERED, the UE remains switched on, and the USIM in the UE remains the same, then timer T35ef is kept running until it expires or it is stopped.

If the UE is switched off when the timer T35ef is running, and if the USIM in the UE remains the same when the UE is switched on, the UE shall behave as follows:

let t1 be the time remaining for T35ef timeout at switch off and let t be the time elapsed between switch off and switch on. If t1 is greater than t, then the timer shall be restarted with the value t1 – t. If t1 is equal to or less than t, then the timer need not be restarted. If the UE is not capable of determining t, then the UE shall restart the timer with the value t1.

NOTE: As described in this subclause, upon PLMN change or inter-system change, the UE does not stop the timer T35cd or T35ef. This means the timer T35cd or T35ef can still be running or be deactivated for the given 5GSM procedure, the PLMN, the S-NSSAI and optionally the DNN combination when the UE returns to the PLMN or when it performs inter-system change back from S1 mode to N1 mode. Thus the UE can still be prevented from sending another PDU SESSION ESTABLISHMENT REQUEST message in the PLMN for the same S-NSSAI and optionally the same DNN.

Upon PLMN change, if T35cd is running or is deactivated for a S-NSSAI, a DNN, and old PLMN, but T35cd is not running and is not deactivated for the S-NSSAI, the DNN, and new PLMN, then the UE is allowed to send a PDU SESSION ESTABLISHMENT REQUEST message for the same S-NSSAI and the same DNN in the new PLMN.

Upon PLMN change, if T35ef is running or is deactivated for a S-NSSAI and old PLMN, but T35cd is not running and is not deactivated for the S-NSSAI and new PLMN, then the UE is allowed to send a PDU SESSION ESTABLISHMENT REQUEST message for the same S-NSSAI in the new PLMN.

6.4.2.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Expiry of timer T3581.

The UE shall, on the first expiry of the timer T3581, retransmit the PDU SESSION MODIFICATION REQUEST message and shall reset and start timer T3581. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3581, the UE shall abort the procedure and shall release the allocated PTI.

b) Invalid PDU session identity.

Upon receipt of the PDU SESSION MODIFICATION REJECT message including 5GSM cause #43 "invalid PDU session identity", the UE shall release the existing PDU session locally without peer-to-peer signalling between the UE and the SMF.

c) Collision of network-requested PDU session release procedure and UE-requested PDU session modification procedure.

If the UE receives a PDU SESSION RELEASE COMMAND message during the UE-requested PDU session modification procedure, and the PDU session indicated in the PDU SESSION RELEASE COMMAND message is the PDU session that the UE wants to modify, the UE shall abort the PDU session modification procedure and proceed with the network-requested PDU session release procedure.

6.4.2.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) If the PDU session is an emergency PDU session, the SMF shall reject the PDU SESSION MODIFICATION REQUEST message with 5GSM cause #31 "request rejected, unspecified".

b) No PDU session active for the received PDU session identity.

If the PDU session ID in the PDU SESSION MODIFICATION REQUEST message does not belong to any PDU session in state PDU SESSION ACTIVE in the SMF, the SMF shall set the 5GSM cause IE to #43 "Invalid PDU session identity" in the PDU SESSION MODIFICATION REJECT message.

6.4.3 UE-requested PDU session release procedure

6.4.3.1 General

The purpose of the UE-requested PDU session release procedure is to enable by the UE to request a release of a PDU session.

The UE is allowed to initiate the PDU session release procedure even if the timer T3396 is running.

The UE is allowed to initiate the PDU session release procedure even if the timer T35cd is running.

The UE is allowed to initiate the PDU session release procedure even if the timer T35ef is running.

6.4.3.2 UE-requested PDU session release procedure initiation

In order to initiate the UE-requested PDU session release procedure, the UE shall create an PDU SESSION RELEASE REQUEST message.

The UE shall allocate a PTI value currently not used and shall set the PTI IE of the PDU SESSION RELEASE REQUEST message to the allocated PTI value.

The UE shall transport the PDU SESSION RELEASE REQUEST message and the PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, and the UE shall start timer T3582 (see example in figure 6.4.3.2.1).

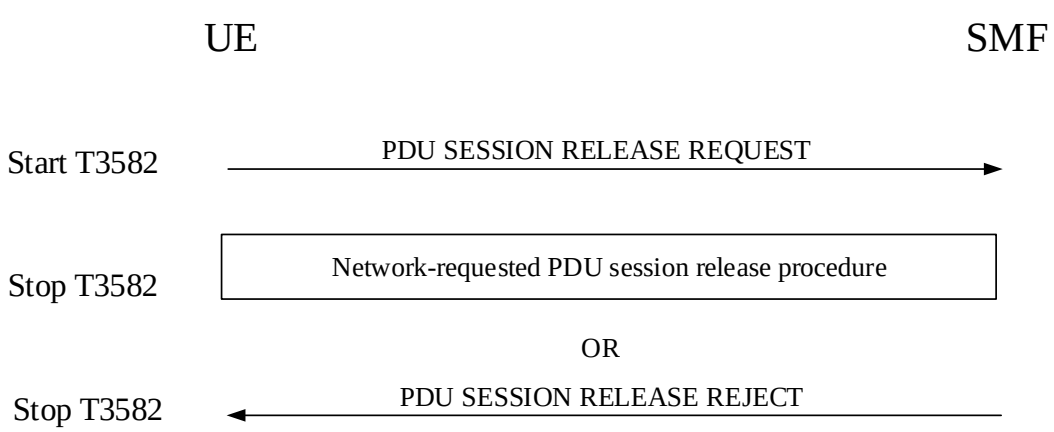


Figure 6.4.3.2.1: UE-requested PDU session release procedure

6.4.3.3 UE-requested PDU session release procedure accepted by the network

Upon receipt of a PDU SESSION RELEASE REQUEST message and a PDU session ID, if the SMF accepts the request to release the PDU session, and shall perform the network-requested PDU session release procedure as specified in subclause 6.3.3.

6.4.3.4 UE-requested PDU session release procedure not accepted by the network

Upon receipt of a PDU SESSION RELEASE REQUEST message, if the SMF does not accept the request to release the PDU session, the SMF shall create an PDU SESSION RELEASE REJECT message.

The SMF shall set the 5GSM cause IE of the PDU SESSION RELEASE REJECT message to indicate the reason for rejecting the PDU session release.

The 5GSM cause IE typically indicates one of the following SM cause values:

#34 service option temporarily out of order;

#35 PTI already in use; or

#43 Invalid PDU session identity.

The SMF shall send the PDU SESSION RELEASE REJECT message.

Upon receipt of a PDU SESSION RELEASE REJECT message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, the UE shall stop timer T3582, shall release the allocated PTI value, and shall consider that the PDU session is not released.

6.4.3.5 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Expiry of timer T3582.

The UE shall, on the first expiry of the timer T3582, retransmit the PDU SESSION RELEASE REQUEST message and shall reset and start timer T3582. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3582, the UE shall abort the procedure, shall release the allocated PTI, shall locally release the PDU session, and shall perform the registration procedure for mobility and periodic registration update with a REGISTRATION REQUEST message including the PDU session status IE.

b) Collision of UE-requested PDU session release procedure and network-requested PDU session modification procedure.

When the UE receives a PDU SESSION MODIFICATION COMMAND message during the UE-requested PDU session release procedure, and the PDU session indicated in PDU SESSION MODIFICATION COMMAND message is the PDU session that the UE wants to release, the UE shall ignore the PDU SESSION MODIFICATION COMMAND message and proceed with the PDU session release procedure.

c) Collision of UE-requested PDU session release procedure and network-requested PDU session release procedure.

When the UE receives a PDU SESSION RELEASE COMMAND message with the PTI IE set to "No procedure transaction identity assigned" during the UE-requested PDU session release procedure, and the PDU session indicated in the PDU SESSION RELEASE COMMAND message is the same as the PDU session that the UE requests to release, the UE shall abort the UE-requested PDU session release procedure and proceed with the network-requested PDU session release procedure.

6.4.3.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) No PDU session active for the received PDU session identity.

If the PDU session ID in the PDU SESSION RELEASE REQUEST message does not belong to any PDU session in state PDU SESSION ACTIVE in the SMF, the SMF shall send the PDU SESSION RELEASE REJECT message to the UE with the 5GSM cause #43 "Invalid PDU session identity".

6.5 5GSM status procedure

6.5.1 General

The purpose of the sending of the 5GSM STATUS message is to report at any time certain error conditions detected upon receipt of 5GSM protocol data. The 5GSM STATUS message can be sent by both the network and the UE (see example in figure 6.5.1.1).

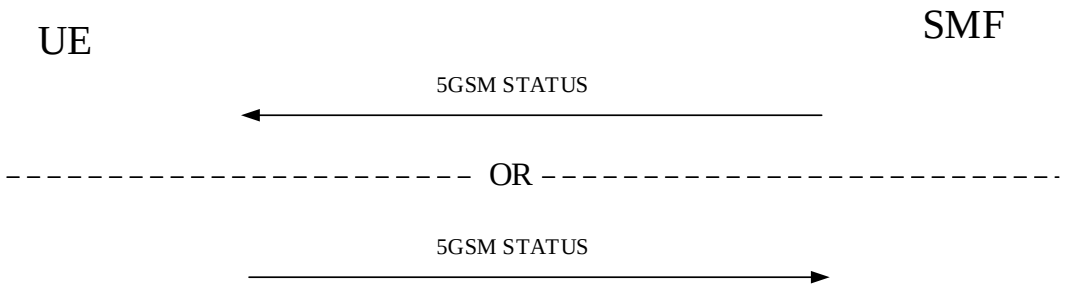


Figure 6.5.1.1: 5GSM status procedure

6.5.2 5GSM status received in the UE

If the 5GSM entity of the UE receives a 5GSM STATUS message the UE shall take different actions depending on the received 5GSM cause value:

#81 (Invalid PTI value);

The UE shall abort any ongoing 5GSM 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 5GSM procedure related to the PTI or PDU session Id and stop any related timer.

On receipt of a 5GSM STATUS message with any other 5GSM cause value no state transition and no specific action shall be taken as seen from the radio interface, i.e. local actions are possible.

6.5.3 5GSM status received in the SMF

If the SMF receives a 5GSM STATUS message the SMF shall take different actions depending on the received 5GSM cause value:

#81 (Invalid PTI value);

The UE shall abort any ongoing 5GSM procedure related to the received PTI value and stop any related timer.

#97 (Message type non-existent or not implemented).

The SMF shall abort any ongoing 5GSM procedure related to the PTI or PDU session Id and stop any related timer.

The local actions to be taken by the SMF on receipt of a 5GSM STATUS message with any other 5GSM cause value are implementation dependent.

6.6 Miscellaneous procedures

6.6.1 Exchange of extended protocol configuration options

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.

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 [11], subclause 11.4.2.

Editor's note: It is FFS to add more details and further alignment to align with 3GPP TS 24.301 [15].

7.2 Message too short or too long

7.2.1 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 [11].

7.2.2 Message too long

The maximum size of an NAS message for NR connected to 5GCN is specified in 3GPP TS 38.323 [29].

The maximum size of an NAS message for E-UTRA connected to 5GCN is specified 3GPP TS 36.323 [25].

The maximum size of an NAS message for non-3GPP access connected to 5GCN is specified in 3GPP TS 24.502 [18]

7.3 Unknown or unforeseen procedure transaction identity or PDU Session identity

7.3.1 Procedure transaction identity

The following UE-requested 5GSM procedures shall apply for handling an unknown, erroneous, or unforeseen PTI received in a 5GSM message:

a) In case the UE receives a PDU SESSION MODIFICATION COMMAND message in which the PTI value is an assigned value that does not match any PTI in use:

   1) if the UE detects that this command is a network retransmission of an already accepted request (see subclause 6.3.2.3), the UE shall respond with a PDU SESSION MODIFICATION COMPLETE message; or

   2) otherwise, the UE shall respond with a PDU SESSION MODIFICATION COMMAND REJECT message including 5GSM cause #47 "PTI mismatch".

b) In case the UE receives a PDU SESSION RELEASE COMMAND message in which the PTI value is an assigned value that does not match any PTI in use:

   1) if the UE detects that this command is a network retransmission of an already accepted request (see subclause 6.3.3.3), the UE shall respond with a PDU SESSION RELEASE COMPLETE message; or

   2) otherwise, the UE shall respond with a 5GSM STATUS message including 5GSM cause #47 "PTI mismatch".

7.3.2 PDU Session identity

Editor's note: It is FFS to add the content.

7.4 Unknown or unforeseen message type

If UE receives a 5GMM message or 5GSM message with message type not defined for the extended protocol discriminator (EPD) or not implemented by the receiver, it shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #97 "message type non-existent or not implemented".

If the network receives a 5GMM or 5GSM message with message type not defined for the EPD or not implemented by the receiver in a protocol state where reception of an unsolicited message with the given EPD 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 EPD or not implemented by the receiver, it shall ignore the message except that it should return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #97 "message type non-existent or not implemented".

NOTE: A message type not defined for the EPD in the given direction is regarded by the receiver as a message type not defined for the EPD, see 3GPP TS 24.007 [11].

If the UE receives a message not compatible with the protocol state, the UE shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) 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,

a) an "imperative message part" error; or

b) a "missing mandatory IE" error

is diagnosed or when a message containing:

a) a syntactically incorrect mandatory IE;

b) an IE unknown in the message, but encoded as "comprehension required" (see 3GPP TS 24.007 [11]); or

c) an out of sequence IE encoded as "comprehension required" (see 3GPP TS 24.007 [11]) 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) or b), the UE shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #96 "invalid mandatory information";

the network shall proceed as follows:

a) If the message is not one of the messages listed in subclause 7.5.3, item c), d) or e) , the network shall either:

1) try to treat the message (the exact further actions are implementation dependent); or

2) ignore the message except that it should return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) with cause #96 "invalid mandatory information".

7.5.2 5GS mobility management

No exceptional cases are described for 5GS mobility management messages.

No semantical or syntactical diagnosis other than presence and length shall be performed on the EPS NAS message container information element in the REGISTRATION REQUEST message.

7.5.3 5GS session management

The following UE procedures shall apply for handling an error encountered with a mandatory information element in a 5GSM message:

a) If the message is a PDU SESSION AUTHENTICATION COMMAND, a PDU SESSION ESTABLISHMENT REJECT message with 5GSM cause #96 "invalid mandatory information" shall be returned.

b) If the message is a PDU SESSION MODIFICATION COMMAND, a PDU SESSION MODIFICATION REJECT message with 5GSM cause #96 "invalid mandatory information" shall be returned.

The following network procedures shall apply for handling an error encountered with a mandatory information element in a 5GSM message:

c) If the message is a PDU SESSION ESTABLISHMENT REQUEST, a PDU SESSION ESTABLISHMENT REJECT message with 5GSM cause #96 "invalid mandatory information" shall be returned.

d) If the message is a PDU SESSION MODIFICATION REQUEST, a PDU SESSION MODIFICATION REJECT message with 5GSM cause #96 "invalid mandatory information" shall be returned.

e) If the message is a PDU SESSION RELEASE REQUEST, a PDU SESSION RELEASE REJECT message with 5GSM 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 [11]).

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 [11]).

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 and clause 9 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:

a) syntactically incorrect optional IEs; and

b) 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 5GMM or 5GSM message the UE diagnoses a "missing conditional IE" error or an "unexpected conditional IE" error, or when it receives a 5GMM or 5GSM message containing at least one syntactically incorrect conditional IE, the UE shall ignore the message and shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) 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:

a) try to treat the message (the exact further actions are implementation dependent); or

b) ignore the message except that it should return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) 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 8, 9). If, however no such reactions are specified, the UE shall ignore the message except that it shall return a status message (5GMM STATUS or 5GSM STATUS depending on the EPD) 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

8.2 5GS mobility management messages

8.2.1 Authentication request

8.2.1.1 Message definition

The AUTHENTICATION REQUEST message is sent by the AMF to the UE to initiate authentication of the UE identity. See table 8.2.1.1.1.

Message type: AUTHENTICATION REQUEST

Significance: dual

Direction: network to UE

Table 8.2.1.1.1: AUTHENTICATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Authentication request message identity	Message type 9.7	M	V	1
	ngKSI	NAS key set identifier 9.10.3.29	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
21	Authentication parameter RAND (5G authentication challenge)	Authentication parameter RAND 9.10.3.13	O	TV	17
20	Authentication parameter AUTN (5G authentication challenge)	Authentication parameter AUTN 9.10.3.14	O	TLV	18
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503

8.2.1.2 Authentication parameter RAND

Authentication parameter RAND IE is included if the AUTHENTICATION REQUEST message is used in a 5G AKA authentication procedure.

8.2.1.3 Authentication parameter AUTN

Authentication parameter AUTN IE is included if the AUTHENTICATION REQUEST message is used in a 5G AKA authentication procedure.

8.2.1.4 EAP message

EAP message IE is included if the AUTHENTICATION REQUEST message is used in an EAP authentication procedure.

8.2.2 Authentication response

8.2.2.1 Message definition

The AUTHENTICATION RESPONSE message is sent by the UE to the AMF to deliver a calculated authentication response to the network. See table 8.2.2.1.1.

Message type: AUTHENTICATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.2.1.1: AUTHENTICATION RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Authentication response message identity	Message type 9.7	M	V	1
2D	Authentication response parameter	Authentication response parameter 9.10.3.15	O	TLV	6-18
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503

8.2.2.2 Authentication response parameter

This IE is included if the message is sent in a 5G AKA based primary authentication and key agreement procedure.

8.2.2.3 EAP message

EAP message IE is included if the EAP message received in a related AUTHENTICATION REQUEST message was an EAP-request.

8.2.3 Authentication result

8.2.3.1 Message definition

The AUTHENTICATION RESULT message is sent by the AMF to the UE to provide result of EAP authentication of the UE identity. See table 8.2.3.1.1.

Message type: AUTHENTICATION RESULT

Significance: dual

Direction: network to UE

Table 8.2.3.1.1: AUTHENTICATION RESULT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Authentication result message identity	Message type 9.7	M	V	1
	ngKSI	NAS key set identifier 9.10.3.29	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	EAP message	EAP message 9.10.2.2	M	LV-E	6-1502

8.2.4 Authentication failure

8.2.4.1 Message definition

The AUTHENTICATION FAILURE message is sent by the UE to the AMF to indicate that authentication of the network has failed. See table 8.2.4.1.1.

Message type: AUTHENTICATION FAILURE

Significance: dual

Direction: UE to network

Table 8.2.4.1.1: AUTHENTICATION FAILURE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Authentication failure message identity	Message type 9.7	M	V	1
	5GMM cause	5GMM cause 9.10.3.2	M	V	1
30	Authentication failure parameter	Authentication failure parameter 9.10.3.12	O	TLV	16

8.2.4.2 Authentication failure parameter

This IE shall be included in a 5G AKA based primary authentication and key agreement procedure if and only if the 5GMM 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 33.501 [24]).

8.2.5 Authentication reject

8.2.5.1 Message definition

The AUTHENTICATION REJECT message is sent by the AMF to the UE to indicate that the authentication procedure has failed and that the UE shall abort all activities. See table 8.2.5.1.1.

Message type: AUTHENTICATION REJECT

Significance: dual

Direction: network to UE

Table 8.2.5.1.1: AUTHENTICATION REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Authentication reject message identity	Message type 9.7	M	V	1

8.2.6 Registration request

8.2.6.1 Message definition

The REGISTRATION REQUEST message is sent by the UE to the AMF. See table 8.2.6.1.1.

Message type: REGISTRATION REQUEST

Significance: dual

Direction: UE to network

Table 8.2.6.1.1: REGISTRATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended Protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Registration request message identity	Message type 9.7	M	V	1
	5GS registration type	5GS registration type 9.10.3.7	M	LV	2
	ngKSI	NAS key set identifier 9.10.3.29	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	5GS mobile identity	5GS mobile identity 9.10.3.4	M	LV	5-TBD
C-	Non-current native NAS key set identifier	NAS key set identifier 9.10.3.29	O	TV	1
10	5GMM capability	5GMM capability 9.10.3.1	O	TLV	3-15
2E	UE security capability	UE security capability 9.10.3.49	O	TLV	4-6
2F	Requested NSSAI	NSSAI 9.10.3.34	O	TLV	4-74
52	Last visited registered TAI	5GS tracking area identity 9.10.3.8	O	TV	7
65	S1 UE network capability	S1 UE network capability 9.10.3.44	O	TLV	4-15
40	Uplink data status	Uplink data status 9.10.2.53	O	TLV	4-34
50	PDU session status	PDU session status 9.10.3.40	O	TLV	4-34
B-	MICO indication	MICO indication 9.10.3.28	O	TV	1
2B	UE status	UE status 9.10.3.52	O	TLV	3
2C	Additional GUTI	5GS mobile identity 9.10.3.4	O	TLV	TBD
25	Allowed PDU session status	Allowed PDU session status 9.10.3.11	O	TLV	4-34
60	UE's usage setting	UE's usage setting 9.10.3.51	O	TLV	3
TBD	Requested DRX parameters	DRX parameters 9.10.3.20	O	TBD	TBD
7C	EPS NAS message container	EPS NAS message container 9.10.3.22	O	TLV-E	TBD
77	Payload container	Payload container 9.10.3.35	O	TLV-E	4-65538

Editor's note: The content of the REGISTRATION REQUEST message when a limited set of IEs including those needed to establish security in the initial message when it has no NAS security context is FFS.

8.2.6.2 Non-current native NAS key set identifier

The UE shall include this IE if the UE has a valid non-current native 5G NAS security context when the UE performs a inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode and the UE uses a mapped 5G NAS security context to protect the REGISTRATION REQUEST message.

8.2.6.3 5GMM capability

The UE shall include this IE, unless the UE performs a periodic registration updating procedure.

8.2.6.4 UE security capability

The UE shall include this IE, unless the UE performs a periodic registration updating procedure.

8.2.6.5 Requested NSSAI

This IE shall be included by the UE when performing the registration procedure if:

a) the UE has a configured NSSAI for the current PLMN;

b) the UE has an allowed NSSAI for the current PLMN; or

c) the UE has neither allowed NSSAI for the current PLMN nor configured NSSAI for the current PLMN and has a configured NSSAI not associated with a PLMN.

8.2.6.6 Last visited registered TAI

This IE shall be included if the UE holds a valid last visited registered TAI.

8.2.6.7 S1 UE network capability

A UE supporting S1 mode shall include this IE, unless the UE performs a periodic registration updating procedure.

8.2.6.8 Uplink data status

This IE shall be included if the UE has uplink user data pending to be sent.

8.2.6.9 PDU session status

This IE shall be included if the UE wants to indicate the PDU sessions associated with the access type the message is sent over that are active within the UE.

8.2.6.10 MICO indication

The UE may include this IE to request the use of MICO mode.

8.2.6.11 UE status

This IE shall be included if the UE in single-registration mode performs the registration procedure due to inter-system change from S1 mode to N1 mode or if the UE in dual-registration mode and EMM state EMM-REGISTERED performs initial registration.

8.2.6.12 Additional GUTI

This IE shall be included if the UE performs the registration procedure due to inter-system change from S1 mode to N1 mode, the UE operates in single-registration mode and the UE has a 5G-GUTI.

8.2.6.13 Allowed PDU session status

This IE shall be included if the REGISTRATION REQUEST message is sent as a response to paging with the access type indicating non-3GPP access and the UE wants to indicate the user-plane resources of PDU session(s) associated with non-3GPP access allowed to be re-established over 3GPP access.

8.2.6.14 UE's usage setting

This IE shall be included if the UE is configured to support IMS voice.

8.2.6.15 Requested DRX parameters

If the UE wants to use or change the UE specific DRX parameters, the UE shall include the Requested DRX parameters IE in the REGISTRATION REQUEST message.

8.2.6.16 EPS NAS message container

The UE operating in the single-registration mode shall include this information element if the UE performs mobility from S1 mode to N1 mode. The content of this message container is the complete integrity protected TRACKING AREA UPATE REQUEST message, using EPS NAS security context.

8.2.6.17 Allowed PDU session status

This IE shall be included if the REGISTRATION REQUEST message is sent as a response to paging with the access type indicating non-3GPP access and the UE wants to indicate the user-plane resources of PDU session(s) associated with non-3GPP access allowed to be re-established over 3GPP access.

8.2.6.18 Payload container

This IE shall be included if the UE has one or more stored UE policy sections for the registration procedure for mobility and periodic registration update due to inter-system change from S1 mode to N1 mode of a UE operating in the single-registration mode or for the registration procedure for initial registration.

8.2.7 Registration accept

8.2.7.1 Message definition

The REGISTRATION ACCEPT message is sent by the AMF to the UE. See table 8.2.7.1.1.

Message type: REGISTRATION ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.7.1.1: REGISTRATION ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Registration accept message identity	Message type 9.7	M	V	1
	5GS registration result	5GS registration result 9.10.3.6	M	LV	2
2C	5G-GUTI	5GS mobile identity 9.10.3.4	O	TLV	13
4A	Equivalent PLMNs	PLMN list 9.10.3.41	O	TLV	5-47
54	TAI list	5GS tracking area identity list 9.10.3.9	O	TLV	9-114
70	Allowed NSSAI	NSSAI 9.10.3.34	O	TLV	4-74
11	Rejected NSSAI	Rejected NSSAI 9.10.3.42	O	TLV	4-42
31	Configured NSSAI	NSSAI 9.10.3.34	O	TLV	4-146
64	5GS network feature support	5GS network feature support 9.10.3.5	O	TLV	3-5
50	PDU session status	PDU session status 9.10.3.40	O	TLV	4-34
26	PDU session reactivation result	PDU session reactivation result 9.10.3.38	O	TLV	4-32
7E	PDU session reactivation result error cause	PDU session reactivation result error cause 9.10.3.39	O	TLV-E	5-515
79	LADN information	LADN information 9.10.3.27	O	TLV-E	12-1707
B-	MICO indication	MICO indication 9.10.3.28	O	TV	1
27	Service area list	Service area list 9.10.3.45	O	TLV	6-114
5E	T3512 value	GPRS timer 3 9.10.2.5	O	TLV	3
5D	Non-3GPP de-registration timer value	GPRS timer 2 9.10.2.4	O	TLV	3
16	T3502 value	GPRS timer 2 9.10.2.4	O	TLV	3
34	Emergency number list	Emergency number list 9.10.3.21	O	TLV	5-50
35	Extended emergency number list	Extended emergency number list 9.10.3.24	O	TLV	TBD
TBD	Transparent container	Transparent container 9.10.3.49	O	TBD	TBD
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503

8.2.7.2 5G-GUTI

This IE may be included to assign a 5G-GUTI to a UE.

8.2.7.3 Equivalent PLMNs

This IE may be included in order to assign a new equivalent PLMNs list to a UE.

8.2.7.4 TAI list

This IE may be included to assign a TAI list to a UE.

8.2.7.5 Allowed NSSAI

This IE shall be included:

a) if the network allows one or more S-NSSAIs received in the requested NSSAI of the REGISTRATION REQUEST message; or

b) if the requested NSSAI was not included in the REGISTRATION REQUEST message or none of the requested NSSAI are present in the subscribed S-NSSAIs and the network has one or more subscribed S-NSSAIs marked as default that are available.

8.2.7.6 Rejected NSSAI

The network may include this IE to inform the UE of the S-NSSAIs that were included in the requested NSSAI in the REGISTRATION REQUEST message but were rejected by the network.

8.2.7.7 Configured NSSAI

The network may include this IE if the network needs to provide the UE with a new configured NSSAI for the current PLMN.

8.2.7.8 5GS 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.

8.2.7.9 PDU session status

This IE shall be included if the network wants to indicate the PDU sessions associated with the access type the message is sent over that are active in the network.

8.2.7.10 PDU session reactivation result

This IE shall be included:

- if the Uplink data status IE is included in the REGISTRATION REQUEST message;

- if the Allowed PDU session status IE is included in the REGISTRATION REQUEST message and there is at least one PDU session indicated in the Allowed PDU session status IE that can be reactivated over 3GPP access.

8.2.7.11 PDU session reactivation result error cause

This IE may be included, if the PDU session reactivation result IE is included and there exist one or more PDU sessions for which the user-plane resources cannot be re-established, to indicate the cause of failure to re-establish the user-plane resources

8.2.7.12 LADN information

The network shall include this IE if there are valid LADN service area(s) for the subscribed DNN(s) of the UE in the current registration area.

8.2.7.13 MICO indication

The network shall include the MICO indication IE if:

a)- the UE included the MICO indication IE in the REGISTRATION REQUEST message; and

b) the network supports and accepts the use of MICO mode.

8.2.7.14 Service area list

This IE may be included to assign new service area restrictions to the UE.

8.2.7.15 T3512 value

The AMF shall include this IE during the initial registration procedure over 3GPP access. The AMF may include this IE during the mobility and periodic registration update procedure over 3GPP access.

8.2.7.16 Non-3GPP de-registration timer value

This IE may be included if the network wants to indicate to the UE registered over non-3GPP access the value of a non-3GPP de-registration timer value.

8.2.7.17 T3502 value

This IE may be included to indicate a value for timer T3502.

8.2.7.18 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 country as in the cell on which this IE is received.

8.2.7.19 Extended 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 (with URN information) valid within the same country as in the cell on which this IE is received.

8.2.7.20 Transparent container

This IE may be sent by the network. If this IE is sent, the contents of this IE includes the list of preferred PLMN/access technology combinations (or HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided') (see 3GPP TS 23.122 [5] annex C) and optional acknowledgement request.

8.2.7.21 EAP message

EAP message IE is included if the REGISTRATION ACCEPT message is sent as part of registration for emergency services and is used to convey EAP-failure message.

8.2.8 Registration complete

8.2.8.1 Message definition

The REGISTRATION COMPLETE message is sent by the UE to the AMF. See table 8.2.8.1.1.

Message type: REGISTRATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.8.1.1: REGISTRATION COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Registration complete message identity	Message type 9.6	M	V	1
TBD	Transparent container	Transparent container 9.10.3.49	O	TBD	TBD

8.2.8.2 Transparent container

This IE may be sent by the UE. If this IE is sent, the contents of this IE indicates the UE acknowledgement of successful reception of the transparent container IE in the REGISTRATION ACCEPT message.

8.2.9 Registration reject

8.2.9.1 Message definition

The REGISTRATION REJECT message is sent by the AMF to the UE. See table 8.2.9.1.1.

Message type: REGISTRATION REJECT

Significance: dual

Direction: network to UE

Table 8.2.9.1.1: REGISTRATION REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Registration reject message identity	Message type 9.6	M	V	1
	5GMM cause	5GMM cause 9.10.3.2	M	V	1
5F	T3346 value	GPRS timer 2 9.10.2.4	O	TLV	3
16	T3502 value	GPRS timer 2 9.10.2.4	O	TLV	3
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503

8.2.9.2 T3346 value

The AMF may include this IE when the general NAS level mobility management congestion control is active

8.2.9.3 T3502 value

This IE may be included to indicate a value for timer T3502 during the initial registration.

8.2.9.4 EAP message

EAP message IE is included if the REGISTRATION REJECT message is used to convey EAP-failure message.

8.2.10 UL NAS transport

8.2.10.1 Message definition

The UL NAS TRANSPORT message transports message payload and associated information to the AMF. See table 8.2.10.1.1.

Message type: UL NAS TRANSPORT

Significance: dual

Direction: UE to network

Table 8.2.10.1.1: UL NAS TRANSPORT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	UL NAS TRANSPORT message identity	Message type 9.7	M	V	1
	Payload container type	Payload container type 9.10.3.36	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Payload container	Payload container 9.10.3.35	M	LV-E	3-65537
70	PDU session ID	PDU session identity 2 9.10.3.37	C	TV	2
61	Old PDU session ID	PDU session identity 2 9.10.3.37	O	TV	2
8-	Request type	Request type 9.10.3.43	O	TV	1
22	S-NSSAI	S-NSSAI 9.10.2.6	O	TLV	3-10
25	DNN	DNN 9.10.3.19	O	TLV	3-102
24	Additional information	Additional information 9.10.2.1	O	TLV	3-n

8.2.10.2 PDU session ID

The UE shall include this IE when the Payload container type IE is set to "N1 SM information".

8.2.10.3 Old PDU session ID

The UE shall include this IE if the UL NAS TRANSPORT message transports a PDU SESSION ESTABLISHMENT REQUEST message upon receiving the PDU SESSION MODIFICATION COMMAND message with the 5GSM cause IE set to #39 "reactivation requested".

8.2.10.4 Request type

The UE shall include this IE when the PDU session ID IE is included and the Payload container IE contains the PDU SESSION ESTABLISHMENT REQUEST message.

8.2.10.5 S-NSSAI

The UE may include this IE when the Request type IE is set to "initial request".

8.2.10.6 DNN

The UE may include this IE when the Request type IE is set to "initial request".

8.2.10.7 Additional information

The UE may include this IE when the Payload container type IE is set to "LTE Positioning Protocol (LPP) message container".

8.2.11 DL NAS transport

8.2.11.1 Message definition

The DL NAS TRANSPORT message transports message payload and associated information to the UE. See table 8.2.11.1.1.

