3GPP TS 24.501 V16.1.0 (2019-06)

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 16)

** 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP..  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

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

***Copyright Notification***

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

© 2019, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword 19

1 Scope 20

2 References 20

3 Definitions and abbreviations 23

3.1 Definitions 23

3.2 Abbreviations 28

4 General 30

4.1 Overview 30

4.2 Coordination between the protocols for 5GS mobility management and 5GS session management 30

4.3 UE domain selection 31

4.3.1 UE's usage setting 31

4.3.2 Domain selection for UE originating sessions / calls 31

4.3.3 Change of UE's usage setting 33

4.3.4 Change or determination of IMS voice availability 33

4.4 NAS security 34

4.4.1 General 34

4.4.2 Handling of 5G NAS security contexts 34

4.4.2.1 General 34

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 36

4.4.2.3 Establishment of a 5G NAS security context during N1 mode to N1 mode handover 37

4.4.2.4 Establishment of an EPS security context during inter-system change from N1 mode to S1 mode in 5GMM-CONNECTED mode 38

4.4.2.5 Establishment of secure exchange of NAS messages 38

4.4.2.6 Change of security keys 40

4.4.3 Handling of NAS COUNT and NAS sequence number 40

4.4.3.1 General 40

4.4.3.2 Replay protection 41

4.4.3.3 Integrity protection and verification 41

4.4.3.4 Ciphering and deciphering 42

4.4.3.5 NAS COUNT wrap around 42

4.4.4 Integrity protection of NAS signalling messages 42

4.4.4.1 General 42

4.4.4.2 Integrity checking of NAS signalling messages in the UE 43

4.4.4.3 Integrity checking of NAS signalling messages in the AMF 43

4.4.5 Ciphering of NAS signalling messages 45

4.4.6 Protection of initial NAS signalling messages 46

4.5 Unified access control 47

4.5.1 General 47

4.5.2 Determination of the access identities and access category associated with a request for access for UEs which are not SNPN enabled or UEs not operating in SNPN access mode 48

4.5.2A Determination of the access identities and access category associated with a request for access for UEs operating in SNPN access mode 52

4.5.3 Operator-defined access categories 55

4.5.4 Access control and checking 56

4.5.4.1 Access control and checking in 5GMM-IDLE mode 56

4.5.4.2 Access control and checking in 5GMM-CONNECTED mode and in 5GMM-CONNECTED mode with RRC inactive indication 57

4.5.5 Exception handling and avoiding double barring 59

4.5.6 Mapping between access categories/access identities and RRC establishment cause 62

4.6 Network slicing 63

4.6.1 General 63

4.6.2 Mobility management aspects 64

4.6.2.1 General 64

4.6.2.2 NSSAI storage 64

4.6.2.3 Provision of NSSAI to lower layers in 5GMM-IDLE mode 66

4.6.3 Session management aspects 67

4.7 NAS over non-3GPP access 67

4.7.1 General 67

4.7.2 5GS mobility management aspects 67

4.7.2.1 General 67

4.7.2.2 Establishment cause for non-3GPP access 68

4.7.3 5GS session management aspects 68

4.7.4 Limited service state over non-3GPP access 69

4.8 Interworking with E-UTRAN connected to EPC 69

4.8.1 General 69

4.8.2 Single-registration mode 69

4.8.2.1 General 69

4.8.2.2 Single-registration mode with N26 interface 70

4.8.2.3 Single-registration mode without N26 interface 70

4.8.2.3.1 Interworking between NG-RAN and E-UTRAN 70

4.8.2.3.2 Interworking between N3IWF connected to 5GCN and E-UTRAN 71

4.8.3 Dual-registration mode 72

4.8.4 Core Network selection for UEs not using CIoT 5GS optimizations 73

4.8.4A Core Network selection and redirection for UEs using CIoT optimizations 73

4.8.4A.1 Core network selection 73

4.8.4A.2 Redirection of the UE by the core network 74

4.9 Disabling and re-enabling of UE's N1 mode capability 74

4.9.1 General 74

4.9.2 Disabling and re-enabling of UE's N1 mode capability for 3GPP access 74

4.9.3 Disabling and re-enabling of UE's N1 mode capability for non-3GPP access 75

4.10 Interworking with ePDG connected to EPC 76

4.11 UE configuration parameter updates 76

4.12 Multi-access (MA) PDU session 76

4.13 Support of NAS signalling using wireline 5G access network 76

4.14 Non-public network 77

4.14.1 General 77

4.14.2 Stand-alone non-public network 77

4.14.3 Public network integrated non-public network 77

5 Elementary procedures for 5GS mobility management 77

5.1 Overview 77

5.1.1 General 77

5.1.2 Types of 5GMM procedures 77

5.1.3 5GMM sublayer states 79

5.1.3.1 General 79

5.1.3.2 5GMM sublayer states 79

5.1.3.2.1 5GMM sublayer states in the UE 79

5.1.3.2.1.1 General 79

5.1.3.2.1.2 Main states 79

5.1.3.2.1.2.1 5GMM-NULL 79

5.1.3.2.1.2.2 5GMM-DEREGISTERED 80

5.1.3.2.1.2.3 5GMM-REGISTERED-INITIATED 80

5.1.3.2.1.2.4 5GMM-REGISTERED 80

5.1.3.2.1.2.5 5GMM-DEREGISTERED-INITIATED 80

5.1.3.2.1.2.6 5GMM-SERVICE-REQUEST-INITIATED 80

5.1.3.2.1.3 Substates of state 5GMM-DEREGISTERED 80

5.1.3.2.1.3.1 General 80

5.1.3.2.1.3.2 5GMM-DEREGISTERED.NORMAL-SERVICE 80

5.1.3.2.1.3.3 5GMM-DEREGISTERED.LIMITED-SERVICE 80

5.1.3.2.1.3.4 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION 80

5.1.3.2.1.3.5 5GMM-DEREGISTERED.PLMN-SEARCH 81

5.1.3.2.1.3.6 5GMM-DEREGISTERED.NO-SUPI 81

5.1.3.2.1.3.7 5GMM-DEREGISTERED.NO-CELL-AVAILABLE 81

5.1.3.2.1.3.8 5GMM-DEREGISTERED.eCALL-INACTIVE 81

5.1.3.2.1.3.9 5GMM-DEREGISTERED.INITIAL-REGISTRATION-NEEDED 81

5.1.3.2.1.4 Substates of state 5GMM-REGISTERED 81

5.1.3.2.1.4.1 General 81

5.1.3.2.1.4.2 5GMM-REGISTERED.NORMAL-SERVICE 82

5.1.3.2.1.4.3 5GMM-REGISTERED.NON-ALLOWED-SERVICE 82

5.1.3.2.1.4.4 5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE 82

5.1.3.2.1.4.5 5GMM-REGISTERED.LIMITED-SERVICE 82

5.1.3.2.1.4.6 5GMM-REGISTERED.PLMN-SEARCH 82

5.1.3.2.1.4.7 5GMM-REGISTERED.NO-CELL-AVAILABLE 82

5.1.3.2.1.4.8 5GMM-REGISTERED.UPDATE-NEEDED 82

5.1.3.2.2 5GS update status in the UE 82

5.1.3.2.3 5GMM sublayer states in the network side 83

5.1.3.2.3.1 General 83

5.1.3.2.3.2 5GMM-DEREGISTERED 83

5.1.3.2.3.3 5GMM-COMMON-PROCEDURE-INITIATED 84

5.1.3.2.3.4 5GMM-REGISTERED 84

5.1.3.2.3.5 5GMM-DEREGISTERED-INITIATED 84

5.1.4 Coordination between 5GMM and EMM 84

5.1.4.1 General 84

5.1.4.2 Coordination between 5GMM and EMM with N26 interface 84

5.1.4.3 Coordination between 5GMM and EMM without N26 interface 85

5.1.5 Coordination between 5GMM and GMM 85

5.2 Behaviour of the UE in state 5GMM-DEREGISTERED and state 5GMM-REGISTERED 85

5.2.1 General 85

5.2.2 UE behaviour in state 5GMM-DEREGISTERED 85

5.2.2.1 General 85

5.2.2.2 Primary substate selection 86

5.2.2.2.1 Selection of the substate after power on 86

5.2.2.3 Detailed description of UE behaviour in state 5GMM-DEREGISTERED 86

5.2.2.3.1 NORMAL-SERVICE 86

5.2.2.3.2 LIMITED-SERVICE 86

5.2.2.3.3 ATTEMPTING-REGISTRATION 86

5.2.2.3.4 PLMN-SEARCH 87

5.2.2.3.5 NO-SUPI 87

5.2.2.3.6 NO-CELL-AVAILABLE 87

5.2.2.3.7 eCALL-INACTIVE 87

5.2.2.3.8 INITIAL-REGISTRATION-NEEDED 87

5.2.2.4 Substate when back to state 5GMM-DEREGISTERED from another 5GMM state 87

5.2.3 UE behaviour in state 5GMM-REGISTERED 88

5.2.3.1 General 88

5.2.3.2 Detailed description of UE behaviour in state 5GMM-REGISTERED 88

5.2.3.2.1 NORMAL-SERVICE 88

5.2.3.2.2 NON-ALLOWED-SERVICE 88

5.2.3.2.3 ATTEMPTING-REGISTRATION-UPDATE 88

5.2.3.2.4 LIMITED-SERVICE 89

5.2.3.2.5 PLMN-SEARCH 90

5.2.3.2.6 NO-CELL-AVAILABLE 90

5.2.3.2.7 UPDATE-NEEDED 90

5.3 General on elementary 5GMM procedures 90

5.3.1 5GMM modes and N1 NAS signalling connection 90

5.3.1.1 Establishment of the N1 NAS signalling connection 90

5.3.1.2 Re-establishment of the N1 NAS signalling connection 91

5.3.1.3 Release of the N1 NAS signalling connection 93

5.3.1.4 5GMM-CONNECTED mode with RRC inactive indication 95

5.3.1.5 Suspend and resume of the N1 NAS signalling connection 97

5.3.2 Permanent identifiers 98

5.3.3 Temporary identities 99

5.3.4 Registration areas 100

5.3.5 Service area restrictions 100

5.3.6 Mobile initiated connection only mode 102

5.3.7 Handling of the periodic registration update timer and mobile reachable timer 103

5.3.8 Handling of timer T3502 105

5.3.9 Handling of NAS level mobility management congestion control 105

5.3.10 Handling of DNN based congestion control 106

5.3.11 Handling of S-NSSAI based congestion control 106

5.3.12 Handling of local emergency numbers 106

5.3.12A Handling of local emergency numbers received via 3GPP access and non-3GPP access 107

5.3.12A.1 General 107

5.3.12A.2 Receiving a REGISTRATION ACCEPT message via non-3GPP access 108

5.3.13 Lists of 5GS forbidden tracking areas 108

5.3.13A Forbidden PLMN lists 109

5.3.14 List of equivalent PLMNs 109

5.3.15 Transmission failure abnormal case in the UE 109

5.3.16 Extended DRX cycle for UEs in 5GMM-IDLE 109

5.3.17 Service Gap Control 110

5.3.18 Restriction on use of enhanced coverage 111

5.3.19 Handling of congestion control for transport of user data via the control plane 112

5.3.20 Specific requirements for UE when receiving non-integrity protected reject messages 112

5.3.21 CIoT 5GS optimizations 116

5.3.22 Interaction between MICO mode with active time and extended idle mode DRX cycle 117

5.4 5GMM common procedures 118

5.4.1 Primary authentication and key agreement procedure 118

5.4.1.1 General 118

5.4.1.2 EAP based primary authentication and key agreement procedure 118

5.4.1.2.1 General 118

5.4.1.2.2 EAP-AKA' related procedures 121

5.4.1.2.2.1 General 121

5.4.1.2.2.2 Initiation 121

5.4.1.2.2.3 UE successfully authenticates network 121

5.4.1.2.2.4 Errors when handling EAP-request/AKA'-challenge message 122

5.4.1.2.2.5 Network successfully authenticates UE 122

5.4.1.2.2.6 UE handling EAP-AKA' notification message 122

5.4.1.2.2.6A EAP based Identification initiation by the network 122

5.4.1.2.2.6B EAP based Identification response by the UE 122

5.4.1.2.2.7 Network sending EAP-success message 123

5.4.1.2.2.8 UE handling EAP-success message 123

5.4.1.2.2.9 Network not successfully authenticates UE 123

5.4.1.2.2.10 Network sending EAP-failure message 123

5.4.1.2.2.11 UE handling EAP-failure message 124

5.4.1.2.2.12 Abnormal cases in the UE 125

5.4.1.2.3 EAP-TLS related procedures 125

5.4.1.2.3.1 General 125

5.4.1.2.4 EAP message reliable transport procedure 126

5.4.1.2.4.1 General 126

5.4.1.2.4.2 EAP message reliable transport procedure initiation by the network 127

5.4.1.2.4.3 EAP message reliable transport procedure accepted by the UE 127

5.4.1.2.4.4 Abnormal cases on the network side 127

5.4.1.2.4.5 Abnormal cases in the UE 128

5.4.1.2.5 EAP result message transport procedure 129

5.4.1.2.5.1 General 129

5.4.1.2.5.2 EAP result message transport procedure initiation by the network 130

5.4.1.3 5G AKA based primary authentication and key agreement procedure 130

5.4.1.3.1 General 130

5.4.1.3.2 Authentication initiation by the network 131

5.4.1.3.3 Authentication response by the UE 131

5.4.1.3.4 Authentication completion by the network 132

5.4.1.3.5 Authentication not accepted by the network 132

5.4.1.3.6 Authentication not accepted by the UE 134

5.4.1.3.7 Abnormal cases 134

5.4.2 Security mode control procedure 138

5.4.2.1 General 138

5.4.2.2 NAS security mode control initiation by the network 138

5.4.2.3 NAS security mode command accepted by the UE 141

5.4.2.4 NAS security mode control completion by the network 143

5.4.2.5 NAS security mode command not accepted by the UE 143

5.4.2.6 Abnormal cases in the UE 143

5.4.2.7 Abnormal cases on the network side 144

5.4.3 Identification procedure 144

5.4.3.1 General 144

5.4.3.2 Identification initiation by the network 145

5.4.3.3 Identification response by the UE 145

5.4.3.4 Identification completion by the network 145

5.4.3.5 Abnormal cases in the UE 145

5.4.3.6 Abnormal cases on the network side 145

5.4.4 Generic UE configuration update procedure 146

5.4.4.1 General 146

5.4.4.2 Generic UE configuration update procedure initiated by the network 148

5.4.4.3 Generic UE configuration update accepted by the UE 149

5.4.4.4 Generic UE configuration update completion by the network 150

5.4.4.5 Abnormal cases in the UE 151

5.4.4.6 Abnormal cases on the network side 152

5.4.5 NAS transport procedure(s) 153

5.4.5.1 General 153

5.4.5.2 UE-initiated NAS transport procedure 153

5.4.5.2.1 General 153

5.4.5.2.2 UE-initiated NAS transport procedure initiation 154

5.4.5.2.3 UE-initiated NAS transport of messages accepted by the network 155

5.4.5.2.4 UE-initiated NAS transport of messages not accepted by the network 158

5.4.5.2.5 Abnormal cases on the network side 159

5.4.5.2.6 Abnormal cases in the UE 162

5.4.5.3 Network-initiated NAS transport procedure 163

5.4.5.3.1 General 163

5.4.5.3.2 Network-initiated NAS transport procedure initiation 164

5.4.5.3.3 Network-initiated NAS transport of messages 166

5.4.6 5GMM status procedure 168

5.4.6.1 General 168

5.4.6.2 5GMM status received in the UE 169

5.4.6.3 5GMM status received in the network 169

5.5 5GMM specific procedures 169

5.5.1 Registration procedure 169

5.5.1.1 General 169

5.5.1.2 Registration procedure for initial registration 170

5.5.1.2.1 General 170

5.5.1.2.2 Initial registration initiation 170

5.5.1.2.3 5GMM common procedure initiation 174

5.5.1.2.4 Initial registration accepted by the network 174

5.5.1.2.5 Initial registration not accepted by the network 182

5.5.1.2.6 Initial registration for emergency services not accepted by the network 186

5.5.1.2.6A Initial registration for initiating a PDU session for emergency services not accepted by the network 186

5.5.1.2.7 Abnormal cases in the UE 187

5.5.1.2.8 Abnormal cases on the network side 189

5.5.1.3 Registration procedure for mobility and periodic registration update 190

5.5.1.3.1 General 190

5.5.1.3.2 Mobility and periodic registration update initiation 191

5.5.1.3.3 5GMM common procedure initiation 196

5.5.1.3.4 Mobility and periodic registration update accepted by the network 197

5.5.1.3.5 Mobility and periodic registration update not accepted by the network 208

5.5.1.3.6 Mobility and periodic registration update for initiating an emergency PDU session not accepted by the network 212

5.5.1.3.7 Abnormal cases in the UE 213

5.5.1.3.8 Abnormal cases on the network side 215

5.5.2 De-registration procedure 217

5.5.2.1 General 217

5.5.2.2 UE-initiated de-registration procedure 218

5.5.2.2.1 UE-initiated de-registration procedure initiation 218

5.5.2.2.2 UE-initiated de-registration procedure completion 219

5.5.2.2.3 UE-initiated de-registration procedure completion for 5GS services over 3GPP access 219

5.5.2.2.4 UE-initiated de-registration procedure completion for 5GS services non-3GPP access 219

5.5.2.2.5 UE-initiated de-registration procedure completion for 5GS services over both 3GPP access and non-3GPP access 220