Message type: DL NAS TRANSPORT

Significance: dual

Direction: network to UE

Table 8.2.11.1.1: DL NAS TRANSPORT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	DL NAS TRANSPORT message identity	Message type 9.7	M	V	1
	Payload container type	Payload container type 9.10.3.36	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Payload container	Payload container 9.10.3.35	M	LV-E	3-65537
70	PDU session ID	PDU session identity 2 9.10.3.37	C	TV	2
24	Additional information	Additional information 9.10.2.1	O	TLV	3-n
58	5GMM cause	5GMM cause 9.10.3.2	O	TV	2
37	Back-off timer value	GPRS timer 3 9.10.2.5	O	TLV	3

8.2.11.2 PDU session ID

The AMF shall include this IE when the Payload container type IE is set to "N1 SM information".

8.2.11.3 Additional information

The AMF may include this IE when the Payload container type IE is set to "LTE Positioning Protocol (LPP) message container".

8.2.11.4 5GMM cause

The AMF shall include this IE when the Payload container IE contains an uplink payload which was not forwarded.

8.2.11.5 Back-off timer value

The AMF shall include this IE when the Payload container IE contains an uplink 5GSM message which was not forwarded due to DNN based congestion control, S-NSSAI and DNN based congestion control or S-NSSAI only based congestion control.

8.2.12 De-registration request (UE originating de-registration)

8.2.12.1 Message definition

The DEREGISTRATION REQUEST message is sent by the UE to the AMF. See table 8.2.12.1.1.

Message type: DEREGISTRATION REQUEST

Significance: dual

Direction: UE to network

Table 8.2.12.1.1: DEREGISTRATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	De-registration request message identity	Message type 9.7	M	V	1
	De-registration type	De-registration type 9.10.3.18	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	5GS mobile identity	5GS mobile identity 9.10.3.4	M	TLV	TBD

8.2.13 De-registration accept (UE originating de-registration)

8.2.13.1 Message definition

The DEREGISTRATION ACCEPT message is sent by the AMF to the UE. See table 8.2.13.1.1.

Message type: DEREGISTRATION ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.13.1.1: DEREGISTRATION ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	De-registration accept message identity	Message type 9.7	M	V	1

8.2.14 De-registration request (UE terminated de-registration)

8.2.14.1 Message definition

The DEREGISTRATION REQUEST message is sent by the AMF to the UE. See table 8.2.14.1.1.

Message type: DEREGISTRATION REQUEST

Significance: dual

Direction: network to UE

Table 8.2.14.1.1: DEREGISTRATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	De-registration request message identity	Message type 9.7	M	V	1
	De-registration type	De-registration type 9.10.3.18	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
58	5GMM cause	5GMM cause 9.10.3.2	O	TV	2
5F	T3346 value	GPRS timer 2 9.10.2.4	O	TLV	3

8.2.14.2 5GMM cause

This information element is included if a 5GMM cause is provided.

8.2.14.3 T3346 value

The AMF may include this IE when the general NAS level mobility management congestion control is active.

8.2.15 De-registration accept (UE terminated de-registration)

8.2.15.1 Message definition

The DEREGISTRATION ACCEPT message is sent by the UE to the AMF. See table 8.2.15.1.1.

Message type: DEREGISTRATION ACCEPT

Significance: dual

Direction: UE to network

Table 8.2.15.1.1.1: DEREGISTRATION ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	De-registration accept message identity	Message type 9.7	M	V	1

8.2.16 Service request

8.2.16.1 Message definition

The SERVICE REQUEST message is sent by the UE to the AMF in order to request the establishment of an N1 NAS signalling connection and/or to request the establishment of user-plane resources for PDU sessions which are activated without user-plane resources. See table 8.2.16.1.1.

Message type: SERVICE REQUEST

Significance: dual

Direction: UE to network

Table 8.2.16.1.1: SERVICE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Service request message identity	Message type 9.7	M	V	1
	ngKSI	NAS key set identifier 9.10.3.29	M	V	1/2
	Service type	Service type 9.10.3.46	M	V	1/2
	5G-S-TMSI	5GS mobile identity 9.10.3.4	M	LV	6
40	Uplink data status	Uplink data status 9.10.3.53	O	TLV	4-34
50	PDU session status	PDU session status 9.10.3.40	O	TLV	4-34
25	Allowed PDU session status	Allowed PDU session status 9.10.3.11	O	TLV	4-34

8.2.16.2 Uplink data status

This IE shall be included if the UE has uplink user data pending to be sent.

8.2.16.3 PDU session status

This IE shall be included if the UE wants to indicate the PDU sessions associated with the access type the message is sent over that are active within the UE.

8.2.16.4 Allowed PDU session status

This IE shall be included if the SERVICE REQUEST message is sent as a response to paging or notification via 3GPP access for PDU session(s) associated with non-3GPP access and the UE wants to indicate the user-plane resources of PDU session(s) associated with non-3GPP access allowed to be re-established over 3GPP access or if there is no PDU session(s) for which the UE allows the user-plane resources to be re-established over 3GPP access.

8.2.17 Service accept

8.2.17.1 Message definition

The SERVICE ACCEPT message is sent by the AMF to the UE in order to accept the service request procedure. See table 8.2.17.1.1.

Message type: SERVICE ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.17.1.1: SERVICE ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Service accept message identity	Message type 9.7	M	V	1
50	PDU session status	PDU session status 9.10.3.40	O	TLV	4-34
26	PDU session reactivation result	PDU session reactivation result 9.10.3.38	O	TLV	4-32
7E	PDU session reactivation result error cause	PDU session reactivation result error cause 9.10.3.39	O	TLV-E	5-515
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503

8.2.17.2 PDU session status

This IE shall be included if the network wants to indicate the PDU sessions associated with the access type the message is sent over that are active within the network.

8.2.17.3 PDU session reactivation result

This IE shall be included:

- if the Uplink data status IE is included in the SERVICE REQUEST message;
- if the Allowed PDU session status IE is included in the SERVICE REQUEST message and there is at least one PDU session indicated in the Allowed PDU session status IE that can be reactivated over 3GPP access.

8.2.17.4 PDU session reactivation result error cause

This IE may be included if the PDU session reactivation result IE is included and there exist one or more PDU sessions for which the user-plane resources cannot be re-established, to indicate the cause of failure to re-establish the user-plane resources.

8.2.17.5 EAP message

EAP message IE is included if the SERVICE ACCEPT message is sent to a UE registered for emergency services and is used to convey EAP-failure message.

8.2.18 Service reject

8.2.18.1 Message definition

The SERVICE REJECT message is sent by the AMF to the UE in order to reject the service request procedure. See table 8.2.18.1.1.

Message type: SERVICE REJECT

Significance: dual

Direction: network to UE

Table 8.2.18.1.1: SERVICE REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Service reject message identity	Message type 9.7	M	V	1
	5GMM cause	5GMM cause 9.10.3.2	M	V	1
50	PDU session status	PDU session status 9.10.3.40	O	TLV	4-34
5F	T3346 value	GPRS timer 2 9.10.24	O	TLV	3
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503

8.2.18.2 PDU session status

This IE shall be included if the network wants to indicate the PDU sessions associated with the access type the message is sent over that are active within the network.

8.2.18.3 T3346 value

The AMF may include this IE when the general NAS level mobility management congestion control is active.

8.2.18.4 EAP message

EAP message IE is included if the SERVICE REJECT message is used to convey EAP-failure message.

8.2.19 Configuration update command

8.2.19.1 Message definition

The CONFIGURATION UPDATE COMMAND message is sent by the AMF to the UE. See table 8.2.19.1.1.

Message type: CONFIGURATION UPDATE COMMAND

Significance: dual

Direction: network to UE

Table 8.2.19.1.1: CONFIGURATION UPDATE COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Configuration update command message identity	Message type 9.7	M	V	1
D-	Configuration update indication	Configuration update indication 9.10.3.16	O	TV	1
2C	5G-GUTI	5GS mobile identity 9.10.3.4	O	TLV	13
54	TAI list	5GS tracking area identity list 9.10.3.9	O	TLV	9-114
70	Allowed NSSAI	NSSAI 9.10.3.34	O	TLV	4-74
27	Service area list	Service area list 9.10.3.45	O	TLV	6-114
43	Full name for network	Network name 9.10.3.33	O	TLV	3-n
45	Short name for network	Network name 9.10.3.33	O	TLV	3-n
46	Local time zone	Time zone 9.10.3.47	O	TV	2
47	Universal time and local time zone	Time zone and time 9.10.3.48	O	TV	8
49	Network daylight saving time	Daylight saving time 9.10.3.17	O	TLV	3
79	LADN information	LADN information 9.10.3.27	O	TLV-E	3-1707
B-	MICO indication	MICO indication 9.10.3.28	O	TV	1
31	Configured NSSAI	NSSAI 9.10.3.34	O	TLV	4-146
11	Rejected NSSAI	Rejected NSSAI 9.10.3.42	O	TLV	4-42

8.2.19.2 Configuration update indication

The AMF shall include this IE if the AMF wants to request an acknowledgement or a registration procedure from the UE.

8.2.19.3 5G-GUTI

This IE may be included to assign a new 5G GUTI to the UE.

8.2.19.4 TAI list

This IE may be included to assign a new TAI list to the UE.

8.2.19.5 Allowed NSSAI

This IE may be included to assign a new allowed NSSAI to the UE.

8.2.19.6 Service area list

This IE may be included to assign a new service area list to the UE.

8.2.19.7 Full name for network

This IE may be included to assign a new full name for network to the UE.

8.2.19.8 Short name for network

This IE may be included to assign a new short name for network to the UE.

8.2.19.9 Local time zone

This IE may be included to assign a new local time zone to the UE.

8.2.19.10 Universal time and local time zone

This IE may be included to assign new universal time and local time zone to the UE.

8.2.19.11 Network daylight saving time

This IE may be included to assign new network daylight saving time to the UE.

8.2.19.12 LADN information

This IE may be included to assign new LADN information to the UE or delete the LADN information at the UE side.

8.2.19.13 MICO indication

This IE may be included to assign a new MICO indication to the UE.

8.2.19.14 Configured NSSAI

The AMF shall include this IE if the AMF wants to provide the UE with a new configured NSSAI for the current PLMN.

8.2.19.15 Rejected NSSAI

The network may include this IE to inform the UE of the S-NSSAIs that were previously sent to the UE in the allowed NSSAI, but are now rejected by the network.

8.2.20 Configuration update complete

8.2.20.1 Message definition

The CONFIGURATION UPDATE COMPLETE message is sent by the UE to the AMF. See table 8.2.20.1.1.

Message type: CONFIGURATION UPDATE COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.20.1.1: CONFIGURATION UPDATE COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Configuration update complete message identity	Message type 9.7	M	V	1

8.2.21 Identity request

8.2.21.1 Message definition

The IDENTITY REQUEST message is sent by the AMF to the UE to request the UE to provide specified identity. See table 8.2.21.1.1

Message type: IDENTITY REQUEST

Significance: dual

Direction: AMF to UE

Table 8.2.21.1.1: IDENTITY REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Identity request message identity	Message type 9.7	M	V	1
	Identity type	5GS identity type 9.10.3.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2

8.2.22 Identity response

8.2.22.1 Message definition

The IDENTITY RESPONSE message is sent by the UE to the AMF to provide the requested identity. See table 8.2.22.1.

Message type: IDENTITY RESPONSE

Significance: dual

Direction: UE to AMF

Table 8.2.22.1.1: IDENTITY RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Identity response message identity	Message type 9.7	M	V	1
	Mobile identity	5GS mobile identity 9.10.3.4	M	LV	2-TBD

8.2.23 Notification

8.2.23.1 Message definition

The NOTIFICATION message is sent by the AMF to the UE to notify the UE to initiate a service request procedure. See table 8.2.23.1.1.

Message type: NOTIFICATION

Significance: dual

Direction: network to UE

Table 8.2.23.1.1: NOTIFICATION message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Notification message identity	Message type 9.7	M	V	1
	Access type	Access type 9.10.3.10	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2

8.2.24 Notification response

8.2.24.1 Message definition

The NOTIFICATION RESPONSE message is sent by the UE to the AMF to notify the failure to initiate the service request procedure as a response of notification. See table 8.2.24.1.1.

Message type: NOTIFICATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.2341.1: NOTIFICATION RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Notification response message identity	Message type 9.7	M	V	1
50	PDU session status	PDU session status 9.10.3.40	O	TLV	4-34

8.2.24.2 PDU session status

This information element shall be included if the UE wants to indicate over non-3GPP access type the PDU sessions associated with the 3GPP access type that are active within the UE.

8.2.25 Security mode command

8.2.25.1 Message definition

The SECURITY MODE COMMAND message is sent by the AMF to the UE to establish NAS signalling security. See table 8.2.25.1.1.

Message type: SECURITY MODE COMMAND

Significance: dual

Direction: network to UE

Table 8.2.25.1.1: SECURITY MODE COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Security mode command message identity	Message type 9.7	M	V	1
	Selected NAS security algorithms	NAS security algorithms 9.10.3.32	M	V	1
	ngKSI	NAS key set identifier 9.10.3.29	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Replayed UE security capabilities	UE security capability 9.10.3.50	M	LV	3-5
E-	IMEISV request	IMEISV request 9.10.3.26	O	TV	1
4F	$Hash_{AMF}$	$Hash_{AMF}$ 9.10.3.25	O	TV	9
57	Selected EPS NAS security algorithms	EPS NAS security algorithms 9.10.3.23	O	TV	2
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7

8.2.25.2 IMEISV request

The AMF may include this information element to request the UE to send its IMEISV with the corresponding SECURITY MODE COMPLETE message.

8.2.25.3 $Hash_{AMF}$

The AMF shall include this information element when the AMF is initiating a SECURITY MODE COMMAND during a registration procedure and the REGISTRATION REQUEST message did not successfully pass the integrity check at the AMF.

8.2.25.4 Selected EPS NAS security algorithms

This IE shall be included if the AMF does not support interworking procedures without N26 interface and the UE set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message.

8.2.25.5 EAP message

This IE is included when the EAP Success message is sent as part of the EAP-based primary authentication and key agreement procedure, as specified in subclause 5.4.1.2.

8.2.26 Security mode complete

8.2.26.1 Message definition

The SECURITY MODE COMPLETE message is sent by the UE to the AMF in response to a SECURITY MODE COMMAND message. See table 8.2.26.1.1.

Message type: SECURITY MODE COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.26.1.1: SECURITY MODE COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Security mode complete message identity	Message type 9.6	M	V	1
2C	IMEISV	5G mobile identity 9.10.3.4	O	TLV	11
7D	NAS message container	NAS message container 9.10.3.31	O	TLV-E	3-n

8.2.26.2 IMEISV

The UE shall include this information element, if the IMEISV was requested within the corresponding SECURITY MODE COMMAND message.

8.2.26.3 NAS message container

The UE shall include this information element:

a) if during an ongoing registration procedure, the AMF included $HASH_{AMF}$ in the SECURITY MODE COMMAND message and $HASH_{AMF}$ has a different value from the hash value locally calculated at the UE as described in 3GPP TS 33.501 [24]; and

b) when the UE has sent an initial NAS message with a limited set of IEs before the SECURITY MODE COMMAND message was received and the UE needs to include the complete initial NAS message in the SECURITY MODE COMPLETE message, as described in 3GPP TS 33.501 [24].

8.2.27 Security mode reject

8.6.27.1 Message definition

The SECURITY MODE REJECT message is sent by the UE to the AMF to indicate that the corresponding security mode command has been rejected. See table 8.2.27.1.1.

Message type: SECURITY MODE REJECT

Significance: dual

Direction: UE to network

Table 8.2.27.1.1: SECURITY MODE REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	Security mode reject message identity	Message type 9.6	M	V	1
	5GMM cause	5GMM cause 9.10.3.2	M	V	1

8.2.28 Security protected 5GS NAS message

8.2.28.1 Message definition

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 8.2.28.1.1.

Message type: SECURITY PROTECTED 5GS NAS MESSAGE

Significance: dual

Direction: both

Table 8.2.28.1.1: SECURITY PROTECTED 5GS NAS MESSAGE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.4	M	V	1/2
	Message authentication code	Message authentication code 9.8	M	V	4
	Sequence number	Sequence number 9.9	M	V	1
	NAS message	NAS message 9.10.3.30	M	V	3-n

8.2.29 5GMM status

8.2.29.1 Message definition

The 5GMM STATUS message is sent by the UE or by the AMF at any time to report certain error conditions. See table 8.2.28.1.1.

Message type: 5GMM STATUS

Significance: local

Direction: both

Table 8.2.29.1.1: 5GMM STATUS message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	Security header type	Security header type 9.3	M	V	1/2
	Spare half octet	Spare half octet 9.5	M	V	1/2
	5GMM STATUS message identity	Message type 9.7	M	V	1
	5GMM cause	5GMM cause 9.10.3.2	M	V	2

8.3 5GS session management messages

8.3.1 PDU session establishment request

8.3.1.1 Message definition

The PDU SESSION ESTABLISHMENT REQUEST message is sent by the UE to the SMF to initiate establishment of a PDU session. See table 8.3.1.1.1.

Message type: PDU SESSION ESTABLISHMENT REQUEST

Significance: dual

Direction: UE to network

Table 8.3.1.1.1: PDU SESSION ESTABLISHMENT REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION ESTABLISHMENT REQUEST message identity	Message type 9.7	M	V	1
9-	PDU session type	PDU session type 9.10.4.8	O	TV	1
A-	SSC mode	SSC mode 9.10.4.12	O	TV	1
28	5GSM capability	5GSM capability 9.10.4.1	O	TLV	3-15
55	Maximum number of supported packet filters	Maximum number of supported packet filters 9.10.4.6	O	TV	3
TBD	SM PDU DN request container	SM PDU DN request container 9.10.4.11	O	TBD	TBD
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.1.2 PDU session type

This IE is included in the message when the UE requests to establish a new PDU session with a DN and requests a PDU session type.

8.3.1.3 SSC mode

This IE is included in the message when the UE requests to establish a new PDU session with a DN and requests an SSC mode.

8.3.1.4 Maximum number of supported packet filters

This IE shall be included in the message when the selected PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet" and the UE can support more than 16 packet filters for this PDU session.

8.3.1.5 5GSM capability

This IE is included in the message when the UE requests to establish a new PDU session of "IPv4", "IPv6", "IPv4v6" or "Ethernet" PDU session type and the UE supports Reflective QoS, or establish a new PDU session of "IPv6" or "IPv4v6" PDU session type and the UE supports acting as a type C host as specified in IETF RFC 4191 [36].

8.3.1.6 SM PDU DN request container

This IE is included in the message when the UE requests to establish a new PDU session with a DN and needs to provide information for the PDU session authentication and authorization by the external DN.

8.3.1.7 Extended protocol configuration options

This IE is included in the message when the UE wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.2 PDU session establishment accept

8.3.2.1 Message definition

The PDU SESSION ESTABLISHMENT ACCEPT message is sent by the SMF to the UE in response to PDU SESSION ESTABLISHMENT REQUEST message and indicates successful establishment of a PDU session. See table 8.3.2.1.1.

Message type: PDU SESSION ESTABLISHMENT ACCEPT

Significance: dual

Direction: network to UE

Table 8.3.2.1.1: PDU SESSION ESTABLISHMENT ACCEPT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION ESTABLISHMENT ACCEPT message identity	Message type 9.7	M	V	1
	Selected PDU session type	PDU session type 9.10.4.8	M	V	1/2
	Selected SSC mode	SSC mode 9.10.4.12	M	V	1/2
	DNN	DNN 9.10.3.19	M	LV	2-TBD
	Authorized QoS rules	QoS rules 9.10.4.9	M	LV-E	7-65538
	Session AMBR	Session-AMBR 9.10.4.10	M	LV	TBD
59	5GSM cause	5GSM cause 9.10.4.2	O	TV	2
29	PDU address	PDU address 9.10.4.7	O	TLV	7, 11 or 15
56	RQ timer value	GPRS timer 9.10.2.3	O	TV	2
22	S-NSSAI	S-NSSAI 9.10.2.6	O	TLV	3-10
7F	Mapped EPS bearer contexts	Mapped EPS bearer contexts 9.10.4.6	O	TLV-E	7-65538
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.2.2 5GSM cause

This IE is included when the selected PDU session type is different from the PDU session type requested by the UE.

8.3.2.3 PDU address

This IE is included when the selected PDU session type is "IPv4", "IPv6" or "IPv4v6".

8.3.2.4 RQ timer value

This IE is included when the network wants to provide the RQ timer value.

8.3.2.5 S-NSSAI

This IE shall be included in the message when the SMF received from the AMF an S-NSSAI together with the PDU SESSION ESTABLISHMENT REQUEST message, and the PDU session is a non-emergency PDU session.

8.3.2.6 Mapped EPS bearer contexts

This IE is included when interworking to EPS is supported for the PDU session context.

8.3.2.7 EAP message

This IE is included when the external DN successfully performed authentication and authorization of the UE using EAP.

8.3.2.8 Extended protocol configuration options

This IE is included in the message when the network wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.3 PDU session establishment reject

8.3.3.1 Message definition

The PDU SESSION ESTABLISHMENT REJECT message is sent by the SMF to the UE in response to PDU SESSION ESTABLISHMENT REQUEST message and indicates unsuccessful establishment of a PDU session. See table 8.3.3.1.1.

Message type: PDU SESSION ESTABLISHMENT REJECT

Significance: dual

Direction: network to UE

Table 8.3.3.1.1: PDU SESSION ESTABLISHMENT REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION ESTABLISHMENT REJECT message identity	Message type 9.7	M	V	1
	5GSM cause	5GSM cause 9.10.4.2	M	V	1
37	Back-off timer value	GPRS timer 3 9.10.2.5	O	TLV	3
F-	Allowed SSC mode	Allowed SSC mode 9.10.4.3	O	TV	1
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.3.2 Back-off timer value

The network may include this IE to request a minimum time interval before procedure retry is allowed.

8.3.3.3 Allowed SSC mode

This IE is included when the network rejects the PDU SESSION ESTABLISHMENT REQUEST with cause #68 "not supported SSC mode.

8.3.3.4 EAP message

This IE is included when the external DN unsuccessfully performed authentication and authorization of the UE using EAP.

8.3.3.5 Extended protocol configuration options

This IE is included in the message when the network wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.4 PDU session authentication command

8.3.4.1 Message definition

The PDU SESSION AUTHENTICATION COMMAND message is sent by the SMF to the UE for authentication of the UE establishing the PDU session or of the UE participating in the PDU session. See table 8.3.4.1.1.

Message type: PDU SESSION AUTHENTICATION COMMAND

Significance: dual

Direction: network to UE

Table 8.3.4.1.1: PDU SESSION AUTHENTICATION COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION AUTHENTICATION COMMAND message identity	Message type 9.7	M	V	1
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.4.2 EAP message

This IE is included when the external DN performs authentication and authorization of the UE using EAP.

8.3.4.3 Extended protocol configuration options

This IE is included in the message when the network wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.5 PDU session authentication complete

8.3.5.1 Message definition

The PDU SESSION AUTHENTICATION COMPLETE message is sent by the UE to the SMF in response to the PDU SESSION AUTHENTICATION COMMAND message and indicates acceptance of the PDU SESSION AUTHENTICATION COMMAND message. See table 8.3.5.1.1.

Message type: PDU SESSION AUTHENTICATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.5.1.1: PDU SESSION AUTHENTICATION COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION AUTHENTICATION COMPLETE message identity	Message type 9.7	M	V	1
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.5.2 EAP message

This IE is included when the external DN performs authentication and authorization of the UE using EAP.

8.3.5.3 Extended protocol configuration options

This IE is included in the message when the UE wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.6 PDU session authentication result

8.3.6.1 Message definition

The PDU SESSION AUTHENTICATION RESULT message is sent by the SMF to the UE for indication of successful result of authentication of the UE participating in the PDU session. See table 8.3.6.1.1.

Message type: PDU SESSION AUTHENTICATION RESULT

Significance: dual

Direction: network to UE

Table 8.3.6.1.1: PDU SESSION AUTHENTICATION RESULT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION AUTHENTICATION RESULT message identity	Message type 9.7	M	V	1
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.6.2 EAP message

This IE is included when the external DN performs authentication and authorization of the UE using EAP and it completes successfully.

8.3.6.3 Extended protocol configuration options

This IE is included in the message when the network wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.7 PDU session modification request

8.3.7.1 Message definition

The PDU SESSION MODIFICATION REQUEST message is sent by the UE to the SMF to request a modification of a PDU session. See table 8.3.7.1.1.

Message type: PDU SESSION MODIFICATION REQUEST

Significance: dual

Direction: UE to network

Table 8.3.7.1.1: PDU SESSION MODIFICATION REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION MODIFICATION REQUEST message identity	Message type 9.7	M	V	1
28	5GSM capability	5GSM capability 9.10.4.1	O	TLV	3-15
55	Maximum number of supported packet filters	Maximum number of supported packet filters 9.10.4.6	O	TV	3
7A	Requested QoS rules	QoS rules 9.10.4.9	O	TLV-E	3-65538
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.7.2 5GSM capability

This IE is included in the message after inter-system change from S1 mode to N1 mode:

a) if the PDU session is of "IPv4", "IPv6", "IPv4v6" or "Ethernet" PDU session type, and the UE supports reflective QoS or revokes the previously indicated support of reflective QoS; or

b) if the PDU session is of "IPv6" or "IPv4v6" PDU session type, and the UE supports acting as a type C host as specified in IETF RFC 4191 [36].

8.3.7.3 Maximum number of supported packet filters

This IE shall be included in the message when the selected PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet", the UE can support more than 16 packet filters for this PDU session, and the UE is sending the message after an inter-system change from S1 mode to N1 mode.

8.3.7.4 Requested QoS rules

This IE is included in the message when the UE requests a specific QoS handling.

8.3.7.5 Extended protocol configuration options

This IE is included in the message when the UE wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.8 PDU session modification reject

8.3.8.1 Message definition

The PDU SESSION MODIFICATION REJECT message is sent by the SMF to the UE to indicate rejection of the PDU SESSION MODIFICATION REQUEST. See table 8.3.8.1.1.

Message type: PDU SESSION MODIFICATION REJECT

Significance: dual

Direction: network to UE

Table 8.3.8.1.1: PDU SESSION MODIFICATION REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION MODIFICATION REJECT message identity	Message type 9.7	M	V	1
	5GSM cause	5GSM cause 9.10.4.2	M	V	1
37	Back-off timer value	GPRS timer 3 9.10.2.5	O	TLV	3
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.8.2 Back-off timer value

The network may include this IE to request a minimum time interval before procedure retry is allowed.

8.3.8.3 Extended protocol configuration options

This IE is included in the message when the network wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.9 PDU session modification command

8.3.9.1 Message definition

The PDU SESSION MODIFICATION COMMAND message is sent by the SMF to the UE to indicate a modification of a PDU session. See table 8.3.9.1.1

Message type: PDU SESSION MODIFICATION COMMAND

Significance: dual

Direction: network to UE

Table 8.3.9.1.1: PDU SESSION MODIFICATION COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION MODIFICATION COMMAND message identity	Message type 9.7	M	V	1
59	5GSM cause	5GSM cause 9.10.4.2	O	TV	2
2A	Session AMBR	Session-AMBR 9.10.4.10	O	TLV	8
56	RQ timer value	GPRS timer 9.10.2.3	O	TV	2
7A	Authorized QoS rules	QoS rules 9.10.4.9	O	TLV-E	7-65538
7F	Mapped EPS bearer contexts	Mapped EPS bearer contexts 9.10.4.5	O	TLV-E	7-65538
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.9.2 5GSM cause

This IE is included when the network performs the PDU session anchor relocation for SSC mode 3.

8.3.9.3 Session-AMBR

This IE is included when the session-AMBR of the PDU session is modified.

8.3.9.4 RQ timer value

This IE is included when the network wants to provide the RQ timer value.

8.3.9.5 Authorized QoS rules

This IE is included when the authorized QoS rules of the PDU session are modified.

8.3.9.6 Mapped EPS bearer contexts

This IE is included when interworking to EPS is supported for the PDU session context and the mapped EPS bearer contexts is modified.

8.3.9.7 Extended protocol configuration options

This IE is included in the message when the network wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.10 PDU session modification complete

8.3.10.1 Message definition

The PDU SESSION MODIFICATION COMPLETE message is sent by the UE to the SMF in response to the PDU SESSION MODIFICATION COMMAND message and indicates an acceptance of the PDU SESSION MODIFICATION COMMAND message. See table 8.3.10.1.1.

Message type: PDU SESSION MODIFICATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.10.1.1: PDU SESSION MODIFICATION COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION MODIFICATION COMPLETE message identity	Message type 9.7	M	V	1
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.10.2 Extended protocol configuration options

This IE is included in the message when the UE wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.11 PDU session modification command reject

8.3.11.1 Message definition

The PDU SESSION MODIFICATION COMMAND REJECT message is sent by the UE to the SMF to indicate rejection of the PDU SESSION MODIFICATION COMMAND message. See table 8.3.11.1.1.

Message type: PDU SESSION MODIFICATION COMMAND REJECT

Significance: dual

Direction: UE to network

Table 8.3.11.1.1: PDU SESSION MODIFICATION COMMAND REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION MODIFICATION COMMAND REJECT message identity	Message type 9.7	M	V	1
	5GSM cause	5GSM cause 9.10.4.2	M	V	1
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.11.2 Extended protocol configuration options

This IE is included in the message when the UE wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.12 PDU session release request

8.3.12.1 Message definition

The PDU SESSION RELEASE REQUEST message is sent by the UE to the SMF to request a release of a PDU session. See table 8.3.12.1.1.

Message type: PDU SESSION RELEASE REQUEST

Significance: dual

Direction: UE to network

Table 8.3.12.1.1: PDU SESSION RELEASE REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION RELEASE REQUEST message identity	Message type 9.7	M	V	1
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.12.2 Extended protocol configuration options

This IE is included in the message when the UE wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.13 PDU session release reject

8.3.13.1 Message definition

The PDU SESSION RELEASE REJECT message is sent by the SMF to the UE to indicate rejection of request a release of a PDU session. See table 8.3.13.1.1.

Message type: PDU SESSION RELEASE REJECT

Significance: dual

Direction: network to UE

Table 8.3.13.1.1: PDU SESSION RELEASE REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU RELEASE REJECT message identity	Message type 9.7	M	V	1
	5GSM cause	5GSM cause 9.10.4.2	M	V	1
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.13.2 Extended protocol configuration options

This IE is included in the message when the network wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.14 PDU session release command

8.3.14.1 Message definition

The PDU SESSION RELEASE COMMAND message is sent by the SMF to the UE to indicate a release of a PDU session. See table 8.3.14.1.1.

Message type: PDU SESSION RELEASE COMMAND

Significance: dual

Direction: network to UE

Table 8.3.14.1.1: PDU SESSION RELEASE COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION RELEASE COMMAND message identity	Message type 9.7	M	V	1
	5GSM cause	5GSM cause 9.10.4.2	M	V	1
37	Back-off timer value	GPRS timer 3 9.10.2.5	O	TLV	3
78	EAP message	EAP message 9.10.2.2	O	TLV-E	7-1503
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.14.2 Back-off timer value

The network may include this IE to request a minimum time interval before procedure retry is allowed.

8.3.14.3 EAP message

This IE is included when the external DN performs re-authentication and re-authorization of the UE using EAP and it completes unsuccessfully.

8.3.14.4 Extended protocol configuration options

This IE is included in the message when the network wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

8.3.15 PDU session release complete

8.3.15.1 Message definition

The PDU SESSION RELEASE COMPLETE message is sent by the UE to the SMF in response to the PDU SESSION RELEASE COMMAND message and indicates an acceptance of a release of the PDU session. See table 8.3.15.1.1.

Message type: PDU SESSION RELEASE COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.15.1.1: PDU SESSION RELEASE COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	PDU SESSION RELEASE COMPLETE message identity	Message type 9.7	M	V	1
7B	Extended protocol configuration options	Extended protocol configuration options 9.10.4.4	O	TLV-E	4-65538

8.3.15.2 Extended protocol configuration options

This IE is included in the message when the UE wants to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

8.3.16 5GSM status

8.3.16.1 Message definition

The 5GSM STATUS message is sent by the SMF or the UE to pass information on the status of the indicated PDU session and report certain error conditions. See table 8.3.16.1.1.

Message type: 5GSM STATUS

Significance: dual

Direction: both

Table 8.3.16.1.1: 5GSM STATUS message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	5GSM STATUS message identity	Message type 9.7	M	V	1
	5GSM cause	5GSM cause 9.10.4.2	M	V	1

9 General message format and information elements coding

9.1 Overview

Within the protocols defined in the present document, every 5GS NAS message is a standard L3 message as defined in 3GPP TS 24.007 [11]. This means that the message consists of the following parts:

1) if the message is a plain 5GS NAS message:
   a) extended protocol discriminator;
   b) security header type or PDU session identity;
   c) procedure transaction identity;
   d) message type;
   e) other information elements, as required.
2) if the message is a security protected 5GS NAS message:
   a) extended protocol discriminator;
   b) security header type;
   c) message authentication code;
   d) sequence number;
   e) plain 5GS NAS message, as defined in item 1

The organization of a plain 5GS NAS message is illustrated in the example shown in figure .9.1.1.