5.5.2.2.6 Abnormal cases in the UE 220

5.5.2.2.7 Abnormal cases in the network side 221

5.5.2.3 Network-initiated de-registration procedure 222

5.5.2.3.1 Network-initiated de-registration procedure initiation 222

5.5.2.3.2 Network-initiated de-registration procedure completion by the UE 222

5.5.2.3.3 Network-initiated de-registration procedure completion by the network 225

5.5.2.3.4 Abnormal cases in the UE 225

5.5.2.3.5 Abnormal cases in the network side 226

5.5.3 eCall inactivity procedure 227

5.6 5GMM connection management procedures 227

5.6.1 Service request procedure 227

5.6.1.1 General 227

5.6.1.2 Service request procedure initiation 229

5.6.1.3 Common procedure initiation 232

5.6.1.4 Service request procedure accepted by the network 232

5.6.1.5 Service request procedure not accepted by the network 234

5.6.1.6 Service request procedure for initiating an emergency PDU session not accepted by the network 239

5.6.1.7 Abnormal cases in the UE 239

5.6.1.8 Abnormal cases on the network side 242

5.6.2 Paging procedure 243

5.6.2.1 General 243

5.6.2.2 Paging for 5GS services 243

5.6.2.2.1 General 243

5.6.2.2.2 Abnormal cases on the network side 244

5.6.2.2.3 Abnormal cases in the UE 244

5.6.3 Notification procedure 244

5.6.3.1 General 244

5.6.3.2 Notification procedure initiation 244

5.6.3.3 Notification procedure completion 245

5.6.3.4 Abnormal cases on the network side 246

5.6.3.5 Abnormal cases on the UE side 246

6 Elementary procedures for 5GS session management 246

6.1 Overview 246

6.1.1 General 246

6.1.2 Types of 5GSM procedures 247

6.1.3 5GSM sublayer states 247

6.1.3.1 General 247

6.1.3.2 5GSM sublayer states in the UE 247

6.1.3.2.1 Overview 247

6.1.3.2.2 PDU SESSION INACTIVE 248

6.1.3.2.3 PDU SESSION ACTIVE PENDING 248

6.1.3.2.4 PDU SESSION ACTIVE 248

6.1.3.2.5 PDU SESSION INACTIVE PENDING 248

6.1.3.2.6 PDU SESSION MODIFICATION PENDING 248

6.1.3.2.7 PROCEDURE TRANSACTION INACTIVE 248

6.1.3.2.8 PROCEDURE TRANSACTION PENDING 248

6.1.3.3 5GSM sublayer states in the network side 249

6.1.3.3.1 Overview 249

6.1.3.3.2 PDU SESSION INACTIVE 249

6.1.3.3.3 PDU SESSION ACTIVE 249

6.1.3.3.4 PDU SESSION INACTIVE PENDING 249

6.1.3.3.5 PDU SESSION MODIFICATION PENDING 250

6.1.3.3.6 PROCEDURE TRANSACTION INACTIVE 250

6.1.3.3.7 PROCEDURE TRANSACTION PENDING 250

6.1.4 Coordination between 5GSM and ESM 250

6.1.4.1 Coordination between 5GSM and ESM with N26 interface 250

6.1.4.2 Coordination between 5GSM and ESM without N26 interface 258

6.2 General on elementary 5GSM procedures 261

6.2.1 Principles of PTI handling for 5GSM procedures 261

6.2.2 PDU session types 262

6.2.3 PDU session management 262

6.2.4 IP address allocation 263

6.2.4.1 General 263

6.2.4.2 IP address allocation via NAS signalling 263

6.2.5 Quality of service 264

6.2.5.1 General 264

6.2.5.1.1 QoS rules 264

6.2.5.1.1.1 General 264

6.2.5.1.1.2 Signalled QoS rules 264

6.2.5.1.1.3 Derived QoS rules 265

6.2.5.1.1.4 QoS flow descriptions 266

6.2.5.1.2 Session-AMBR 266

6.2.5.1.2A Session-TMBR 266

6.2.5.1.3 UL user data packet matching 266

6.2.5.1.4 Reflective QoS 267

6.2.5.1.4.1 General 267

6.2.5.1.4.2 Derivation of packet filter for UL direction from DL user data packet 267

6.2.5.1.4.3 Creating a derived QoS rule by reflective QoS in the UE 269

6.2.5.1.4.4 Updating a derived QoS rule by reflective QoS in the UE 269

6.2.5.1.4.5 Deleting a derived QoS rule in the UE 269

6.2.5.1.4.6 Ignoring RQI in the UE 270

6.2.6 Local area data network (LADN) 270

6.2.7 Handling of DNN based congestion control 271

6.2.8 Handling of S-NSSAI based congestion control 271

6.2.9 Interaction with upper layers 272

6.2.9.1 General 272

6.2.9.2 URSP 272

6.2.10 Handling of 3GPP PS data off 273

6.2.11 Multi-homed IPv6 PDU session 273

6.2.12 Handling of network rejection not due to congestion control 274

6.2.13 Handling of Small data rate control 274

6.2.14 Handling of Serving PLMN rate control 275

6.2.15 Handling of Reliable Data Service 275

6.3 Network-requested 5GSM procedures 276

6.3.1 PDU session authentication and authorization procedure 276

6.3.1.1 General 276

6.3.1.2 PDU EAP message reliable transport procedure 277

6.3.1.2.1 PDU EAP message reliable transport procedure initiation 277

6.3.1.2.2 PDU EAP message reliable transport procedure accepted by the UE 278

6.3.1.2.3 Abnormal cases on the network side 278

6.3.1.2.4 Abnormal cases in the UE 278

6.3.1.3 PDU EAP result message transport procedure 279

6.3.1.3.1 PDU EAP result message transport procedure initiation 279

6.3.2 Network-requested PDU session modification procedure 279

6.3.2.1 General 279

6.3.2.2 Network-requested PDU session modification procedure initiation 279

6.3.2.3 Network-requested PDU session modification procedure accepted by the UE 281

6.3.2.4 Network-requested PDU session modification procedure not accepted by the UE 286

6.3.2.5 Abnormal cases on the network side 290

6.3.2.6 Abnormal cases in the UE 290

6.3.3 Network-requested PDU session release procedure 291

6.3.3.1 General 291

6.3.3.2 Network-requested PDU session release procedure initiation 291

6.3.3.3 Network-requested PDU session release procedure accepted by the UE 293

6.3.3.4 N1 SM delivery skipped 299

6.3.3.5 Abnormal cases on the network side 299

6.3.3.6 Abnormal cases in the UE 300

6.4 UE-requested 5GSM procedures 300

6.4.1 UE-requested PDU session establishment procedure 300

6.4.1.1 General 300

6.4.1.2 UE-requested PDU session establishment procedure initiation 300

6.4.1.3 UE-requested PDU session establishment procedure accepted by the network 305

6.4.1.4 UE requested PDU session establishment procedure not accepted by the network 312

6.4.1.4.1 General 312

6.4.1.4.2 Handling of network rejection due to congestion control 314

6.4.1.4.3 Handling of network rejection not due to congestion control 320

6.4.1.5 Handling the maximum number of established PDU sessions 324

6.4.1.6 Abnormal cases in the UE 324

6.4.1.7 Abnormal cases on the network side 325

6.4.2 UE-requested PDU session modification procedure 326

6.4.2.1 General 326

6.4.2.2 UE-requested PDU session modification procedure initiation 326

6.4.2.3 UE-requested PDU session modification procedure accepted by the network 328

6.4.2.4 UE-requested PDU session modification procedure not accepted by the network 328

6.4.2.4.1 General 328

6.4.2.4.2 Handling of network rejection due to congestion control 329

6.4.2.4.3 Handling of network rejection not due to congestion control 335

6.4.2.5 Abnormal cases in the UE 337

6.4.2.6 Abnormal cases on the network side 338

6.4.3 UE-requested PDU session release procedure 338

6.4.3.1 General 338

6.4.3.2 UE-requested PDU session release procedure initiation 339

6.4.3.3 UE-requested PDU session release procedure accepted by the network 339

6.4.3.4 UE-requested PDU session release procedure not accepted by the network 340

6.4.3.5 Abnormal cases in the UE 340

6.4.3.6 Abnormal cases on the network side 340

6.5 5GSM status procedure 341

6.5.1 General 341

6.5.2 5GSM status received in the UE 341

6.5.3 5GSM status received in the SMF 341

6.6 Miscellaneous procedures 342

6.6.1 Exchange of extended protocol configuration options 342

7 Handling of unknown, unforeseen, and erroneous protocol data 342

7.1 General 342

7.2 Message too short or too long 342

7.2.1 Message too short 342

7.2.2 Message too long 343

7.3 Unknown or unforeseen procedure transaction identity or PDU Session identity 343

7.3.1 Procedure transaction identity 343

7.3.2 PDU Session identity 344

7.4 Unknown or unforeseen message type 344

7.5 Non-semantical mandatory information element errors 345

7.5.1 Common procedures 345

7.5.2 5GS mobility management 345

7.5.3 5GS session management 345

7.6 Unknown and unforeseen IEs in the non-imperative message part 346

7.6.1 IEIs unknown in the message 346

7.6.2 Out of sequence IEs 346

7.6.3 Repeated IEs 346

7.7 Non-imperative message part errors 346

7.7.1 Syntactically incorrect optional IEs 347

7.7.2 Conditional IE errors 347

7.8 Messages with semantically incorrect contents 347

8 Message functional definitions and contents 347

8.1 Overview 347

8.2 5GS mobility management messages 347

8.2.1 Authentication request 347

8.2.1.1 Message definition 347

8.2.1.2 Authentication parameter RAND 348

8.2.1.3 Authentication parameter AUTN 348

8.2.1.4 Void 348

8.2.1.5 EAP message 348

8.2.2 Authentication response 348

8.2.2.1 Message definition 348

8.2.2.2 Authentication response parameter 349

8.2.2.3 EAP message 349

8.2.3 Authentication result 349

8.2.3.1 Message definition 349

8.2.3.2 ABBA 350

8.2.4 Authentication failure 350

8.2.4.1 Message definition 350

8.2.4.2 Authentication failure parameter 350

8.2.5 Authentication reject 350

8.2.5.1 Message definition 350

8.2.5.2 EAP message 351

8.2.6 Registration request 351

8.2.6.1 Message definition 351

8.2.6.2 Non-current native NAS key set identifier 353

8.2.6.3 5GMM capability 353

8.2.6.4 UE security capability 353

8.2.6.5 Requested NSSAI 353

8.2.6.6 Last visited registered TAI 353

8.2.6.7 S1 UE network capability 353

8.2.6.8 Uplink data status 353

8.2.6.9 PDU session status 353

8.2.6.10 MICO indication 353

8.2.6.11 UE status 353

8.2.6.12 Additional GUTI 354

8.2.6.13 Allowed PDU session status 354

8.2.6.14 UE's usage setting 354

8.2.6.15 Requested DRX parameters 354

8.2.6.16 EPS NAS message container 354

8.2.6.17 LADN indication 354

8.2.6.17A Payload container type 354

8.2.6.18 Payload container 354

8.2.6.19 Network slicing indication 354

8.2.6.20 5GS update type 354

8.2.6.21 NAS message container 355

8.2.6.22 Requested extended DRX parameters 355

8.2.6.23 EPS bearer context status 355

8.2.6.24 T3324 value 355

8.2.6.25 Mobile station classmark 2 355

8.2.6.26 Supported codecs 355

8.2.7 Registration accept 355

8.2.7.1 Message definition 355

8.2.7.2 5G-GUTI 357

8.2.7.3 Equivalent PLMNs 357

8.2.7.4 TAI list 357

8.2.7.5 Allowed NSSAI 357

8.2.7.6 Rejected NSSAI 357

8.2.7.7 Configured NSSAI 357

8.2.7.8 5GS network feature support 357

8.2.7.9 PDU session status 357

8.2.7.10 PDU session reactivation result 357

8.2.7.11 PDU session reactivation result error cause 358

8.2.7.12 LADN information 358

8.2.7.13 MICO indication 358

8.2.7.14 Network slicing indication 358

8.2.7.15 Service area list 358

8.2.7.16 T3512 value 358

8.2.7.17 Non-3GPP de-registration timer value 358

8.2.7.18 T3502 value 358

8.2.7.19 Emergency number list 358

8.2.7.20 Extended emergency number list 358

8.2.7.21 SOR transparent container 359

8.2.7.22 EAP message 359

8.2.7.23 NSSAI inclusion mode 359

8.2.7.24 Operator-defined access category definitions 359

8.2.7.25 Negotiated DRX parameters 359

8.2.7.26 Non-3GPP NW provided policies 359

8.2.7.27 Negotiated extended DRX parameters 359

8.2.7.28 T3447 value 359

8.2.7.29 T3448 value 359

8.2.7.30 T3324 value 360

8.2.7.31 EPS bearer context status 360

8.2.8 Registration complete 360

8.2.8.1 Message definition 360

8.2.8.2 SOR transparent container 360

8.2.9 Registration reject 360

8.2.9.1 Message definition 360

8.2.9.2 T3346 value 361

8.2.9.3 T3502 value 361

8.2.9.4 EAP message 361

8.2.10 UL NAS transport 361

8.2.10.1 Message definition 361

8.2.10.2 PDU session ID 362

8.2.10.3 Old PDU session ID 362

8.2.10.4 Request type 362

8.2.10.5 S-NSSAI 362

8.2.10.6 DNN 362

8.2.10.7 Additional information 362

8.2.10.8 MA PDU session information 363

8.2.11 DL NAS transport 363

8.2.11.1 Message definition 363

8.2.11.2 PDU session ID 363

8.2.11.3 Additional information 363

8.2.11.4 5GMM cause 363

8.2.11.5 Back-off timer value 364

8.2.12 De-registration request (UE originating de-registration) 364

8.2.12.1 Message definition 364

8.2.13 De-registration accept (UE originating de-registration) 364

8.2.13.1 Message definition 364

8.2.14 De-registration request (UE terminated de-registration) 365

8.2.14.1 Message definition 365

8.2.14.2 5GMM cause 365

8.2.14.3 T3346 value 365

8.2.15 De-registration accept (UE terminated de-registration) 365

8.2.15.1 Message definition 365

8.2.16 Service request 366

8.2.16.1 Message definition 366

8.2.16.2 Uplink data status 366

8.2.16.3 PDU session status 366

8.2.16.4 Allowed PDU session status 367

8.2.16.5 NAS message container 367

8.2.17 Service accept 367

8.2.17.1 Message definition 367

8.2.17.2 PDU session status 367

8.2.17.3 PDU session reactivation result 367

8.2.17.4 PDU session reactivation result error cause 368

8.2.17.5 EAP message 368

8.2.17.6 T3448 value 368

8.2.18 Service reject 368

8.2.18.1 Message definition 368

8.2.18.2 PDU session status 368

8.2.18.3 T3346 value 369

8.2.18.4 EAP message 369

8.2.18.5 T3448 value 369

8.2.19 Configuration update command 369

8.2.19.1 Message definition 369

8.2.19.2 Configuration update indication 370

8.2.19.3 5G-GUTI 370

8.2.19.4 TAI list 370

8.2.19.5 Allowed NSSAI 371

8.2.19.6 Service area list 371

8.2.19.7 Full name for network 371

8.2.19.8 Short name for network 371

8.2.19.9 Local time zone 371

8.2.19.10 Universal time and local time zone 371

8.2.19.11 Network daylight saving time 371

8.2.19.12 LADN information 371

8.2.19.13 MICO indication 371

8.2.19.14 Network slicing indication 371

8.2.19.15 Configured NSSAI 371

8.2.19.16 Rejected NSSAI 371

8.2.19.17 Operator-defined access category definitions 371

8.2.19.18 SMS indication 371

8.2.19.19 372

8.2.20 Configuration update complete 372

8.2.20.1 Message definition 372

8.2.21 Identity request 372

8.2.21.1 Message definition 372

8.2.22 Identity response 373

8.2.22.1 Message definition 373

8.2.23 Notification 373

8.2.23.1 Message definition 373

8.2.24 Notification response 374

8.2.24.1 Message definition 374

8.2.24.2 PDU session status 374

8.2.25 Security mode command 374

8.2.25.1 Message definition 374

8.2.25.2 IMEISV request 375

8.2.25.3 Void 375

8.2.25.4 Selected EPS NAS security algorithms 375

8.2.25.5 Additional 5G security information 375

8.2.25.6 EAP message 375

8.2.25.7 ABBA 375

8.2.25.8 Replayed S1 UE security capabilities 376

8.2.26 Security mode complete 376

8.2.26.1 Message definition 376

8.2.26.2 IMEISV 376

8.2.26.3 NAS message container 376

8.2.27 Security mode reject 376

8.6.27.1 Message definition 376

8.2.28 Security protected 5GS NAS message 377

8.2.28.1 Message definition 377

8.2.29 5GMM status 377

8.2.29.1 Message definition 377

8.3 5GS session management messages 378

8.3.1 PDU session establishment request 378

8.3.1.1 Message definition 378

8.3.1.2 PDU session type 379

8.3.1.3 SSC mode 379

8.3.1.4 Maximum number of supported packet filters 379

8.3.1.5 5GSM capability 379

8.3.1.6 Void 379

8.3.1.7 Always-on PDU session requested 379

8.3.1.8 SM PDU DN request container 379

8.3.1.9 Extended protocol configuration options 379

8.3.2 PDU session establishment accept 380

8.3.2.1 Message definition 380

8.3.2.2 5GSM cause 381

8.3.2.3 PDU address 381

8.3.2.4 RQ timer value 381

8.3.2.5 S-NSSAI 382

8.3.2.6 Always-on PDU session indication 382

8.3.2.7 Mapped EPS bearer contexts 382

8.3.2.8 EAP message 382

8.3.2.9 Authorized QoS flow descriptions 382

8.3.2.10 Extended protocol configuration options 382

8.3.2.11 DNN 382

8.3.2.12 5GSM network feature support 382

8.3.2.13 Session-TMBR 382

8.3.2.14 Serving PLMN rate control 382

8.3.2.15 ATSSS container 382

8.3.2.16 Control plane only indication 382

8.3.3 PDU session establishment reject 383

8.3.3.1 Message definition 383

8.3.3.2 Back-off timer value 383

8.3.3.3 Allowed SSC mode 383

8.3.3.4 EAP message 383

8.3.3.5 Extended protocol configuration options 384

8.3.3.6 Re-attempt indicator 384

8.3.3.7 5GSM congestion re-attempt indicator 384

8.3.4 PDU session authentication command 384

8.3.4.1 Message definition 384

8.3.4.2 Extended protocol configuration options 384

8.3.5 PDU session authentication complete 385

8.3.5.1 Message definition 385

8.3.5.2 Extended protocol configuration options 385

8.3.6 PDU session authentication result 385

8.3.6.1 Message definition 385

8.3.6.2 EAP message 386

8.3.6.3 Extended protocol configuration options 386

8.3.7 PDU session modification request 386

8.3.7.1 Message definition 386

8.3.7.2 5GSM capability 387

8.3.7.3 5GSM cause 387

8.3.7.4 Maximum number of supported packet filters 387

8.3.7.5 Always-on PDU session requested 388

8.3.7.6 Integrity protection maximum data rate 388

8.3.7.7 Requested QoS rules 388

8.3.7.8 Requested QoS flow descriptions 388

8.3.7.9 Extended protocol configuration options 388

8.3.7.10 Mapped EPS bearer contexts 388

8.3.8 PDU session modification reject 388

8.3.8.1 Message definition 388

8.3.8.2 Back-off timer value 389

8.3.8.3 Extended protocol configuration options 389

8.3.8.4 Re-attempt indicator 389

8.3.8.5 5GSM congestion re-attempt indicator 389

8.3.9 PDU session modification command 389

8.3.9.1 Message definition 389

8.3.9.2 5GSM cause 390

8.3.9.3 Session-AMBR 390

8.3.9.4 RQ timer value 390

8.3.9.5 Always-on PDU session indication 390

8.3.9.6 Authorized QoS rules 390

8.3.9.7 Mapped EPS bearer contexts 390

8.3.9.8 Authorized QoS flow descriptions 391

8.3.9.9 Extended protocol configuration options 391

8.3.9.10 Session-TMBR 391

8.3.10 PDU session modification complete 391

8.3.10.1 Message definition 391

8.3.10.2 Extended protocol configuration options 391

8.3.11 PDU session modification command reject 391

8.3.11.1 Message definition 391

8.3.11.2 Extended protocol configuration options 392

8.3.12 PDU session release request 392

8.3.12.1 Message definition 392

8.3.12.2 5GSM cause 392

8.3.12.3 Extended protocol configuration options 393

8.3.13 PDU session release reject 393

8.3.13.1 Message definition 393

8.3.13.2 Extended protocol configuration options 393

8.3.14 PDU session release command 393

8.3.14.1 Message definition 393

8.3.14.2 Back-off timer value 394

8.3.14.3 EAP message 394

8.3.14.4 Extended protocol configuration options 394

8.3.14.5 5GSM congestion re-attempt indicator 394

8.3.15 PDU session release complete 394

8.3.15.1 Message definition 394

8.3.15.2 5GSM cause 395

8.3.15.3 Extended protocol configuration options 395

8.3.16 5GSM status 395

8.3.16.1 Message definition 395

9 General message format and information elements coding 396

9.1 Overview 396

9.1.1 NAS message format 396

9.1.2 Field format and mapping 397

9.2 Extended protocol discriminator 397

9.3 Security header type 397

9.4 PDU session identity 398

9.5 Spare half octet 398

9.6 Procedure transaction identity 398

9.7 Message type 398

9.8 Message authentication code 400

9.9 Plain 5GS NAS message 400

9.10 Sequence number 400

9.11 Other information elements 401

9.11.1 General 401

9.11.2 Common information elements 401

9.11.2.1 Additional information 401

9.11.2.1A DNN 401

9.11.2.2 EAP message 402

9.11.2.3 GPRS timer 402

9.11.2.4 GPRS timer 2 402

9.11.2.5 GPRS timer 3 402

9.11.2.6 Intra N1 mode NAS transparent container 402

9.11.2.7 N1 mode to S1 mode NAS transparent container 403

9.11.2.8 S-NSSAI 404

9.11.2.9 S1 mode to N1 mode NAS transparent container 405

9.11.3 5GS mobility management (5GMM) information elements 406

9.11.3.1 5GMM capability 406

9.11.3.2 5GMM cause 408

9.11.3.2A 5GS DRX parameters 409

9.11.3.3 5GS identity type 410

9.11.3.4 5GS mobile identity 411

9.11.3.5 5GS network feature support 416

9.11.3.6 5GS registration result 418

9.11.3.7 5GS registration type 419

9.11.3.8 5GS tracking area identity 420

9.11.3.9 5GS tracking area identity list 421

9.11.3.9A 5GS update type 425

9.11.3.10 ABBA 425

9.11.3.11 Access type 426

9.11.3.12 Additional 5G security information 426

9.11.3.13 Allowed PDU session status 427

9.11.3.14 Authentication failure parameter 428

9.11.3.15 Authentication parameter AUTN 428

9.11.3.16 Authentication parameter RAND 428

9.11.3.17 Authentication response parameter 428

9.11.3.18 Configuration update indication 428

9.11.3.19 Daylight saving time 428

9.11.3.20 De-registration type 428

9.11.3.21 Void 429

9.11.3.22 Void 429

9.11.3.23 Emergency number list 429

9.11.3.24 EPS NAS message container 429

9.11.3.25 EPS NAS security algorithms 430

9.11.3.26 Extended emergency number list 430

9.11.3.27 Void 430

9.11.3.28 IMEISV request 430

9.11.3.29 LADN indication 430

9.11.3.30 LADN information 431

9.11.3.31 MICO indication 432

9.11.3.32 NAS key set identifier 432

9.11.3.33 NAS message container 433

9.11.3.34 NAS security algorithms 433

9.11.3.35 Network name 434

9.11.3.36 Network slicing indication 434

9.11.3.37 NSSAI 435

9.11.3.37A NSSAI inclusion mode 436

9.11.3.38 Operator-defined access category definitions 436

9.11.3.39 Payload container 439

9.11.3.40 Payload container type 442

9.11.3.41 PDU session identity 2 442

9.11.3.42 PDU session reactivation result 443

9.11.3.43 PDU session reactivation result error cause 443

9.11.3.44 PDU session status 444

9.11.3.45 PLMN list 444

9.11.3.46 Rejected NSSAI 444

9.11.3.47 Request type 446

9.11.3.48 S1 UE network capability 446

9.11.3.48A S1 UE security capability 446

9.11.3.49 Service area list 446

9.11.3.50 Service type 450

9.11.3.50A SMS indication 450

9.11.3.51 SOR transparent container 451

9.11.3.52 Time zone 453

9.11.3.53 Time zone and time 453

9.11.3.53A UE parameters update transparent container 453

9.11.3.54 UE security capability 454

9.11.3.55 UE's usage setting 458

9.11.3.56 UE status 458

9.11.3.57 Uplink data status 459

9.11.3.58 Non-3GPP NW provided policies 459

9.11.3.59 EPS bearer context status 459

9.11.3.60 Extended DRX parameters 460

9.11.3.61 Mobile station classmark 2 460

9.11.3.62 Supported codec list 460

9.11.3.63 MA PDU session information 460

9.11.4 5GS session management (5GSM) information elements 460

9.11.4.1 5GSM capability 460

9.11.4.2 5GSM cause 461

9.11.4.3 Always-on PDU session indication 462

9.11.4.4 Always-on PDU session requested 463

9.11.4.5 Allowed SSC mode 463

9.11.4.6 Extended protocol configuration options 464

9.11.4.7 Integrity protection maximum data rate 464

9.11.4.8 Mapped EPS bearer contexts 465

9.11.4.9 Maximum number of supported packet filters 467

9.11.4.10 PDU address 467

9.11.4.11 PDU session type 468

9.11.4.12 QoS flow descriptions 469

9.11.4.13 QoS rules 473

9.11.4.14 Session-AMBR 478

9.11.4.15 SM PDU DN request container 479

9.11.4.16 SSC mode 480

9.11.4.17 Re-attempt indicator 480

9.11.4.18 5GSM network feature support 481

9.11.4.19 Session-TMBR 481

9.11.4.20 Serving PLMN rate control 482

9.11.4.21 5GSM congestion re-attempt indicator 483

9.11.4.22 ATSSS container 483

9.11.4.23 Control plane only indication 483

9.12 3GPP specific coding information defined within present document 484

9.12.1 Serving network name (SNN) 484

10 List of system parameters 485

10.1 General 485

10.2 Timers of 5GS mobility management 485

10.3 Timers of 5GS session management 492

Annex A (informative): Cause values for 5GS mobility management 496

A.1 Causes related to UE identification 496

A.2 Cause related to subscription options 496

A.3 Causes related to PLMN specific network failures and congestion/authentication failures 497

A.4 Causes related to invalid messages 498

Annex B (informative): Cause values for 5GS session management 500

B.1 Causes related to nature of request 500

B.2 Protocol errors (e.g., unknown message) 502

Annex C (normative): Storage of 5GMM information 504

C.1 Storage of 5GMM information for UEs which are not SNPN enabled or UEs not operating in SNPN access mode 504

C.2 Storage of 5GMM information for UEs operating in SNPN access mode 505

Annex D (normative): UE policy delivery service 506

D.1 General 506

D.1.1 Overview 506

D.1.2 Principles of PTI handling for UE policy delivery service procedures 506

D.2 Procedures 507

D.2.1 Network-requested UE policy management procedure 507

D.2.1.1 General 507

D.2.1.2 Network-requested UE policy management procedure initiation 507

D.2.1.3 Network-requested UE policy management procedure accepted by the UE 508

D.2.1.4 Network-requested UE policy management procedure not accepted by the UE 508

D.2.1.5 Abnormal cases on the network side 508

D.2.1.6 Abnormal cases in the UE 509

D.2.2 UE-initiated UE state indication procedure 509

D.2.2.1 General 509

D.2.2.2 UE-initiated UE state indication procedure initiation 510

D.2.2.3 UE-initiated UE state indication procedure accepted by the network 510

D.2.2.4 Abnormal cases on the network side 510

D.3 UE policy re-assembly at the UE 510

D.4 Void 510

D.5 Message functional definition and contents 510

D.5.1 Manage UE policy command 510

D.5.1.1 Message definition 510

D.5.2 Manage UE policy complete 511

D.5.2.1 Message definition 511

D.5.3 Manage UE policy command reject 511

D.5.3.1 Message definition 511

D.5.4 UE state indication 512

D.5.4.1 Message definition 512

D.6 Information elements coding 513

D.6.1 UE policy delivery service message type 513

D.6.2 UE policy section management list 513

D.6.3 UE policy section management result 517

D.6.4 UPSI list 519

D.6.5 UE policy classmark 520

D.6.6 UE OS Id 521

D.7 Timers of UE policy delivery service 521

Annex E (informative): Change history 523

# 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 resources.

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), between the NG-RAN and the non-3GPP access network connected to the EPC, and between the non-3GPP access network connected to the 5G core network (5GCN) and the E-UTRAN.

For both NAS protocols the present document specifies procedures for the support of mobility between the NG-RAN and the non-3GPP access network connected to the 5GCN.

In addition, the present document specifies the procedures in the 5GS for UE policy delivery service between the UE and the policy control function (PCF) for both 3GPP access and non-3GPP access.

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

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

[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".

[4A] 3GPP TS 23.040: "Technical realization of Short Message Service (SMS)".

[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".

[6A] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[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 24.526: "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".

[20A] 3GPP TS 29.502: "5G System; Session Management Services; Stage 3".