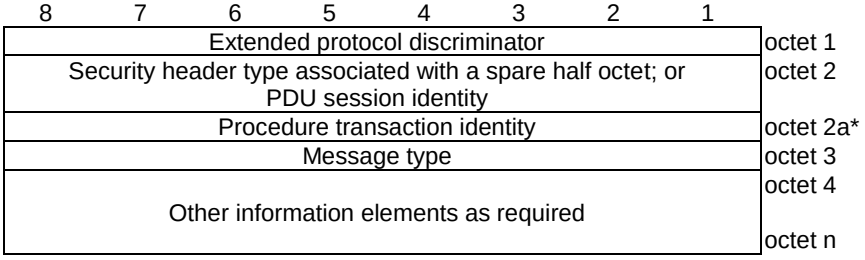


Figure .9.1.1: General message organization example for a plain 5GS NAS message

The PDU session identity and the procedure transaction identity are only used in messages with extended protocol discriminator 5GS session management. Octet 2a with the procedure transaction identity shall only be included in these messages.

The organization of a security protected 5GS NAS message is illustrated in the example shown in figure 9.1.2.

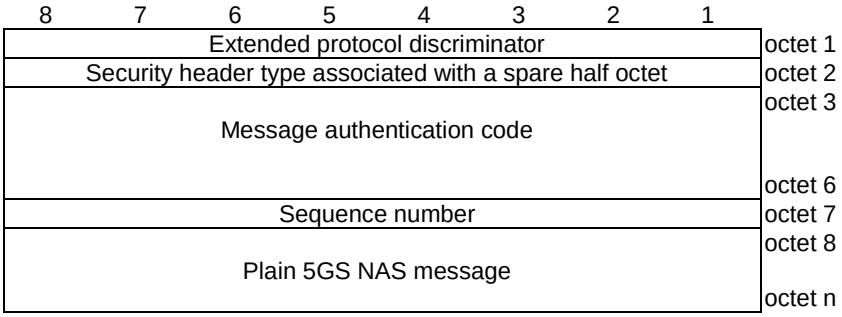


Figure 9.1.2: General message organization example for a security protected 5GS NAS message

Unless specified otherwise in the message descriptions of clause 8 and clause 9, 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 most significant bit of the field is represented by the highest numbered bit of the lowest numbered octet of the field. The least significant bit of the field is represented by the lowest numbered bit of the highest numbered octet of the field.

9.2 Extended protocol discriminator

Bits 1 to 8 of the first octet of every 5GS NAS message contain the Extended protocol discriminator (EPD) IE. The EPD and its use are defined in 3GPP TS 24.007 [11]. The extended protocol discriminator in the header (see 3GPP TS 24.007 [11]) of a security protected 5GS NAS message is encoded as "5GS mobility management messages".

9.3 Security header type

Bits 1 to 4 of the second octet of every 5GMM message contain the Security header type IE. This IE includes control information related to the security protection of a 5GMM 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)				
Bits				
4	**3**	**2**	**1**	
0	0	0	0	Plain 5GS NAS message, not security protected
				Security protected 5GS NAS message:
0	0	0	1	Integrity protected
0	0	1	0	Integrity protected and ciphered
0	0	1	1	Integrity protected with new 5G NAS security context (NOTE 1)
0	1	0	0	Integrity protected and ciphered with new 5G NAS security context (NOTE 2)
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.

An 5GMM message received with the security header type encoded as 0000 shall be treated as not security protected, plain 5GS NAS message. A protocol entity sending a not security protected 5GMM message shall send the message as plain 5GS NAS message and encode the security header type as 0000.

9.4 PDU session identity

Bits 1 to 8 of the second octet of every 5GSM message contain the PDU session identity IE. The PDU session identity and its use to identify a message flow are defined in 3GPP TS 24.007 [11].

9.5 Spare half octet

This element is used in the description of 5GMM and 5GSM 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.

9.6 Procedure transaction identity

Bits 1 to 8 of the third octet of every 5GSM message contain the procedure transaction identity. The procedure transaction identity and its use are defined in 3GPP TS 24.007 [11].

9.7 Message type

The Message type IE and its use are defined in 3GPP TS 24.007 [11]. Tables 9.7.1 and 9.7.2 define the value part of the message type IE used in the 5GS mobility management protocol and 5GS session management protocol.

Table 9.7.1: Message types for 5GS mobility management

Bits 8	7	6	5	4	3	2	1	
0	1	-	-	-	-	-	-	5GS mobility management messages
0	1	0	0	0	0	0	1	Registration request
0	1	0	0	0	0	1	0	Registration accept
0	1	0	0	0	0	1	1	Registration complete
0	1	0	0	0	1	0	0	Registration reject
0	1	0	0	0	1	0	1	Deregistration request (UE originating)
0	1	0	0	0	1	1	0	Deregistration accept (UE originating)
0	1	0	0	0	1	1	1	Deregistration request (UE terminated)
0	1	0	0	1	0	0	0	Deregistration accept (UE terminated)
0	1	0	0	1	1	0	0	Service request
0	1	0	0	1	1	0	1	Service reject
0	1	0	0	1	1	1	0	Service accept
0	1	0	1	0	1	0	0	Configuration update command
0	1	0	1	0	1	0	1	Configuration update complete
0	1	0	1	0	1	1	0	Authentication request
0	1	0	1	0	1	1	1	Authentication response
0	1	0	1	1	0	0	0	Authentication reject
0	1	0	1	1	0	0	1	Authentication failure
0	1	0	1	1	0	1	0	Authentication result
0	1	0	1	1	0	1	1	Identity request
0	1	0	1	1	1	0	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	1	0	0	5GMM status
0	1	1	0	0	1	0	1	Notification
0	1	1	0	0	1	1	0	Notification response
0	1	1	0	0	1	1	1	UL NAS transport
0	1	1	0	1	0	0	0	DL NAS transport

Table 9.7.2: Message types for 5GS session management

Bits 8	7	6	5	4	3	2	1	
1	1	-	-	-	-	-	-	5GS session management messages
1	1	0	0	0	0	0	1	PDU session establishment request
1	1	0	0	0	0	1	0	PDU session establishment accept
1	1	0	0	0	0	1	1	PDU session establishment reject
1	1	0	0	0	1	0	1	PDU session authentication command
1	1	0	0	0	1	1	0	PDU session authentication complete
1	1	0	0	0	1	1	1	PDU session authentication result
1	1	0	0	1	0	0	1	PDU session modification request
1	1	0	0	1	0	1	0	PDU session modification reject
1	1	0	0	1	0	1	1	PDU session modification command
1	1	0	0	1	1	0	0	PDU session modification complete
1	1	0	0	1	1	0	1	PDU session modification command reject
1	1	0	1	0	0	0	1	PDU session release request
1	1	0	1	0	0	1	0	PDU session release reject
1	1	0	1	0	0	1	1	PDU session release command
1	1	0	1	0	1	0	0	PDU session release complete
1	1	0	1	0	1	1	0	5GSM status

9.8 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 5GS NAS message if a valid 5G NAS security context exists and security functions are started.

Editor's note: The usage of MAC is FFS.

9.9 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 5GS NAS message. The usage of SN is specified in subclause 4.4.3.

9.10 Other information elements

9.10.1 General

9.10.2 Common information elements

9.10.2.1 Additional information

The purpose of the Additional information information element is to provide additional information to upper layers in relation to the NAS transport mechanism.

The Additional information information element is coded as shown in figure 9.10.2.1.1 and table 9.10.2.1.1.

The Additional information is a type 4 information element with a minimum length of 3 octets.

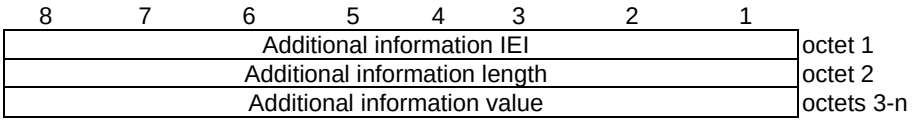


Figure 9.10.2.1.1: Additional information information element

Table 9.10.2.1.1 : Additional information information element

Additional information value (octet 3 to octet n) The coding of the additional information value is dependent on the LCS application.

9.10.2.2 EAP message

The purpose of the EAP message information element is to transport an EAP message as specified in IETF RFC 3748 [34].

The EAP message information element is coded as shown in figure 9.10.2.2.1 and table 9.10.2.2.1.

The EAP message is a type 6 information element with minimum length of 7 octets and maximum length of 1503 octets.

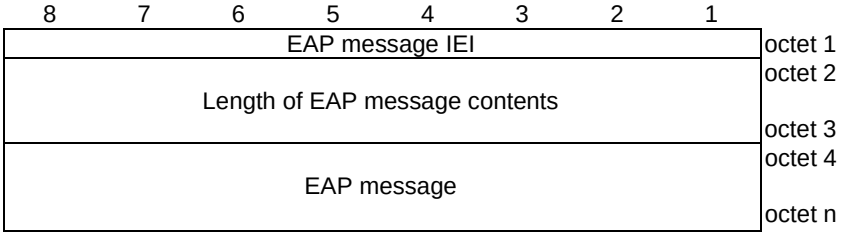


Figure 9.10.2.2.1: EAP message information element

Table 9.10.2.2.1: EAP message information element

EAP message (octet 4 to n) An EAP message as specified in IETF RFC 3748 [34].

9.10.2.3 GPRS timer

See subclause 10.5.7.3 in 3GPP TS 24.008 [12].

9.10.2.4 GPRS timer 2

See subclause 10.5.7.4 in 3GPP TS 24.008 [12].

9.10.2.5 GPRS timer 3

See subclause 10.5.7.4a in 3GPP TS 24.008 [12].

9.10.2.6 S-NSSAI

The purpose of the S-NSSAI information element is to identify a network slice.

The S-NSSAI information element is coded as shown in figure 9.8.2.6.1 and table 9.8.2.6.1.

The S-NSSAI is a type 4 information element with a minimum length of 3 octets and a maximum length of 10 octets.

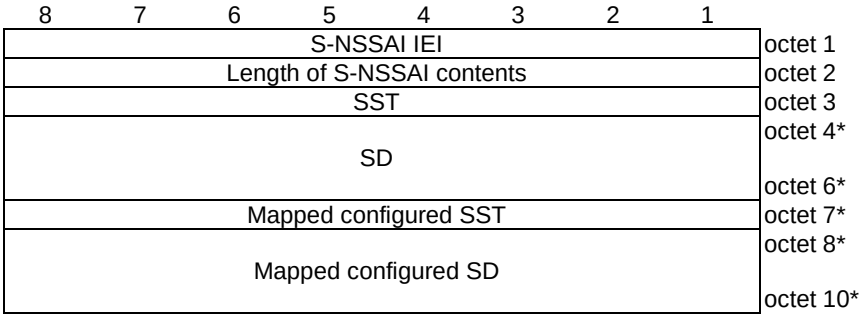


Figure 9.10.2.6.1: S-NSSAI information element

Table 9.10.2.6.1: S-NSSAI information element

Slice/service type (SST) (octet 3) This field contains the 8 bit SST value. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. Slice differentiator (SD) (octet 4 to octet 6) This field contains the 24 bit SD value. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. mapped configured Slice/service type (SST) (octet 7) This field contains the 8 bit SST value of an S-NSSAI in the configured NSSAI for the HPLMN to which the SST value is mapped. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. mapped configured Slice differentiator (SD) (octet 8 to octet 10) This field contains the 24 bit SD value of an S-NSSAI in the configured NSSAI for the HPLMN to which the SD value is mapped. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. NOTE 1: Octet 3 shall always be included. NOTE 2: If the octet 4 is included, then octet 5 and octet 6 shall be included. NOTE 3: If the octet 7 is included, then octets 8, 9, and 10 may be included. NOTE 4: If the octet 8 is included, then octet 9 and octet 10 shall be included.

9.10.2.7 S1 mode to N1 mode NAS transparent container

The purpose of the S1 mode to N1 mode NAS transparent container information element is to provide the UE with parameters that enable the UE to create a mapped 5G NAS security context and take this context into use after inter-system change to N1 mode in 5GMM-CONNECTED mode.

The S1 mode to N1 mode NAS transparent container information element is coded as shown in figure 9.10.2.7.1 and table 9.0.2.7.1.

The S1 mode to N1 mode NAS transparent container is a type 4 information element with a minimum length of 10 octets and a maximum length of 12 octets.

Octets 11 and 12 are optional. If octet 11 is included, then also octet 12 shall be included.

The value part of the S1 mode to N1 mode NAS transparent container information element is included in specific information elements within some RRC messages sent to the UE.

NOTE: For these cases the coding of the information element identifier and length information of RRC is defined in 3GPP TS 38.331 [30].

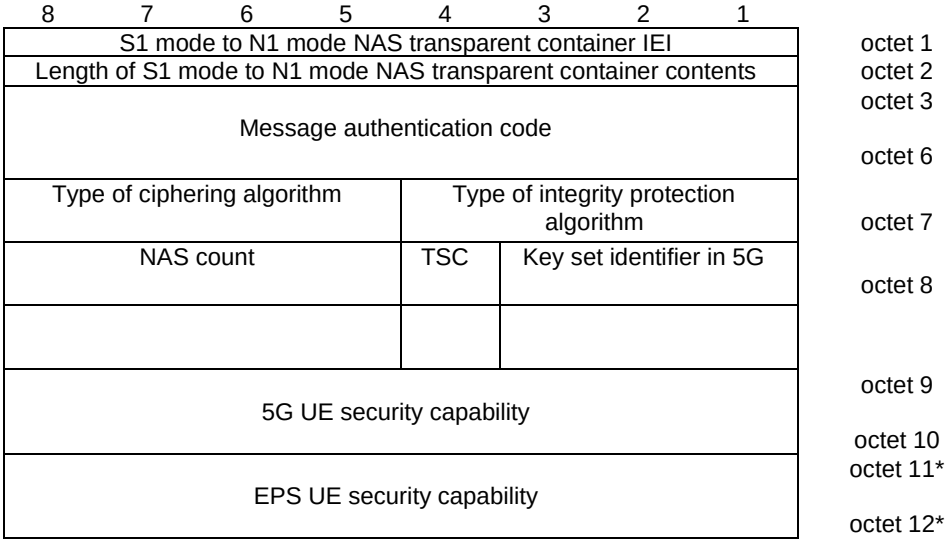


Figure 9.10.2.7.1: S1 mode to N1 mode NAS transparent container information element

Table 9.10.2.7.1: S1 mode to N1 mode NAS transparent container information element

Message authentication code (octet 2 to 5) This field is coded as the Message authentication code information element (see subclause 9.8.3.28). Type of integrity protection algorithm (octet 6, bit 1 to 4) and type of ciphering algorithm (octet 6, bit 5 to 8) 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 9.8.3.32). NAS count (octet 7, bits 5 to 8) This field is coded as the 4 LSB of the Sequence number information element (see subclause 9.8.3.48) Key set identifier in 5G (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 9.8.3.29). 5G UE security capability (octets 9 to 10) This field is coded as octets 3 and 4 of the UE security capability information element (see subclause 9.8.3.57). EPS UE security capability (octets 11 to 12) This field is coded as octets 5 and 6 of the UE security capability information element (see subclause 9.8.3.57).

9.10.3 5GS mobility management (5GMM) information elements

9.10.3.1 5GMM capability

The purpose of the 5GMM capability information element is to provide the network with information concerning aspects of the UE related to the 5GCN or interworking with the EPS. The contents might affect the manner in which the network handles the operation of the UE.

The 5GMM capability information element is coded as shown in figure 9.10.3.1.1 and table 9.10.3.1.1.

The 5GMM capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

8	7	6	5	4	3	2	1	
5GMM capability IEI								octet 1
Length of 5GMM capability contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	HO attach	S1 mode	octet 3
0	0	0	0	0	0	0	0	
Spare								octet 4* -15*

Figure 9.10.3.1.1: 5GMM capability information element

Table 9.10.3.1.1: 5GMM capability information element

EPC NAS supported (S1 mode) (octet 3, bit 1) 0 S1 mode not supported 1 S1 mode supported
Attach request message containing PDN connectivity request with request type handover to transfer PDU session from N1 mode to S1 mode supported (HO attach) (octet 3, bit 2) 0 Attach request message containing PDN connectivity request with request type handover to transfer PDU session from N1 mode to S1 mode not supported 1 Attach request message containing PDN connectivity request with request type handover to transfer PDU session from N1 mode to S1 mode supported
All other bits in octet 3 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.10.3.2 5GMM cause

The purpose of the 5GMM cause information element is to indicate the reason why a 5GMM request from the UE is rejected by the network.

The 5GMM cause information element is coded as shown in figure 9.10.3.1.2 and table 9.10.3.1.2.

The 5GMM cause is a type 3 information element with 2 octets length.

8	7	6	5	4	3	2	1	
5GMM cause IEI								octet 1
Cause value								octet 2

Figure 9.10.3.1.2: 5GMM cause information element

Table 9.10.3.1.2 : 5GMM cause information element

Cause value (octet 2)								
Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	1	1	Illegal UE
0	0	0	0	0	1	0	1	PEI not accepted
0	0	0	0	0	1	1	0	Illegal ME
0	0	0	0	0	1	1	1	5GS services not allowed
0	0	0	0	1	0	1	0	Implicitly de-registered
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	1	0	1	0	1	Synch failure
0	0	0	1	1	0	1	1	N1 mode not allowed
0	0	0	1	1	1	0	0	Restricted service area
0	0	1	0	1	0	1	1	LADN not available
0	1	0	0	0	0	1	1	Insufficient resources for specific slice and DNN
0	1	0	0	0	1	0	1	Insufficient resources for specific slice
0	1	0	1	1	0	1	0	Payload was not forwarded
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".								

9.10.3.3 5GS identity type

The purpose of the 5GS identity type information element is to specify which identity is requested.

The 5GS identity type is a type 1 information element.

The 5GS identity type information element is coded as shown in figure 9.10.3.3.1 and table 9.0.3.3.1.

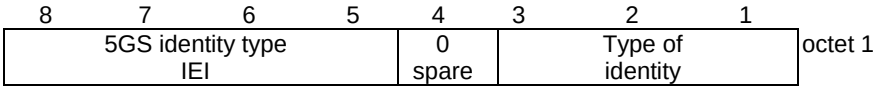


Figure 9.10.3.3.1: 5GS identity type information element

Table 9.10.3.3.1: 5GS identity type information element

Type of identity (octet 1)			
Bits			
3	**2**	**1**	
0	0	1	SUCI
1	1	0	5G-GUTI
0	1	1	IMEI
1	0	0	5G-S-TMSI
1	0	1	IMEISV
All other values are interpreted as SUCI by this version of the protocol.			

9.10.3.4 5GS mobile identity

The purpose of the 5GS mobile identity information element is to provide either the SUCI, the 5G-GUTI, the IMEI, the IMEISV or the 5G-S-TMSI.

The 5GS mobile identity information element is coded as shown in figures 9.10.3.4.1, 9.10.3.4.2, 9.10.3.4.3 and 9.10.3.4.4, and table 9.10.3.4.1.

The 5GS mobile identity is a type 4 information element with a minimum length of 3 octets and a maximum length of TBD octets.

Editor's note: The maximum length of 5GS mobile identity is TBD and will be updated based on CT4 specification.

8	7	6	5	4	3	2	1	
5GS mobile identity IEI								octet 1
Length of 5GS mobile identity contents								octet 2
1	1	1	1	odd/ even indic	Type of identity			octet 3
MCC digit 2				MCC digit 1				octet 4
MNC digit 3				MCC digit 3				octet 5
MNC digit 2				MNC digit 1				octet 6
AMF Region ID								octet 7
AMF Region ID (continued)								octet 8
AMF Set ID				AMF Pointer				octet 9
5G-TMSI								octet 10
5G-TMSI (continued)								octet 11
5G-TMSI (continued)								octet 12
5G-TMSI (continued)								octet 13

Figure 9.10.3.4.1: 5GS mobile identity information element for type of identity "5G-GUTI"

8	7	6	5	4	3	2	1	
5GS mobile identity IEI								octet 1
Length of 5GS mobile identity contents								octet 2
Identity digit 1				odd/ even indic	Type of identity			octet 3
Identity digit p+1				Identity digit p				octet 4*

Figure 9.10.3.4.2: 5GS mobile identity information element for type of identity "SUCI" or "IMEI" or "IMEISV"

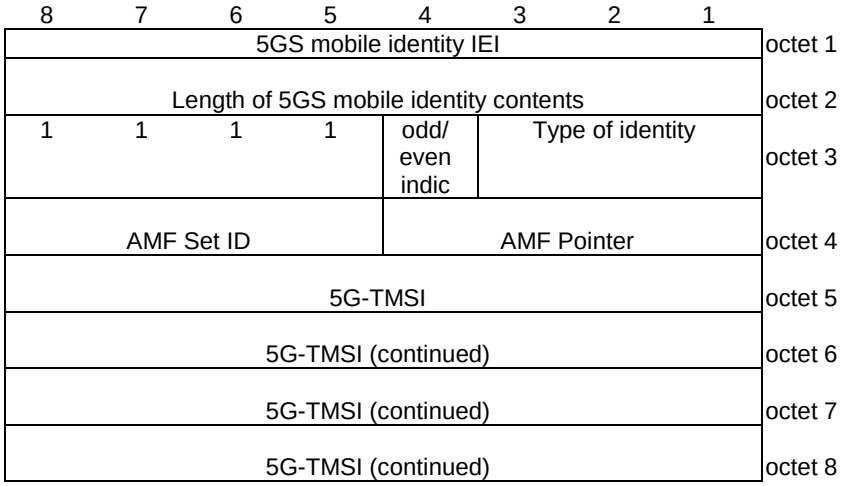


Figure 9.10.3.4.3: 5GS mobile identity information element for type of identity "5G-S-TMSI"

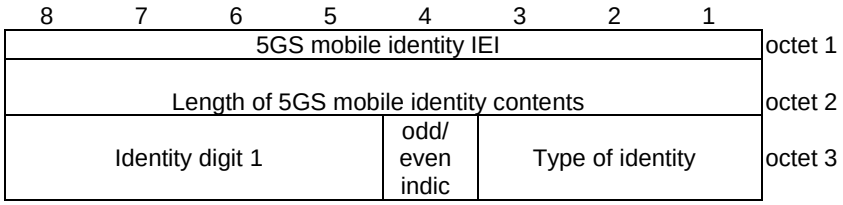


Figure 9.10.3.4.4: 5GS mobile identity information element for type of identity "No identity"

Table 9.10.3.4.1: 5GS mobile identity information element

Type of identity (octet 3)
Bits

3	2	1	
0	0	0	No identity (NOTE)
0	0	1	SUCI
1	1	0	5G-GUTI
0	1	1	IMEI
1	0	0	5G-S-TMSI
1	0	1	IMEISVI

All other values are reserved.

Odd/even indication (octet 3)
Bit

4	
0	even number of identity digits and also when the GUTI or 5G-TMSI is used
1	odd number of identity digits

Identity digits (octet 4 etc.)

For the SUCI, 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 5G-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 5G-GUTI are as defined in 3GPP TS 23.003 [4].

MCC, Mobile country code (octet 4, octet 5 bits 1 to 4)

The MCC field is coded as in ITU-T Recommendation E.212 [42], 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 [12].

For the IMEI, this field is coded using BCD coding. The format of the IMEI is described in 3GPP TS 23.003 [4].

For the IMEISV, this field is coded using BCD coding. Bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". The format of the IMEISV is described in 3GPP TS 23.003 [4].

For the 5G-S-TMSI, bits 5 to 8 of octet 3 are coded as "1111" and bit 8 of octet 4 is the most significant bit and bit 1 of the last octet is the least significant bit. The coding of the 5G-S-TMSI is left open for each administration.

For Type of identity "No identity", the identity digit bits shall be encoded with all 0s and the length of mobile identity contents parameter shall be set to 1.

NOTE: This can be used when the requested identity is not available at the UE during the identification procedure.

9.10.3.5 5GS network feature support

The purpose of the 5GS network feature support information element is to indicate whether certain features are supported by the network.

The 5GS network feature support information element is coded as shown in figure 9.10.3.5.1 and table 9.10.3.5.1.

The 5GS network feature support is a type 4 information element with a minimum length of 3 octets and a maximum length of 5 octets.

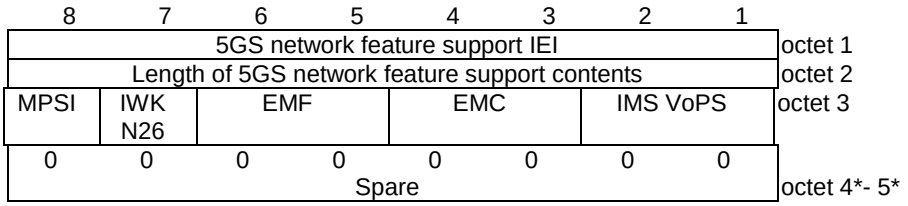


Figure 9.10.3.5.1: 5GS network feature support information element

Table 9.10.3.5.1: 5GS network feature support information element

IMS voice over PS session indicator (IMS VoPS) (octet 3, bit1 and bit 2)
This bit indicates the support of IMS voice via 5GS
Bit

2	**1**	
0	0	IMS voice over PS session not supported
0	1	IMS voice over PS session supported over 3GPP access
1	0	IMS voice over PS session supported over non-3GPP access
1	1	reserved

Emergency service support indicator (EMC) (octet 3, bit 3 and bit 4)
This bit indicates the support of emergency services in 5GS
Bit

4	**3**	
0	0	Emergency services not supported
0	1	Emergency services supported in NR connected to 5GCN only
1	0	Emergency services supported in E-UTRA connected to 5GCN only
1	1	Emergency services supported in NR connected to 5GCN and E-UTRA connected to 5GCN

Emergency service fallback indicator (EMF) (octet 3, bit 5 and bit 6)
This bit indicates the support of emergency services fallback
Bit

6	**5**	
0	0	Emergency services fallback not supported
0	1	Emergency services fallback supported in NR connected to 5GCN only
1	0	Emergency services fallback supported in E-UTRA connected to 5GCN only
1	1	Emergency services fallback supported in NR connected to 5GCN and E-UTRA connected to 5GCN

Interworking without N26 interface indicator (IWK N26) (octet 3, bit 6)
This bit indicates whether the network supports interworking procedure without N26 interface
Bit

7	
0	Interworking without N26 not supported
1	Interworking without N26 supported

MPS indicator (MPSI) (octet 3, bit 7)
This bit indicates the support of MPS in the RPLMN or equivalent PLMN.
Bit

0	Access identity 1 not valid in RPLMN or equivalent PLMN
1	Access identity 1 valid in RPLMN or equivalent PLMN

All bits in octets 4 to 5 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.10.3.6 5GS registration result

The purpose of the 5GS registration result information element is to specify the result of a registration procedure.

The 5GS registration result information element is coded as shown in figure 9.10.3.6.1 and table 9.10.3.6.1.

The 5GS registration result is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
5GS registration result IEI								octet 1
Length of 5GS registration result contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	SMS allowed	5GS registration result value			octet 3

Figure 9.10.3.6.1: 5GS registration result information element

Table 9.10.3.6.1: 5GS registration result information element

5GS registration result value (octet 3, bits 1 to 3) Bits **3 2 1** 0 0 1 3GPP access 0 1 0 Non-3GPP access 0 1 1 3GPP access and non-3GPP access 1 1 1 reserved All other values are unused and shall be treated as "3GPP access", if received by the UE. SMS over NAS transport allowed (SMS allowed) (octet 3, bit 4) Bit **4** 0 SMS over NAS not allowed 1 SMS over NAS allowed Bits 5 to 8 of octet 3 are spare and shall be coded as zero.

9.10.3.7 5GS registration type

The purpose of the 5GS registration type information element is to indicate the type of the requested registration.

The 5GS registration type information element is coded as shown in figure 9.10.3.7.1 and table 9.10.3.7.1.

The 5GS registration type is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
5GS registration type IEI								octet 1
Length of 5GS registration type contents								octet 2
0 Spare	0 Spare	0 Spare	FOR	SMS requested	5GS registration type value			octet 3

Figure 9.10.3.7.1: 5GS registration type information element

Table 9.10.3.7.1: 5GS registration type information element

5GS registration type value (octet 3, bits 1 to 3) Bits **3 2 1** 0 0 1 initial registration 0 1 0 mobility registration updating 0 1 1 periodic registration updating 1 0 0 emergency registration 1 1 1 reserved All other values are unused and shall be interpreted as "initial registration", if received by the network.
SMS over NAS transport requested (SMS requested) (octet 3, bit 4) Bit **4** 0 SMS over NAS not supported 1 SMS over NAS supported
Follow-on request bit (FOR) (octet 3, bit 5) Bit **5** 0 No follow-on request pending 1 Follow-on request pending Bits 6 to 8 of octet 3 are spare and shall be coded as zero.

9.10.3.8 5GS tracking area identity

The purpose of the 5GS tracking area identity information element is to provide an unambiguous identification of tracking areas within the area covered by the 5GS.

The 5GS tracking area identity information element is coded as shown in figure 9.10.3.8.1 and table 9.10.3.8.1.

The 5GS tracking area identity is a type 3 information element with a length of 7 octets.

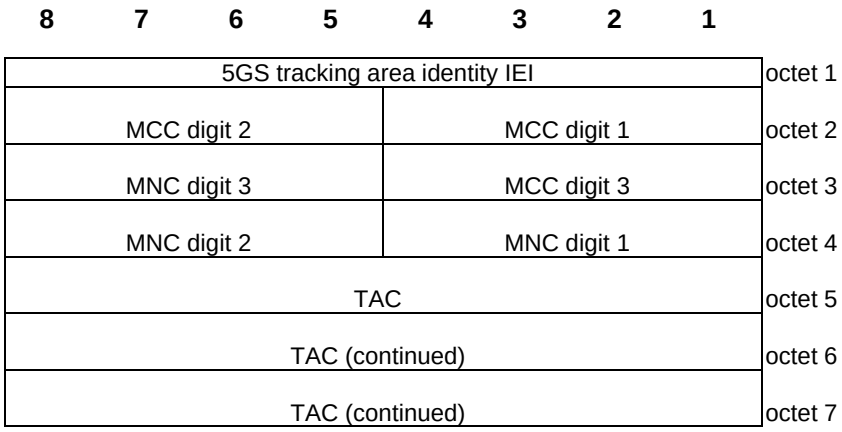


Figure 9.10.3.8.1: 5GS tracking area identity information element

Table 9.10.3.8.1: 5GS tracking area identity information element

MCC, Mobile country code (octets 2 and 3)
The MCC field is coded as in ITU-T Rec. E212 [39], 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 (octets 5 to 7)
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 3 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.

9.10.3.9 5GS tracking area identity list

The purpose of the 5GS 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 "00" and "01" allow a more compact encoding, when the different TAIs are sharing the PLMN identity.

The 5GS tracking area identity list information element is coded as shown in figure 9.10.3.8.1, figure 9.10.3.8.2, figure 9.10.3.9.3, figure 9.10.3.9.4 and table 9.10.3.9.1.

The 5GS tracking area identity list is a type 4 information element, with a minimum length of 9 octets and a maximum length of 114 octets. The list can contain a maximum of 16 different tracking area identities.