[21] 3GPP TS 29.525: "5G System; UE Policy Control Service; Stage 3".

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

[22A] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[22B] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

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

[23A] 3GPP TS 33.401: "3GPP System Architecture Evolution; 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".

[25A] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC) protocol specification".

[25B] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description".

[25C] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[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)".

[31A] IEEE Std 802.3™-2018: "Ethernet".

[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: "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6"

[35A] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

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

[37] IETF RFC 7542: "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 public networks and subscriptions", 2016-09-23.

[43] IEEE Std 802-2014: "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture" (30 June 2014).

[44] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[45] 3GPP TS 24.250: "Protocol for Reliable Data Service; Stage 3".

[46] 3GPP TS 24.193: "Access Traffic Steering, Switching and Splitting; Stage 3".

[47] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

# 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 an 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.

**5G-EA:** 5GS encryption algorithms. The term 5G-EA, 5G-EA0, 128-5G-EA1-3 and 5G-EA4-7 used in the present document corresponds to the term NEA, NEA0, NEA1-3 and NEA4-7 defined in 3GPP TS 33.501 [24].

**5G-IA:** 5GS integrity algorithms. The term 5G-IA, 5G-IA0, 128-5G-IA1-3 and 5G-IA4-7 used in the present document corresponds to the term NIA, NIA0, NIA1-3 and NIA4-7 defined in 3GPP TS 33.501 [24].

**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.

**Aggregate maximum bit rate:** The maximum bit rate that limits the aggregate bit rate of a set of non-GBR bearers of a UE. Definition derived from 3GPP TS 23.501 [8].

**Always-on PDU session:** A PDU session for which user-plane resources have to be established during every transition from 5GMM-IDLE mode to 5GMM-CONNECTED mode. A UE requests a PDU session to be established as an always-on PDU session based on indication from upper layers and the network decides whether a PDU session is established as an always-on PDU session.

NOTE 1: How the upper layers in the UE are configured to provide an indication is outside the scope of the present document.

**Cleartext IEs:** Information elements that can be sent without confidentiality protection in initial NAS messages as specified in subclause 4.4.6.

**Control plane CIoT 5GS optimization:** signalling optimizations to enable efficient transport of user data (IP, Ethernet, Unstructured or SMS) over control plane via the AMF including optional header compression of IP data and Ethernet data.

**User plane CIoT 5GS optimization:** signalling optimizations to enable efficient transport of user data (IP, Ethernet or Unstructured) over the user plane.

**UE supporting CIoT 5GS optimizations:** A UE that supports control plane CIoT 5GS optimization or user plane CIoT 5GS optimization and one or more other CIoT 5GS optimizations when the UE is in N1 mode.

**Registered for 5GS services with control plane CIoT 5GS optimization:** A UE supporting CIoT 5GS optimizations is registered for 5GS services, and control plane CIoT 5GS optimization along with one or more other CIoT 5GS optimizations have been accepted by the network.

**Registered** **for 5GS services with user plane CIoT 5GS optimization:** A UE supporting CIoT 5GS optimizations is registered for 5GS services, and user plane CIoT 5GS optimization along with one or more other CIoT 5GS optimizations have been accepted by the network.

**Registered** **for 5GS services with CIoT 5GS optimization:** A UE is registered for 5GS services with control plane CIoT 5GS optimization or registered for 5GS services with user plane CIoT 5GS optimization.

**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.

**Emergency PDU session:** A PDU session which was established with the request type "initial emergency request" or "existing emergency PDU session".

**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.

**Initial NAS message:** A NAS message is considered as an initial NAS message, if this NAS message can trigger the establishment of an N1 NAS signalling connection. For instance, the REGISTRATION REQUEST message is an initial NAS message.

**Initial registration for emergency services:** A registration performed with 5GS registration type "emergency registration" in the REGISTRATION REQUEST message.

**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.

**Mapped S-NSSAI:** An S-NSSAI in the subscribed S-NSSAIs for the HPLMN, which is mapped to an S-NSSAI of the registered PLMN in case of a roaming scenario.

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

**In NB-N1 mode:** Indicates this paragraph applies only to a system which operates in NB-N1 mode. For a multi-access system this case applies if the current serving radio access network provides access to network services via E-UTRA connected to 5GCN by NB-IoT (see 3GPP TS 36.300 [25B], 3GPP TS 36.331 [25A], 3GPP TS 36.306 [25C]).

**In WB-N1 mode:** Indicates this paragraph applies only to a system which operates in WB-N1 mode. For a multi-access system this case applies if the system operates in N1 mode with E-UTRA connected to 5GCN, but not in NB-N1 mode.

**In WB-N1/CE mode:** Indicates this paragraph applies only when a UE, which is a CE mode B capable UE (see 3GPP TS 36.306 [25C]), is operating in CE mode A or B in WB-N1 mode.

**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.

**N6 PDU session:** A PDU session established between the UE and the User Plane Function (UPF) for transmitting the UE's IP data, Ethernet data or Unstructured data related to a specific application.

**NEF PDU session:** A PDU session established between the UE and the Network Exposure Function (NEF) for transmitting the UE's Unstructured data related to a specific application.

**Network slicing information:** information stored at the UE consisting of one or more of the following:

a) default configured NSSAI;

b) configured NSSAI for a PLMN;

c) mapped S-NSSAI(s) for the configured NSSAI for a PLMN;

d) for each access type:

1) allowed NSSAI for a PLMN;

2) mapped S-NSSAI(s) for the allowed NSSAI for a PLMN.

**Non-cleartext IEs:** Information elements that are not cleartext IEs.

**Non-emergency PDU session:** Any PDU session which is not an emergency PDU session.

**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.

**PDU session with suspended user-plane resources:** A PDU session for which user-plane resources were established or re-established, and for which data radio bearers were suspended when transiting to 5GMM-CONNECTED mode with RRC inactive indication.

**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, or allocated by the UE or the PCF for the UE policy delivery procedures. The procedure transaction identity is released when the procedure is completed but it should not be released immediately.

**RAT frequency selection priority index:** A parameter provided by the AMF to the NG-RAN via the N2 reference point. The AMF selects an RFSP index for a particular UE based on the subscribed RFSP index, the locally configured operator's policies, the allowed NSSAI and the UE context information, including the UE's usage setting, if received during the registration procedure. Definition derived from 3GPP TS 23.501 [8].

**Registered for emergency services:** A UE is considered as "registered for emergency services" when it has successfully completed initial registration for emergency services.

**Registered PLMN**: The PLMN on which the UE is registered. The identity of the registered PLMN (MCC and MNC) is provided to the UE within the GUAMI field of the 5G-GUTI.

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

**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 registration area:** 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".

**Local release:** Release of a PDU session without peer-to-peer signalling between the network and the UE,

NOTE 3: Local release can include communication among network entities.

**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.

**Routing indicator:** Routing Indicator is an identifier assigned by the UE's home network operator to be used together with the Home Network Identifier for routing network signalling. Routing Indicator is provisioned in the USIM. The term Routing indicator used in the present document corresponds to the term Routing ID used in 3GPP TS 23.501 [8].

**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].

**UE using 5GS services with control plane CIoT 5GS optimization:** AUE that is registered for 5GS services with the control plane CIOT 5GS optimization accepted by the network.

**User-plane resources:** Resources established between the UE and the UPF. The user-plane resources consist of either user plane radio bearers via the Uu reference point, a tunnel via the N3 reference point and a tunnel via the N9 reference point (if any) for 3GPP access, or IPsec tunnels via the NWu reference point, a tunnel via the N3 reference point and a tunnel via the N9 reference point (if any) for non-3GPP access.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.261 [2] apply:

**Non-public network**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.003 [4] apply:

**5G-GUTI**

**5G-S-TMSI**

**PEI**

**SUPI**

**SUCI**

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

**Country**

**EHPLMN**

**HPLMN**

**Selected PLMN**

**Shared network**

**SNPN identity**

**Steering of Roaming (SOR)**

**Steering of Roaming information**

**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 23.216 [6A] apply:

**SRVCC**

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-RG**

**5G-BRG**

**5G-CRG**

**5G System**

**Allowed area**

**Allowed NSSAI**

**AMF region**

**AMF set**

**Closed access group**

**Configured NSSAI**

**Local area data network**

**Network slice**

**NG-RAN**

**Non-allowed area**

**PDU session**

**PDU session type**

**Requested NSSAI**

**Routing ID**

**Service data flow**

**Service Gap Control**

**Serving PLMN rate control**

**SNPN access mode**

**SNPN enabled UE**

**Stand-alone Non-Public Network**

**UE presence in LADN service area**

**Wireline 5G Access Network**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.503 [10] apply:

**UE local configuration**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.008 [12] apply:

**GMM**

**MM**

**A/Gb mode**

**Iu mode**

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

**CIoT EPS optimization**

**Control plane CIoT EPS optimization**

**EENLV**

**EMM**

**EMM-DEREGISTERED**

**EMM-DEREGISTERED-INITIATED**

**EMM-IDLE mode**

**EMM-NULL**

**EMM-****REGISTERED**

**EMM-REGISTERED-INITIATED**

**EMM-SERVICE-REQUEST-INITIATED**

**EMM-TRACKING-AREA-UPDATING-INITIATED**

**EPS**

**EPS security context**

**EPS services**

**Lower layer failure**

**Megabit**

**Message header**

**NAS signalling connection recovery**

**NB-S1 mode**

**Non-EPS services**

**S1 mode**

**User plane CIoT EPS optimization**

**WB-S1 mode**

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**

**ABBA**

**Current 5G NAS security context**

**Full native 5G NAS security context**

**K'**AME

**K**AMF

**K**ASME

**Mapped 5G NAS security context**

**Mapped security context**

**Native 5G NAS security context**

**NCC**

**Non-current 5G NAS security context**

**Partial native 5G NAS 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

5G-RG 5G Residential Gateway

5G-BRG 5G Broadband Residential Gateway

5G-CRG 5G Cable Residential Gateway

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

CAG Closed access group

DL Downlink

DN Data Network

DNN Data Network Name

eDRX Extended DRX cycle

E-UTRAN Evolved Universal Terrestrial Radio Access Network

EAP-AKA' Improved Extensible Authentication Protocol method for 3rd generation Authentication and Key Agreement

ECIES Elliptic Curve Integrated Encryption Scheme

EPD Extended Protocol Discriminator

EMM EPS Mobility Management

EPC Evolved Packet Core Network

EPS Evolved Packet System

ESM EPS Session Management

FN-RG Fixed Network RG

FN-BRG Fixed Network Broadband RG

FN-CRG Fixed Network Cable RG

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

MAC Message Authentication Code

Mbps Megabits per second

MFBR Maximum Flow Bit Rate

MICO Mobile Initiated Connection Only

N3IWF Non-3GPP Inter-Working Function

NAI Network Access Identifier

NITZ Network Identity and Time Zone

NR New Radio

ngKSI Key Set Identifier for Next Generation Radio Access Network

NPN Non-public network

NSSAI Network Slice Selection Assistance Information

OS Operating System

OS Id OS Identity

PTI Procedure Transaction Identity

QFI QoS Flow Identifier

QoS Quality of Service

QRI QoS Rule Identifier

(R)AN (Radio) Access Network

RFSP RAT Frequency Selection Priority

RG Residential Gateway

RPLMN Registered PLMN

RQA Reflective QoS Attribute

RQI Reflective QoS Indication

RSNPN Registered SNPN

S-NSSAI Single NSSAI

SA Security Association

SDF Service Data Flow

SMF Session Management Function

SGC Service Gap Control

SNN Serving Network Name

SNPN Stand-alone Non-Public Network

SOR Steering of Roaming

TA Tracking Area

TAC Tracking Area Code

TAI Tracking Area Identity

Tbps Terabits per second

TMBR Total Maximum Bit Rate

UL Uplink

UPF User Plane Function

UPSC UE Policy Section Code

UPSI UE Policy Section Identifier

URN Uniform Resource Name

URSP UE Route Selection Policy

W-5GAN Wireline 5G Access Network

# 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  9.11.3.32 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | ABBA | ABBA  9.11.3.10 | M | LV | 3-n |
| 21 | Authentication parameter RAND (5G authentication challenge) | Authentication parameter RAND  9.11.3.16 | O | TV | 17 |
| 20 | Authentication parameter AUTN (5G authentication challenge) | Authentication parameter AUTN  9.11.3.15 | O | TLV | 18 |
| 78 | EAP message | EAP message  9.11.2.2 | 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 Void

#### 8.2.1.5 EAP message

EAP message IE is included if the AUTHENTICATION REQUEST message is used in an EAP based primary authentication and key agreement 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  9.11.3.17 | O | TLV | 18 |
| 78 | EAP message | EAP message  9.11.2.2 | 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  9.11.3.32 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |
| 38 | ABBA | ABBA  9.11.3.10 | O | TLV | 4-n |

#### 8.2.3.2 ABBA

This IE shall be included if the message contains an EAP message IE with an EAP-success message.

### 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  9.11.3.2 | M | V | 1 |
| 30 | Authentication failure parameter | Authentication failure parameter  9.11.3.14 | 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 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |

#### 8.2.5.2 EAP message

EAP message IE is included if the AUTHENTICATION REJECT message is used to convey EAP-failure message.

### 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  9.11.3.7 | M | V | 1/2 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
|  | 5GS mobile identity | 5GS mobile identity  9.11.3.4 | M | LV-E | 6-n |
| C- | Non-current native NAS key set identifier | NAS key set identifier  9.11.3.32 | O | TV | 1 |
| 10 | 5GMM capability | 5GMM capability  9.11.3.1 | O | TLV | 3-15 |
| 2E | UE security capability | UE security capability  9.11.3.54 | O | TLV | 4-10 |
| 2F | Requested NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-74 |
| 52 | Last visited registered TAI | 5GS tracking area identity  9.11.3.8 | O | TV | 7 |
| 17 | S1 UE network capability | S1 UE network capability  9.11.3.48 | O | TLV | 4-15 |
| 40 | Uplink data status | Uplink data status  9.11.3.57 | O | TLV | 4-34 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| B- | MICO indication | MICO indication  9.11.3.31 | O | TV | 1 |
| 2B | UE status | UE status  9.11.3.56 | O | TLV | 3 |
| 77 | Additional GUTI | 5GS mobile identity  9.11.3.4 | O | TLV-E | 14 |
| 25 | Allowed PDU session status | Allowed PDU session status  9.11.3.13 | O | TLV | 4-34 |
| 18 | UE's usage setting | UE's usage setting  9.11.3.55 | O | TLV | 3 |
| 51 | Requested DRX parameters | 5GS DRX parameters  9.11.3.2A | O | TLV | 3 |
| 70 | EPS NAS message container | EPS NAS message container  9.11.3.24 | O | TLV-E | 4-n |
| 74 | LADN indication | LADN indication  9.11.3.29 | O | TLV-E | 3-811 |
| 8- | Payload container type | Payload container type  9.11.3.40 | O | TV | 1 |
| 7B | Payload container | Payload container  9.11.3.39 | O | TLV-E | 4-65538 |
| 9- | Network slicing indication | Network slicing indication  9.11.3.36 | O | TV | 1 |
| 53 | 5GS update type | 5GS update type  9.11.3.9A | O | TLV | 3 |
| TBD | Mobile station classmark 2 | Mobile station classmark 2  9.11.3.61 | O | TLV | 5 |
| TBD | Supported codecs | Supported codec list  9.11.3.62 | O | TLV | 5-n |
| 71 | NAS message container | NAS message container  9.11.3.33 | O | TLV-E | 4-n |
| 60 | EPS bearer context status | EPS bearer context status  9.11.3.60 | O | TLV | 4 |
| XX | Requested extended DRX parameters | Extended DRX parameters  9.11.3.60 | O | TLV | 3 |
| TBD | T3324 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |

#### 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 the 5GS registration type IE:

a) indicates "initial registration" or "mobility registration updating", and:

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

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

3) the UE has neither allowed NSSAI for the current PLMN nor configured NSSAI for the current PLMN and has a default configured NSSAI.

#### 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 when the UE needs to indicate the PDU sessions that are associated with the access type that 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 supports 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 security context.

#### 8.2.6.17 LADN indication

The UE shall include this information element when the UE needs to request LADN information for specific LADN DNN(s) or to indicate a request for LADN information.

#### 8.2.6.17A Payload container type

This IE shall be included if the UE includes the Payload container IE.

NOTE: In this version of the protocol, the Payload container type IE in the REGISTRATION REQUEST message is set to "UE policy container" as described in subclauses 5.5.1.2.2 and 5.5.1.3.2.

#### 8.2.6.18 Payload container

This IE shall be included if the UE has one or more stored UE policy sections identified by a UPSI with the PLMN ID part indicating the HPLMN or the selected PLMN 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.

#### 8.2.6.19 Network slicing indication

This IE shall be included when a requested NSSAI is included in the REGISTRATION REQUEST message and the requested NSSAI is created from the default configured NSSAI.

#### 8.2.6.20 5GS update type

This IE shall be included when the UE is performing the registration procedure to indicate any of the following:

a) the UE requests the use of SMS over NAS or there is a change in the UE's requirements to use SMS over NAS;

b) a change in the UE's radio capability for NG-RAN; or

c) the UE requests CIoT 5GS optimizations.

#### 8.2.6.21 NAS message container

This IE shall be included if the UE is sending a REGISTRATION REQUEST message as an initial NAS message, the UE has a valid 5G NAS security context and the UE needs to send non-cleartext IEs.

#### 8.2.6.22 Requested extended DRX parameters

The UE shall include this IE if the UE needs to use extended DRX or change the extended DRX parameters.

#### 8.2.6.23 EPS bearer context status

The UE shall include this IE if the UE operating in the single-registration mode performs inter-system change from S1 mode to N1 mode and the UE has locally deactivated EPS bearer context(s) for which interworking to 5GS is supported while the UE was in S1 mode without notifying the network.

#### 8.2.6.24 T3324 value

The UE may include this IE during the registration update procedure if it requests to use MICO mode and use the active time timer.

#### 8.2.6.25 Mobile station classmark 2

This IE shall be included if the UE supports 5G-SRVCC from NG-RAN to UTRAN (see 3GPP TS 23.216 [6A]).

#### 8.2.6.26 Supported codecs

This IE shall be included if the UE supports 5G-SRVCC from NG-RAN to UTRAN.

### 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  9.11.3.6 | M | LV | 2 |
| 77 | 5G-GUTI | 5GS mobile identity  9.11.3.4 | O | TLV-E | 14 |
| 4A | Equivalent PLMNs | PLMN list  9.11.3.45 | O | TLV | 5-47 |
| 54 | TAI list | 5GS tracking area identity list  9.11.3.9 | O | TLV | 9-114 |
| 15 | Allowed NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-74 |
| 11 | Rejected NSSAI | Rejected NSSAI  9.11.3.46 | O | TLV | 4-42 |
| 31 | Configured NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-146 |
| 21 | 5GS network feature support | 5GS network feature support  9.11.3.5 | O | TLV | 3-5 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| 26 | PDU session reactivation result | PDU session reactivation result  9.11.3.42 | O | TLV | 4-34 |
| 72 | PDU session reactivation result error cause | PDU session reactivation result error cause  9.11.3.43 | O | TLV-E | 5-515 |
| 79 | LADN information | LADN information  9.11.3.30 | O | TLV-E | 12-1715 |
| B- | MICO indication | MICO indication  9.11.3.31 | O | TV | 1 |
| 9- | Network slicing indication | Network slicing indication  9.11.3.36 | O | TV | 1 |
| 27 | Service area list | Service area list  9.11.3.49 | O | TLV | 6-114 |
| 5E | T3512 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 5D | Non-3GPP de-registration timer value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 16 | T3502 value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 34 | Emergency number list | Emergency number list  9.11.3.23 | O | TLV | 5-50 |
| 7A | Extended emergency number list | Extended emergency number list  9.11.3.26 | O | TLV-E | 7-65538 |
| 73 | SOR transparent container | SOR transparent container  9.11.3.51 | O | TLV-E | 20-n |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| A- | NSSAI inclusion mode | NSSAI inclusion mode  9.11.3.37A | O | TV | 1 |
| 76 | Operator-defined access category definitions | Operator-defined access category definitions  9.11.3.38 | O | TLV-E | 3-n |
| 51 | Negotiated DRX parameters | 5GS DRX parameters  9.11.3.2A | O | TLV | 3 |
| D- | Non-3GPP NW policies | Non-3GPP NW provided policies  9.11.3.58 | O | TV | 1 |
| 60 | EPS bearer context status | EPS bearer context status  9.11.3.59 | O | TLV | 4 |
| xx | Negotiated extended DRX parameters | Extended DRX parameters  9.11.3.60 | O | TLV | 3 |
| tbd | T3447 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| XX | T3448 value | GPRS timer 3  9.11.2.4 | O | TLV | 3 |
| TBD | T3324 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |

#### 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 when the network needs to indicate the PDU sessions that are 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 for which the user-plane resources can be re-established 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 Network slicing indication

This IE shall be included if the user's network slicing subscription has changed in the UDM.

#### 8.2.7.15 Service area list

This IE may be included to assign new service area restrictions to the UE.

#### 8.2.7.16 T3512 value

The AMF shall include this IE during a registration procedure over 3GPP access when the 5GS registration type IE does not indicate "periodic registration updating". The AMF may include this IE during the mobility and periodic registration update procedure over 3GPP access when the 5GS registration type IE indicates "periodic registration updating".

#### 8.2.7.17 Non-3GPP de-registration timer value

This IE may be included if the network needs to indicate to the UE registered over non-3GPP access the value of a non-3GPP de-registration timer value.

#### 8.2.7.18 T3502 value

This IE may be included to indicate a value for timer T3502.

#### 8.2.7.19 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 PLMN from which this IE is received.

#### 8.2.7.20 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 PLMN from which this IE is received or valid only in the PLMN from which this IE is received.

#### 8.2.7.21 SOR 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.

#### 8.2.7.22 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.

#### 8.2.7.23 NSSAI inclusion mode

This IE shall be included if required by operatory policy.

#### 8.2.7.24 Operator-defined access category definitions

This IE may be included to assign new operator-defined access category definitions to the UE or delete the operator-defined access category definitions at the UE side.

#### 8.2.7.25 Negotiated DRX parameters

The network shall include this IE if the Requested DRX parameters IE was included in the REGISTRATION REQUEST message.

#### 8.2.7.26 Non-3GPP NW provided policies

The AMF shall not include this IE during a registration procedure over non-3GPP access.

This IE is included if the network needs to indicate whether emergency numbers provided via non-3GPP access can be used to initiate UE detected emergency calls (see 3GPP TS 24.302 [16]). 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.

NOTE: In this version of the specification, this IE is applicable in case the UE is connected to a PLMN using an ePDG as specified in 3GPP TS 24.302 [16].

#### 8.2.7.27 Negotiated extended DRX parameters

The network shall include the Negotiated extended DRX parameters IE if:

- the UE included the Requested extended DRX parameters IE in the REGISTRATION REQUEST message; and

- the network supports eDRX and accepts the use of eDRX.

#### 8.2.7.28 T3447 value

The network may include T3447 value IE if:

- the UE has indicated support for service gap control in the REGISTRATION REQUEST message; and

- the 5GMM context contains a service gap time value.

#### 8.2.7.29 T3448 value

The network may include this IE if the congestion control for transport of user data via the control plane is active and the UE supports the control plane CIoT 5GS optimizations.

#### 8.2.7.30 T3324 value

The AMF shall include this IE if the UE has requested active time value in the REGISTRATION REQEUST message and the AMF decides to accept the use of MICO mode and the use of the active time.

#### 8.2.7.31 EPS bearer context status

This IE shall be included when the network generated an EPS bearer context status information for the UE during the inter-system change from S1 mode to N1 mode and the network supports N26 interface.

### 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  9.7 | M | V | 1 |
| 73 | SOR transparent container | SOR transparent container  9.11.3.51 | O | TLV-E | 20 |

#### 8.2.8.2 SOR 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 SOR 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  9.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.11.3.2 | M | V | 1 |
| 5F | T3346 value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 16 | T3502 value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.11.2.2 | 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  9.11.3.40 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Payload container | Payload container  9.11.3.39 | M | LV-E | 3-65537 |
| 12 | PDU session ID | PDU session identity 2  9.11.3.41 | C | TV | 2 |
| 59 | Old PDU session ID | PDU session identity 2  9.11.3.41 | O | TV | 2 |
| 8 | Request type | Request type  9.11.3.47 | O | TV | 1 |
| 22 | S-NSSAI | S-NSSAI  9.11.2.8 | O | TLV | 3-10 |
| 25 | DNN | DNN  9.11.2.1A | O | TLV | 3-102 |
| 24 | Additional information | Additional information  9.11.2.1 | O | TLV | 3-n |
| Z | MA PDU session information | MA PDU session information | O | TV | 1 |

#### 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" and the Payload container type IE is set to "N1 SM information".

#### 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 or the PDU SESSION MODIFICATION REQUEST which is not initiated to indicate a change of 3GPP PS data off UE status associated to a PDU session.

#### 8.2.10.5 S-NSSAI

The UE may include this IE when the Request type IE is set to "initial request" or "existing PDU session" and the Payload container type IE is set to "N1 SM information".

#### 8.2.10.6 DNN

The UE may include this IE when the Request type IE is set to "initial request" or "existing PDU session" and the Payload container type IE is set to "N1 SM information".

#### 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".

#### 8.2.10.8 MA PDU session information

The UE may include this IE if the Request type IE is included in the UL NAS TRANSPORT message.

### 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  9.11.3.40 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Payload container | Payload container  9.11.3.39 | M | LV-E | 3-65537 |
| 12 | PDU session ID | PDU session identity 2  9.11.3.41 | C | TV | 2 |
| 24 | Additional information | Additional information  9.11.2.1 | O | TLV | 3-n |
| 58 | 5GMM cause | 5GMM cause  9.11.3.2 | O | TV | 2 |
| 37 | Back-off timer value | GPRS timer 3  9.11.2.5 | 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 and the Payload container type IE is not set to "Multiple payloads".

#### 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 and the Payload container type IE is not set to "Multiple payloads".

### 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  9.11.3.20 | M | V | 1/2 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
|  | 5GS mobile identity | 5GS mobile identity  9.11.3.4 | M | LV-E | 6-n |

### 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  9.11.3.20 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
| 58 | 5GMM cause | 5GMM cause  9.11.3.2 | O | TV | 2 |
| 5F | T3346 value | GPRS timer 2  9.11.2.4 | 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 established 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  9.11.3.32 | M | V | 1/2 |
|  | Service type | Service type  9.11.3.50 | M | V | 1/2 |
|  | 5G-S-TMSI | 5GS mobile identity  9.11.3.4 | M | LV-E | 9 |
| 40 | Uplink data status | Uplink data status  9.11.3.57 | O | TLV | 4-34 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| 25 | Allowed PDU session status | Allowed PDU session status  9.11.3.13 | O | TLV | 4-34 |
| 71 | NAS message container | NAS message container  9.11.3.33 | O | TLV-E | 4-n |

#### 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 when the UE needs to indicate the PDU sessions that are associated with the access type that 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 needs 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.

#### 8.2.16.5 NAS message container

This IE shall be included if the UE is sending a SERVICE REQUEST message as an initial NAS message and the UE needs to send non-cleartext IEs.

### 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  9.11.3.44 | O | TLV | 4-34 |
| 26 | PDU session reactivation result | PDU session reactivation result  9.11.3.42 | O | TLV | 4-34 |
| 72 | PDU session reactivation result error cause | PDU session reactivation result error cause  9.11.3.43 | O | TLV-E | 5-515 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| XX | T3448 value | GPRS timer 3  9.11.2.4 | O | TLV | 3 |

#### 8.2.17.2 PDU session status

This IE shall be included when the network needsto indicate the PDU sessions that are associated with the access type that 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 for which user-plane resources can be re-established 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.

#### 8.2.17.6 T3448 value

The network may include this IE if the congestion control for transport of user data via the control plane is active and the UE supports the control plane CIoT 5GS optimizations.

### 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  9.11.3.2 | M | V | 1 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| 5F | T3346 value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| XX | T3448 value | GPRS timer 3  9.11.2.4 | O | TLV | 3 |

#### 8.2.18.2 PDU session status

This IE shall be included when the network needs to indicate the PDU sessions that are associated with the access type that 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.

#### 8.2.18.5 T3448 value

The network may include this IE if the congestion control for transport of user data via the control plane is active and the UE supports the control plane CIoT 5GS optimizations.

### 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  9.11.3.18 | O | TV | 1 |
| 77 | 5G-GUTI | 5GS mobile identity  9.11.3.4 | O | TLV-E | 14 |
| 54 | TAI list | 5GS tracking area identity list  9.11.3.9 | O | TLV | 9-114 |
| 15 | Allowed NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-74 |
| 27 | Service area list | Service area list  9.11.3.49 | O | TLV | 6-114 |
| 43 | Full name for network | Network name  9.11.3.35 | O | TLV | 3-n |
| 45 | Short name for network | Network name  9.11.3.35 | O | TLV | 3-n |
| 46 | Local time zone | Time zone  9.11.3.52 | O | TV | 2 |
| 47 | Universal time and local time zone | Time zone and time  9.11.3.53 | O | TV | 8 |
| 49 | Network daylight saving time | Daylight saving time  9.11.3.19 | O | TLV | 3 |
| 79 | LADN information | LADN information  9.11.3.30 | O | TLV-E | 3-1715 |
| B- | MICO indication | MICO indication  9.11.3.31 | O | TV | 1 |
| 9- | Network slicing indication | Network slicing indication  9.11.3.36 | O | TV | 1 |
| 31 | Configured NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-146 |
| 11 | Rejected NSSAI | Rejected NSSAI  9.11.3.46 | O | TLV | 4-42 |
| 76 | Operator-defined access category definitions | Operator-defined access category definitions  9.11.3.38 | O | TLV-E | 3-n |
| F- | SMS indication | SMS indication  9.11.3.50A | O | TV | 1 |
| Tbd | T3447 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |

#### 8.2.19.2 Configuration update indication

The AMF shall include this IE if the AMF needs 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 request the UE to re-negotiate MICO mode.

#### 8.2.19.14 Network slicing indication

This IE shall be included if the user's network slicing subscription has changed in the UDM.

#### 8.2.19.15 Configured NSSAI

The AMF shall include this IE when the AMF needs to provide the UE with a new configured NSSAI for the current PLMN.

#### 8.2.19.16 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 considered to be rejected by the network.

#### 8.2.19.17 Operator-defined access category definitions

This IE may be included to assign new operator-defined access category definitions to the UE or delete the operator-defined access category definitions at the UE side.

#### 8.2.19.18 SMS indication

This IE may be included to indicate that the ability for the UE to use SMS over NAS has changed.

#### 8.2.19.19

This IE may be included to assign a new T3447 value to the UE.