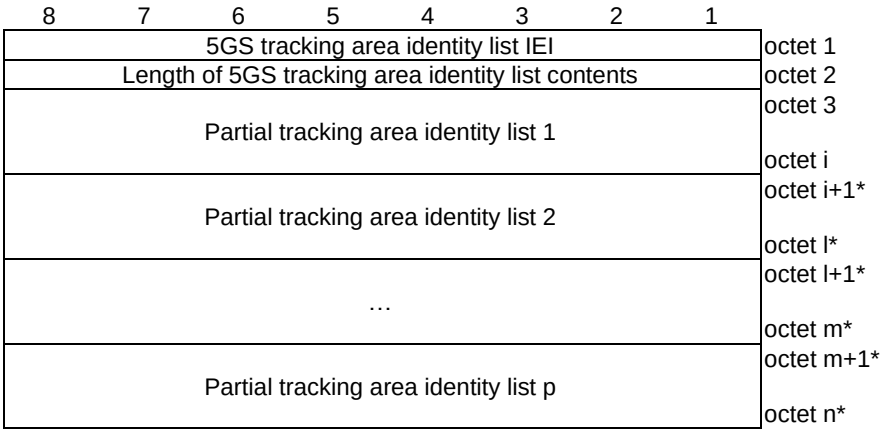


Figure 9.10.3.9.1: 5GS tracking area identity list information element

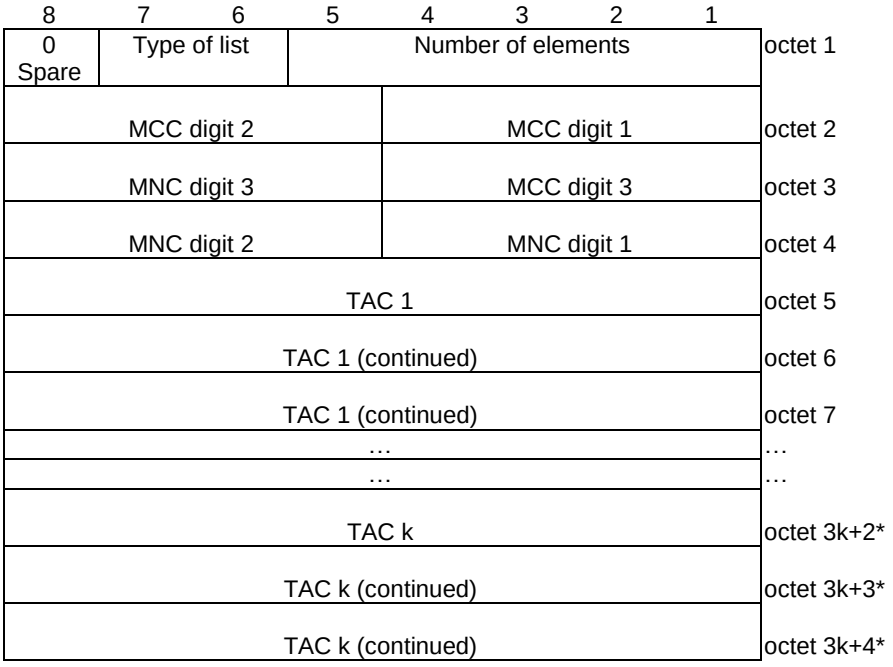


Figure 9.10.3.9.2: Partial tracking area identity list – type of list = "00"

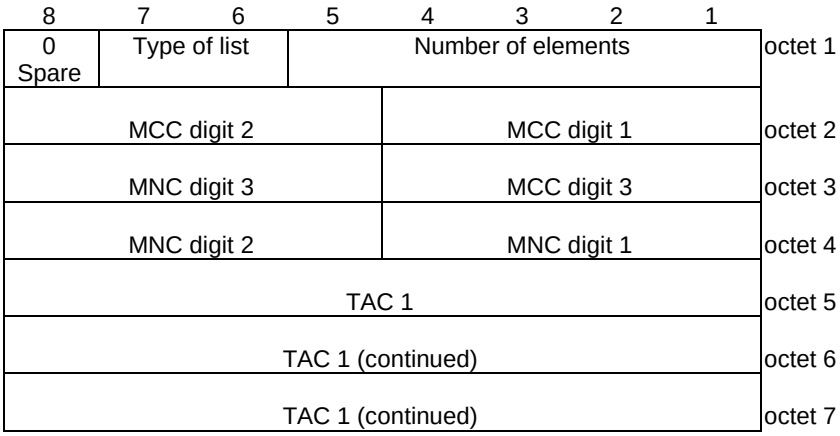


Figure 9.10.3.9.3: Partial tracking area identity list – type of list = "01"

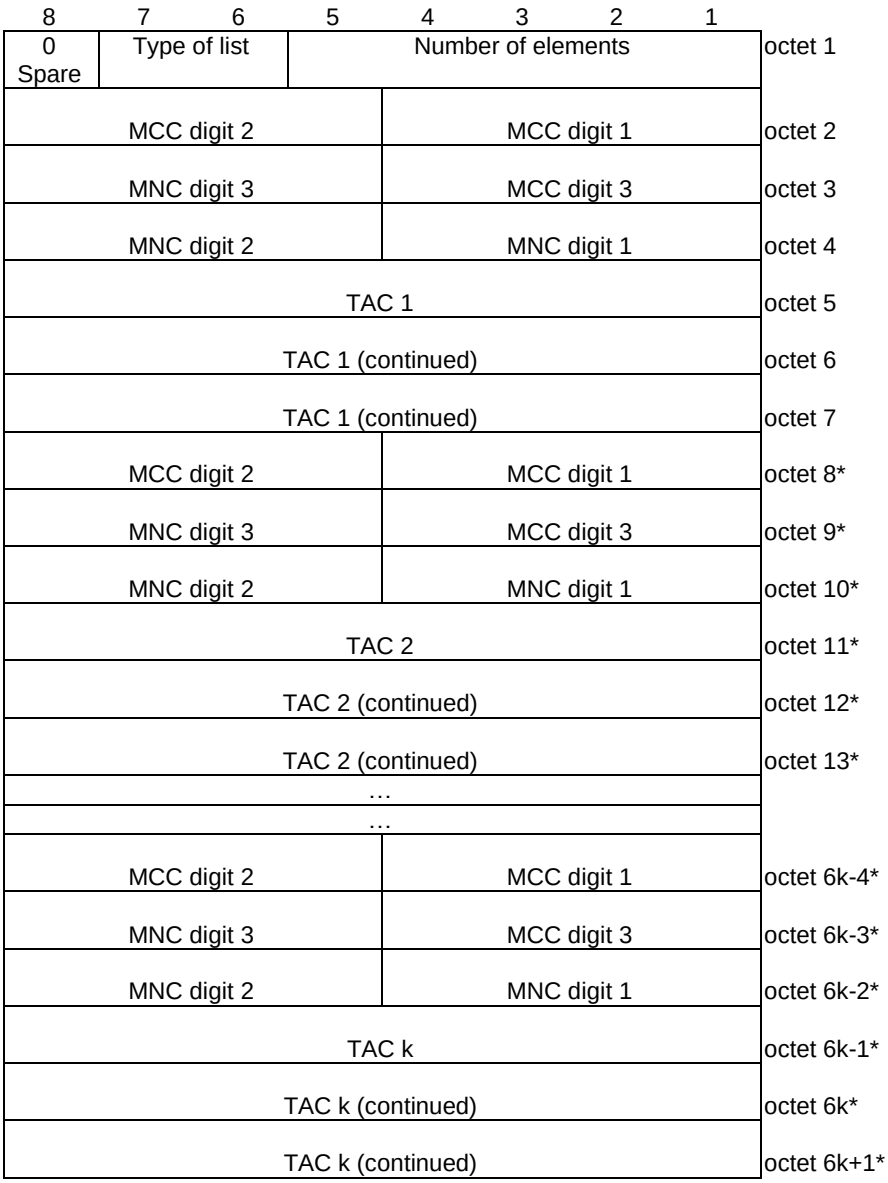


Figure 9.10.3.9.4: Partial tracking area identity list – type of list = "10"

Table 9.10.3.9.1: Tracking area identity list information element

Value part of the Tracking area identity list information element (octets 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 (see NOTE)

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 = "00" and number of elements = k:

octet 2 to 4 contain the MCC+MNC, and
for j = 1, …, k:
octets 3j+2 to 3j+4 contain the TAC of the j-th TAI belonging to the partial list,

For type of list = "01" and number of elements = k:

octet 2 to 4 contain the MCC+MNC, and
octets 5 to 7 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 = "10" and number of elements = k:

for j = 1, …, k.
octets 6j-4 to 6j-2 contain the MCC+MNC, and
octets 6j-1 to 6j+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 [42], 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 third 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 3 octets.
NOTE: If the "list of TAIs belonging to different PLMNs" is used, the PLMNs included in the list need to be present in the list of "equivalent PLMNs".

9.10.3.10 Access type

The purpose of the access type information element is to indicate the access type over which the downlink signalling or user data is pending to be sent to the UE.

The access type is a type 1 information element.

The access type information element is coded as shown in figure 9.10.3.10.1 and table 9.10.3.10.1.

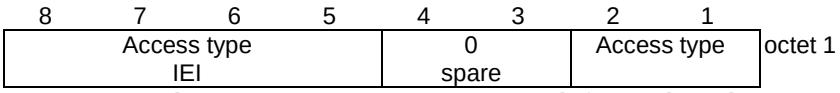


Figure 9.10.3.10.1: Access type information element

Table 9.10.3.10.1: Access type information element

Access type value (octet 1, bit 1 to bit 2) Bits **2 1** 0 1 3GPP access 1 0 Non-3GPP access All other values are reserved.

9.10.3.11 Allowed PDU session status

The purpose of the Allowed PDU session status information element is to indicate to the network user-plane resources of PDU sessions associated with non-3GPP access that are allowed to be re-established over 3GPP access or if there is no PDU session(s) for which the UE allows the user-plane resources to be re-established over 3GPP access..

The Allowed PDU session status information element is coded as shown in figure 9.10.3.11.1 and table 9.10.3.11.1.

The Allowed PDU session status is a type 4 information element with minimum length of 4 octets and maximum length of 34 octets.

8	7	6	5	4	3	2	1	
Allowed PDU session status IEI								octet 1
Length of Allowed PDU session status contents								octet 2
PSI (7)	PSI (6)	PSI (5)	PSI (4)	PSI (3)	PSI (2)	PSI (1)	PSI (0)	octet 3
PSI (15)	PSI (14)	PSI (13)	PSI (12)	PSI (11)	PSI (10)	PSI (9)	PSI (8)	octet 4
0	0	0	0	0	0	0	0	
Spare								octet 5* -34*

Figure 9.10.3.11.1: Allowed PDU session status information element

Table 9.10.3.11.1: Allowed PDU session status information element

PSI(x) shall be coded as follows: PSI(0): Bit 1octet 3 is spare and shall be coded as zero. PSI(1) – PSI(15): 0 indicates that the user-plane resources of corresponding PDU session is not allowed to be re-established over 3GPP access. 1 indicates that the user-plane resources of corresponding PDU session can be re-established over 3GPP access. If there is no PDU session that can be re-established over 3GPP access, all bits in PSI(5) – PSI(15) shall be coded as zero. All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.10.3.12 Authentication failure parameter

See subclause 10.5.3.2.2 in 3GPP TS 24.008 [12].

9.10.3.13 Authentication parameter AUTN

See subclause 10.5.3.1.1 in 3GPP TS 24.008 [12].

Editor's note: The format of the Authentication parameter AUTN IE in 3GPP TS 24.008 [12] is TLV with a length of 18 octets.

9.10.3.14 Authentication parameter RAND

See subclause 10.5.3.1 in 3GPP TS 24.008 [12].

Editor's note: The format of the Authentication parameter RAND IE in 3GPP TS 24.008 [12] is TV with a length of 17 octets.

9.10.3.15 Authentication response parameter

See subclause 9.9.3.4 in 3GPP TS 24.301 [15].

9.10.3.16 Configuration update indication

The purpose of the Configuration update indication information element is to indicate the additional information associated with the generic UE configuration update procedure.

The Configuration update indication information element is coded as shown in figure 9.10.3.16.1 and table 9.10.3.16.1.

The Configuration update indication is a type 1 information element.

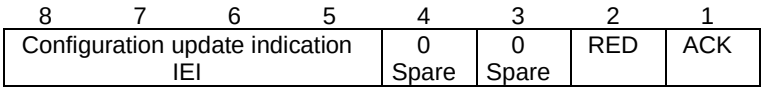


Figure 9.10.3.16.1: Configuration update indication

Table 9.10.3.16.1: Configuration update indication

Acknowledgement (ACK) value (octet 1, bit 1) Bit **1** 0 acknowledgement not requested 1 acknowledgement requested Registration requested (RED) value (octet 1, bit 2) Bit **2** 0 registration not requested 1 registration requested Bits 3 and 4 are spare and shall be coded as zero,

9.10.3.17 Daylight saving time

See subclause 10.5.3.12 in 3GPP TS 24.008 [12].

9.10.3.18 De-registration type

The purpose of the De-registration type information element is to indicate the type of de-registration.

The De-registration type information element is coded as shown in figure 9.10.3.18.1 and table 9.10.3.18.1.

The De-registration type is a type 1 information element.

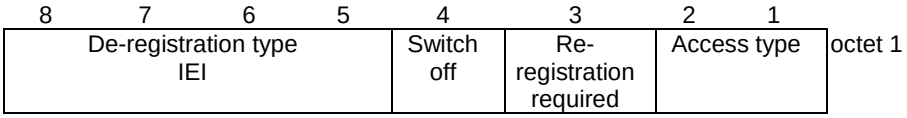


Figure 9.10.3.18.1: Deregistration type information element

Table 9.10.3.18.1: Deregistration type information element

Switch off (octet 1, bit 4) In the UE to network direction: Bit **4** 0 Normal de-registration 1 Switch off In the network to UE direction bit 4 is spare. The network shall set this bit to zero. Re-registration required (octet 1, bit 3) In the network to UE direction: Bit **3** 0 re-registration not required 1 re-registration required In the UE to network direction bit 3 is spare. The UE shall set this bit to zero. Access type (octet 1,bit 2, bit 1) Bit **2 1** 0 1 3GPP access 1 0 Non-3GPP access 1 1 3GPP access and non-3GPP access All other values are reserved.

9.10.3.19 DNN

The purpose of the DNN information element is to identify the data network.

The DNN information element is coded as shown in figure 9.10.3.19.1.

The DNN is a type 4 information element with a minimum length of 3 octets and a maximum length of 102 octets.

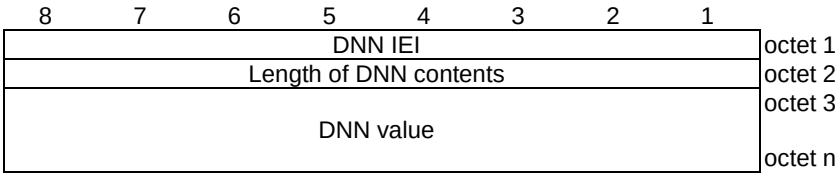


Figure 9.10.3.19.1: DNN information element

A DNN value field contains an APN as defined in 3GPP TS 23.003 [4].

9.10.3.20 DRX parameters

Editor's note: The DRX parameters need to be defined by RAN WGs.

9.10.3.21 Emergency number list

See subclause 10.5.3.13 in 3GPP TS 24.008 [12].

9.10.3.22 EPS NAS message container

The purpose of the EPS NAS message container information element is to transport an EPS NAS message as specified in 3GPP TS 24.301 [15].

The EPS NAS message container information element is coded as shown in figure 9.10.3.22.1 and table 9.10.3.22.1.

The EPS NAS message container is a type 6 information element.

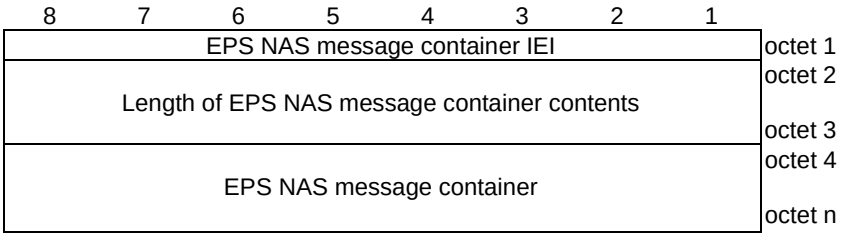


Figure 9.10.3.22.1: EPS NAS message container information element

Table 9.10.3.22.1: EPS NAS message container information element

EPS NAS message container (octet 4 to n) An EPS NAS message as specified in 3GPP TS 24.301 [15].

9.10.3.23 EPS NAS security algorithms

See subclause 9.9.3.23 in 3GPP TS 24.301 [15].

9.10.3.24 Extended emergency number list

See subclause 9.9.3.37A in 3GPP TS 24.301 [15].

9.10.3.25 $Hash_{AMF}$

The purpose of the $Hash_{AMF}$ information element is to transfer a 64-bit hash value to the UE so the UE can check the AMF calculated value against the value locally calculated by the UE to determine whether the REGISTRATION REQUEST message sent by the UE has been modified.

The $Hash_{AMF}$ information element is coded as shown in figure 9.10.3.25.1 and table 9.10.3.25.1.

The $Hash_{AMF}$ is a type 3 information element with a length of 9 octets.

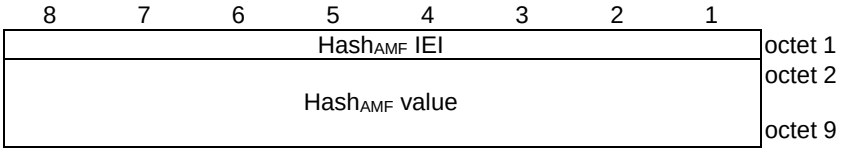


Figure 9.10.3.25.1: $Hash_{AMF}$ information element

Table 9.10.3.25.1: $Hash_{AMF}$ information element

$Hash_{AMF}$ value (octet 2 to 9) This field contains the binary representation of the $Hash_{AMF}$. Bit 8 of octet 2 represents the most significant bit of the $Hash_{AMF}$ and bit 1 of octet 9 the least significant bit.

9.10.3.26 IMEISV request

See subclause 10.5.5.10 in 3GPP TS 24.008 [12].

9.10.3.27 LADN information

The purpose of the LADN information information element is to provide the UE the LADN service area for each available LADN in the current registration area or to delete the LADN information at the UE.

The LADN information information element is coded as shown in figure 9.10.3.27.1, figure 9.10.3.27.2 and table 9.10.3.27.1.

The LADN information is a type 6 information element with a minimum length of 3 octets and a maximum length of 1707 octets.

The LADN information information element can contain a minimum of 0 and a maximum of 8 different LADNs each including a DNN and a tracking area identity lists.

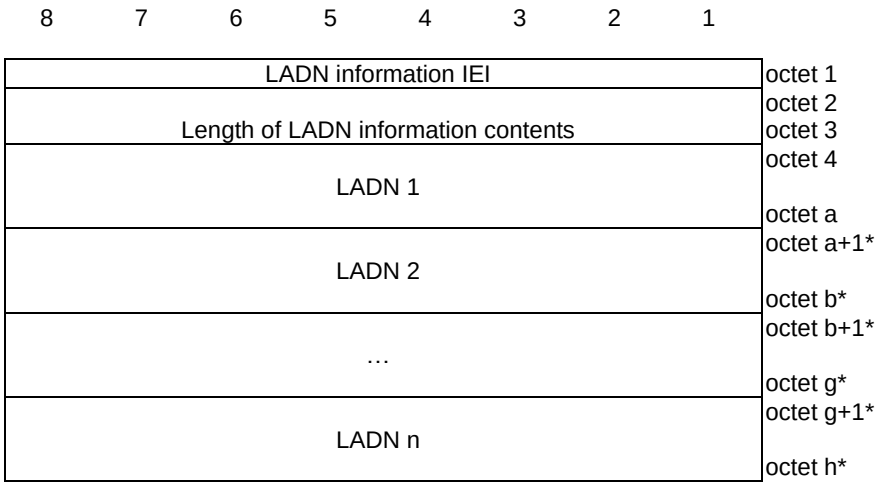


Figure 9.10.3.27.1: LADN information information element

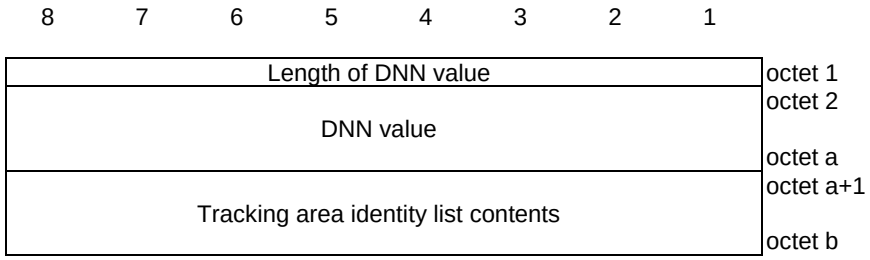


Figure 9.10.3.27.2: LADN

Table 9.10.3.27.1: LADN information information element

Value part of the LADN information information element (octet 3 to h) The value part of the LADN information information element consists of one or several LADNs. Each LADN consists one DNN value and one Tracking area identity list contents. The length of each LADN is determined by the length of DNN value and the length of Tracking area identity list contents. The UE shall store the complete list received. If more than 8 LADNs are included in this information element, the UE shall store the first 8 LADNs and ignore the remaining octets of the information element. LADN (octet 4 to octet a): DNN value is coded as DNN value part of DNN information element as specified in subclause 9.8.3.15 starting with the third octet. Tracking area identity list contents (octet a+1 to octet b): Tracking area identity list contents is coded as the value part of the Tracking area identity list information element as specified in subclause 9.8.3.8 starting with the third octet.

9.10.3.28 MICO indication

The purpose of the MICO indication information element is to indicate the use of MICO mode or the re-negotiation of MICO mode.

The MICO indication information element is coded as shown in figure 9.10.3.28.1 and table 9.10.3.28.1.

The MICO indication is a type 1 information element.

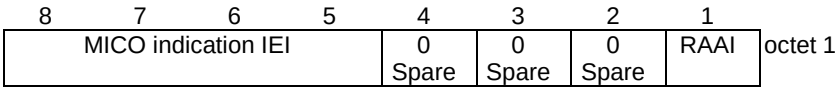


Figure 9.10.3.28.1: MICO indication

Table 9.10.3.28.1: MICO indication

Registration Area Allocation Indication (RAAI) (octet 1) In the network to UE direction: Bit **1** 0 all PLMN registration area not allocated 1 all PLMN registration area allocated In the UE to network direction bit 1 is spare. The UE shall set this bit to zero. Bits 2, 3 and 4 are spare and shall be coded as zero,

9.10.3.29 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 9.10.3.29.1 and table 9.10.3.29.1.

The NAS key set identifier is a type 1 information element.

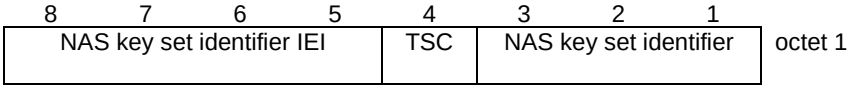


Figure 9.10.3.29.1: NAS key set identifier information element

Table 9.10.3.29.1: NAS key set identifier information element

Type of security context flag (TSC) (octet 1) Bit **4** 0 1 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 1 1 0 1 1 1	native security context (for KSI_{AMF}) mapped security context (for KSI_{ASME}) possible values for the NAS key set identifier no key is available (UE to network); reserved (network to UE)

9.10.3.30 NAS message

This IE includes a complete plain 5GS NAS message as specified in subclause 8.2. The SECURITY PROTECTED 5GS NAS MESSAGE message is not a plain 5GS NAS message and shall not be included in this IE.

9.10.3.31 NAS message container

The purpose of the NAS message container IE is to encapsulate a NAS message without NAS security header.

The NAS message container information element is coded as shown in figure 9.10.3.31.1 and table 9.10.3.31.1.

The NAS message container is a type 6 information element.

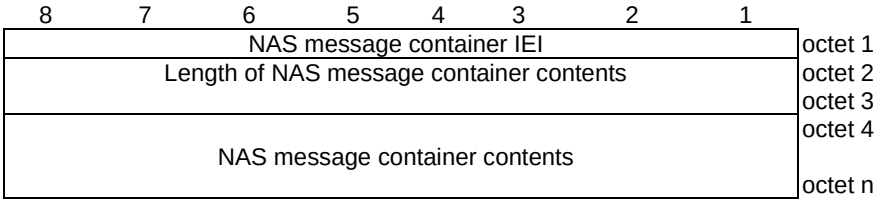


Figure 9.10.3.31.1: NAS message container information element

Table 9.10.3.31.1: NAS message container information element

NAS message container contents (octet 4 to octet n); Max value of 65535 octets This IE can contain a REGISTRATION REQUEST message as defined in subclause 5.5.1, or a SERVICE REQUEST message as defined in subclause 5.6.1.

9.10.3.32 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 9.10.3.32.1 and table 9.10.3.32.1.

The NAS security algorithms is a type 3 information element with a length of 2 octets.

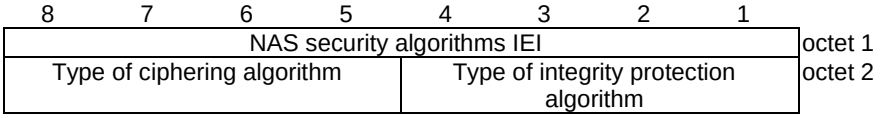


Figure 9.10.3.32.1: NAS security algorithms information element

Table 9.10.3.32.1: NAS security algorithms information element

Type of integrity protection algorithm (octet 2, bit 1 to 3)
Bits

4	3	2	1	
0	0	0	0	5GS integrity algorithm 5G-IA0 (null integrity protection algorithm)
0	0	0	1	5GS integrity algorithm 128-5G-IA1
0	0	1	0	5GS integrity algorithm 128-5G-IA2
0	0	1	1	5GS integrity algorithm 128-5G-IA3
0	1	0	0	5GS integrity algorithm 5G-IA4
0	1	0	1	5GS integrity algorithm 5G-IA5
0	1	1	0	5GS integrity algorithm 5G-IA6
0	1	1	1	5GS integrity algorithm 5G-IA7

All other values are reserved.

Type of ciphering algorithm (octet 2, bit 5 to 7)
Bits

8	7	6	5	
0	0	0	0	5GS encryption algorithm 5G-EA0 (null ciphering algorithm)
0	0	0	1	5GS encryption algorithm 128-5G-EA1
0	0	1	0	5GS encryption algorithm 128-5G-EA2
0	0	1	1	5GS encryption algorithm 128-5G-EA3
0	1	0	0	5GS encryption algorithm 5G-EA4
0	1	0	1	5GS encryption algorithm 5G-EA5
0	1	1	0	5GS encryption algorithm 5G-EA6
0	1	1	1	5GS encryption algorithm 5G-EA7

All other values are reserved.

9.10.3.33 Network name

See subclause 10.5.3.5a in 3GPP TS 24.008 [12].

9.10.3.34 NSSAI

The purpose of the NSSAI information element is to identify a collection of S-NSSAIs

The NSSAI information element is coded as shown in figure 9.10.3.34.1 and table 9.10.3.34.1.

The NSSAI is a type 4 information element with a minimum length of 4 octets and a maximum length of 146 octets.

NOTE 1: The number of S-NSSAI values in a requested NSSAI or allowed NSSAI cannot exceed eight.

NOTE 2: The number of S-NSSAI values in a configured NSSAI cannot exceed sixteen.

NOTE 3: An NSSAI can include more than one S-NSSAIs with same SST values, and optionally same SD values, which are associated with different mapped SST values and optionally mapped SD values.

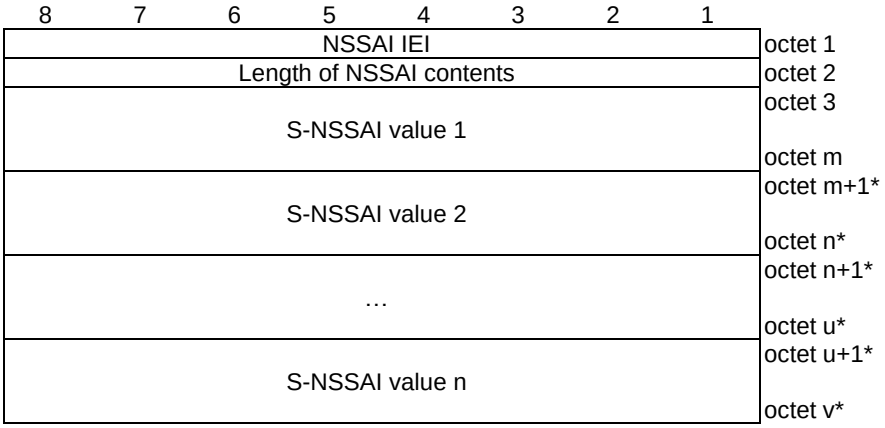


Figure 9.10.3.34.1: NSSAI information element

Table 9.10.3.34.1: NSSAI information element

Value part of the NSSAI information element (octet 3 to v) The value part of the NSSAI information element consists of one or more S-NSSAI values. Each S-NSSAI value consists of one S-NSSAI and optionally one mapped configured S-NSSAI from the configured NSSAI for the HPLMN. If the recipient of this information element is the UE, the UE shall store the complete list received. If the NSSAI information element conveys an allowed NSSAI and more than 8 S-NSSAI values are included in this information element, the UE shall store the first 8 S-NSSAI values and ignore the remaining octets of the information element. If the NSSAI information element conveys a configured NSSAI and more than 16 S-NSSAI values are included in this information element, the UE shall store the first 16 S-NSSAI values and ignore the remaining octets of the information element. S-NSSAI value: S-NSSAI value is coded as the length and value part of S-NSSAI information element as specified in subclause 9.8.2.6 starting with the second octet.

9.10.3.35 Payload container

The purpose of the Payload container information element is to transport a payload.

The Payload container information element is coded as shown in figure 9.10.3.35.1 and table 9.10.3.35.1.

The Payload container is a type 6 information element with a minimum length of 4 octets and a maximum length of 65538 octets.

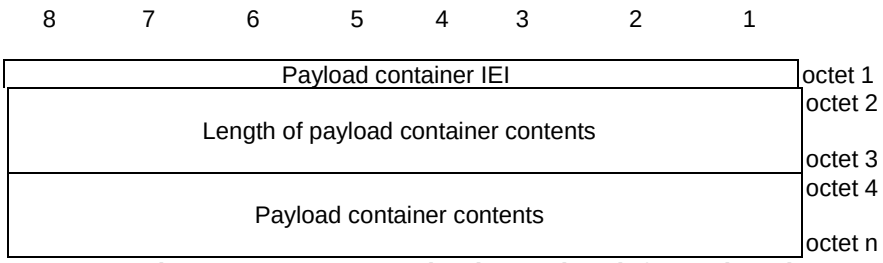


Figure 9.10.3.35.1: Payload container information element

Table 9.10.3.35.1: Payload container information element

Payload container contents (octet 4 to octet n); max value of 65535 octets The coding of Payload container contents is dependent on the particular application.

9.10.3.36 Payload container type

The purpose of the Payload container type information element indicates type of payload included in the payload container information element.

The Payload container information element is coded as shown in figure 9.10.3.36.1 and table 9.10.3.36.1.

The Payload container is a type 1 information element with a length of half octet.

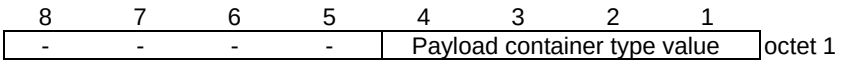


Figure 9.10.3.36.1: Payload container information element

Table 9.10.3.36.1: Payload container information element

Payload container type value (octet 1, bit 1 to bit 4)
Bits
4 3 2 1
0 0 0 1 N1 SM information
0 0 1 0 SMS
0 0 1 1 LTE Positioning Protocol (LPP) message container
0 1 0 0 Transparent container
0 1 0 1 UE policy container
All other values are reserved.

9.10.3.37 PDU session identity 2

The purpose of the PDU session identity 2 information element is to indicate the identity of a PDU session in a 5GMM message.

The PDU session identity 2 information element is coded as shown in figure 9.10.3.37.1 and table 9.10.3.37.1.

The PDU session identity 2 is a type 3 information element with a length of 2 octets .

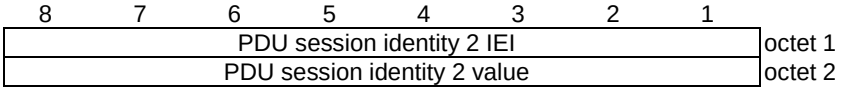


Figure 9.10.3.37.1: PDU session identity 2 information element

Table 9.10.3.37.1: PDU session identity 2 information element

PDU session identity 2 value (octet 2)
The coding of the DU session identity 2 value is identical to the coding of the PDU session identity value as defined in 3GPP TS 24.007 [11] .

9.10.3.38 PDU session reactivation result

The purpose of the PDU session reactivation result information element is to indicate the result of PDU sessions user-plane resource activation.

The PDU session reactivation result information element is coded as shown in figure 9.10.3.38.1 and table 9.10.3.38.1.

The PDU session reactivation result is a type 4 information element with minimum length of 4 octets and maximum length of 34 octets.

8	7	6	5	4	3	2	1	
PDU session reactivation result IEI								octet 1
Length of PDU session reactivation result								octet 2
PSI (7)	PSI (6)	PSI (5)	PSI (4)	PSI (3)	PSI (2)	PSI (1)	PSI (0)	octet 3
PSI (15)	PSI (14)	PSI (13)	PSI (12)	PSI (11)	PSI (10)	PSI (9)	PSI (8)	octet 4
0	0	0	0	0	0	0	0	octet 5* -34*
Spare								

Figure 9.10.3.38.1: PDU session reactivation result information element

Table 9.10.3.38.1: PDU session reactivation result information element

PSI(x) shall be coded as follows: PSI(0): Bit 0 of octet 3 is spare and shall be coded as zero. PSI(1) – PSI(15): 0 indicates PDU session user-plane resource reactivation was not requested in the Uplink data status IE or was not allowed to be reactivated in the Allowed PDU session status IE or user-plane resource reactivation is successful. 1 indicates either PDU session reactivation was requested in the Uplink data status IE but user-plane resource reactivation is not successful or indicates PDU session was allowed to be reactivated in the Allowed PDU session status IE but user-plane resource reactivation is either not performed or not successful. All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.10.3.39 PDU session reactivation result error cause

The purpose of the PDU session reactivation result error cause information element is to indicate error causes for PDU session ID(s) where there was a failure to activate the user-plane resources.