### 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  9.11.3.3 | 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  9.11.3.4 | M | LV-E | 3-n |

### 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  9.11.3.11 | 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  9.11.3.44 | O | TLV | 4-34 |

#### 8.2.24.2 PDU session status

This information element shall be included when the UE needs to indicate over non-3GPP access the type of the PDU sessions that are 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  9.11.3.34 | M | V | 1 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Replayed UE security capabilities | UE security capability  9.11.3.54 | M | LV | 3-9 |
| E- | IMEISV request | IMEISV request  9.11.3.28 | O | TV | 1 |
| 57 | Selected EPS NAS security algorithms | EPS NAS security algorithms  9.11.3.25 | O | TV | 2 |
| 36 | Additional 5G security information | Additional 5G security information  9.11.3.12 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 38 | ABBA | ABBA  9.11.3.10 | O | TLV | 4-n |
| 19 | Replayed S1 UE security capabilities | S1 UE security capability  9.11.3.48A | O | TLV | 4-7 |

#### 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 Void

#### 8.2.25.4 Selected EPS NAS security algorithms

This IE shall be included if the AMF supports 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 Additional 5G security information

The network shall include this IE if:

a) the network needs to provide the UE with horizontal derivation parameter; or

b) the initial NAS message (i.e. REGISTRATION REQUEST or SERVICE REQUEST) does not successfully pass the integrity check at the AMF (see subclause 5.4.2.2).

#### 8.2.25.6 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.

#### 8.2.25.7 ABBA

This IE shall be included if the message contains an EAP message IE with an EAP-success message.

#### 8.2.25.8 Replayed S1 UE security capabilities

This IE shall be included if the Selected EPS NAS security algorithms information element is included.

### 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 |
| 77 | IMEISV | 5G mobile identity  9.11.3.4 | O | TLV-E | 12 |
| 71 | NAS message container | NAS message container  9.11.3.33 | O | TLV-E | 4-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 or service request procedure, the AMF included the Additional 5G security information with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message as described in 3GPP TS 33.501 [24]; and

b) if during an ongoing registration procedure, the UE does not have a valid 5G NAS security context.

### 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  9.11.3.2 | 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 plain 5GS 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  9.5 | M | V | 1/2 |
|  | Message authentication code | Message authentication code  9.8 | M | V | 4 |
|  | Sequence number | Sequence number  9.10 | M | V | 1 |
|  | Plain 5GS NAS message | Plain 5GS NAS message  9.9 | 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  9.11.3.2 | M | V | 1 |

## 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 |
|  | Integrity protection maximum data rate | Integrity protection maximum data rate  9.11.4.7 | M | V | 2 |
| 9- | PDU session type | PDU session type  9.11.4.11 | O | TV | 1 |
| A- | SSC mode | SSC mode  9.11.4.16 | O | TV | 1 |
| 28 | 5GSM capability | 5GSM capability  9.11.4.1 | O | TLV | 3-15 |
| 55 | Maximum number of supported packet filters | Maximum number of supported packet filters  9.11.4.9 | O | TV | 3 |
| B- | Always-on PDU session requested | Always-on PDU session requested  9.11.4.4 | O | TV | 1 |
| 39 | SM PDU DN request container | SM PDU DN request container  9.11.4.15 | O | TLV | 3-255 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.1.2 PDU session type

This IE shall be included in the message when the UE requests to establish a new PDU session.

#### 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:

a) the UE requests to establish a new PDU session of "IPv4", "IPv6", "IPv4v6" or "Ethernet" PDU session type and the UE supports Reflective QoS;

b) the UE requests to establish a new PDU session of "IPv6" or "IPv4v6" PDU session type and the UE supports multi-homed IPv6 PDU session;

c) the UE requests to transfer an existing PDN connection of "IPv4", "IPv6", "IPv4v6" or "non-IP" PDN type mapping to "Ethernet" PDU session type in the EPS to the 5GS and the UE supports Reflective QoS;

d) the UE requests to transfer an existing PDN connection of "IPv4", "IPv6" or "IPv4v6" PDN type in an untrusted non-3GPP access connected to the EPC to the 5GS and the UE supports Reflective QoS;

e) the UE requests to transfer an existing PDN connection of "IPv6" or "IPv4v6" PDN type in the EPS or in an untrusted non-3GPP access connected to the EPC to the 5GS and the UE supports multi-homed IPv6 PDU session;

f) the UE requests to establish a new PDU session of "Ethernet" PDU session type and the UE supports Ethernet PDN type in S1 mode;

g) the UE requests to transfer an existing PDU session of "Ethernet" PDN type in the EPS and the UE supports Ethernet PDN type in S1 mode; or

h) the UE supports ATSSS-LL functionality or MPTCP functionality or both (see 3GPP TS 24.193 [46]).

#### 8.3.1.6 Void

#### 8.3.1.7 Always-on PDU session requested

The UE shall include this IE if the UE requests to establish a PDU session as an always-on PDU session.

#### 8.3.1.8 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.

#### 8.3.1.9 Extended protocol configuration options

This IE is included in the message when the UE needs 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  9.11.4.11 | M | V | 1/2 |
|  | Selected SSC mode | SSC mode  9.11.4.16 | M | V | 1/2 |
|  | Authorized QoS rules | QoS rules  9.11.4.13 | M | LV-E | 6-65538 |
|  | Session AMBR | Session-AMBR  9.11.4.14 | M | LV | 7 |
| 59 | 5GSM cause | 5GSM cause  9.11.4.2 | O | TV | 2 |
| 29 | PDU address | PDU address  9.11.4.10 | O | TLV | 7, 11 or 15 |
| 56 | RQ timer value | GPRS timer  9.11.2.3 | O | TV | 2 |
| 22 | S-NSSAI | S-NSSAI  9.11.2.8 | O | TLV | 3-10 |
| 8- | Always-on PDU session indication | Always-on PDU session indication  9.11.4.3 | O | TV | 1 |
| 75 | Mapped EPS bearer contexts | Mapped EPS bearer contexts  9.11.4.8 | O | TLV-E | 7-65538 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 79 | Authorized QoS flow descriptions | QoS flow descriptions  9.11.4.12 | O | TLV-E | 6-65538 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 25 | DNN | DNN  9.11.2.1A | O | TLV | 3-102 |
| xx | 5GSM network feature support | 5GSM network feature support  9.11.4.18 | O | TLV | 3-15 |
| xx | Session-TMBR | Session-TMBR  9.11.4.19 | O | TLV | 8 |
| TBD | Serving PLMN rate control | Serving PLMN rate control  9.11.4.20 | O | TLV | 4 |
| XX | ATSSS container | ATSSS container  9.11.4.22 | O | TLV-E | 3-65538 |
| XX | Control plane only indication | Control plane only indication  9.11.4.23 | O | TV | 1 |

#### 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 needs 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 Always-on PDU session indication

The network shall include this IE if the network decides to inform the UE whether the PDU session is established as an always-on PDU session.

#### 8.3.2.7 Mapped EPS bearer contexts

This IE is included when interworking with EPS is supported for the PDU session.

#### 8.3.2.8 EAP message

This IE is included when the external DN successfully performed authentication and authorization of the UE using EAP.

#### 8.3.2.9 Authorized QoS flow descriptions

This IE is included when the network needs to provide authorized QoS flow descriptions.

#### 8.3.2.10 Extended protocol configuration options

This IE is included in the message when the network needs to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

#### 8.3.2.11 DNN

The IE shall be included in the message when the PDU session is a non-emergency PDU session.

#### 8.3.2.12 5GSM network feature support

This IE is included when the network needs to indicate support of 5GSM network features.

#### 8.3.2.13 Session-TMBR

The IE is included when the network needs to send session-TMBR.

#### 8.3.2.14 Serving PLMN rate control

This IE shall be included when the network wishes to indicate the maximum uplink control plane user data the UE is allowed to send per 6 minute interval.

#### 8.3.2.15 ATSSS container

The IE shall be included in the message when the PDU session is an MA PDU session.

#### 8.3.2.16 Control plane only indication

The network shall include the control plane only indication IE if the network determines that the associated PDU session is only for control plane CIoT 5GS optimization.

### 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  9.11.4.2 | M | V | 1 |
| 37 | Back-off timer value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| F- | Allowed SSC mode | Allowed SSC mode  9.11.4.5 | O | TV | 1 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| TBD | Re-attempt indicator | Re-attempt indicator  9.11.4.17 | O | TLV | 3 |
| 61 | 5GSM congestion re-attempt indicator | 5GSM congestion re-attempt indicator  9.11.4.21 | O | TLV | 3 |

#### 8.3.3.2 Back-off timer value

The network may include this IE if the 5GSM cause is not #28 "unknown PDU session type", #46 "out of LADN service area", #50 "PDU session type IPv4 only allowed", #51 "PDU session type IPv6 only allowed", #54 "PDU session does not exist", or #68 "not supported SSC mode", 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 needs to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

#### 8.3.3.6 Re-attempt indicator

The network may include this IE if the network includes the Back-off timer value IE and the 5GSM cause value is not #26 "insufficient resources", #28 "unknown PDU session type", #46 "out of LADN service area", #54 "PDU session does not exist", #67 "insufficient resources for specific slice and DNN", #68 "not supported SSC mode", or #69 "insufficient resources for specific slice".

#### 8.3.3.7 5GSM congestion re-attempt indicator

The network may include this IE only if it includes the Back-off timer value IE and the 5GSM cause value is either #67 "insufficient resources for specific slice and DNN" or #69 "insufficient resources for specific slice".

### 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 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.4.2 Extended protocol configuration options

This IE is included in the message when the network needs to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

NOTE: How the Extended protocol configuration options IE is used by the network and the UE during the PDU session authentication and authorization procedure is not specified in this release of the specification.

### 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 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.5.2 Extended protocol configuration options

This IE is included in the message when the UE needs to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

NOTE: How the Extended protocol configuration options IE is used by the network and the UE during the PDU session authentication and authorization procedure is not specified in this release of the specification.

### 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  9.11.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.6.2 EAP message

This IE shall be 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 needs to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

NOTE: How the Extended protocol configuration options IE is used by the network and the UE during the PDU session authentication and authorization procedure is not specified in this release of the specification.

### 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  9.11.4.1 | O | TLV | 3-15 |
| 59 | 5GSM cause | 5GSM cause  9.11.4.2 | O | TV | 2 |
| 55 | Maximum number of supported packet filters | Maximum number of supported packet filters  9.11.4.9 | O | TV | 3 |
| B- | Always-on PDU session requested | Always-on PDU session requested  9.11.4.4 | O | TV | 1 |
| 13 | Integrity protection maximum data rate | Integrity protection maximum data rate  9.11.4.7 | O | TV | 3 |
| 7A | Requested QoS rules | QoS rules  9.11.4.13 | O | TLV-E | 7-65538 |
| 79 | Requested QoS flow descriptions | QoS flow descriptions  9.11.4.12 | O | TLV-E | 6-65538 |
| 75 | Mapped EPS bearer contexts | Mapped EPS bearer contexts  9.11.4.8 | O | TLV-E | 7-65538 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

NOTE: It is possible for UEs compliant with earlier versions of this specification to send the Mapped EPS bearer contexts IE with IEI of value "7F" for this message.

#### 8.3.7.2 5GSM capability

This IE is included in the message:

1) for a PDN connection established when in S1 mode, after the first inter-system change from S1 mode to N1 mode, if the UE is operating in single-registration mode in the network supporting N26 interface and:

a) if the PDU session is of "IPv4", "IPv6", "IPv4v6" or "Ethernet" PDU session type, and the UE supports reflective QoS; or

b) if the PDU session is of "IPv6" or "IPv4v6" PDU session type, and the UE supports multi-homed IPv6 PDU session; or

2) if the UE needs to revoke the previously indicated support of reflective QoS.

#### 8.3.7.3 5GSM cause

This IE is included in the message when the UE releases the PDU session due to semantic or syntactical errors in QoS operations, or due to semantic or syntactical errors in packet filters.

#### 8.3.7.4 Maximum number of supported packet filters

This IE shall be included in the message for a PDN connection established when in S1 mode, after the first inter-system change from S1 mode to N1 mode, if the UE is operating in single-registration mode in the network supporting N26 interface, the PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet", and the UE can support more than 16 packet filters for this PDU session.

#### 8.3.7.5 Always-on PDU session requested

This IE shall be included in the message for a PDN connection established when in S1 mode, after the first inter-system change from S1 mode to N1 mode, if the UE is operating in single-registration mode in the network supporting N26 interface and the UE requests the PDU session to be an always-on PDU session in the 5GS.

#### 8.3.7.6 Integrity protection maximum data rate

This IE shall be included in the message for a PDN connection established when in S1 mode, after the first inter-system change from S1 mode to N1 mode, if the UE is operating in single-registration mode in the network supporting N26 interface.

#### 8.3.7.7 Requested QoS rules

This IE is included in the message when the UE requests a specific QoS handling.

#### 8.3.7.8 Requested QoS flow descriptions

This IE is included in the message when the UE requests a specific QoS flow descriptions.

#### 8.3.7.9 Extended protocol configuration options

This IE is included in the message when the UE needs to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the network.

#### 8.3.7.10 Mapped EPS bearer contexts

This IE is included when the UE requests to delete one or more mapped EPS bearer contexts.

### 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  9.11.4.2 | M | V | 1 |
| 37 | Back-off timer value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| TBD | Re-attempt indicator | Re-attempt indicator  9.11.4.17 | O | TLV | 3 |
| 61 | 5GSM congestion re-attempt indicator | 5GSM congestion re-attempt indicator  9.11.4.21 | O | TLV | 3 |

#### 8.3.8.2 Back-off timer value

The network may include this IE if the 5GSM cause is not #46 "out of LADN service area", 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 needs to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

#### 8.3.8.4 Re-attempt indicator

The network may include this IE only if it includes the Back-off timer value IE and the 5GSM cause value is not #26 "insufficient resources", #46 "out of LADN service area", #67 "insufficient resources for specific slice and DNN", or #69 "insufficient resources for specific slice".

#### 8.3.8.5 5GSM congestion re-attempt indicator

The network may include this IE only if it includes the Back-off timer value IE and the 5GSM cause value is either #67 "insufficient resources for specific slice and DNN" or #69 "insufficient resources for specific slice".

### 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  9.11.4.2 | O | TV | 2 |
| 2A | Session AMBR | Session-AMBR  9.11.4.14 | O | TLV | 8 |
| 56 | RQ timer value | GPRS timer  9.11.2.3 | O | TV | 2 |
| 8- | Always-on PDU session indication | Always-on PDU session indication  9.11.4.3 | O | TV | 1 |
| 7A | Authorized QoS rules | QoS rules  9.11.4.13 | O | TLV-E | 7-65538 |
| 75 | Mapped EPS bearer contexts | Mapped EPS bearer contexts  9.11.4.8 | O | TLV-E | 7-65538 |
| 79 | Authorized QoS flow descriptions | QoS flow descriptions  9.11.4.12 | O | TLV-E | 6-65538 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| xx | Session-TMBR | Session-TMBR  9.11.4.19 | O | TLV | 8 |

NOTE: It is possible for networks compliant with earlier versions of this specification to send the Mapped EPS bearer contexts IE with IEI of value "7F" for this message.

#### 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 needs to provide the RQ timer value.

#### 8.3.9.5 Always-on PDU session indication

The network shall include this IE if the network decides to inform the UE whether the PDU session is an always-on PDU session.

#### 8.3.9.6 Authorized QoS rules

This IE is included when the authorized QoS rules of the PDU session are modified.

#### 8.3.9.7 Mapped EPS bearer contexts

This IE is included when interworking with EPS is supported for the PDU session and the mapped EPS bearer contexts is modified.

#### 8.3.9.8 Authorized QoS flow descriptions

This IE is included when the authorized QoS flow descriptions of the PDU session are modified.

#### 8.3.9.9 Extended protocol configuration options

This IE is included in the message when the network needs to transmit (protocol) data (e.g. configuration parameters, error codes or messages/events) to the UE.

#### 8.3.9.10 Session-TMBR

The IE is included when the network needs to send session-TMBR.

### 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  9.11.4.6 | O | TLV-E | 4-65538 |

NOTE: It is possible for UEs compliant with earlier versions of this specification to include the 5GSM cause IE with IEI 59 in the PDU SESSION MODIFICATION COMPLETE message, and therefore the IEI 59 cannot be used for other optional IEs other than the 5GSM cause IE for future extensions of the PDU SESSION MODIFICATION COMPLETE message.

#### 8.3.10.2 Extended protocol configuration options

This IE is included in the message when the UE needs 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  9.11.4.2 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.11.2 Extended protocol configuration options

This IE is included in the message when the UE needs 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 |
| 59 | 5GSM cause | 5GSM cause  9.11.4.2 | O | TV | 2 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.12.2 5GSM cause

This IE is included in the message when the UE releases the PDU session due to semantic or syntactical errors in QoS operations, or due to semantic or syntactical errors in packet filters.

#### 8.3.12.3 Extended protocol configuration options

This IE is included in the message when the UE needs 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 SESSION RELEASE REJECT message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.11.4.2 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.13.2 Extended protocol configuration options

This IE is included in the message when the network needs 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  9.11.4.2 | M | V | 1 |
| 37 | Back-off timer value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 61 | 5GSM congestion re-attempt indicator | 5GSM congestion re-attempt indicator  9.11.4.21 | O | TLV | 3 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | 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.

#### 8.3.14.5 5GSM congestion re-attempt indicator

The network may include this IE only if it includes the Back-off timer value IE and the 5GSM cause value is either #67 "insufficient resources for specific slice and DNN" or #69 "insufficient resources for specific slice".

### 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 |
| 59 | 5GSM cause | 5GSM cause  9.11.4.2 | O | TV | 2 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.15.2 5GSM cause

This IE is included in the message when the UE needs to indicate to the network that an error encountered with a mandatory information element in the PDU SESSION RELEASE COMMAND message.

#### 8.3.15.3 Extended protocol configuration options

This IE is included in the message when the UE needs 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  9.11.4.2 | M | V | 1 |

# 9 General message format and information elements coding

## 9.1 Overview

### 9.1.1 NAS message format

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 associated with a half spare octet 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 associated with a half spare octet;

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.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Extended protocol discriminator | | | | | | | | octet 1 |
| Security header type associated with a spare half octet; or  PDU session identity | | | | | | | | octet 2 |
| Procedure transaction identity | | | | | | | | octet 2a\* |
| Message type | | | | | | | | octet 3 |
|  | | | | | | | | octet 4 |
| Other information elements as required | | | | | | | |  |
|  | | | | | | | | octet n |

Figure 9.1.1.1: 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.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Extended protocol discriminator | | | | | | | | octet 1 |
| Security header type associated with a spare half octet | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
| Message authentication code | | | | | | | |  |
|  | | | | | | | |  |
|  | | | | | | | | octet 6 |
| Sequence number | | | | | | | | octet 7 |
|  | | | | | | | | octet 8 |
| Plain 5GS NAS message | | | | | | | |  |
|  | | | | | | | | octet n |

Figure 9.1.1.2: General message organization example for a security protected 5GS NAS message

Unless specified otherwise in the message descriptions of clause 8 and annex D, a particular information element shall not be present more than once in a given message.

### 9.1.2 Field format and mapping

When a field is contained within a single octet, the lowest numbered bit of the field represents the least significant bit.

When a field extends over more than one octet, the order of bit values progressively decreases as the octet number increases. In that part of the field contained in a given octet, the lowest numbered bit represents the least significant bit. 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.

For example, a bit number can be identified as a couple (o, b) where o is the octet number and b is the relative bit number within the octet. Figure 9.1.2.1 illustrates a field that spans from bit (1, 3) to bit (2, 7). The most significant bit of the field is mapped on bit (1, 3) and the least significant bit is mapped on bit (2, 7).

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  |  |  |  |  | 24 | 23 | 22 | 1st octet of field |
| 21 | 20 |  |  |  |  |  |  | 2nd octet of field |

Figure 9.1.2.1: Field mapping convention

## 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. | | | | |

A 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. Bits 1 to 8 of the first octet of every UE policy delivery 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 message if a valid 5G NAS security context exists and security functions are started.

The message authentication code (MAC) is also included in the Intra N1 mode NAS transparent container IE and in the S1 mode to N1 mode NAS transparent container IE.

The usage of MAC is specified in subclause 4.4.3.3.

## 9.9 Plain 5GS NAS message

This IE includes a complete plain 5GS NAS message as specified in subclauses 8.2 and 8.3. The SECURITY PROTECTED 5GS NAS MESSAGE message (see subclause 8.2.28) is not plain 5GS NAS messages and shall not be included in this IE.

## 9.10 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 message.

The NAS message sequence number (SN) with the eight least significant bits of the NAS COUNT is also included in the Intra N1 mode NAS transparent container IE and in the S1 mode to N1 mode NAS transparent container IE.

The usage of SN is specified in subclause 4.4.3.

## 9.11 Other information elements

### 9.11.1 General

The different formats (V, LV, T, TV, TLV, LV-E, TLV-E) and the five categories of information elements (type 1, 2, 3, 4 and 6) are defined in 3GPP TS 24.007 [11].

The first octet of an information element in the non-imperative part contains the IEI of the information element. If this octet does not correspond to an IEI known in the message, the receiver shall determine whether this IE is of type 1 or 2 (i.e. it is an information element of one octet length) or an IE of type 4 (i.e. that the next octet is the length indicator indicating the length of the remaining of the information element) (see 3GPP TS 24.007 [11]).

This allows the receiver to jump over unknown information elements and to analyse any following information elements of a particular message.

The definitions of information elements which are:

a) common for the 5GMM and 5GSM protocols;

b) used by access stratum protocols; or

c) sent to upper layers

are described in subclause 9.11.2.

The information elements of the 5GMM or 5GSM protocols can be defined by reference to an appropriate specification which provides the definition of the information element, e.g., "see subclause 10.5.6.3A in 3GPP TS 24.008 [12]".

### 9.11.2 Common information elements

#### 9.11.2.1 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 9.11.2.1.1 and table 9.11.2.1.1.

The Additional information is a type 4 information element with a minimum length of 3 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Additional information IEI | | | | | | | | octet 1 |
| Additional information length | | | | | | | | octet 2 |
| Additional information value | | | | | | | | octets 3-n |

Figure 9.11.2.1.1: Additional information information element

Table 9.11.2.1.1 : 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. |

#### 9.11.2.1A DNN

The purpose of the DNN information element is to identify the data network.

The DNN information element is coded as shown in figure 9.11.2.1A.1.

The DNN is a type 4 information element with a minimum length of 3 octets and a maximum length of 102 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| DNN IEI | | | | | | | | octet 1 |
| Length of DNN contents | | | | | | | | octet 2 |
| DNN value | | | | | | | | octet 3  octet n |

Figure 9.11.2.1A.1: DNN information element

A DNN value field contains an APN as defined in 3GPP TS 23.003 [4].

#### 9.11.2.2 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 9.11.2.2.1 and table 9.11.2.2.1.

The EAP message is a type 6 information element with minimum length of 7 octets and maximum length of 1503 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| EAP message IEI | | | | | | | | octet 1 |
| Length of EAP message contents | | | | | | | | octet 2  octet 3 |
| EAP message | | | | | | | | octet 4  octet n |

Figure 9.11.2.2.1: EAP message information element

Table 9.11.2.2.1: EAP message information element

|  |
| --- |
| EAP message (octet 4 to n) |
| An EAP message as specified in IETF RFC 3748 [34]. |

#### 9.11.2.3 GPRS timer

See subclause 10.5.7.3 in 3GPP TS 24.008 [12].

#### 9.11.2.4 GPRS timer 2

See subclause 10.5.7.4 in 3GPP TS 24.008 [12].

#### 9.11.2.5 GPRS timer 3

See subclause 10.5.7.4a in 3GPP TS 24.008 [12].

#### 9.11.2.6 Intra N1 mode NAS transparent container

The purpose of the Intra N1 mode NAS transparent container information element is to provide the UE with parameters that enable the UE to handle the 5G NAS security context after N1 mode to N1 mode handover.

The Intra N1 mode NAS transparent container information element is coded as shown in figure 9.11.2.6.1 and table 9.11.2.6.1.

The Intra N1 mode NAS transparent container is a type 4 information element with a length of 9 octets.

The value part of the Intra 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].

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Intra N1 mode NAS transparent container IEI | | | | | | | | octet 1 |
| Length of Intra N1 mode NAS transparent container contents | | | | | | | | octet 2 |
| Message authentication code | | | | | | | | octet 3  octet 6 |
| Type of ciphering algorithm | | | | Type of integrity protection algorithm | | | | octet 7 |
| 0 | 0 Spare | 0 | KACF | TSC | Key set identifier in 5G | | | octet 8 |
| Sequence number | | | | | | | | octet 9 |

Figure 9.11.2.6.1: Intra N1 mode NAS transparent container information element

Table 9.11.2.6.1: Intra N1 mode NAS transparent container information element

|  |  |
| --- | --- |
| Message authentication code (octet 3 to 6) | |
|  | |
| This field is coded as the Message authentication code information element (see subclause 9.8). | |
|  | |
| Type of integrity protection algorithm (octet 7, bit 1 to 4) and type of ciphering algorithm (octet 7, 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 9.11.3.34). | |
|  | |
| K\_AMF\_change\_flag (KACF) (octet 8, bit 5) | |
| Bit | |
| 5 |  |
| 0 | a new KAMF has not been calculated by the network |
| 1 | a new KAMF has been calculated by the network |
|  | |
| Key set identifier in 5G (octet 8, bit 1 to 3) and Type of security context flag (TSC) (octet 8, 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 9.11.3.32). | |
|  | |
| Sequence number (octet 9) | |
|  | |
| This field is coded as the Sequence number information element (see subclause 9.10) | |
|  | |

#### 9.11.2.7 N1 mode to S1 mode NAS transparent container

The purpose of the N1 mode to S1 mode NAS transparent container information element is to provide the UE with information that enables the UE to create a mapped EPS security context.

The N1 mode to S1 mode NAS transparent container information element is coded as shown in figure 9.11.2.7.1 and table 9.11.2.7.1.

The N1 mode to S1 mode NAS transparent container is a type 3 information element with a length of 2 octets.

The value part of the N1 mode to S1 mode NAS transparent container information element is included in specific information elements within some RRC messages sent to the UE; see 3GPP TS 38.331 [30]. For these cases the coding of the information element identifier and length information is defined in 3GPP TS 38.331 [30].

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| N1 mode to S1 mode NAS transparent container IEI | | | | | | | | octet 1 |
| Sequence number | | | | | | | | octet 2 |

Figure 9.11.2.7.1: N1 mode to S1 mode NAS transparent container information element

Table 9.11.2.7.1: N1 mode to S1 mode NAS transparent container information element

|  |
| --- |
| Sequence number (octet 2) |
|  |
| This field is coded as the Sequence number information element (see subclause 9.10). |

#### 9.11.2.8 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 9.11.2.8.1 and table 9.11.2.8.1.

The S-NSSAI is a type 4 information element with a minimum length of 3 octets and a maximum length of 10 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| S-NSSAI IEI | | | | | | | | octet 1 |
| Length of S-NSSAI contents | | | | | | | | octet 2 |
| SST | | | | | | | | octet 3 |
| SD | | | | | | | | octet 4\*  octet 6\* |
| Mapped HPLMN SST | | | | | | | | octet 7\* |
| Mapped HPLMN SD | | | | | | | | octet 8\*  octet 10\* |

Figure 9.11.2.8.1: S-NSSAI information element

Table 9.11.2.8.1: S-NSSAI information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Length of S-NSSAI contents (octet 2) | | | | | | | | |
|  | | | | | | | | |
| This field indicates the length of the included S-NSSAI contents, and it can have the following values. Depending on the value of the length field the following S-NSSAI contents are included: | | | | | | | | |
| Bits | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | SST | |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | SST and mapped HPLMN SST | |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | SST and SD | |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | SST, SD and mapped HPLMN SST | |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | SST, SD, mapped HPLMN SST and mapped HPLMN SD | |
| All other values are reserved. | | | | | | | | |
| 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]. | | | | | | | | |
| If the SST encoded in octet 3 is not associated with a valid SD value, and the sender needs to include a mapped HPLMN SST (octet 7) and a mapped HPLMN SD (octets 8 to 10), then the sender shall set the SD value (octets 4 to 6) to "no SD value associated with the SST". | | | | | | | | |
|  | | | | | | | | |
| mapped HPLMN Slice/service type (SST) (octet 7) | | | | | | | | |
| This field contains the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of 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 HPLMN Slice differentiator (SD) (octet 8 to octet 10)  This field contains the 24 bit SD value of an S-NSSAI in the S-NSSAI(s) of 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. | | | | | | | | |

#### 9.11.2.9 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 9.11.2.9.1 and table 9.11.2.9.1.

The S1 mode to N1 mode NAS transparent container is a type 4 information element with a length of 10 octets.

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].

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| S1 mode to N1 mode NAS transparent container IEI | | | | | | | | | | | | | | | | octet 1 | |
| Length of S1 mode to N1 mode NAS transparent container contents | | | | | | | | | | | | | | | | octet 2 | |
| Message authentication code | | | | | | | | | | | | | | | | octet 3  octet 6 | |
| Type of ciphering algorithm | | | | | | | | Type of integrity protection algorithm | | | | | | | | octet 7 | |
| 0  Spare | | NCC | | | | | | TSC | | Key set identifier in 5G | | | | | | octet 8 | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | octet 9  octet 10 | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | |

Figure 9.11.2.9.1: S1 mode to N1 mode NAS transparent container information element

Table 9.11.2.9.1: S1 mode to N1 mode NAS transparent container information element

|  |  |
| --- | --- |
| Message authentication code (octet 3 to 6) | |
|  | |
| This field is coded as the Message authentication code information element (see subclause 9.8). | |
|  | |
| Type of integrity protection algorithm (octet 7, bit 1 to 4) and type of ciphering algorithm (octet 7, 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 9.11.3.34). | |
|  | |
| NCC (octet 8, bits 5 to 7) | |
|  | |
| This field contains the 3 bit Next hop chaining counter (see 3GPP TS 33.501 [24]) | |
|  | |
| Key set identifier in 5G (octet 8, bit 1 to 3) and type of security context flag (TSC) (octet 8, 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 9.11.3.32). | |
|  | |
| Octets 9 and 10 are spare and shall be coded as zero. | |
| NOTE: In earlier versions of this protocol, octets 9 and 10 can have any value. In this version of the protocol, octets 9 and 10 can always be ignored by the UE. | |

### 9.11.3 5GS mobility management (5GMM) information elements

#### 9.11.3.1 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 9.11.3.1.1 and table 9.11.3.1.1.

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 | |
| SGC | | 5G-HC-CP CIoT | | N3 data | | 5G-CP CIoT | | RestrictEC | | LPP | | HO attach | | S1 mode | | octet 3 | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 5G-UP CIoT | | 5GSRVCC | | octet 4\* | |
| 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | octet 5\*-15\* | |
| Spare | | | | | | | | | | | | | | | |