The PDU session reactivation result error cause information element is coded as shown in figure 9.10.3.39.1 and table 9.10.3.39.1.

The PDU session reactivation result error cause is a type 6 information element with a minimum length of 5 octets and a maximum length of 515 octets.

8	7	6	5	4	3	2	1	
PDU session reactivation result error cause IEI								octet 1
Length of PDU session reactivation result error cause								octet 2 octet 3
PDU session ID								octet 4
cause value								octet 5
….								
PDU session ID								octet 514*
cause value								octet 515*

Figure 9.10.3.39.1: PDU session reactivation result error cause information element

Table 9.10.3.39.1: PDU session reactivation result error cause information element

PDU session ID is coded same as PDU session ID IE (see subclause 9.4). The cause value is coded same as second octet of 5GMM cause information element (see subclause 9.10.3.2).

9.10.3.40 PDU session status

The purpose of the PDU session status information element is to indicate the state of each PDU session that can be identified by a PDU session identity.

The PDU session status information element is coded as shown in figure 9.10.3.40.1 and table 9.10.3.40.1.

The PDU session status information element is a type 4 information element with minimum length of 4 octets and a maximum length of 34 octets.

8	7	6	5	4	3	2	1	
PDU session status IEI								octet 1
Length of PDU session status contents								octet 2
PSI (7)	PSI (6)	PSI (5)	PSI (4)	PSI (3)	PSI (2)	PSI (1)	PSI (0)	octet 3
PSI (15)	PSI (14)	PSI (13)	PSI (12)	PSI (11)	PSI (10)	PSI (9)	PSI (8)	octet 4
0	0	0	0	0	0	0	0	octet 5*-34*
spare								

Figure 9.10.3.40.1: PDU session status information element

Table 9.10.3.40.1: PDU session status information element

PSI(x) shall be coded as follows: PSI(0): Bit 1 of octet 3 is spare and shall be coded as zero. PSI(1) – PSI(15): 0 indicates that the 5GSM state of the corresponding PDU session is PDU SESSION INACTIVE. 1 indicates that the 5GSM state of the corresponding PDU session is not PDU SESSION INACTIVE All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.10.3.41 PLMN list

See subclause 10.5.1.13 in 3GPP TS 24.008 [12].

9.10.3.42 Rejected NSSAI

The purpose of the Rejected NSSAI information element is to identify a collection of rejected S-NSSAIs

The Rejected NSSAI information element is coded as shown in figure 9.10.3.42.1, figure 9.10.3.42.2 and table 9.10.3.42.1.

The Rejected NSSAI is a type 4 information element with a minimum length of 4 octets and a maximum length of 42 octets.

NOTE: The number of rejected S-NSSAI(s) cannot exceed eight.

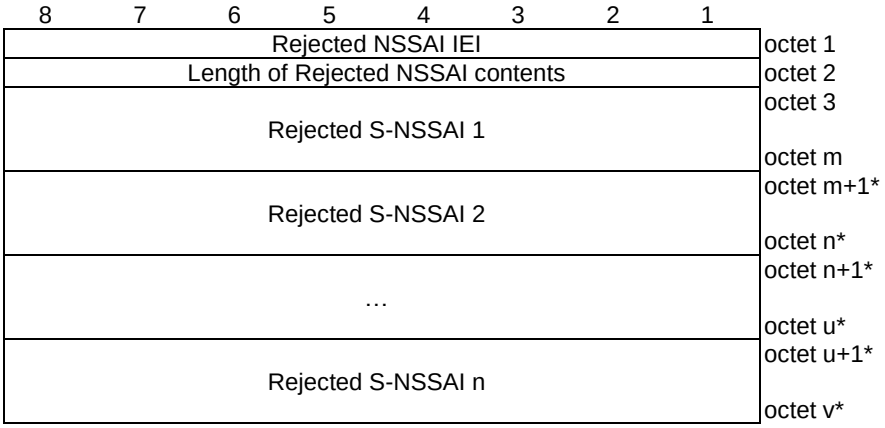


Figure 9.10.3.42.1: Rejected NSSAI information element

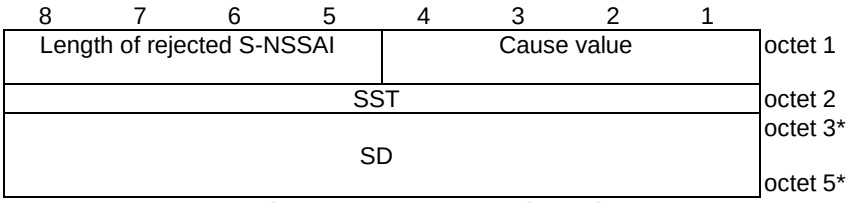


Figure 9.10.3.42.2: Rejected S-NSSAI

Table 9.10.3.42.1: Rejected NSSAI information element

Value part of the Rejected NSSAI information element (octet 3 to v)
The value part of the Rejected NSSAI information element consists of one or more rejected S-NSSAIs. Each rejected S-NSSAI consists of one S-NSSAI and an associated cause value. The length of each rejected S-NSSAI can be determined by the 'length of rejected S-NSSAI' field in the first octet of the rejected S-NSSAI.
The UE shall store the complete list received. If more than 8 rejected S-NSSAIs are included in this information element, the UE shall store the first 8 rejected S-NSSAIs and ignore the remaining octets of the information element.

Rejected S-NSSAI:

Cause value (octet 1)

Bits				
4	**3**	**2**	**1**	
0	0	0	0	S-NSSAI not available in the current PLMN
0	0	0	1	S-NSSAI not available in the current registration area

All other values are reserved.

Slice/service type (SST) (octet 2)

This field contains the 8 bit SST value. The coding of the SST value part is defined in 3GPP TS 23.003 [4].

Slice differentiator (SD) (octet 3 to octet 5)

This field contains the 24 bit SD value. The coding of the SD value part is defined in 3GPP TS 23.003 [4].

NOTE: If octet 3 is included, then octet 4 and octet 5 shall be included.

9.10.3.43 Request type

The purpose of the Request type information element is to indicate type of the PDU session establishment.

The Request type information element is coded as shown in figure 9.10.3.43.1 and table 9.10.3.43.1.

The Request type is a type 1 information element.

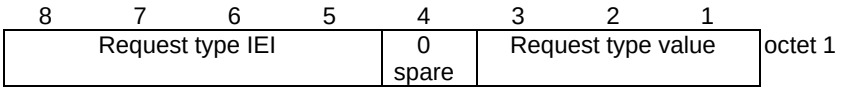


Figure 9.10.3.43.1: Request type information element

Table 9.10.3.43.1: Request type information element

Request type value (octet 1, bit 1 to bit 4) Bits **3 2 1** 0 0 1 initial request 0 1 0 existing PDU session 0 1 1 initial emergency request 1 0 0 existing emergency PDU session 1 1 1 reserved All other values are unused and shall be interpreted as "initial request", if received by the network.

9.10.3.44 S1 UE network capability

See subclause 9.9.3.34 in 3GPP TS 24.301 [15].

9.10.3.45 Service area list

The purpose of the Service area list information element is to transfer a list of allowed tracking areas for an allowed area or a list of non-allowed tracking areas for a non-allowed area from the network to the UE.

The coding of the information element allows combining different types of lists. The lists of type "00" and "01" allow a more compact encoding, when the different TAIs are sharing the PLMN identity. The lists of type "11" indicate all TAIs in the PLMN are allowed area.

The Service area list information element is coded as shown in figure 9.10.3.45.1, figure 9.10.3.45.2, figure 9.10.3.45.3, figure 9.10.3.45.4, figure 9.10.3.45.5 and table 9.10.3.45.1.

The Service area list is a type 4 information element with a minimum length of 6 octets and a maximum length of 114 octets. The list can contain a maximum of 16 different tracking area identities.

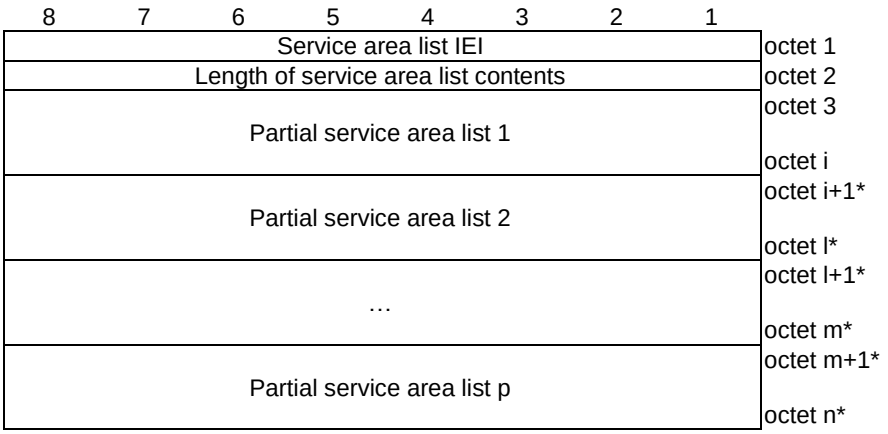


Figure 9.10.3.45.1: Service area list information element

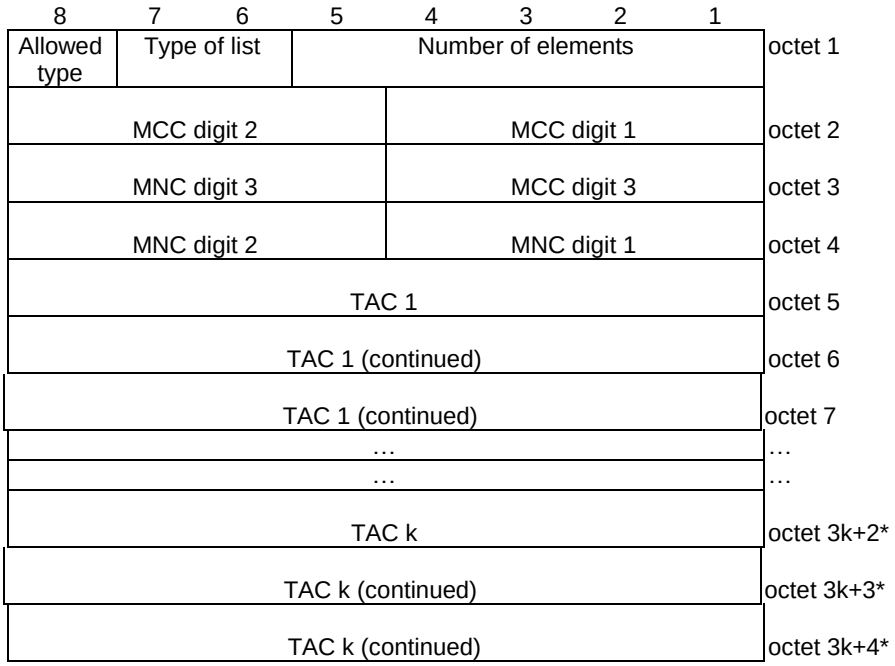


Figure 9.10.3.45.2: Partial service area list – type of list = "00"

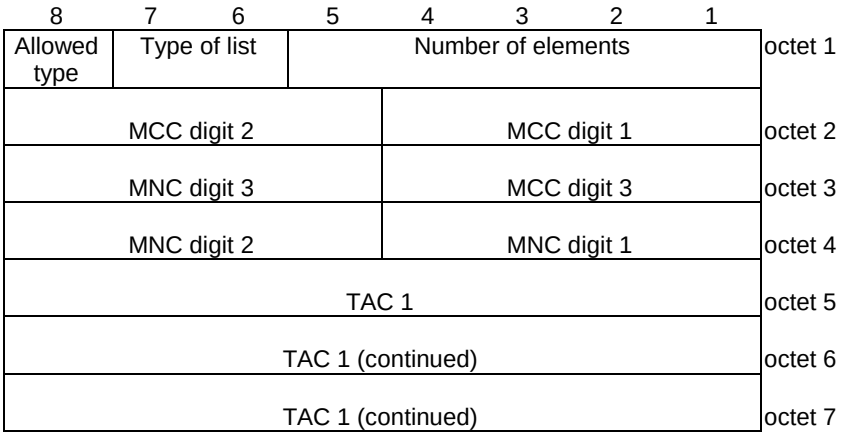


Figure 9.10.3.45.3: Partial service area list – type of list = "01"

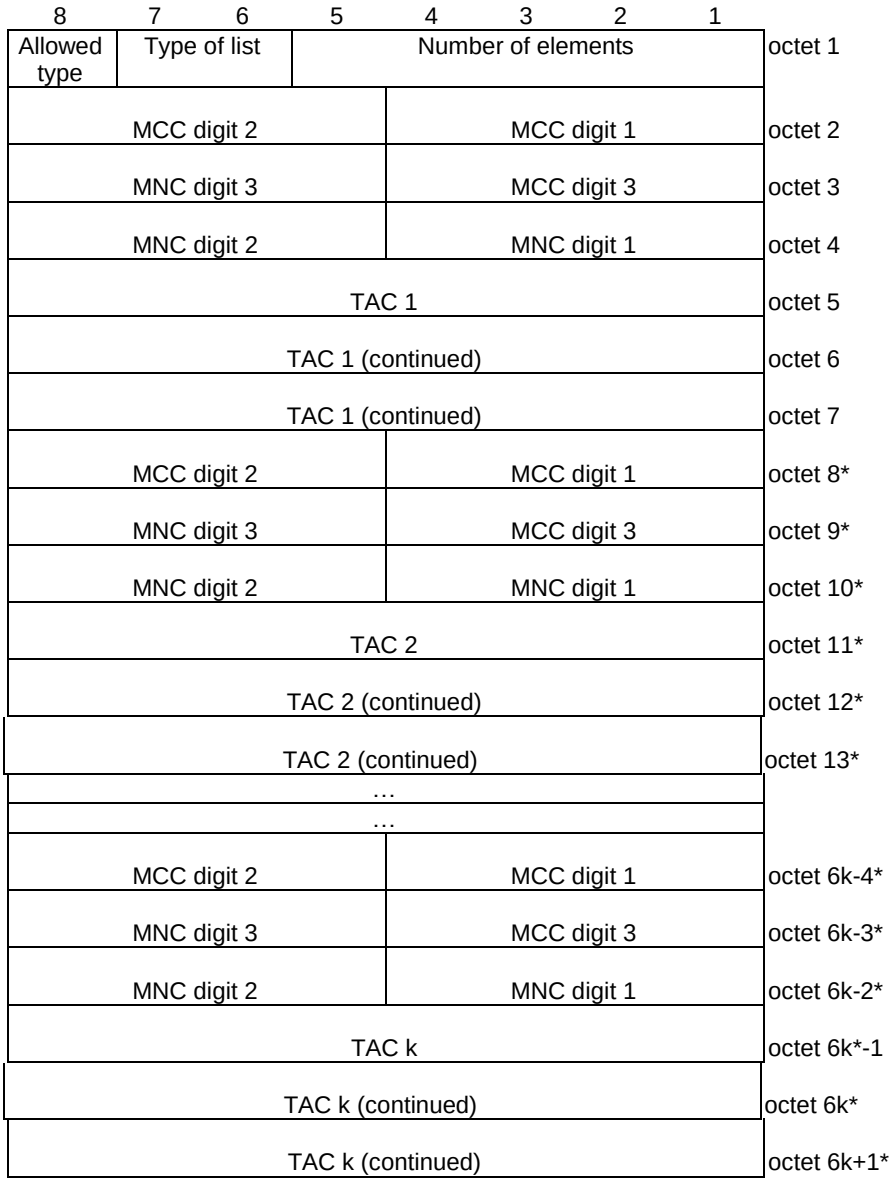


Figure 9.10.3.45.4: Partial service area list – type of list = "10"

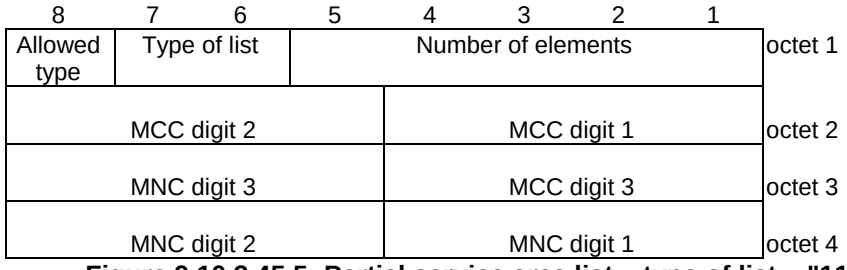


Figure 9.10.3.45.5: Partial service area list – type of list = "11"

Table 9.10.3.45.1: Service area list information element

Value part of the Service area list information element (octets 3 to n)

The value part of the Service area list information element consists of one or several partial service area lists. The length of each partial service area list can be determined from the 'type of list' field and the 'number of elements' field in the first octet of the partial service area list.
For allowed type "0", TAIs contained in all partial service area lists are in the allowed area. For allowed type "1", TAIs contained in all partial service area lists are in the non-allowed area.
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 service area list:

Allowed type (octet 1)
Bit

8	
0	TAIs in the list are in the allowed area
1	TAIs in the list are in the non-allowed area

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 (see NOTE)
1	1	All TAIs belonging to the PLMN are in the allowed area

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.

For type of list = "00" and number of elements = k:

octets 2 to 4 contain the MCC+MNC, and
for j = 1, …, k:
octets 3j+2 to 3j+4 contain the TAC of the j-th TAI belonging to the partial list,

For type of list = "01" and number of elements = k:

octets 2 to 4 contain the MCC+MNC, and
octets 5 to 7 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 = "10" and number of elements = k:

for j = 1, …, k.
octets 6j-4 to 6j-1 contain the MCC+MNC, and
octets 6j-1 to 6j+1 contain the TAC of the j-th TAI belonging to the partial list.

For type of list = "11":

Allowed type shall be coded as "0" and number of elements shall be ignored, and
octets 2 to 4 contain the MCC+MNC.
If allowed type is coded as "1", it shall be interpreted as "0".

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 the third 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 3 octets.

NOTE: If the "list of TAIs belonging to different PLMNs" is used, the PLMNs included in the list need to be present in the list of equivalent PLMNs.

9.10.3.46 Service type

The purpose of the service type information element is to specify the purpose of the service request procedure.

The service type is a type 1 information element.

The service type information element is coded as shown in figure 9.10.3.46.1 and table 9.10.3.46.1.

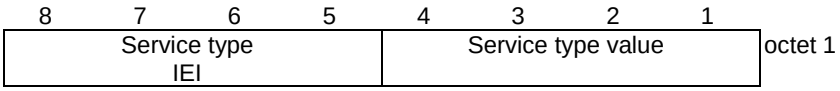


Figure 9.10.3.46.1: Service type information element

Table 9.10.3.46.1: Service type information element

Service type value (octet 1)

Service type value
Bits

4	3	2	1	
0	0	0	0	signalling
0	0	0	1	data
0	0	1	0	mobile terminated services
0	0	1	1	emergency services
0	1	0	0	emergency services fallback
0	1	0	1	high priority access
0	1	1	0	unused; shall be interpreted as "signalling", if received by the network
0	1	1	1	unused; shall be interpreted as "signalling", if received by the network
1	0	0	0	unused; shall be interpreted as "signalling", if received by the network
1	0	0	1	unused; shall be interpreted as "data", if received by the network
1	0	1	0	unused; shall be interpreted as "data", if received by the network
1	0	1	1	unused; shall be interpreted as "data", if received by the network

All other values are reserved.

9.10.3.47 Time zone

See subclause 10.5.3.8 in 3GPP TS 24.008 [12].

9.10.3.48 Time zone and time

See subclause 10.5.3.9 in 3GPP TS 24.008 [12].

9.10.3.49 Transparent container

Editor's note: The IE coding is FFS.

9.10.3.50 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 N1 mode and S1 mode for NAS security as well as which security algorithms are supported over NR and E-UTRA for AS security.

The UE security capability information element is coded as shown in figure 9.10.3.50.1 and table 9.10.3.50.1.

The UE security capability is a type 4 information element with a minimum length of 4 octets and a maximum length of 6 octets.

Octets 5 and 6 are optional. If octet 5 is included, then also octet 6 shall be included.

If the UE did not indicate support of any security algorithm for NAS security in S1 mode and did not indicate support of any security algorithm for AS security over E-UTRA, octets 5 and 6 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
5G-EA0	128-5G-EA1	128-5G-EA2	128-5G-EA3	5G-EA4	5G-EA5	5G-EA6	5G-EA7	octet 3
5G-IA0	128-5G-IA1	128-5G-IA2	128-5G-IA3	5G-IA4	5G-IA5	5G-IA6	5G-IA7	octet 4
EEA0	128-EEA1	128-EEA2	128-EEA3	EEA4	EEA5	EEA6	EEA7	octet 5*
EIA0	128-EIA1	128-EIA2	128-EIA3	EIA4	EIA5	EIA6	EIA7	octet 6*

Figure 9.10.3.50.1: UE security capability information element

Table 9.10.3.50.1: UE security capability information element

5GS encryption algorithms supported (see NOTE 1) (octet 3)
5GS encryption algorithm 5G-EA0 supported (octet 3, bit 8)
0 5GS encryption algorithm 5G-EA0 not supported
1 5GS encryption algorithm 5G-EA0 supported
5GS encryption algorithm 128-5G-EA1 supported (octet 3, bit 7)
0 5GS encryption algorithm 128-5G-EA1 not supported
1 5GS encryption algorithm 128-5G-EA1 supported
5GS encryption algorithm 128-5G-EA2 supported (octet 3, bit 6)
0 5GS encryption algorithm 128-5G-EA2 not supported
1 5GS encryption algorithm 128-5G-EA2 supported
5GS encryption algorithm 128-5G-EA3 supported (octet 3, bit 5)
0 5GS encryption algorithm 128-5G-EA31 not supported
1 5GS encryption algorithm 128-5G-EA3 supported
5GS encryption algorithm 5G-EA4 supported (octet 3, bit 4)
0 5GS encryption algorithm 5G-EA4 not supported
1 5GS encryption algorithm 5G-EA4 supported
5GS encryption algorithm 5G-EA5 supported (octet 3, bit 3)
0 5GS encryption algorithm 5G-EA5 not supported
1 5GS encryption algorithm 5G-EA5 supported
5GS encryption algorithm 5G-EA6 supported (octet 3, bit 2)
0 5GS encryption algorithm 5G-EA6 not supported
1 5GS encryption algorithm 5G-EA6 supported
5GS encryption algorithm 5G-EA7 supported (octet 3, bit 1)
0 5GS encryption algorithm 5G-EA7 not supported
1 5GS encryption algorithm 5G-EA7 supported
5GS integrity algorithms supported (see NOTE 2) (octet 4)
5GS integrity algorithm 5G-IA0 supported (octet 4, bit 8)
0 5GS integrity algorithm 5G-IA0 not supported
1 5GS integrity algorithm 5G-IA0 supported
5GS integrity algorithm 128-5G-IA1 supported (octet 4, bit 7)
0 5GS integrity algorithm 128-5G-IA1 not supported
1 5GS integrity algorithm 128-5G-IA1 supported
5GS integrity algorithm 128-5G-IA2 supported (octet 4, bit 6)
0 5GS integrity algorithm 128-5G-IA2 not supported
1 5GS integrity algorithm 128-5G-IA2 supported
5GS integrity algorithm 128-5G-IA3 supported (octet 4, bit 5)
0 5GS integrity algorithm 128-5G-IA3 not supported
1 5GS integrity algorithm 128-5G-IA3 supported
5GS integrity algorithm 5G-IA4 supported (octet 4, bit 4)
0 5GS integrity algorithm 5G-IA4 not supported
1 5GS integrity algorithm 5G-IA4 supported
5GS integrity algorithm 5G-IA5 supported (octet 4, bit 3)
0 5GS integrity algorithm 5G-IA5 not supported
1 5GS integrity algorithm 5G-IA5 supported
5GS integrity algorithm 5G-IA6supported (octet 4, bit 2)
0 5GS integrity algorithm 5G-IA6 not supported
1 5GS integrity algorithm 5G-IA6 supported
5GS integrity algorithm 5G-IA7 supported (octet 4, bit 1)
0 5GS integrity algorithm 5G-IA7 not supported

1 5GS integrity algorithm 5G-IA7 supported
EPS encryption algorithms supported (see NOTE 3) (octet 5)
EPS encryption algorithm EEA0 supported (octet 5, bit 8)
0 EPS encryption algorithm EEA0 not supported
1 EPS encryption algorithm EEA0 supported
EPS encryption algorithm 128-EEA1 supported (octet 5, bit 7)
0 EPS encryption algorithm 128-EEA1 not supported
1 EPS encryption algorithm 128-EEA1 supported
EPS encryption algorithm 128-EEA2 supported (octet 5, bit 6)
0 EPS encryption algorithm 128-EEA2 not supported
1 EPS encryption algorithm 128-EEA2 supported
EPS encryption algorithm 128-EEA3 supported (octet 5, bit 5)
0 EPS encryption algorithm 128-EEA3 not supported
1 EPS encryption algorithm 128-EEA3 supported
EPS encryption algorithm EEA4 supported (octet 5, bit 4)
0 EPS encryption algorithm EEA4 not supported
1 EPS encryption algorithm EEA4 supported
EPS encryption algorithm EEA5 supported (octet 5, bit 3)
0 EPS encryption algorithm EEA5 not supported
1 EPS encryption algorithm EEA5 supported
EPS encryption algorithm EEA6 supported (octet 5, bit 2)
0 EPS encryption algorithm EEA6 not supported
1 EPS encryption algorithm EEA6 supported
EPS encryption algorithm EEA7 supported (octet 5, bit 1)
0 EPS encryption algorithm EEA7 not supported
1 EPS encryption algorithm EEA7 supported
EPS integrity algorithms supported (see NOTE 4) (octet 6)
EPS integrity algorithm EIA0 supported (octet 6, bit 8)
0 EPS integrity algorithm EIA0 not supported
1 EPS integrity algorithm EIA0 supported
EPS integrity algorithm 128-EIA1 supported (octet 6, bit 7)
0 EPS integrity algorithm 128-EIA1 not supported
1 EPS integrity algorithm 128-EIA1 supported
EPS integrity algorithm 128-EIA2 supported (octet 6, bit 6)
0 EPS integrity algorithm 128-EIA2 not supported
1 EPS integrity algorithm 128-EIA2 supported
EPS integrity algorithm 128-EIA3 supported (octet 6, bit 5)
0 EPS integrity algorithm 128-EIA3 not supported
1 EPS integrity algorithm 128-EIA3 supported
EPS integrity algorithm EIA4 supported (octet 6, bit 4)
0 EPS integrity algorithm EIA4 not supported
1 EPS integrity algorithm EIA4 supported
EPS integrity algorithm EIA5 supported (octet 6, bit 3)
0 EPS integrity algorithm EIA5 not supported
1 EPS integrity algorithm EIA5 supported
EPS integrity algorithm EIA6 supported (octet 6, bit 2)
0 EPS integrity algorithm EIA6 not supported
1 EPS integrity algorithm EIA6 supported
EPS integrity algorithm EIA7 supported (octet 6, bit 1)
0 EPS integrity algorithm EIA7 not supported

1	EPS integrity algorithm EIA7 supported
NOTE 1:	The code points in octet 3 are used to indicate support for 5GS encryption algorithms for NAS security in N1 mode and support for 5GS encryption algorithms for AS security over NR.
NOTE 2:	The code points in octet 4 are used to indicate support for 5GS integrity algorithms for NAS security in N1 mode and support for 5GS integrity algorithms for AS security over NR.
NOTE 3:	The code points in octet 5 are used to indicate support for EPS encryption algorithms for NAS security in S1 mode and support for EPS encryption algorithms for AS security over E-UTRA.
NOTE 4:	The code points in octet 6 are used to indicate support for EPS integrity algorithms for NAS security in S1 mode and support for EPS integrity algorithms for AS security over E-UTRA.

9.10.3.51 UE's usage setting

The purpose of the UE's usage setting information element is to provide the network with the UE's usage setting as defined in 3GPP TS 24.301 [15]. The network uses the UE's usage setting to select the RFSP index.

The UE's usage setting information element is coded as shown in figure 9.10.3.51.1 and table 9.10.3.51.1.

The UE's usage setting is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
UE's usage setting IEI								octet 1
Length of UE's usage setting contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	UE's usage setting	octet 3

Figure 9.10.3.51.1: UE's usage setting information element

Table 9.10.3.51.1: UE's usage setting information element

UE's usage setting (octet 3, bit 1)
0 voice centric
1 data centric
All other bits in the octet 3 are spare and shall be coded as zero,

9.10.3.52 UE status

The purpose of the UE status information element is to provide the network with information concerning aspects of the current UE registration status which is used for interworking with EPS.

The UE status information element is coded as shown in figure 9.10.3.52.1 and table 9.10.3.52.1.

The UE status is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
UE status IEI								octet 1
Length of UE status contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	N1 mode reg	S1 mode reg	octet 3

Figure 9.10.3.52.1: UE status information element

Table 9.10.3.52.1: UE status information element

EMM registration status (S1 mode reg) (octet 3, bit 1) 0 UE is not in EMM-REGISTERED state 1 UE is in EMM-REGISTERED state 5GMM registration status (N1 mode reg) (octet 3, bit 2) 0 UE is not in 5GMM-REGISTERED state 1 UE is in 5GMM-REGISTERED state All other bits in the octet 3 are spare and shall be coded as zero.

9.10.3.53 Uplink data status

The purpose of the Uplink data status information element is to indicate to the network which preserved PDU session contexts have uplink data pending.

The Uplink data status information element is coded as shown in figure 9.10.3.53.1 and table 9.10.3.53.1.

The Uplink data status information element is a type 4 information element with minimum length of 4 octets a maximum length of 34 octets.

8	7	6	5	4	3	2	1	
Uplink data status IEI								octet 1
Length of uplink data status contents								octet 2
PSI (7)	PSI (6)	PSI (5)	PSI (4)	PSI (3)	PSI (2)	PSI (1)	PSI (0)	octet 3
PSI (15)	PSI (14)	PSI (13)	PSI (12)	PSI (11)	PSI (10)	PSI (9)	PSI (8)	octet 4
0	0	0	0	0	0	0	0	
spare								octet 5* -34*

Figure 9.10.3.53.1: Uplink data status information element

Table 9.10.3.53.1: Uplink data status information element

PSI(x) shall be coded as follows: PSI(0): Bit 1 of octet 3 is spare and shall be coded as zero. PSI(1) – PSI(15): 0 indicates that no uplink data are pending for the corresponding PDU session identity. 1 indicates that uplink data are pending for the corresponding PDU session identity. All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.10.4 5GS session management (5GSM) information elements

9.10.4.1 5GSM capability

The purpose of the 5GSM capability information element is to indicate UE capability related to the PDU session management.

The 5GSM capability information element is coded as shown in figure 9.10.4.1.1 and table 9.10.4.1.1.

The 5GSM capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

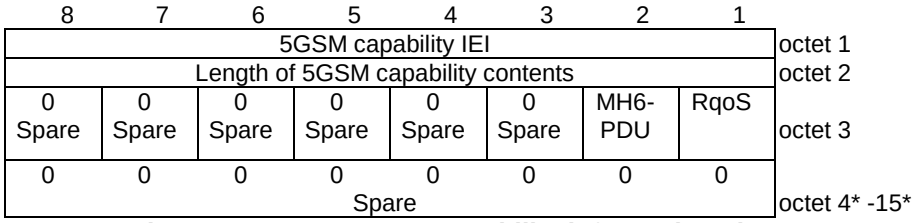


Figure 9.10.4.1.1: 5GSM capability information element

Table 9.10.4.1.1: 5GSM capability information element

5GSM capability value RqoS(octet 3, bit 1) This bit indicates the 5GSM capability to support reflective QoS. 0 Reflective QoS not supported 1 Reflective QoS supported Multi-homed IPv6 PDU session (MH6-PDU) (octet 3, bit 2) This bit indicates the 5GSM capability for Multi-homed IPv6 PDU session. 0 Multi-homed IPv6 PDU session not supported 1 Multi-homed IPv6 PDU session supported
All other bits in octet 3 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.10.4.2 5GSM cause

The purpose of the 5GSM cause information element is to indicate the reason why a 5GSM request is rejected.

The 5GSM cause information element is coded as shown in figure 9.10.4.2.1 and table 9.10.4.2.1.

The 5GSM cause is a type 3 information element with 2 octets length.

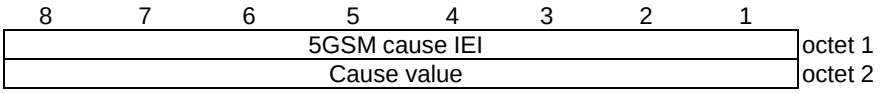


Figure 9.10.4.2.1: 5GSM cause information element

Table 9.10.4.2.1: 5GSM cause information element

Cause value (octet 2) Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	1	1	0	1	0	Insufficient resources
0	0	0	1	1	0	1	1	Missing or unknown DNN
0	0	0	1	1	1	0	0	Unknown PDU session type
0	0	0	1	1	1	0	1	User authentication failed
0	0	0	1	1	1	1	1	Request rejected, unspecified
0	0	1	0	0	0	1	0	Service option temporarily out of order
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	1	1	Reactivation requested
0	0	1	1	0	0	1	0	PDU session type IPv4 only allowed
0	0	1	1	0	0	1	1	PDU session type IPv6 only allowed
0	1	0	0	0	0	1	1	Insufficient resources for specific slice and DNN
0	1	0	0	0	1	0	0	Not supported SSC mode
0	1	0	0	0	1	0	1	Insufficient resources for specific slice
0	1	0	0	0	1	1	0	Missing or unknown DNN in a slice
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
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".								

9.10.4.3 Allowed SSC mode

The purpose of the Allowed SSC mode information element is to indicate the SSC modes allowed to be used by the UE for the PDU session.

The Allowed SSC mode information element is coded as shown in figure 9.10.4.3.1 and table 9.10.4.3.1.

The Allowed SSC mode is a type 1 information element.

8	7	6	5	4	3	2	1	
Allowed SSC mode IEI				0 Spare	SSC3	SSC2	SSC1	octet 1

Figure 9.10.4.3.1: Allowed SSC mode information element

Table 9.10.4.3.1: Allowed SSC mode information element

SSC1 (octet 1, bit 1) **1** 0 SSC mode 1 not allowed 1 SSC mode 1 allowed SSC1 (octet 1, bit 2) **2** 0 SSC mode 2 not allowed 1 SSC mode 2 allowed SSC3 (octet 1, bit 3) **3** **0** SSC mode 3 not allowed **1** SSC mode 3 allowed Bit 4 is spare and shall be encoded as zero.

9.10.4.4 Extended protocol configuration options

See subclause 10.5.6.3A in 3GPP TS 24.008 [12].

9.10.4.5 Mapped EPS bearer contexts

The purpose of the mapped EPS bearer contexts information element is to indicate a set of EPS contexts for a PDU session context, as described in subclause 6.1.4.1.

The mapped EPS bearer contexts information element is a type 6 information element with a minimum length of 7 octet and a maximum length of 65538 octets.

The mapped EPS bearer contexts information element is coded as shown in figure 9.10.4.5.1, figure 9.10.4.5.2, figure 9.10.4.5.3 and table 9.10.4.5.1.

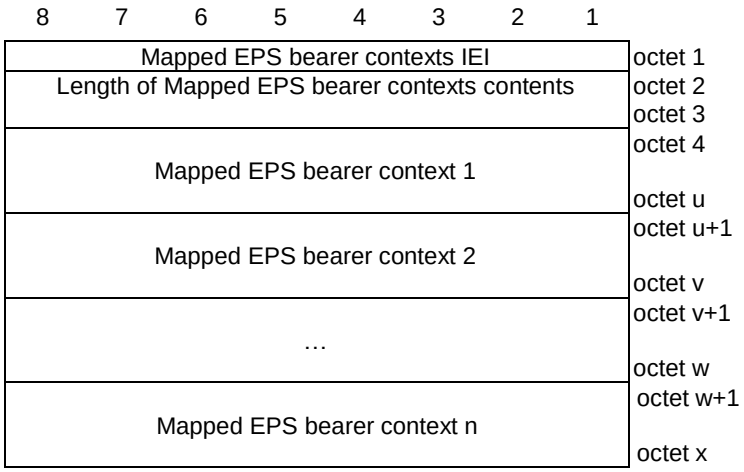


Figure 9.10.4.5.1: Mapped EPS bearer contexts

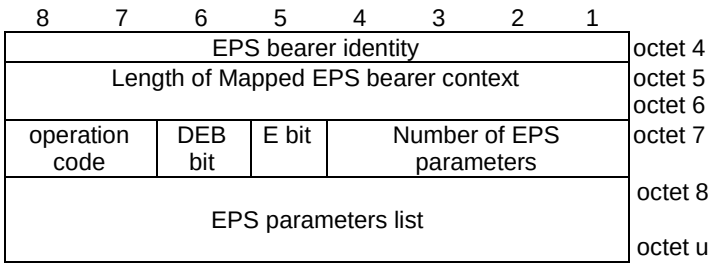


Figure 9.10.4.5.2: Mapped EPS bearer context

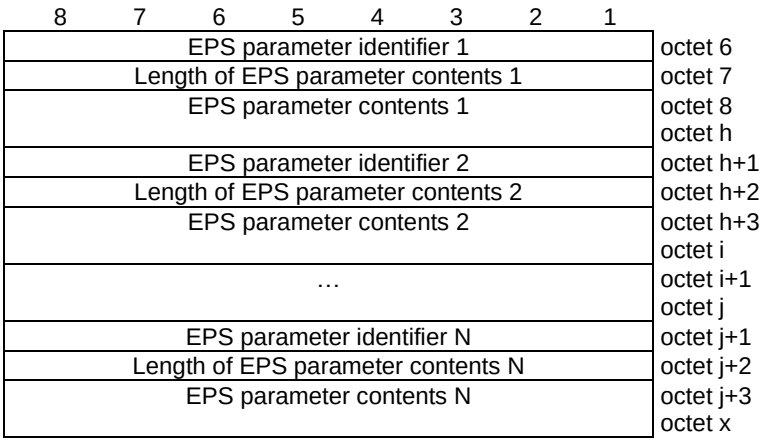


Figure 9.10.4.5.3: EPS parameters list

Table 9.10.4.5.1: Mapped EPS bearer contexts information element

EPS bearer identity (octet 4)

The EPS bearer identity is used to identity the EPS bearer, and is coded as specified in subclause 9.3.2 of 3GPP TS 24.301 [15].

Operation code (bits 8 to 7 of octet 7)
Bits
8 7
0 0 Reserved
0 1 Create new EPS bearer
1 0 Delete existing EPS bearer
1 1 Modify existing EPS bearer

DEB bit (bit 6 of octet 7)
The DEB bit indicates whether the EPS bearer is the default EPS bearer and it is encoded as follows:
Bit
6
0 the EPS bearer is not the default EPS bearer.
1 the EPS bearer is the default EPS bearer.

E bit (bit 5 of octet 7)
For the "create new EPS bearer" operation, the E bit is encoded as follows:
Bit
5
0 parameters list is not included
1 parameters list is included
For the "modify existing EPS bearer" operation, the E bit is encoded as follows:
Bit
5
0 previously provided parameters list extension
1 previously provided parameters list replacement

If the E bit is set to "parameters list is not included", the number of EPS parameters field has zero value. If the E bit is set to "parameters list is included", the number of EPS parameters field has non-zero value. If the E bit is set to "previously provided parameters list extension" or "previously provided parameters list replacement", the number of parameters field can have zero or non-zero value.

Number of EPS parameters (bits 4 to 1 of octet 7)
The number of EPS parameters contains the binary coding for the number of EPS parameters in the EPS parameters list field. The number of EPS parameters field is encoded in bits 5 through 1 of octet x+1 where bit 5 is the most significant and bit 1 is the least significant bit.

EPS parameters list (octets 8 to u)
The EPS parameters list contains a variable number of EPS parameters.

Each EPS parameter included in the EPS parameters list is of variable length and consists of:
- an EPS parameter identifier (1 octet);
- the length of the EPS parameter contents (1 octet); and
- the EPS parameter contents itself (variable amount of octets).

The EPS parameter identifier field is used to identify each EPS parameter included in the EPS parameters list and it contains the hexadecimal coding of the EPS parameter identifier. Bit 8 of the EPS parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following EPS parameter identifiers are specified:
- 01H (Mapped EPS QoS parameters);
- 02H (Mapped extended EPS QoS parameters); and
- 03H (Traffic flow template).
- 04H (APN-AMBR).
- 05H (extended APN-AMBR).

If the EPS parameters list contains an EPS parameter identifier that is not supported

by the receiving entity the corresponding EPS parameter shall be discarded. The length of EPS parameter contents field contains the binary coded representation of the length of the EPS parameter contents field. The first bit in transmission order is the most significant bit. When the parameter identifier indicates mapped EPS QoS parameters, the length and parameter contents field are coded as specified in subclause 9.9.4.3 of 3GPP TS 24.301 [15]. When the parameter identifier indicates mapped extended EPS QoS parameters, the length and parameter contents field are coded as specified in subclause 9.9.4.30 of 3GPP TS 24.301 [15]. When the parameter identifier indicates traffic flow template, the length and parameter contents field are coded from octet 2 as shown figure 10.5.144 and table 10.5.162 of 3GPP TS 24.008 [12]. When the parameter identifier indicates APN-AMBR, the length and parameter contents field are coded as specified in subclause 9.9.4.2 of 3GPP TS 24.301 [15]. When the parameter identifier indicates Extended APN-AMBR, the length and parameter contents field are coded as specified in subclause 9.9.4.29 of 3GPP TS 24.301 [15].

9.10.4.6 Maximum number of supported packet filters

The purpose of the Maximum number of supported packet filters information element is for the UE to indicate to the network the maximum number of packet filters, associated with signaled QoS rules, that can be supported by the UE for the PDU session that is being established, when the PDU session type "IPv4", "IPv6", "IPv4v6" or "Ethernet".

The Maximum number of supported packet filters is coded as shown in figure 9.10.4.6.1 and table 9.10.4.6.2.

The Maximum number of supported packet filters is a type 3 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
Maximum number of supported packet filters IEI								octet 1
Maximum number of supported packet filters								octet 2
								octet 3

Figure 9.10.4.6.1: Maximum number of supported packet filters information element

Table 9.10.4.6.2: Maximum number of supported packet filters information element

Maximum number of supported packet filters (octet 2 to 3) In the Maximum number of supported packet filters field bit 8 of the first octet is the most significant bit and bit 7 of second octet is the least significant bit. Bit 6 to bit 1 of the second octet are spare bits and shall be coded as zero. The number of supported packet filters shall be in the range of 17 to 1024.

9.10.4.7 PDU address

The purpose of the PDU address information element is to assign to the UE:

- an IPv4 address associated with a PDU session;
- an interface identifier for the IPv6 link local address associated with the PDU session; or
- an IPv4 address and an interface identifier for the IPv6 link local address, associated with the PDU session.

The PDU address information element is coded as shown in figure 9.10.4.7.1 and table 9.10.4.7.1.

The PDU address is a type 4 information element with minimum length of 7 octets and a maximum length of 15 octets.

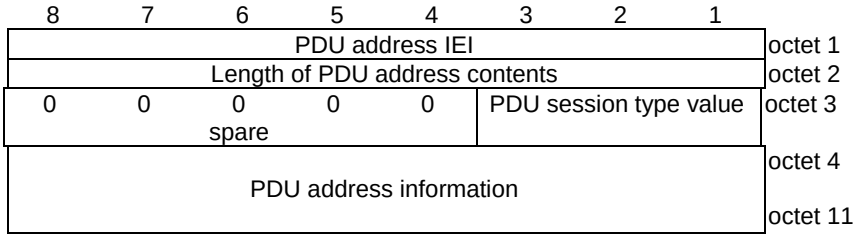


Figure 9.10.4.7.1: PDU address information element

Table 9.10.4.7.1: PDU address information element

PDU session 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. PDU address information (octet 4 to 15) If the PDU session type value indicates IPv4, the PDU address information in octet 4 to octet 7 contains an IPv4 address. If the PDU session type value indicates IPv6, the PDU address information in octet 4 to octet 11 contains an interface identifier for the IPv6 link local address. If the PDU session type value indicates IPv4v6, the PDU address information in octet 4 to octet 11 contains an interface identifier for the IPv6 link local address and in octet 12 to octet 15 contains an IPv4 address.

9.10.4.8 PDU session type

The purpose of the PDU session type information element is to indicate type of the PDU session.

The PDU session type information element is coded as shown in figure 9.10.4.8.1 and table 9.10.4.8.1.

The PDU session type is a type 1 information element.

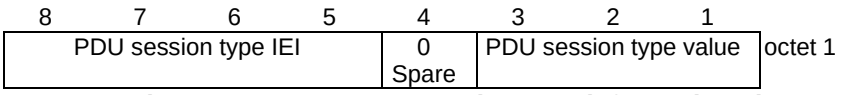


Figure 9.10.4.8.1: PDU session type information element

Table 9.10.4.8.1: PDU session type information element

PDU session type value (octet 1, bit 1 to bit 3) Bits **3 2 1** 0 0 1 IPv4 0 1 0 IPv6 0 1 1 IPv4v6 1 0 0 Unstructured 1 0 1 Ethernet 1 1 1 reserved All other values are unused and shall be interpreted as "IPv4v6", if received by the UE or the network.

9.10.4.9 QoS rules

The purpose of the QoS rules information element is to indicate a set of QoS rules to be used by the UE, where each QoS rule is a set of parameters as described in subclause 6.2.5.1.1.2:

a) for classification and marking of uplink user traffic; and

b) for identification of a QoS flow which the network is to use for a particular downlink user traffic.

NOTE: The UE needs to be aware of a QoS flow which the network is to use for a particular downlink user traffic e.g. to determine whether a resource is available for downlink media of a media stream of an SDP media description provided by the UE in an IMS session.

The QoS rules may contain a set of packet filters consisting of zero or more packet filters for UL direction, zero or more packet filters for DL direction, zero or more packet filters for both UL and DL directions or any combinations of these. The set of packet filters determine the traffic mapping to QoS flows.

The QoS rules information element is a type 6 information element with a minimum length of 7 octets. The maximum length for the information element is 65538 octets.

The QoS rules information element is coded as shown in figure 9.10.4.9.1, figure 9.10.4.9.2, figure 9.10.4.9.3, figure 9.10.4.9.4, figure 9.10.4.9.5 and table 9.10.4.9.1.

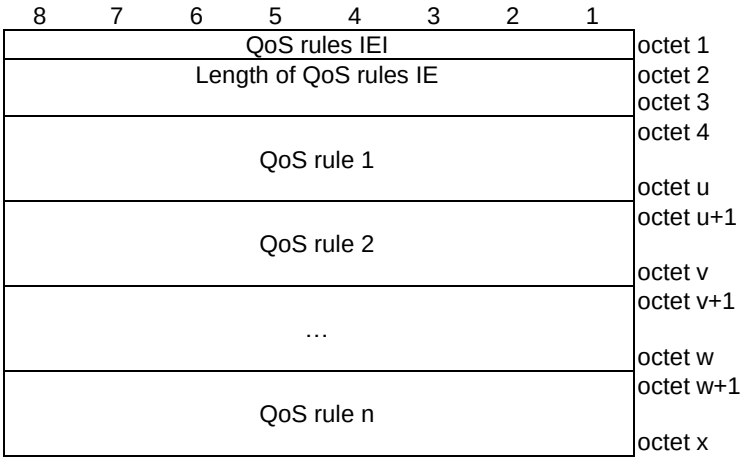


Figure 9.10.4.9.1: QoS rules information element

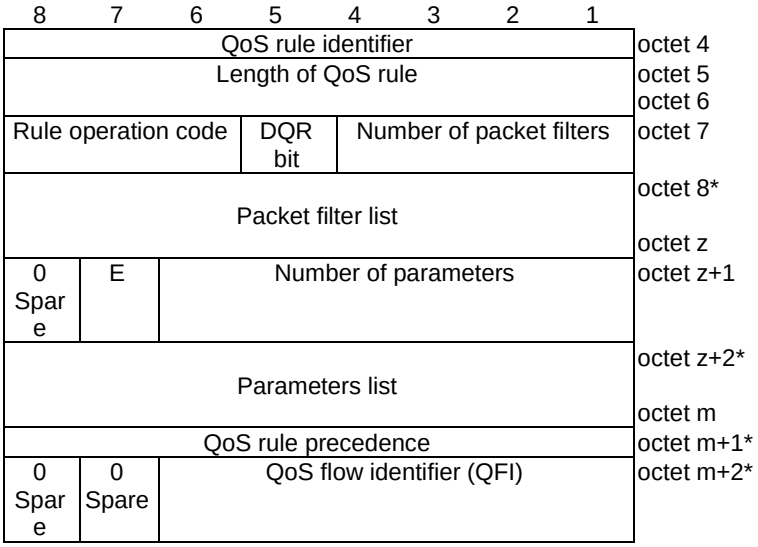


Figure 9.10.4.9.2: QoS rule (u=m+2)

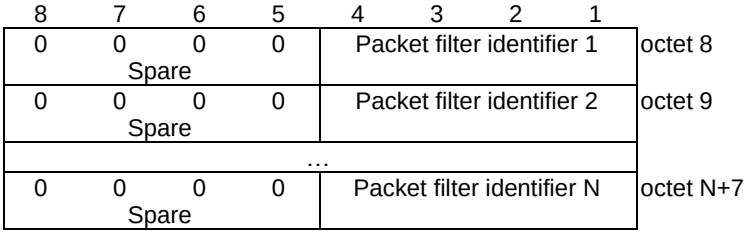


Figure 9.10.4.9.3: Packet filter list when the rule operation is "modify existing QoS rule and delete packet filters" (z=N+7)

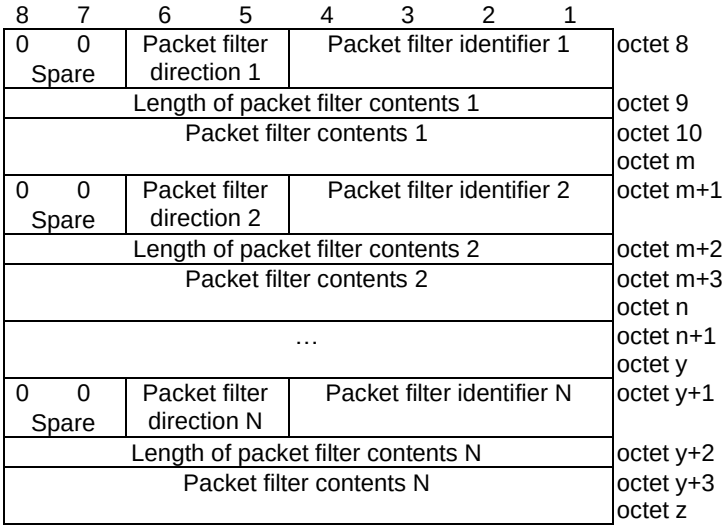


Figure 9.10.4.9.4: Packet filter list when the rule operation is "create new QoS rule", or "modify existing QoS rule and add packet filters" or "modify existing QoS rule and replace packet filters"

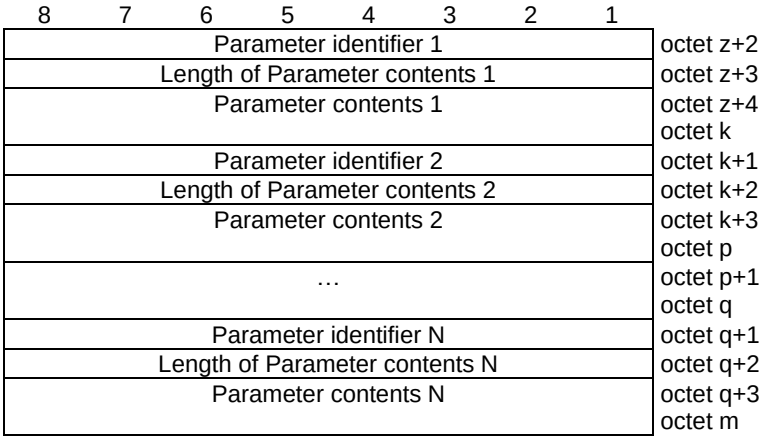


Figure 9.10.4.9.5: Parameters list

Table 9.10.4.9.1: QoS rules information element

QoS rule identifier (octet 4)
The QoS rule identifier field is used to identify the QoS rule.

QoS rule precedence (octet m+1)
The QoS rule precedence field is used to specify the precedence of the QoS rule among all QoS rules (both the signalled QoS rules as described in subclause 6.2.5.1.1.2 and the derived QoS rules as described in subclause 6.2.5.1.1.3) associated with the PDU session of the QoS flow. This field includes the binary coded value of the QoS rule precedence in the range from 0 to 255 (decimal). The higher the value of the QoS rule precedence field, the lower the precedence of that QoS rule is.
The value 80 (decimal) is reserved.

QoS flow identifier (QFI) (bits 6 to 1 of octet m+2)
The QoS flow identifier (QFI) field contains the QoS flow identifier.
Bits
6 5 4 3 2 1
0 0 0 0 0 0QFI 0
to
1 1 1 1 1 1QFI 63

DQR bit (bit 5 of octet 7)
The DQR bit indicates whether the QoS rule is the default QoS rule and it is encoded as follows:
Bit
5
0 the QoS rule is not the default QoS rule.
1 the QoS rule is the default QoS rule.

Rule operation code (bits 8 to 6 of octet 7)
Bits
8 7 6
0 0 0 Reserved
0 0 1 Create new QoS rule
0 1 0 Delete existing QoS rule
0 1 1 Modify existing QoS rule and add packet filters
1 0 0 Modify existing QoS rule and replace packet filters
1 0 1 Modify existing QoS rule and delete packet filters
1 1 0 Modify existing QoS rule without modifying packet filters
1 1 1 Reserved

E bit (bit 7 of octet z+1)
For the "create new QoS rule" operation, the E bit is encoded as follows:
Bit
7
0 parameters list is not included
1 parameters list is included
For the "modify existing QoS rule and add packet filters" operation, the "modify existing QoS rule and replace packet filters", the "modify existing QoS rule and delete packet filters" operation and the "modify existing QoS rule without modifying packet filters" operation, the E bit is encoded as follows:
Bit
7
0 previously provided parameters list extension
1 previously provided parameters list replacement

If the E bit is set to "parameters list is not included", the number of parameters field has zero value. If the E bit is set to "parameters list is included", the number of parameters field has non-zero value. If the E bit is set to "previously provided parameters list extension" or "previously provided parameters list replacement", the number of parameters field can have zero or non-zero value.

Number of packet filters (bits 4 to 1 of octet 7)
The number of packet filters contains the binary coding for the number of packet

filters in the packet filter list. The number of packet filters field is encoded in bits 4 through 1 of octet 7 where bit 4 is the most significant and bit 1 is the least significant bit. For the "delete existing QoS rule" operation and for the "modify existing QoS rule without modifying packet filters" operation, the number of packet filters shall be coded as 0. For the "create new QoS rule" operation and the "modify existing QoS rule and replace packet filters" operation, the number of packet filters shall be greater than or equal to 0 and less than or equal to 15. For all other operations, the number of packet filters shall be greater than 0 and less than or equal to 15.

Packet filter list (octets 8 to z)
The packet filter list contains a variable number of packet filters.

For the "delete existing QoS rule" operation, the length of QoS rule field is set to one.

For the "delete existing QoS rule" operation and the "modify existing QoS rule without modifying packet filters" operation, the packet filter list shall be empty.

For the "modify existing QoS rule and delete packet filters" operation, the packet filter list shall contain a variable number of packet filter identifiers. This number shall be derived from the coding of the number of packet filters field in octet 7.

For the "create new QoS rule" operation and for the "modify existing QoS rule and replace packet filters" operation, the packet filter list shall contain 0 or a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.

For the "modify existing QoS rule and add packet filters" operation, the packet filter list shall contain a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.

Each packet filter is of variable length and consists of
a packet filter direction (2 bits);
- a packet filter identifier (4 bits);
- the length of the packet filter contents (1 octet); and
- the packet filter contents itself (variable amount of octets).

The packet filter direction field is used to indicate for what traffic direction the filter applies.

Bits	
6	5
0	0 reserved
0	1 downlink only
1	0 uplink only
1	1 bidirectional (see NOTE 1)

The packet filter identifier field is used to identify each packet filter in a QoS rule. The least significant 4 bits are used.

The length of the packet filter contents field contains the binary coded representation of the length of the packet filter contents field of a packet filter. The first bit in transmission order is the most significant bit.

The packet filter contents field is of variable size and contains a variable number (at least one) of packet filter components. Each packet filter component shall be encoded as a sequence of a one octet packet filter component type identifier and a fixed length packet filter component value field. The packet filter component type identifier shall be transmitted first.

In each packet filter, there shall not be more than one occurrence of each packet filter component type. Among the "IPv4 remote address type" and "IPv6 remote address/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "IPv4 local address type" and "IPv6 local address/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "single local port type" and "local port range type" packet filter components, only one shall be present in one packet filter. Among the "single remote port type" and "remote port range type" packet filter components, only one

shall be present in one packet filter. If the "match-all type" packet filter component is present in the packet filter, no other packet filter component shall be present in the packet filter and the length of the packet filter contents field shall be set to one.

The term local refers to the UE and the term remote refers to an external network entity.

Packet filter component type identifier
Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 1 Match-all type
0 0 0 1 0 0 0 0 IPv4 remote address type
0 0 0 1 0 0 0 1 IPv4 local address type
0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type
0 0 1 0 0 0 1 1 IPv6 local address/prefix length type
0 0 1 1 0 0 0 0 Protocol identifier/Next header type
0 1 0 0 0 0 0 0 Single local port type
0 1 0 0 0 0 0 1 Local port range type
0 1 0 1 0 0 0 0 Single remote port type
0 1 0 1 0 0 0 1 Remote port range type
0 1 1 0 0 0 0 0 Security parameter index type
0 1 1 1 0 0 0 0 Type of service/Traffic class type
1 0 0 0 0 0 0 0 Flow label type
1 0 0 0 0 0 0 1 Destination MAC address type
1 0 0 0 0 0 1 0 Source MAC address type
1 0 0 0 0 0 1 1 802.1Q C-TAG VID type
1 0 0 0 0 1 0 0 802.1Q S-TAG VID type
1 0 0 0 0 1 0 1 802.1Q C-TAG PCP/DEI type
1 0 0 0 0 1 1 0 802.1Q S-TAG PCP/DEI type
1 0 0 0 0 1 1 1 Ethertype type
All other values are reserved.

The description and valid combinations of packet filter component type identifiers in a packet filter are defined in 3GPP TS 23.501 [8].

For "match-all type", the packet filter component shall not include the packet filter component value field.

For "IPv4 remote address type", the packet filter component value field shall be encoded as a sequence of a four octet IPv4 address field and a four octet IPv4 address mask field. The IPv4 address field shall be transmitted first.

For "IPv4 local address type", the packet filter component value field shall be encoded as defined for "IPv4 remote address type".

For "IPv6 remote address/prefix length type", the packet filter component value field shall be encoded as a sequence of a sixteen octet IPv6 address field and one octet prefix length field. The IPv6 address field shall be transmitted first.

For "IPv6 local address/prefix length type", the packet filter component value field shall be encoded as defined for "IPv6 remote address /prefix length".

For "protocol identifier/Next header type", the packet filter component value field shall be encoded as one octet which specifies the IPv4 protocol identifier or Ipv6 next header.

For "single local port type" and "single remote port type", the packet filter component value field shall be encoded as two octets which specify a port number.

For "local port range type" and "remote port range type", the packet filter component value field shall be encoded as a sequence of a two octet port range low limit field and a two octet port range high limit field. The port range low limit field shall be transmitted first.

For "security parameter index", the packet filter component value field shall be encoded as four octets which specify the IPSec security parameter index.

For "type of service/traffic class type", the packet filter component value field shall be encoded as a sequence of a one octet type-of-service/traffic class field and a one octet type-of-service/traffic class mask field. The type-of-service/traffic class field shall be transmitted first.

For "flow label type", the packet filter component value field shall be encoded as three octets which specify the IPv6 flow label. The bits 8 through 5 of the first octet shall be spare whereas the remaining 20 bits shall contain the IPv6 flow label.

For "destination MAC address type" and "source MAC address type", the packet filter component value field shall be encoded as 6 octets which specify a MAC address.

For "802.1Q C-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the customer-VLAN tag (C-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.

For "802.1Q S-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the service-VLAN tag (S-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.

For "802.1Q C-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q C-TAG PCP and DEI. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.

For "802.1Q S-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q S-TAG PCP. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.

For "ethertype type", the packet filter component value field shall be encoded as two octets which specify an ethertype.

Number of parameters (bits 6 to 1 of octet z+1)
The number of parameters field contains the binary coding for the number of parameters in the parameters list field. The number of parameters field is encoded in bits 6 through 1 of octet z+1 where bit 6 is the most significant and bit 1 is the least significant bit.

Parameters list (octets z+2 to v)

The parameters list contains a variable number of parameters.

Each parameter included in the parameters list is of variable length and consists of:
- a parameter identifier (1 octet);
- the length of the parameter contents (1 octet); and
- the parameter contents itself (variable amount of octets).

The parameter identifier field is used to identify each parameter included in the parameters list and it contains the hexadecimal coding of the parameter identifier. Bit 8 of the parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following parameter identifiers are specified:
- 01H (5QI);
- 02H (GFBR uplink);
- 03H (GFBR downlink);
- 04H (MFBR uplink);
- 05H (MFBR downlink);
- 06H (Averaging window); and
- 07H (EPS bearer identity).

If the parameters list contains a parameter identifier that is not supported by the receiving entity the corresponding parameter shall be discarded.
The length of parameter contents field contains the binary coded representation of the length of the parameter contents field. The first bit in transmission order is the

most significant bit.

When the parameter identifier indicates 5QI, the parameter contents field contains the binary representation of 5G QoS identifier (5QI) that is one octet in length.

5QI:
Bits
8 7 6 5 4 3 2 1
In network to UE direction:

0 0 0 0 0 0 0 0	Reserved
0 0 0 0 0 0 0 1	5QI 1
0 0 0 0 0 0 1 0	5QI 2
0 0 0 0 0 0 1 1	5QI 3
0 0 0 0 0 1 0 0	5QI 4
0 0 0 0 0 1 0 1	5QI 5
0 0 0 0 0 1 1 0	5QI 6
0 0 0 0 0 1 1 1	5QI 7
0 0 0 0 1 0 0 0	5QI 8
0 0 0 0 1 0 0 1	5QI 9
0 0 0 0 1 0 1 0	
to	Spare
0 1 0 0 0 0 0 0	
0 1 0 0 0 0 0 1	5QI 65
0 1 0 0 0 0 1 0	5QI 66
0 1 0 0 0 0 1 1	
to	Spare
0 1 0 0 0 1 0 0	
0 1 0 0 0 1 0 1	5QI 69
0 1 0 0 0 1 1 0	5QI 70
0 1 0 0 0 1 1 1	
to	Spare
0 1 0 0 1 0 1 0	
0 1 0 0 1 0 1 1	5QI 75
0 1 0 0 1 1 0 0	
to	Spare
0 1 0 0 1 1 1 0	
0 1 0 0 1 1 1 1	5QI 79
0 1 0 1 0 0 0 0	
to	Spare
0 1 1 1 1 1 1 1	
1 0 0 0 0 0 0 0	
to	Operator-specific 5Qis
1 1 1 1 1 1 1 0	
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 5QI value (excluding the reserved 5QI values) that it does not understand, the UE shall choose a 5QI value from the set of 5QI values defined in this version of the protocol (see 3GPP TS 23.501 [8]) and associated with:

- GBR QoS flows, if the QoS flow includes a GFBR uplink parameter and a GFBR downlink parameter; and
- non-GBR QoS flows, if the QoS flow does not include a GFBR uplink parameter or does not include a GFBR downlink parameter.

The UE shall use this chosen 5QI value for internal operations only. The UE shall use the received 5QI value in subsequent NAS signalling procedures.

When the parameter identifier indicates "GFBR uplink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for uplink followed by two octets containing the value of the guaranteed flow bit rate for uplink.
Unit of the guaranteed flow bit rate for uplink (octet 1)
Bits
8 7 6 5 4 3 2 1

0 0 0 0 0 0 0 0	value is not used
0 0 0 0 0 0 0 1	value is incremented in multiples of 1 Kbps
0 0 0 0 0 0 1 0	value is incremented in multiples of 4 Kbps

0 0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps
0 0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps
0 0 0 0 0 0 1 0 1 value is incremented in multiples of 256 Kbps
0 0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps
0 0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps
0 0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps
0 0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps
0 0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps
0 0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps
0 0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps
0 0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps
0 0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps
0 0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps
0 0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps
0 0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps
0 0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps
0 0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps
0 0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps
0 0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps
0 0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps
0 0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps
0 0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps
0 0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps
Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol.

Value of the guaranteed flow bit rate for uplink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for uplink in units defined by the unit of the guaranteed flow bit rate for uplink.

When the parameter identifier indicates "GFBR downlink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for downlink followed by two octets containing the value of the guaranteed flow bit rate for downlink.

Unit of the guaranteed flow bit rate for downlink (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.

Value of the guaranteed flow bit rate for downlink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for downlink in units defined by the unit of the guaranteed flow bit rate for downlink.

When the parameter identifier indicates "MFBR uplink", the parameter contents field contains the one octet indicating the unit of the maximum flow bit rate for uplink followed by two octets containing the value of maximum flow bit rate for uplink.

Unit of the maximum flow bit rate for uplink (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.

Value of the maximum flow bit rate for uplink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for uplink in units defined by the unit of the maximum flow bit rate for uplink.

When the parameter identifier indicates "MFBR downlink", the parameter contents field contains one octet indicating the unit of the maximum flow bit rate for downlink followed by two octets containing the value of the maximum flow bit rate for downlink.

Unit of the maximum flow bit rate for downlink (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.

Value of the maximum flow bit rate for downlink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for downlink in units defined by the unit of the maximum flow bit rate for downlink.

When the parameter identifier indicates "averaging window", the parameter contents field contains the binary representation of the averaging window for both uplink and downlink in milliseconds and the parameter contents field is two octets in length.

When the parameter identifier indicates EPS bearer identity, the length of EPS bearer identity is one octet and parameter contents field is coded as specified in subclause 9.3.2 of 3GPP TS 24.301 [15] (see NOTE 2). The UE shall not include the EPS bearer identity parameter in any UE initiated 5GSM messages.
NOTE 1: A packet filter with the "bidirectional" packet filter direction is used both as a packet filter with the "downlink only" packet filter direction and a packet filter with the "uplink only" packet filter direction. NOTE 2: The total number of EPS bearer identities included in all QoS rules of a UE cannot exceed eleven.

9.10.4.10 Session-AMBR

The purpose of the Session-AMBR information element is to indicate the initial subscribed PDU session aggregate maximum bit rate when the UE establishes a PDU session or to indicate the new subscribed PDU session aggregate maximum bit rate if it is changed by the network.

The Session-AMBR information element is coded as shown in figure 9.10.4.10.1 and table 9.10.4.10.1.

The Session-AMBR is a type 4 information element with a length of 8 octets.

8	7	6	5	4	3	2	1	
Session-AMBR IEI								octet 1
Length of Session-AMBR contents								octet 2
Unit for Session-AMBR for downlink								octet 3
Session-AMBR for downlink								octet 4-5
Unit for Session-AMBR for uplink								octet 6
Session-AMBR for uplink								octet 7-8

Figure 9.10.4.10.1: Session-AMBR information element

Table 9.10.4.10.1: Session-AMBR information element

Unit for Session-AMBR for downlink (octet 3) 0 0 0 0 0 0 0 0 value is not used 0 0 0 0 0 0 0 1 value is incremented in multiples of 1 Kbps 0 0 0 0 0 0 1 0 value is incremented in multiples of 4 Kbps 0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps 0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps 0 0 0 0 0 1 0 1 value is incremented in multiples of 256 kbps 0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps 0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps 0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps 0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps 0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps 0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps 0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps 0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps 0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps 0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps 0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps 0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps 0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps 0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps 0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps 0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps 0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps 0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps 0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps 0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol. Session-AMBR for downlink (octets 4 and 5) Octets 4 and 5 represent the binary coded value of PDU session aggregated maximum bit rate for downlink in units defined by octet 3. Unit for Session-AMBR for uplink (octet 6) The coding is identical to the unit coding defined for Session-AMBR for downlink (octet 3) Session-AMBR for uplink (octets 7 and 8) Octets 7 and 8 represent the binary coded value of PDU session aggregated maximum bit rate for uplink in units defined by octet 6.

9.10.4.11 SM PDU DN request container

The SM PDU DN request container contains a DN-specific identity of the UE in the network access identifier (NAI) format.

9.10.4.12 SSC mode

The purpose of the SSC mode information element is to indicate SSC mode.

The SSC mode information element is coded as shown in figure 9.10.4.12.1 and table 9.10.4.12.1.

The SSC mode is a type 1 information element.

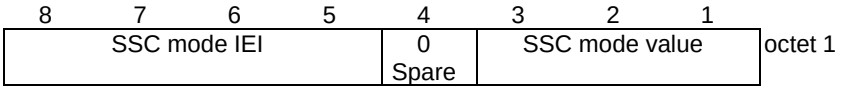


Figure 9.10.4.12.1: SSC mode information element

Table 9.10.4.12.1: SSC mode information element

SSC mode value (octet 1, bit 1 to bit 4)			
Bits			
3	**2**	**1**	
0	0	1	SSC mode 1
0	1	0	SSC mode 2
0	1	1	SSC mode 3
1	0	0	unused; shall be interpreted as "SSC mode 1", if received by the network
1	0	1	unused; shall be interpreted as "SSC mode 2", if received by the network
1	1	0	unused; shall be interpreted as "SSC mode 3", if received by the network
All other values are reserved.			

9.11 3GPP specific coding information defined within present document

9.11.1 Serving network name (SNN)

The serving network name (SNN) is used in the network name field of the AT_KDF_INPUT attribute defined in IETF RFC 5448 [40].

SNN shall take the generic format of an octet string without terminating null characters.

SNN is of maximum length of 1020 octets.

SNN consists of SNN-prefix and SNN-value, delimited by a colon.

SNN-value identifies the serving PLMN.

MCC and MNC in the SNN-PLMN-ID are MCC and MNC of the serving PLMN. If the MNC of the serving PLMN has two digits, then a zero is added at the beginning.

ABNF syntax of SNN is specified in table 9.11.1.1

Table 9.11.1.1: ABNF syntax of SNN

```
SNN = SNN-prefix ":" SNN-value
SNN-prefix = %x35.47 ; "5G"
SNN-value = SNN-PLMN-ID
SNN-PLMN-ID = SNN-mnc-string SNN-mnc-digits "." SNN-mcc-string SNN-mcc-digits "." SNN-3gppnetwork-
string "." SNN-org-string

SNN-mnc-digits = DIGIT DIGIT DIGIT ; MNC of the PLMN ID
SNN-mcc-digits = DIGIT DIGIT DIGIT ; MCC of the PLMN ID
SNN-mnc-string = %x6d.6e.63 ; "mnc" in lower case
SNN-mcc-string = %x6d.63.63 ; "mcc" in lower case
SNN-3gppnetwork-string = %x33.67.70.70.6e.65.74.77.6f.72.6b ; "3gppnetwork" in lower case
SNN-org-string = %x6f.72.67 ; "org" in lower case
```

NOTE: SNN-prefix allows for distinguishing of ANID specified in 3GPP TS 24.302 [16] and SNN as either of SNN or ANID can be carried in the AT_KDF_INPUT attribute.

EXAMPLE: If PLMN ID contains MCC = 234 and MNC = 15, SNN is 5G:mnc015.mcc234.3gppnetwork.org.

10 List of system parameters

10.1 General

10.2 Timers of 5GS mobility management

Timers of 5GS mobility management are shown in table 10.2.1 and table 10.2.2

Table 10.2.1: Timers of 5GS mobility management – UE side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T3510	15s	5GMM-REGISTERED-INITIATED	Transmission of REGISTRATION REQUEST message	REGISTRATION ACCEPT message received or REGISTRATION REJECT message received	Start T3511 or T3502 as specified in subclause 5.5.1.2.7 if T3510 expired during registration procedure for initial registration. Start T3511 or T3502 as specified in subclause 5.5.1.3.6 if T3510 expired during the registration procedure for mobility and periodic registration update
T3502	Default 12 min. NOTE 1	5GMM-REGISTERED	At registration failure and the attempt counter is equal to 5	Transmission of REGISTRATION REQUEST message	Initiation of the registration procedure, if still required
T3511	10s	5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE	At registration failure due to lower layer failure, T3510 timeout or registration rejected with other 5GMM cause values than those treated in subclause 5.5.1.2.5 for initial registration or subclause 5.5.1.3.5 for mobility and periodic registration	Transmission of REGISTRATION REQUEST message	Retransmission of the REGISTRATION REQUEST, if still required
T3512	Default 54 min NOTE 1	5GMM-REGISTERED	In 5GMM-REGISTERED, when 5GMM-CONNECTED mode is left	When entering state 5GMM-DEREGISTERED or when entering 5GMM-CONNECTED mode	Initiation of the periodic registration procedure if the UE is not registered for emergency services. Locally deregister if the UE is registered for emergency services
T3516	30s	5GMM-REGISTERED-INITIATED 5GMM-REGISTERED 5GMM-DEREGISTERED-INITIATED 5GMM-SERVICE-REQUEST-INITIATED	RAND and RES stored as a result of an 5G authentication challenge	SECURITY MODE COMMAND received SERVICE REJECT received REGISTRATION ACCEPT received AUTHENTICATION REJECT received AUTHENTICATION FAILURE sent 5GMM-DEREGISTERED, 5GMM-NULL or 5GMM-IDLE mode entered	Delete the stored RAND and RES

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T3517	15s	5GMM-SERVICE-REQUEST-INITIATED	Transmission of SERVICE REQUEST message	SERVICE ACCEPT message received, or SERVICE REJECT message received	Abort the procedure
T3519	60s	5GMM-REGISTERED-INITIATED	Transmission of IDENTITY RESPONSE message with freshly generated SUCI	REGISTRATION ACCEPT message with new 5G-GUTI received CONFIGURATION UPDATE COMMAND message with new 5G-GUTI received	Delete stored SUCI
T3520	15s	5GMM-REGISTERED-INITIATED 5GMM-DEREGISTERED-INITIATED 5GMM-SERVICE-REQUEST-INITIATED	Transmission of AUTHENTICATION FAILURE message with any of the 5GMM cause #20, #21 , #26 or #29	AUTHENTICATION REQUEST message received or AUTHENTICATION REJECT message received or SECURITY MODE COMMAND message received when entering 5GMM-IDLE mode indication of transmission failure of AUTHENTICATION FAILURE message from lower layers	On first expiry, the UE should consider the network as false and follow item g of subclause 5.4.1.3.7, if the UE is not registered for emergency services. On first expiry, the UE will follow subclause 5.4.1.3.7 under "For items c, d, e and f:", if the UE is registered for emergency services.
T3521	15s	5GMM-DEREGISTERED-INITIATED	Transmission of DEREGISTRATION REQUEST message when de-registration procedure is not due to a "switch off"	DEREGISTRATION ACCEPT message received	Retransmission of DEREGISTRATION REQUEST message
T3540	10s	5GMM-REGISTERED-INITIATED 5GMM-DEREGISTERED-INITIATED 5GMM-SERVICE-REQUEST-INITIATED	REGISTRATION REJECT message or DEREGISTRATION REQUEST message received with any of the 5GMM cause #7, #11, #12 or #13 SERVICE REJECT message received with any of the 5GMM cause #7, #11, #12 or #13	N1 NAS signalling connection released PDU sessions have been set up	Release the NAS signalling connection for the cases a) and b) as described in subclause 5.3.1.2
		5GMM-DEREGISTERED 5GMM-DEREGISTERED. NORMAL-SERVICE	REGISTRATION REJECT message or SERVICE REJECT message received with the 5GMM cause #9 or #10	N1 NAS signalling connection released	Release the NAS signalling connection for the cases c) as described in subclause 5.3.1.2 and initiation of the registration procedure as specified in subclause 5.5.1.2.2 or 5.5.1.3.2

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
Non-3GPP de-registration timer	Default 54 min. NOTE 1 NOTE 2	All 5GMM state over non-3GPP access except 5GMM-DEREGISTERED over non-3GPP access	Entering 5GMM-IDLE mode over non-3GPP access	N1 NAS signalling connection over non-3GPP access established or when entering state 5GMM-DEREGISTERED over non-3GPP access	Implicitly de-register the UE for non-3GPP access on 1st expiry

NOTE 1: The value of this timer is provided by the network operator during the registration procedure.
NOTE 2: The default value of this timer is used if the network does not indicate a value in the REGISTRATION ACCEPT message and the UE does not have a stored value for this timer.

Editor's note: The exact default value of the non-3GPP de-registration timer is FFS.

Table 10.2.2: Timers of 5GS mobility management – AMF side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
T3550	6s	5GMM-COMMON-PROCEDURE-INITIATED	Transmission of REGISTRATION ACCEPT message at initial registration. Transmission of REGISTRATION ACCEPT message with 5G-GUTI at mobility or periodic registration	REGISTRATION COMPLETE message received	Retransmission of REGISTRATION ACCEPT message
T3560	6s	5GMM-COMMON-PROCEDURE-INITIATED	Transmission of AUTHENTICATION REQUEST message Transmission of SECURITY MODE COMMAND message	AUTHENTICATION RESPONSE message received AUTHENTICATION FAILURE message received SECURITY MODE COMPLETE message received SECURITY MODE REJECT message received	Retransmission of AUTHENTICATION REQUEST message or SECURITY MODE COMMAND message
T3570	6s	5GMM-COMMON-PROCEDURE-INITIATED	Transmission of IDENTITY REQUEST message	IDENTITY RESPONSE message received	Retransmission of IDENTITY REQUEST message
T3513	NOTE 4	5GMM-REGISTERED	Paging procedure initiated	Paging procedure completed as specified in subclause 5.6.2.2.1	Network dependent
T3522	6s	5GMM-DEREGISTERED-INITIATED	Transmission of DEREGISTRATION REQUEST message	DEREGISTRATION ACCEPT message received	Retransmission of DEREGISTRATION REQUEST message
T3555	6s	5GMM-REGISTERED	Transmission of CONFIGURATION UPDATE COMMAND message with Acknowledgement requested flag IE	CONFIGURATION UPDATE COMPLETE message received	Retransmission of CONFIGURATION UPDATE COMMAND message
T3565	6s	5GMM-REGISTERED	Transmission of NOTIFICATION message	SERVICE REQUEST message received NOTIFICATION RESPONSE message received	Retransmission of NOTIFICATION message
Mobile reachable timer	NOTE 1	All except 5GMM-DEREGISTERED	Entering 5GMM-IDLE mode	N1 NAS signalling connection established	Network dependent, but typically paging is halted on 1st expiry, and start implicit de-registration timer, if the UE is not registered for emergency services. Implicitly de-register the UE which is registered for emergency services
Implicit de-registration timer	NOTE 2	All except 5GMM-DEREGISTERED	The mobile reachable timer expires while the network is in 5GMM-IDLE mode	N1 NAS signalling connection established	Implicitly detach the UE on 1st expiry

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON EXPIRY
Non-3GPP implicit de-registration timer	NOTE 3	All except 5GMM-DEREGISTERED	Entering 5GMM-IDLE mode over non-3GPP access	N1 NAS signalling connection over non-3GPP access established	Implicitly de-register the UE for non-3GPP access on 1st expiry
NOTE 1: The default value of this timer is 4 minutes greater than T3512. If the UE is registered for emergency services, the value of this timer is set equal to T3512.					
NOTE 2: The value of this timer is network dependent. If MICO is activated, the default value of this timer is 4 minutes greater than T3512.					
NOTE 3: The value of this timer is network dependent. The default value of this timer is 4 minutes greater than the non-3GPP de-registration timer.					
NOTE 4: The value of this timer is network dependent.					

10.3 Timers of 5GS session management

Timers of 5GS session management are shown in table 10.3.1 and table 10.3.2.

Table 10.3.1: Timers of 5GS session management – UE side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3580	TBD	TBD	Transmission of PDU SESSION ESTABLISHMENT REQUEST message	PDU SESSION ESTABLISHMENT ACCEPT message received or PDU SESSION ESTABLISHMENT REJECT message received	Retransmission of PDU SESSION ESTABLISHMENT REQUEST message
T3581	TBD	TBD	Transmission of PDU SESSION MODIFICATION REQUEST message	PDU SESSION MODIFICATION COMMAND message with the same PTI is received or PDU SESSION MODIFICATION REJECT message received	Retransmission of PDU SESSION MODIFICATION REQUEST message
T3582	TBD	TBD	Transmission of PDU SESSION RELEASE REQUEST message	PDU SESSION RELEASE COMMAND message with the same PTI is received or PDU SESSION RELEASE REJECT message received	Retransmission of PDU SESSION RELEASE REQUEST message
T3583	Default 1 min. NOTE 2	PDU SESSION ACTIVE	UE creates or updates a derived QoS rule	UE deletes the derived QoS rule (see subclause 6.2.5.1.4.5)	On 1st expiry: Deletion of the derived QoS rule
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 network may provide the value of this timer applicable to the derived QoS rules of a specific PDU session as RQ timer value in the PDU SESSION ESTABLISHMENT ACCEPT message and PDU SESSION MODIFICATION COMMAND message. The maximum value of the timer is 30 min. If the network indicates a value greater than the maximum value, then the UE shall use the maximum value.					

Table 10.3.2: Timers of 5GS session management – SMF side

TIMER NUM.	TIMER VALUE	STATE	CAUSE OF START	NORMAL STOP	ON THE 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3590	TBD	TBD	Transmission of PDU SESSION AUTHENTICATION COMMAND message	PDU SESSION AUTHENTICATION COMPLETE message received	Retransmission of PDU SESSION AUTHENTICATION COMMAND message
T3591	TBD	TBD	Transmission of PDU SESSION MODIFICATION COMMAND message	PDU SESSION MODIFICATION COMPLETE message received or PDU SESSION MODIFICATION COMMAND REJECT message received	Retransmission of PDU SESSION MODIFICATION COMMAND message
T3592	TBD	TBD	Transmission of PDU SESSION RELEASE COMMAND message	PDU SESSION RELEASE COMPLETE message received or N1 SM delivery skipped indication received	Retransmission of PDU SESSION RELEASE COMMAND message
T3593	TBD (NOTE 2)	TBD	Reception of PDU SESSION MODIFICATION COMPLETE message for transmitted PDU SESSION MODIFICATION COMMAND message where the PDU SESSION MODIFICATION COMMAND message included 5GSM cause #39	PDU SESSION RELEASE REQUEST message received	Network-requested PDU session release procedure performed

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: If the PDU Session Address Lifetime value is sent to the UE in the PDU SESSION MODIFICATION COMMAND message then timer T3593 shall be started with the same value, otherwise it shall use a default value.

Annex A (informative): Cause values for 5GS mobility management

A.1 Causes related to UE identification

Cause #3 – Illegal UE

This 5GMM 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.

Cause #6 – Illegal ME

This 5GMM 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 5GMM cause is sent to the UE when the network cannot derive the UE's identity from the 5G-GUTI or 5G-S-TMSI because of e.g. no matching identity/context in the network, failure to validate the UE's identity due to integrity check failure of the received message.

Cause #10 – Implicitly de-registered

This 5GMM cause is sent to the UE either if the network has implicitly de-registered the UE, e.g. after the implicit de-registration timer has expired, or if the 5GMM context data related to the subscription does not exist in the AMF e.g. because of a AMF restart, or because of a registration request for mobility or registration update is routed to a new AMF.

A.2 Cause related to subscription options

Cause #5 – PEI not accepted

This cause is sent to the UE if the network does not accept an initial registration procedure for emergency services using a PEI.

Cause #7 – 5GS services not allowed

This 5GMM cause is sent to the UE when it is not allowed to operate 5GS services.

Cause #11 – PLMN not allowed

This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, 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 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a tracking area where the HPLMN determines that the UE, by subscription, is not allowed to operate.

NOTE 1: If 5GMM 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 5GMM cause is sent to a UE which requests service, or if the network initiates a de-registration request, in a tracking area of a PLMN which by subscription offers roaming to that UE but not in that tracking area.

Cause #27 – N1 mode not allowed

This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a PLMN where the UE by subscription, is not allowed to operate in N1 mode.

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

Cause #20 – MAC failure

This 5GMM cause is sent to the network if the USIM detects that the MAC in the AUTHENTICATION REQUEST message is not fresh.

Cause #21 – Synch failure

This 5GMM cause is sent to the network if the USIM detects that the SQN in the AUTHENTICATION REQUEST message is out of range.

Cause #22 – Congestion

This 5GMM 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 5GMM 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 5GMM cause is sent to the network if the security mode command is rejected by the UE for unspecified reasons.

Cause #26 – Non-5G authentication unacceptable

This 5GMM cause is sent to the network in N1 mode if the "separation bit" in the AMF field of AUTN is set to 0 in the AUTHENTICATION REQUEST message (see 3GPP TS 33.501 [24]).

Cause #28 – Restricted service area

This 5GMM cause is sent to the UE if it requests service in a tracking area which is a part of the UE's non-allowed area or is not a part of the UE's allowed area.

Cause #29 – ngKSI already in use

This 5GMM cause is sent to the network in N1 mode if the ngKSI value received in the AUTHENTICATION REQUEST message is already associated with one of the 5G security contexts stored in the UE.

Cause #43 – LADN not available

This 5GMM cause is sent to the UE if the user-plane resources of the PDU session are not activated when the UE is located outside the LADN service area.

Cause #67 – Insufficient resources for specific slice and DNN

This 5GMM cause is sent by the network to indicate that the requested service cannot be provided due to insufficient resources for specific slice and DNN.

Cause #69 – Insufficient resources for specific slice

This 5GMM cause is sent by the network to indicate that the requested service cannot be provided due to insufficient resources for specific slice.

A.4 Causes related to invalid messages

Cause #95 – Semantically incorrect message

This 5GMM cause is used to report receipt of a message with semantically incorrect contents.

Cause #96 – Invalid mandatory information

This cause 5GMM indicates that the equipment sending this 5GMM cause has received a message with a non-semantical mandatory IE error.

Cause #97 – Message type non-existent or not implemented

This 5GMM cause indicates that the equipment sending this 5GMM 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 5GMM cause.

Cause #98 – Message type not compatible with protocol state

This 5GMM cause indicates that the equipment sending this 5GMM cause has received a message not compatible with the protocol state.

Cause #99 – Information element non-existent or not implemented

This 5GMM cause indicates that the equipment sending this 5GMM 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 5GMM cause. However, the information element is not required to be present in the message in order for the equipment sending the 5GMM cause to process the message.

Cause #100 – Conditional IE error

This 5GMM 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 5GMM cause indicates that a message has been received which is incompatible with the protocol state.

Cause #111 – Protocol error, unspecified

This 5GMM cause is used to report a protocol error event only when no other 5GMM cause in the protocol error class applies.

Annex B (informative): Cause values for 5GS session management

B.1 Causes related to nature of request

Cause #26 – Insufficient resources

This 5GSM cause is used by the UE or by the network to indicate that the requested service cannot be provided due to insufficient resources.

Cause #27 – Missing or unknown DNN

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN because the DNN was not included although required or if the DNN could not be resolved.

Cause #28 – Unknown PDU session type

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN because the requested PDU session type could not be recognised or is not allowed.

Cause #29 – User authentication or authorization failed

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN due to a failed user authentication or revoked by the external DN or revoked by the external packet data network.

Cause #31 – Request rejected, unspecified

This 5GSM cause is used by the network or by the UE to indicate that the requested service or operation or the request for a resource was rejected due to unspecified reasons.

Cause #34 – Service option temporarily out of order

This 5GSM cause is sent when the network cannot serve the request because of temporary outage of one or more functions required for supporting the service.

Cause #35 – PTI already in use

This 5GSM 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 5GSM cause is used to indicate a regular UE or network initiated release of PDU session resources.

Cause #39 – Reactivation requested

This 5GSM cause is used by the network to request a PDU session reactivation.

Cause #43 –Invalid PDU session identity

This 5GSM cause is used by the network or the UE to indicate that the PDU session identity value provided to it is not a valid value or the PDU session context identified by the PDU session identity IE in the request or the command is not active.

Cause #50 – PDU session type IPv4 only allowed

This 5GSM cause is used by the network to indicate that only PDU session type IPv4 is allowed for the requested IP connectivity.

Cause #51 – PDU session type IPv6 only allowed

This 5GSM cause is used by the network to indicate that only PDU session type IPv6 is allowed for the requested IP connectivity.

Cause #54 –PDU session does not exist

This 5GSM cause is used by the network to indicate that the network does not have any information about the PDU session which is requested by the UE to transfer between 3GPP access and non-3GPP access or from the EPS to the 5GS.

Cause #67 – Insufficient resources for specific slice and DNN

This 5GSM cause is by the network to indicate that the requested service cannot be provided due to insufficient resources for specific slice and DNN.

Cause #68 – Not supported SSC mode

This 5GSM cause is used by the network to indicate that the requested SSC mode is not supported.

Cause #69 –Insufficient resources for specific slice

This 5GSM cause is used by the network to indicate that the requested service cannot be provided due to insufficient resources for specific slice.

Cause #70 – Missing or unknown DNN in a slice

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN because the DNN was not included although required or if the DNN could not be resolved, in the slice.

Cause #81 – Invalid PTI value

This 5GSM cause is used by the network or UE to indicate that the PTI provided to it is unassigned or reserved.

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

Cause #95 – Semantically incorrect message

This 5GSM cause is used to report receipt of a message with semantically incorrect contents.

Cause #96 – Invalid mandatory information

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message with a non-semantical mandatory IE error.

Cause #97 – Message type non-existent or not implemented

This 5GSM cause indicates that the equipment sending this 5GSM 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 5GSM cause.

Cause #98 – Message type not compatible with protocol state

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message not compatible with the protocol state.

Cause #99 – Information element non-existent or not implemented

This 5GSM cause indicates that the equipment sending this 5GSM 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 5GSM cause. However, the information element is not required to be present in the message in order for the equipment sending the 5GSM cause to process the message.

Cause #100 – Conditional IE error

This 5GSM 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 5GSM cause indicates that a message has been received which is incompatible with the protocol state.

Cause #111 – Protocol error, unspecified

This 5GSM cause is used to report a protocol error event only when no other 5GSM cause in the protocol error class applies.

Annex C (normative): Storage of 5GMM information

The following 5GMM parameters shall be stored on the USIM if the corresponding file is present:

a) 5G-GUTI;

b) last visited registered TAI;

c) 5GS update status; and

d) 5G NAS security context parameters from a full native 5G NAS security context (see 3GPP TS 33.501 [24]).

The presence and format of corresponding files on the USIM is specified in 3GPP TS 31.102 [22].

If the corresponding file is not present on the USIM, these 5GMM parameters are stored in a non-volatile memory in the ME together with the SUPI from the USIM. These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

The following 5GMM parameters shall be stored in a non-volatile memory in the ME together with the SUPI from the USIM:

- configured NSSAI(s).

Each configured NSSAI consists of S-NSSAIs stored together with a PLMN identity, if it is associated with a PLMN. The configured NSSAI(s) can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME; else the UE shall delete the configured NSSAI(s).

If the UE is registered for emergency services, the UE shall not store the 5GMM 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 deregistered.

If the UE is configured for eCall only mode as specified in 3GPP TS 31.102 [22], the UE shall not store the 5GMM 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 enters 5GMM-DEREGISTERED.eCALL-INACTIVE state, the UE is switched-off or the USIM is removed.

Annex D (normative): UE policy delivery protocol

D.1 General

The PCF can provide the UE with one or more UE policies using the network-requested UE policy management procedure. The PCF provides each UE policy using one or more UE policy sections, each identified by a UE policy section identifier (UPSI). The UPSI is composed of two parts:

a) a PLMN ID part containing the PLMN ID for the PLMN of the PCF which provides the UE policies; and

b) a UE policy section code (UPSC) containing a value assigned by the PCF.

The UE processes the UE policy sections, each identified by the UPSI, received from the PCF and informs the PCF of the result.

Editor's note: How the PCF decides whether to divide a UE policy into UE policy sections needs to be specified by CT3.

The message coding rules for the messages exchanged between the UE and the PCF for UE policy delivery are specified in subclause D.4.

D.2 Procedures

D.2.1 Network-requested UE policy management procedure

D.2.1.1 General

The purpose of the network-requested UE policy management procedure is to enable the network to:

a) send one or more new UE policy sections to the UE;

b) modify one or more UE policy sections stored at the UE; or

c) delete one or more UE policy sections stored at the UE.

D.2.1.2 Network-requested UE policy management procedure initiation

In order to initiate the network-requested UE policy management procedure, the PCF shall:

a) encode the information about the UE policy sections to be stored, modified or deleted in a UE policy section modification list IE as specified in subclause D.5.2 and include it in a MANAGE UE POLICY COMMAND message.

b) send the MANAGE UE POLICY COMMAND message to the UE via the AMF as specified in 3GPP TS 23.502 [9]; and

c) start timer T35xx (see example in figure D.2.2.1).

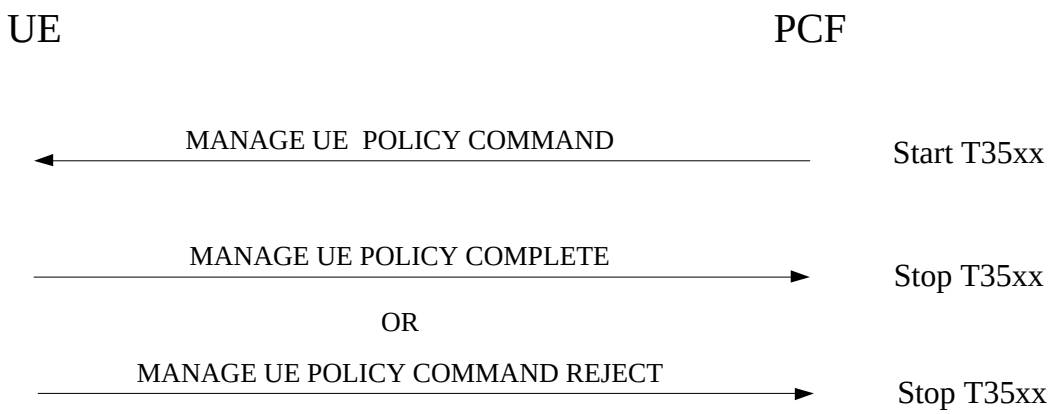


Figure D.2.2.1: Network-requested UE policy management procedure

Upon receipt of the MANAGE UE POLICY COMMAND message, for each instruction included in the UE policy section management list IE, the UE shall:

a) if the instruction indicates to store the UE policy section:

   1) attempt to delete UE policy rules and UE policy parameters stored at the UE associated with the same UPSI as the UPSI associated with the instruction, if any; and

   2) attempt to store the UE policy rules and UE policy parameters included in the UE policy section of the instruction and associate these UE policy rules and UE policy parameters with the UPSI of the instruction; and

b) if the instruction indicates to delete the UE policy section, attempt to delete UE policy rules and UE policy parameters stored at the UE associated with the same UPSI as the UPSI of the instruction, if any.

Editor's note: How the PCF indicates to the UE the operation to perform on a UE policy section is FFS, e.g. by providing an operation code, or using the UPSI.

D.2.1.3 Network-requested UE policy management procedure accepted by the UE

If all instructions included in the UE policy section management list IE were executed successfully by the UE, the UE shall:

a) create a MANAGE UE POLICY COMPLETE message; and

b) transport the MANAGE UE POLICY COMPLETE message using the NAS transport procedure as specified in subclause 5.4.5.

Upon receipt of the MANAGE UE POLICY COMPLETE message, the PCF shall stop timer T35xx.

D.2.1.4 Network-requested UE policy management procedure not accepted by the UE

If the UE could not execute all instructions included in the UE policy section management list IE successfully, the UE shall:

a) encode the UPSI associated with the instructions which could not be executed successfully and the associated UE Policy Delivery Protocol (UPDP) cause indicating the cause of the failure in a UE policy section management result IE as specified in subclause D.5.3 and include it in a MANAGE UE POLICY COMMAND REJECT message, and

b) transport the MANAGE UE POLICY COMMAND REJECT message using the NAS transport procedure as specified in subclause 5.4.5.

Upon receipt of the MANAGE UE POLICY COMMAND REJECT message, the PCF shall stop timer T35xx.

Editor's note: Further actions at the PCF upon receiving a MODIFY UE POLICY COMMAND REJECT message from the UE need to be specified by CT3.

Upon receipt of the N15 indication that the UE is not reachable, the PCF shall stop the T35xx.

Editor's note: Further actions at the PCF upon receiving the N15 indication that the UE is not reachable need to be specified by CT3.

D.2.1.5 Abnormal cases on the network side

Editor's note: Abnormal cases are FFS.

D.2.1.6 Abnormal cases in the UE

Editor's note: Abnormal cases are FFS.

D.2.2 UE-initiated UPSI list transport procedure

D.2.2.1 General

The purpose of the UE-initiated UPSI list transport procedure is to deliver the UPSI(s) of the UE policy section(s) stored in the UE to the PCF if the UE has one or more stored UE policy sections.

D.2.2.2 UE-initiated UPSI list transport procedure initiation

In order to initiate the UE-initiated UPSI list transport procedure, the UE shall create a UPSI LIST TRANSPORT message. The UE shall:

a) allocate a PTI value currently not used and set the PTI IE to the allocated PTI value; and

b) include the UPSI(s) of the UE policy section(s) available in the UE in the UPSI list IE.

The UE shall send the UPSI LIST TRANSPORT message (see example in figure D.2.2.2.1). The UE shall transport the created UPSI LIST TRANSPORT message using the registration procedure (see subclause 5.5.1).

Figure D.2.2.2.1: UE-initiated UPSI list transport procedure

D.2.2.3 UE-initiated UPSI list transport procedure accepted by the network

Upon receipt of the UPSI LIST TRANSPORT message, the PCF shall operate as described in 3GPP TS 23.502 [9] and 3GPP TS 29.507 [21].

D.2.2.4 Abnormal cases on the network side

Editor's note: Abnormal cases are FFS.

D.3 UE policy re-assembly at the UE

When the UE needs to apply ANSDP as specified in 3GPP TS 24.502 [18], the UE shall consider all UE policy parts with ANSDP contents currently stored at the UE.

When the UE needs to apply URSP as specified in 3GPP TS 24.5xx [19], the UE shall consider all UE policy parts with URSP contents currently stored at the UE.

Editor's note: The reference to 3GPP TS 24.5xx needs to be replaced with a reference to the correct TS number for UE policies in 5GS once the TS number is allocated.

D.4 Message coding rules

Editor's note: The message coding rules for the messages exchanged between the UE and the PCF for UE policy delivery protocol are FFS.

D.5 Message functional definition and contents

D.5.1 Manage UE policy command

D.5.1.1 Message definition

The MANAGE UE POLICY COMMAND message is sent by the PCF to the UE to request the UE to manage UE policy sections. See table D.5.1.1.1

Message type: MANAGE UE POLICY COMMAND

Significance: dual

Direction: network to UE

Table D.5.1.1.1: MANAGE UE POLICY COMMAND message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	PTI	Procedure transaction identity 9.6,	M	V	1
	MANAGE UE POLICY COMMAND message identity	UE policy delivery protocol message type D.6.1	M	V	1
	UE policy section management list	UE policy section management list D.6.2	M	LV-E	3-65538

D.5.2 Manage UE policy complete

D.5.2.1 Message definition

The MANAGE UE POLICY COMPLETE message is sent by the UE to the PCF to report that all received instructions have been successfully executed at the UE. See table D.5.2.1.1

Message type: MANAGE UE POLICY COMPLETE

Significance: dual

Direction: UE to network

Table D.5.2.1.1: MANAGE UE POLICY COMPLETE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	PTI	Procedure transaction identity 9.6,	M	V	1
	MANAGE UE POLICY COMPLETE message identity	UE policy delivery protocol message type D.6.1	M	V	1

D.5.3 Manage UE policy command reject

D.5.3.1 Message definition

The MANAGE UE POLICY COMMAND REJECT message is sent by the UE to the PCF to report that one or more instructions could not be successfully executed at the UE. See table D.5.3.1.1

Message type: MANAGE UE POLICY COMMAND REJECT

Significance: dual

Direction: UE to network

Table D.5.3.1.1: MANAGE UE POLICY COMMAND REJECT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	PTI	Procedure transaction identity 9.6	M	V	1
	MANAGE UE POLICY COMMAND REJECT message identity	UE policy delivery protocol message type D.6.1.	M	V	1
	UE policy section management result	UE policy section management result D.6.3	M	LV-E	3-65538

D.5.4 UPSI list transport

D.5.4.1 Message definition

The UPSI LIST TRANSPORT message is sent by the UE to the PCF to deliver the UPSI(s) of the UE policy section(s) stored in the UE. See table D.5.4.1.1

Message type: UPSI LIST TRANSPORT

Significance: dual

Direction: UE to network

Table D.5.4.1.1: UPSI LIST TRANSPORT message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	PTI	Procedure transaction identity 9.6	M	V	1
	UPSI LIST TRANSPORT message identity	UE policy delivery message type D.6.1	M	V	1
	UPSI list	UPSI list D.6.4	M	TLV-E	9-65538

D.6 Information elements coding

D.6.1 UE policy delivery protocol message type

Table D.6.1.1: UE policy delivery protocol message type

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	MANAGE UE POLICY COMMAND message
0 0 0 0 0 0 1 0	MANAGE UE POLICY COMPLETE message
0 0 0 0 0 0 1 1	MANAGE UE POLICY COMMAND REJECT message
0 0 0 0 0 1 0 0	UPSI LIST TRANSPORT message
All other values are reserved	

D.6.2 UE policy section management list

The purpose of the UE policy section management list information element is to transfer from the PCF to the UE a list of instructions to be performed at the UE for management of UE policy section stored at the UE.

The UE policy section management list information element is coded as shown in figure D.6.2.1, figure D.6.2.2, figure D.6.2.3, figure D.6.2.4, figure D.6.2.5, figure D.6.2.6, figure D.6.2.7 and table D.6.2.1.

The UE policy section management list information element has a minimum length of 15 octets and a maximum length of 65538 octets.

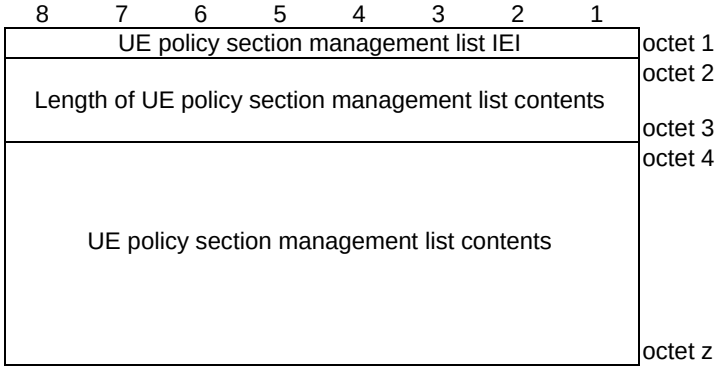


Figure D.6.2.1: UE policy section management list information element

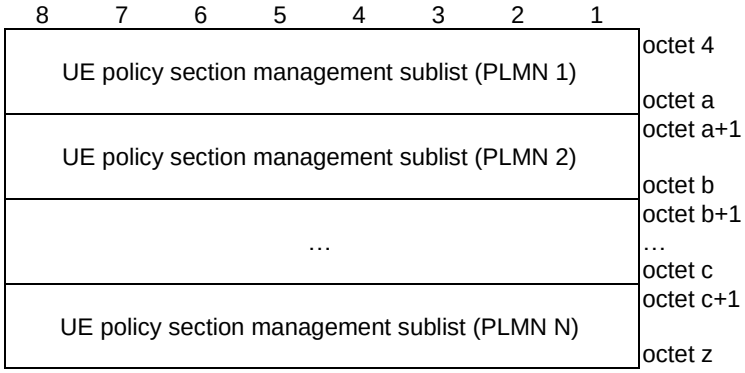


Figure D.6.2.2: UE policy section management list contents

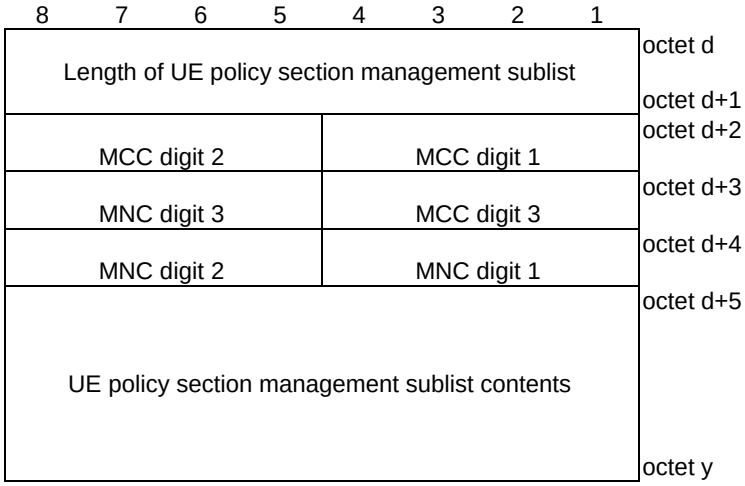


Figure D.6.2.3: UE policy section management sublist

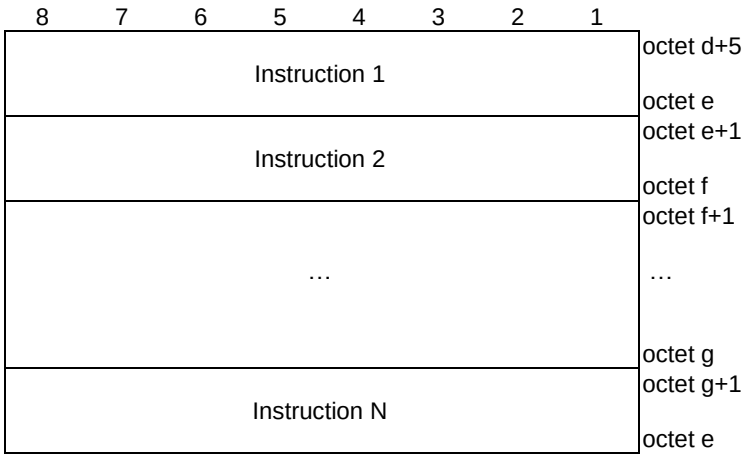


Figure D.6.2.4: UE policy section management sublist contents

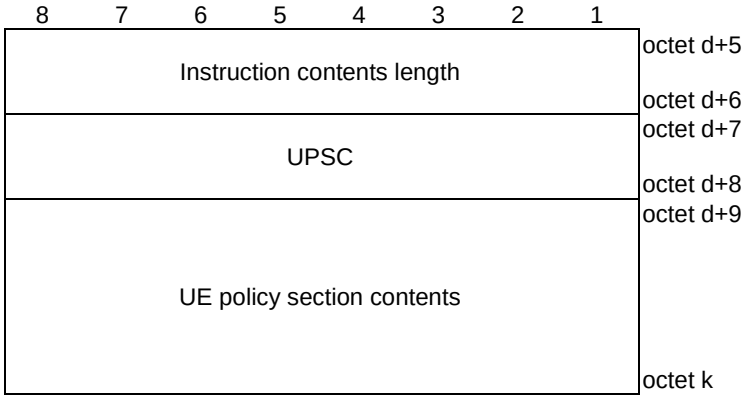


Figure D.6.2.5: Instruction

Editor's note: How the PCF indicates to the UE the operation to perform on a UE policy section is FFS, e.g. by providing an operation code, or using the UPSI.

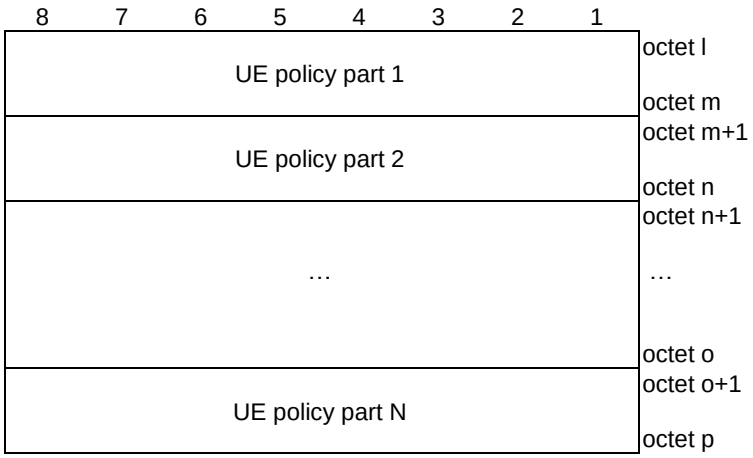


Figure D.6.2.6: UE policy section contents

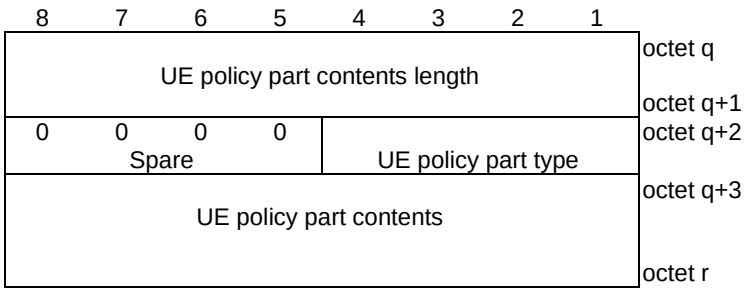


Figure D.6.2.7: UE policy part

Table D.6.2.1: UE policy section management list information element

Value part of the UE policy section management list information element (octets 4 to z)

The value part of the UE policy section management list information element consists of one or several UE policy section management sublists.

UE policy section management sublist:

Length of UE policy section management sublist (octets d to d+1)

This field contains the binary encoding of the length of the UE policy section management sublist in units of octets.

MCC, Mobile country code (octet d+2, and bits 4 to 1 of octet d+3)

The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A.

MNC, Mobile network code (bits 8 to 5 of octet d+3, and octet d+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. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111".

UE policy section management sublist contents (octets d+5 to y)

The UE policy section management sublist contents consist of one or several instructions.

Instruction:

Instruction contents length (octets d+5 to d+6)

This field contains the binary encoding of the instruction contents length in units of octets.

UPSC (octets d+7 to d+8)

This field contains the binary encoding of the UPSC. The value of the UPSC is set by the PCF.

UE policy section contents (octets d+9 to k)

The UE policy section contents consist of one or several UE policy parts.

UE policy part:

UE policy part contents length (octets q to q+1)

This field contains the binary encoding of the UE policy part contents length in units of octets.

UE policy part type (bits 4 to 1 of octet q+2)
Bits

4	**3**	**2**	**1**	
0	0	0	0	Reserved
0	0	0	1	URSP
0	0	1	0	ANDSP

All other values are reserved.

Bits 8 to 5 of octet q+2 are spare and shall be coded as zero.

UE policy part contents

This field contains a UE policy part encoded as specified in 3GPP TS 24.5xx [19].

Editor's note: The reference to 3GPP TS 24.5xx needs to be replaced with a reference to the correct TS number for UE policies in 5GGS once the TS number is allocated.

Editor's note: How the PCF indicates to the UE the operation to perform on a UE policy section is FFS, e.g. by providing an operation code, or using the UPSI.

D.6.3 UE policy section management result

The purpose of the UE policy section management result information element is to transfer from the UE to the PCF information about instructions for UE policy section management which the UE could not execute successfully.

The UE policy section management result information element is coded as shown in figure D.6.3.1, figure D.6.3.2, figure D.6.3.3, figure D.6.3.4, figure D.6.3.5 and table D.6.3.1.

The UE policy section management result information element has a minimum length of 10 octets and a maximum length of 65538 octets.

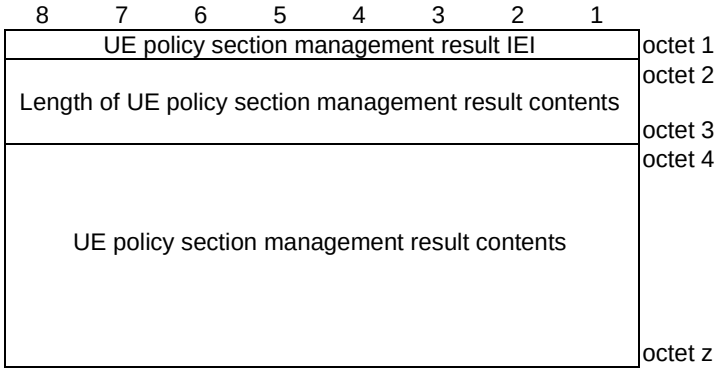


Figure D.6.3.1: UE policy section management result information element

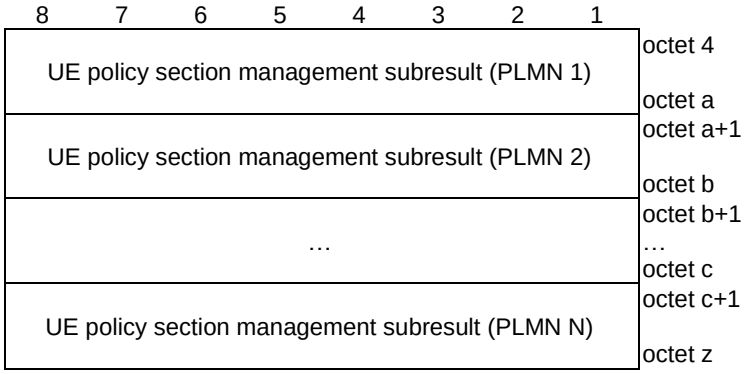


Figure D.6.3.2: UE policy section management result contents

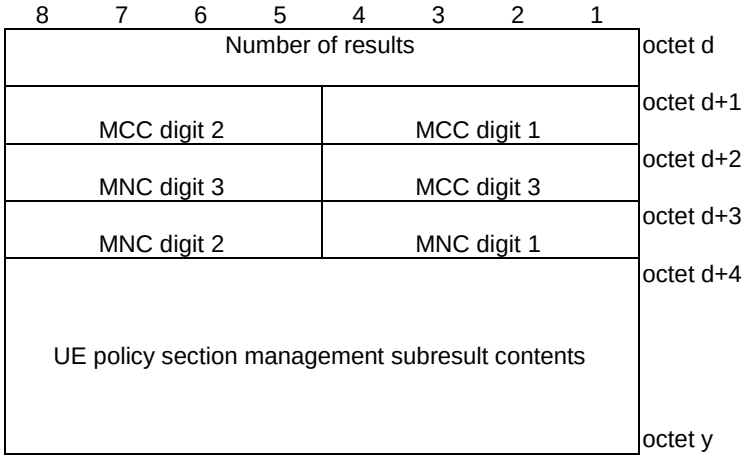


Figure D.6.3.3: UE policy section management result

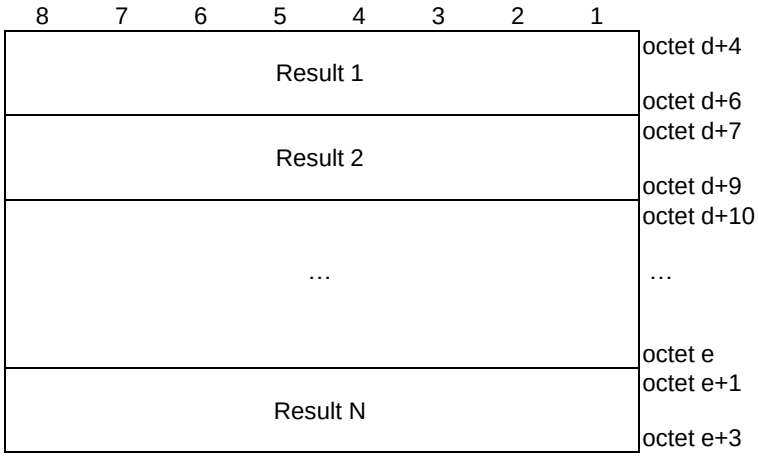


Figure D.6.3.4: UE policy section management result contents

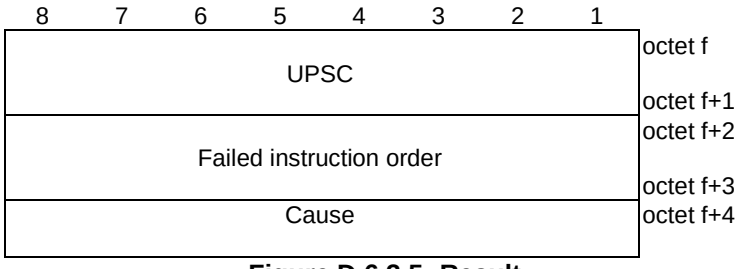


Figure D.6.3.5: Result

Table D.6.3.1: UE policy section management result information element

Value part of the UE policy section management result information element (octets 4 to z) The value part of the UE policy section management result information element consists of one or several UE policy section management subresults. UE policy section management subresult: Number of results (octet d) This field contains the binary encoding of number of results included in the UE policy section management subresult. MCC, Mobile country code (octet d+2, and bits 4 to 1 of octet d+3) The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. MNC, Mobile network code (bits 8 to 5 of octet d+3, and octet d+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. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111". UE policy section management subresult contents (octets d+4 to y) The UE policy section management subresult contents consist of one or several results. Each PSI field is 2 octet long and contains the binary encoding of a PSI. Result (octet f to f+3) UPSC (octet f to f+1) This field contains the binary encoding of the UPSC. The value of the UPSC is set by the PCF Failed instruction order (octets f+2 to f+3) This field contains the binary encoding of the order of the failed instruction in the UE policy section management sublist. Cause (octet f+4) Bits **8 7 6 5 4 3 2 1** 0 1 1 0 1 1 1 1 Protocol error, unspecified The receiving entity shall treat any other value as 0110 1111, "protocol error, unspecified".

D.6.4 UPSI list

The purpose of the UPSI list information element is to transfer from the UE to the PCF a list of UPSIs.

The UPSI list information element is coded as shown in figure D.6.4.1, figure D.6.4.2, and table D.6.4.1.

The UPSI list information element has a minimum length of 9 octets and a maximum length of 65538 octets.

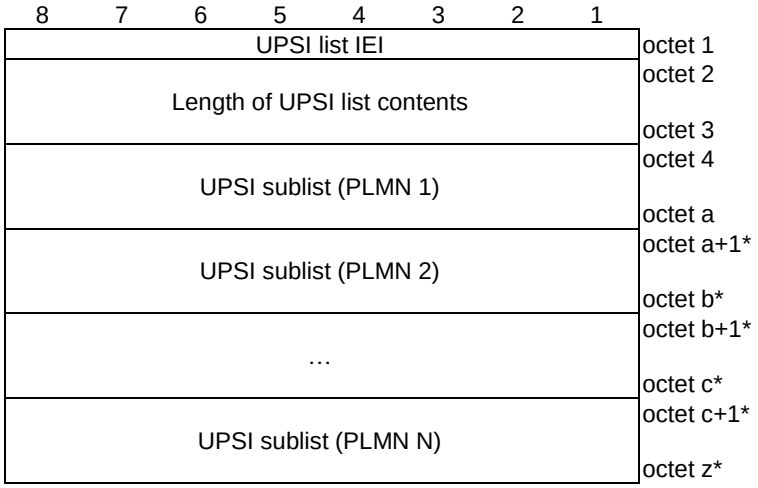


Figure D.6.4.1: UPSI list information element

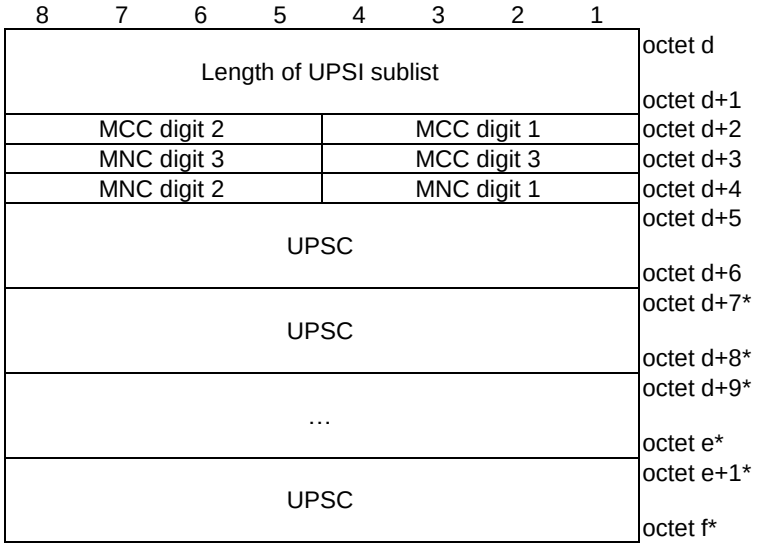


Figure D.6.4.2: UPSI sublist

Table D.6.4.1: UPSI list information element

MCC, Mobile country code (octet d+2, and bits 4 to 1 of octet d+3) The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. MNC, Mobile network code (bits 8 to 5 of octet d+3, and octet d+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. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111". UPSC (octets d+5 to d+6) This field contains the binary encoding of the UPSC. The value of the UPSC is set by the PCF.

Annex E (informative): Change history

Change history							
Date	**Meeting**	**Tdoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2017-10	CT1#106	C1-174182				Draft skeleton provided by the rapporteur.	0.0.0
2017-11	CT1#106					Implementing the following p-CRs agreed by CT1: C1-174183, C1-174184, C1-174185.	0.1.0
2017-12	CT1#107					Implementing the following p-CRs agreed by CT1: C1-175098, C1-175313. Corrections done by the rapporteur.	0.2.0
2017-12	CT1 e-mail review					Editorial corrections.	0.2.1
2017-12	CT1 e-mail review					Re-introduction of table in subclause 8.2.23.1	0.2.2
2018-02	CT1#108					Implementing the following p-CRs agreed by CT1: C1-180663, C1-180224, C1-180046, C1-180437, C1-180438, C1-180448, C1-180307, C1-180211, C1-180316, C1-180221, C1-180281, C1-180339, C1-180361, C1-180148, C1-180415, C1-180451, C1-180453, C1-180455, C1-180459, C1-180482, C1-180483, C1-180484, C1-180619, C1-180620, C1-180623, C1-180624, C1-180627, C1-180628, C1-180664, C1-180665, C1-180668, C1-180672, C1-180673, C1-180679, C1-180680, C1-180684, C1-180707, C1-180721, C1-180725, C1-180736, C1-180737, C1-180738, C1-180739, C1-180740, C1-180741, C1-180750, C1-180751, C1-180013, C1-180311, C1-180312, C1-180197, C1-180313, C1-180283, C1-180037, C1-180041, C1-180464, C1-180465, C1-180466, C1-180469, C1-180645, C1-180646, C1-180648, C1-180688, C1-180689, C1-180690, C1-180473, C1-180720, C1-180226, C1-180632, C1-180633, C1-180635, C1-180640, C1-180669, C1-180731, C1-180732, C1-180734, C1-180735, C1-180746, C1-180209, C1-180040, C1-180015, C1-180035, C1-180198, C1-180421, C1-180487, C1-180488, C1-180490, C1-180621, C1-180622, C1-180701, C1-180162, C1-180190, C1-180604, C1-180605, C1-180606, C1-180611, C1-180614, C1-180616, C1-180704, C1-180719, C1-180722, C1-180747, C1-180755, C1-180756 Corrections done by the rapporteur.	0.3.0
2018-02	CT1 e-mail review					Resolution of collision among C1-180679, C1-180721 and C1-180740. Resolution of collision among C1-180605, C1-180616 and C1-180704. Re-implementation of parts of C1-180035, C1-180488, C1-180605, C1-180606, C1-180729 and C1-180734 as some of the proposed changes were not implemented correctly in the previous version. Implementation of C1-180646 which was missed. Editorial corrections. Corrections done by the rapporteur.	0.3.1
2018-03	CT1#109					Implementing the following p-CRs agreed by CT1: C1-181362, C1-181377, C1-181456, C1-181457, C1-181703, C1-181748, C1-181462, C1-181786, C1-181168, C1-181269, C1-181278, C1-181307, C1-181180, C1-181279, C1-181280, C1-181281, C1-181354, C1-181283, C1-181284, C1-181287, C1-181305, C1-181352, C1-181364, C1-181365, C1-181366, C1-181399, C1-181466, C1-181467, C1-181468, C1-181470, C1-181471, C1-181473, C1-181474, C1-181477, C1-181628, C1-181629, C1-181633, C1-181661, C1-181663, C1-181666, C1-181668, C1-181670, C1-181681, C1-181682, C1-181683, C1-181684, C1-181695, C1-181696, C1-181707, C1-181713, C1-181715, C1-181716, C1-181717, C1-181718, C1-181733, C1-181734, C1-181735, C1-181736, C1-181737, C1-181738, C1-181739, C1-181740, C1-181741, C1-181747, C1-181752, C1-181764, C1-181770, C1-181771, C1-181781, C1-181782, C1-181785, C1-181182, C1-181120, C1-181121, C1-181395, C1-181480, C1-181482, C1-181484, C1-181485, C1-181486, C1-181487, C1-181488, C1-181650, C1-181651, C1-181652, C1-181678, C1-181726, C1-181751, C1-181273, C1-181274, C1-181276, C1-181277, C1-181496, C1-181784, C1-181312, C1-181357, C1-181605, C1-181606, C1-181609, C1-181645, C1-181674, C1-181675, C1-181677, C1-181679, C1-181708, C1-	0.4.0

						181710, C1-181728, C1-181613, C1-181615, C1-181680, C1-181750, C1-181618, C1-181619, C1-181779, C1-181360, C1-181636, C1-181640, C1-181643, C1-181729, C1-181730, C1-181731, C1-181732 Corrections done by the rapporteur.	
2018-03	CT1 e-mail review					Re-implementation of C1-181168 and C1-181307. Re-implementation of C1-181656 and C1-181606 so that C1-181656 is implemented first. Reverting to the old title. Editorial corrections of some of the implemented p-CRs as well as adding some missing parts. Corrections done by the rapporteur.	0.4.1
2018-03	CT#79	CP-180101				Version 1.0.0 created for presentation to TSG CT#79 for information.	1.0.0
2018-05	CT1#110					Implementing the following p-CRs agreed by CT1: C1-182219, C1-182493, C1-182496, C1-182202, C1-182497, C1-182053, C1-182311, C1-182019, C1-182359, C1-182360, C1-182361, C1-182358, C1-182305, C1-182306, C1-182354, C1-182117, C1-182182, C1-182455, C1-182459, C1-182491, C1-182600, C1-182601, C1-182605, C1-182606, C1-182607, C1-182608, C1-182609, C1-182610, C1-182614, C1-182615, C1-182621, C1-182662, C1-182664, C1-182665, C1-182708, C1-182728, C1-182730, C1-182733, C1-182724, C1-182757, C1-182759, C1-182760, C1-182768, C1-182772, C1-182775, C1-182786, C1-182787, C1-182791, C1-182831, C1-182832, C1-182833, C1-182834, C1-182835, C1-183836, C1-182838, C1-182840, C1-182844, C1-182067, C1-182073, C1-182303, C1-182321, C1-182352, C1-182385, C1-182645, C1-182646, C1-182647, C1-182648, C1-182650, C1-182651, C1-182657, C1-182659, C1-182660, C1-182741, C1-182742, C1-182761, C1-182762, C1-182763, C1-182764, C1-182765, C1-182774, C1-182789, C1-182789, C1-182815, C1-182845, C1-182797, C1-182232, C1-182230, C1-182666, C1-182667, C1-182671, C1-182673, C1-182677, C1-182800, C1-182824, C1-182710, C1-182072, C1-182078, C1-182174, C1-182190, C1-182456, C1-182636, C1-182637, C1-182638, C1-182639, C1-182726, C1-182729, C1-182747, C1-182749, C1-182766, C1-182767, C1-182841, C1-182847, C1-182043, C1-182057, C1-182260, C1-182044, C1-182617, C1-182618, C1-182619, C1-182620, C1-182622, C1-182623, C1-182624, C1-182627, C1-182628, C1-182629, C1-182802, C1-182808, C1-182345, C1-182461, C1-182630 Corrections done by the rapporteur.	1.1.0
2018-05	CT1 e-mail review					Re-implementation of C1-182768, C1-182841, C1-182841, C1-182619, C1-182665, C1-182497, C1-182067 and C1-182078 to correct some editorials as well as adding some missing parts. Corrections done by the rapporteur.	1.1.1
2018-06	CT1#111					Implementing the following p-CRs agreed by CT1: C1-183268, C1-183109, C1-183281, C1-183517, C1-183518, C1-183519, C1-183791, C1-183115, C1-183527, C1-183812, C1-183813, C1-183141, C1-183148, C1-183406, C1-183070, C1-183207, C1-183273, C1-183276, C1-183277, C1-183415, C1-183143, C1-183146, C1-183197, C1-183260, C1-183142, C1-183151, C1-183154, C1-183225, C1-183205, C1-183223, C1-183314, C1-183278, C1-183367, C1-183279, C1-183381, C1-183399, C1-183413, C1-183467, C1-183530, C1-183532, C1-183533, C1-183534, C1-183535, C1-183538, C1-183539, C1-183715, C1-183716, C1-183717, C1-183718, C1-183720, C1-183721, C1-183737, C1-183739, C1-183741, C1-183744, C1-183745, C1-183748, C1-183749, C1-183750, C1-183751, C1-183774, C1-183775, C1-183779, C1-183780, C1-183781, C1-183809, C1-183822, C1-183824, C1-183825, C1-183826, C1-183845, C1-183858, C1-183761, C1-183147, C1-183237, C1-183329, C1-183353, C1-183378, C1-183387, C1-183401, C1-183408, C1-183499, C1-183541, C1-183542, C1-183543, C1-183545, C1-183726, C1-183756, C1-183757, C1-183758, C1-183759, C1-183762, C1-183795, C1-183796, C1-183802, C1-183827, C1-183846, C1-183847, C1-183848, C1-183211, C1-183731, C1-183784, C1-183578, C1-183585, C1-183831, C1-183861, C1-183247, C1-183562, C1-183563, C1-183798, C1-183194, C1-183238, C1-183256, C1-183528, C1-183427, C1-183706, C1-183707, C1-183709, C1-183763, C1-183766, C1-183767, C1-183768, C1-183769, C1-183770, C1-183771, C1-183772, C1-183773, C1-183785, C1-183787, C1-183788, C1-183789, C1-183799, C1-183805, C1-183816, C1-183832, C1-183834, C1-183849, C1-183850, C1-183114, C1-183457, C1-183458, C1-183510, C1-183511, C1-183512, C1-183513, C1-	1.2.0

						183515, C1-183800, C1-183806, C1-183470 Corrections done by the rapporteur.	
2018-06	CT1 e-mail review					Re-implementation of C1-183535, C1-183813, C1-183408, C1-183766 and C1-183831. Implementation of C1-183816 which was missed. Editorial corrections of some of the implemented p-CRs. Corrections done by the rapporteur.	1.2.1
2018-06	CT#80	CP-181094				Version 2.0.0 created for presentation to TSG CT#80 for approval.	2.0.0
2018-06	CT#80					Version 15.0.0 created after approval	15.0.0