Figure 9.11.3.1.1: 5GMM capability information element

Table 9.11.3.1.1: 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 message for handover support (HO attach) (octet 3, bit 2) | | | | | | | | | | | | | | | | | | | | | | | |
| 0 | | | | | |  | | | |  | | | |  | | | | ATTACH REQUEST message containing PDN CONNECTIVITY REQUEST message with request type set to "handover" or "handover of emergency bearer services" to transfer PDU session from N1 mode to S1 mode not supported | | | | | |
| 1 | | | | | |  | | | |  | | | |  | | | | ATTACH REQUEST message containing PDN CONNECTIVITY REQUEST message with request type set to "handover" or "handover of emergency bearer services" to transfer PDU session from N1 mode to S1 mode supported | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | | | |
| LTE Positioning Protocol (LPP) capability (octet 3, bit 3) | | | | | | | | | | | | | | | | | | | | | | |
| 0 | | | | | |  | | | |  | | | |  | | | | LPP in N1 mode not supported | | | | |
| 1 | | | | | |  | | | |  | | | |  | | | | LPP in N1 mode supported (see 3GPP TS 36.355 [26]) | | | | |
|  | | | | | | | | | | | | | | | | | | | | | | | | |
| Restriction on use of enhanced coverage support (RestrictEC) (octet 3, bit 4)  This bit indicates the capability to support restriction on use of enhanced coverage. | | | | | | | | | | | | | | | | | | | | | | |
| 0 | | | | |  | | | |  | | | |  | | | | Restriction on use of enhanced coverage not supported | | | | | |
| 1 | | | | |  | | | |  | | | |  | | | | Restriction on use of enhanced coverage supported | | | | | |
| Control plane CIoT 5GS optimization (5G-CP CIoT) (octet 3, bit 5)  This bit indicates the capability for control plane CIoT 5GS optimization. | | | | | | | | | | | | | | | | | | | | | | |
| 0 | | | | | | | |  | | | |  | | | |  | | | | Control plane CIoT 5GS optimization not supported | | |
| 1 | | | | | | | |  | | | |  | | | |  | | | | Control plane CIoT 5GS optimization supported | | |
| N3 data transfer (N3 data) (octet 3, bit 6)  This bit indicates the capability for N3 data transfer. | | | | | | | | | | | | | | | | | | | | | | |
| 0 | | | | | | | |  | | | |  | | | |  | | | | N3 data transfer supported | | |
| 1 | | | | | | | |  | | | |  | | | |  | | | | N3 data transfer not supported | | |
| Header compression for control plane CIoT 5GS optimization (5G-HC-CP CIoT) (octet 3, bit 7)  This bit indicates the capability for header compression for control plane CIoT 5GS optimization. | | | | | | | | | | | | | | | | | | | | | | |
| 0 | | | | | | | |  | | | |  | | | |  | | | | Header compression for control plane CIoT 5GS optimization not supported | | |
| 1 | | | | | | | |  | | | |  | | | |  | | | | Header compression for control plane CIoT 5GS optimization supported | | |
|  | | | | | | | | | | | | | | | | | | | | | |
| Service gap control (SGC) (octet 3, bit 8) | | | | | | | | | | | | | | | | | | | | | |
| 0 | | | | |  | | | |  | | | |  | | | | service gap control not supported | | | | |
| 1 | | | | |  | | | |  | | | |  | | | | service gap control supported | | | | |
|  | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5G-SRVCC from NG-RAN to UTRAN (5GSRVCC) capability (octet 4, bit 1) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0 | | | | | | | | | |  | | | |  | | | |  | | | | 5G-SRVCC from NG-RAN to UTRAN not supported | | | | | | | | |
| 1 | | | | | | | | | |  | | | |  | | | |  | | | | 5G-SRVCC from NG-RAN to UTRAN supported (see 3GPP TS 23.216 [6A]) | | | | | | | | |
| User plane CIoT 5GS optimization (5G-UP CIoT) (octet 4, bit 2)  This bit indicates the capability for user plane CIoT 5GS optimization. | | | | | | | | | | | | | | | | | | | | | | |
| 0 | | | | | | | |  | | | |  | | | |  | | | | User plane CIoT 5GS optimization not supported | | |
| 1 | | | | | | | |  | | | |  | | | |  | | | | User plane CIoT 5GS optimization supported | | |
| All other bits in octet 4 and bits in octets 5 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | | | | | | | | | | | | | | | | | | | | |

#### 9.11.3.2 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 9.11.3.2.1 and table 9.11.3.2.1.

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 9.11.3.2.1: 5GMM cause information element

Table 9.11.3.2.1: 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 | 0 | 1 |  | UE identity cannot be derived by the network |
| 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 | 0 | 1 | 1 | 1 | 1 |  | No suitable cells in tracking area |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |  | MAC failure |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |  | Synch failure |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |  | Congestion |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |  | UE security capabilities mismatch |
| 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |  | Security mode rejected, unspecified |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |  | Non-5G authentication unacceptable |
| 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 | 0 | 1 | 1 | 1 | 1 | 1 |  | Redirection to EPC required |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |  | LADN not available |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |  | Maximum number of PDU sessions reached |
| 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 | 0 | 0 | 1 | 1 | 1 |  | ngKSI already in use |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |  | Non-3GPP access to 5GCN not allowed |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |  | Serving network not authorized |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |  | Temporarily not authorized for this SNPN |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |  | Permanently not authorized for this SNPN |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |  | Payload was not forwarded |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |  | DNN not supported or not subscribed in the slice |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |  | Insufficient user-plane resources for the PDU session |
| 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". | | | | | | | | | |

#### 9.11.3.2A 5GS DRX parameters

The purpose of the 5GS DRX parameters information element is to indicate that the UE wants to use DRX and for the network to indicate the DRX cycle value to be used at paging.

The 5GS DRX parameters is a type 4 information element with a length of 3 octets.

The 5GS DRX parameters information element is coded as shown in figure 9.11.3.2A.1 and table 9.11.3.2A.1.

The value part of a DRX parameter information element is coded as shown in table 9.11.3.2A.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS DRX parameters IEI | | | | | | | | octet 1 |
| Length of 5GS DRX parameters contents | | | | | | | | octet 2 |
| 0 | 0 | 0 | 0 | DRX value | | | |  |
| spare | | | | octet 3 |

Figure 9.11.3.2A.1: 5GS DRX parameters information element

Table 9.11.3.2A.1: 5GS DRX parameters information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DRX value (bits 4 to 1 of octet 3)  This field represents the DRX cycle parameter 'T' as defined in 3GPP TS 38.304 [28]. | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | DRX value not specified |
| 0 | 0 | 0 | 1 | DRX cycle parameter T = 32 |
| 0 | 0 | 1 | 0 | DRX cycle parameter T = 64 |
| 0 | 0 | 1 | 1 | DRX cycle parameter T = 128 |
| 0 | 1 | 0 | 0 | DRX cycle parameter T = 256 |
|  | | | | |
| All other values shall be interpreted as "DRX value not specified" by this version of the protocol.  Bits 5 to 8 of octet 3 are spare and shall be coded as zero. | | | | |
|  | | | | |

#### 9.11.3.3 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 9.11.3.3.1 and table 9.11.3.3.1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | | 2 | 1 |  |
| 5GS identity type  IEI | | | | 0  spare | | | Type of  identity | | | octet 1 |

Figure 9.11.3.3.1: 5GS identity type information element

Table 9.11.3.3.1: 5GS identity type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of identity (octet 1) | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 1 |  | SUCI |
| 0 | 1 | 0 |  | 5G-GUTI |
| 0 | 1 | 1 |  | IMEI |
| 1 | 0 | 0 |  | 5G-S-TMSI |
| 1 | 0 | 1 |  | IMEISV |
| 1 | 1 | 0 |  | MAC address |
|  | | | | |
| All other values are unused and shall be interpreted as "SUCI", if received by the UE. | | | | |

#### 9.11.3.4 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, the 5G-S-TMSI or the MAC address.

The 5GS mobile identity information element is coded as shown in figures 9.11.3.4.1, 9.11.3.4.2, 9.11.3.4.3, 9.11.3.4.4, 9.11.3.4.5, 9.11.3.4.6 and 9.11.3.4.7, and table 9.11.3.4.1.

The 5GS mobile identity is a type 6 information element with a minimum length of 4.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet2  octet 3 |
| 1 | 1 | 1 | 1 | 0  spare | Type of identity | | | octet 4 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 5 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 6 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 7 |
| AMF Region ID | | | | | | | | octet 8 |
| AMF Set ID | | | | | | | | octet 9 |
| AMF Set ID (continued) | | AMF Pointer | | | | | | octet 10 |
| 5G-TMSI | | | | | | | | octet 11 |
| 5G-TMSI (continued) | | | | | | | | octet 12 |
| 5G-TMSI (continued) | | | | | | | | octet 13 |
| 5G-TMSI (continued) | | | | | | | | octet 14 |

Figure 9.11.3.4.1: 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  octet 3 |
| Identity digit 1 | | | | odd/  even  indic | Type of identity | | | octet 4 |
| Identity digit p+1 | | | | Identity digit p | | | | octet 5\* |

Figure 9.11.3.4.2: 5GS mobile identity information element for type of identity or "IMEI" or "IMEISV"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 0  spare | SUPI format | | | 0  spare | Type of identity | | | octet 4 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 5 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 6 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 7 |
| Routing indicator digit 2 | | | | Routing indicator digit 1 | | | | octet 8 |
| Routing indicator digit 4 | | | | Routing indicator digit 3 | | | | octet 9 |
| 0  Spare | 0  Spare | 0  Spare | 0  Spare | Protection scheme Id | | | | octet 10 |
| Home network public key identifier | | | | | | | | octet 11 |
| Scheme output | | | | | | | | octet 12 - x |

Figure 9.11.3.4.3: 5GS mobile identity information element for type of identity "SUCI" and SUPI format "IMSI"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| MSIN digit 2 | | | | MSIN digit 1 | | | | octet 12 |
| … | | | | | | | |  |
| MSIN digit n+1 | | | | MSIN digit n | | | | octet x |

Figure 9.11.3.4.3a: Scheme output for type of identity "SUCI", SUPI format "IMSI" and Protection scheme Id "Null scheme"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 0  Spare | SUPI format | | | 0  Spare | Type of identity | | | octet 4 |
| SUCI NAI | | | | | | | | octet 5 - y |

Figure 9.11.3.4.4: 5GS mobile identity information element for type of identity "SUCI" and SUPI format "Network specific identifier"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 1 | 1 | 1 | 1 | 0  spare | Type of identity | | | octet 4 |
| AMF Set ID | | | | | | | | octet 5 |
| AMF Set ID (continued) | | AMF Pointer | | | | | | octet 6 |
| 5G-TMSI | | | | | | | | octet 7 |
| 5G-TMSI (continued) | | | | | | | | octet 8 |
| 5G-TMSI (continued) | | | | | | | | octet 9 |
| 5G-TMSI (continued) | | | | | | | | octet 10 |

Figure 9.11.3.4.5: 5GS mobile identity information element for type of identity "5G-S-TMSI"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 0 | 0 | 0 | 0 | 0 | Type of identity | | | octet 4 |
| spare | | | | |

Figure 9.11.3.4.6: 5GS mobile identity information element for type of identity "No identity"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 |
| 0  spare | 0  spare | 0  spare | 0  spare | 0  spare | Type of identity | | | octet 4 |
| MAC address | | | | | | | | octet 5  octet 10 |

Figure 9.11.3.4.7: 5GS mobile identity information element for type of identity "MAC address"

Table 9.11.3.4.1: 5GS mobile identity information element

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Type of identity (octet 4)  Bits | | | | | | | | | | | | | |
| 3 | 2 | 1 | |  | | | | | | | | | |
| 0 | 0 | 0 | | No identity (see NOTE 1) | | | | | | | | | |
| 0 | 0 | 1 | | SUCI | | | | | | | | | |
| 0 | 1 | 0 | | 5G-GUTI | | | | | | | | | |
| 0 | 1 | 1 | | IMEI | | | | | | | | | |
| 1 | 0 | 0 | | 5G-S-TMSI | | | | | | | | | |
| 1 | 0 | 1 | | IMEISV | | | | | | | | | |
| 1 | 1 | 0 | | MAC address | | | | | | | | | |
| All other values are reserved. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Odd/even indication (octet 4)  Bit | | | | | | | | | | | | | |
| 4 |  |  | |  | | | | | | | | | |
| 0 |  |  | | even number of identity digits | | | | | | | | | |
| 1 |  |  | | odd number of identity digits | | | | | | | | | |
|  | | | | | | | | | | | | | |
| 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, octet 7 through 9 contain the AMF Region ID, the AMF Set ID and the AMF Pointer values and octet 10 through 13 contain the 5G-TMSI as defined in 3GPP TS 23.003 [4]. | | | | | | | | | | | | | |
| MCC, Mobile country code (octet 5, octet 6 bits 1 to 4)  The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | | | | | | | | | | | | | |
| MNC, Mobile network code (octet 6 bits 5 to 8, octet 7)  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 6 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]. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| AMF Region ID (octet 8)  This field contains the binary encoding of the AMF Region ID. Bit 8 of octet 7 is the most significant bit and bit 1 of octet 7 is the least significant bit.  AMF Set ID (octet 9, octet 10 bits 7 to 8)  This field contains the binary encoding of the AMF Set ID. Bit 8 of octet 9 is the most significant bit and bit 7 of octet 10 is the least significant bit.  AMF Pointer (octet 10 bits 1 to 6)  This field contains the binary encoding of the AMF Pointer. Bit 6 of octet 9 is the most significant bit and bit 1 of octet 9 is the least significant bit.  5G-TMSI (octet 11 to 14)  Bit 8 of octet 11 is the most significant bit and bit 1 of octet 14 is the least significant bit. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Identity digit (octet 4 bits 5 to 8, octet 5 etc.) | | | | | | | | | | | | | |
| For the IMEI, Identity digit 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". The format of the IMEI is described in 3GPP TS 23.003 [4]. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the IMEISV, Identity digit 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 SUCI, bit 8 of octet 4 is spare and shall be coded as zero. Bits 5-7 of octet 4 contain the SUPI format and are coded as shown below. | | | | | | | | | | | | | |
| SUPI format (octet 4, bits 5-7)  Bits | | | | | | | | | | | | | |
| 7 | 6 | 5 | |  | |  | | | | | | | |
| 0 | 0 | 0 | |  | | IMSI | | | | | | | |
| 0 | 0 | 1 | |  | | Network Specific Identifier | | | | | | | |
| All other values are interpreted as IMSI by this version of the protocol. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the SUCI with SUPI format "IMSI", octets 5 through 7 contain the MCC and MNC values as specified below. For subsequent fields, bit 8 of octet 8 is the most significant bit and bit 1 of the last octet the least significant bit. The required fields for the SUCI are as defined in 3GPP TS 23.003 [4]. | | | | | | | | | | | | | |
| MCC, Mobile country code (octet 5, octet 6 bits 1 to 4)  The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | | | | | | | | | | | | | |
| MNC, Mobile network code (octet 6 bits 5 to 8, octet 7)  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 6 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]. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Routing indicator (octets 8-9)  Routing Indicator shall consist of 1 to 4 digits. The coding of this field is the responsibility of home network operator but BCD coding shall be used. If a network operator decides to assign less than 4 digits to Routing Indicator, the remaining digits shall be coded as "1111" to fill the 4 digits coding of Routing Indicator (see NOTE 2). If no Routing Indicator is configured in the USIM, the UE shall code bits 1 to 4 of octet 8 of the Routing Indicator as "0000" and the remaining digits as “1111". | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Protection scheme identifier (octet 10 bits 1 to 4) | | | | | | | | | | | | | |
| Bits | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| 4 | 3 | 2 | 1 | |  | | | | | | |
| 0 | 0 | 0 | 0 | | Null scheme | | | | | | |
| 0 | 0 | 0 | 1 | | ECIES scheme profile A | | | | | | |
| 0 | 0 | 1 | 0 | | ECIES scheme profile B | | | | | | |
| 0 | 0 | 1 | 1 | |  | | | | | | |
| to | | | | | Reserved | | | | | | |
| 1 | 0 | 1 | 1 | |  | | | | | | |
| 1 | 1 | 0 | 0 | |  | | | | | | |
| to | | | | | Operator-specific protection scheme | | | | | | |
| 1 | 1 | 1 | 1 | |  | | | | | | |
|  | | | | | | | | | | | |
| Bits 5-8 of octet 10 are spare and shall be coded as zero. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Home network public key identifier (octet 10) | | | | | | | | | | | | | |
| The Home network public key identifier (PKI) field is coded as defined in 3GPP TS 23.003 [4]. Home network public key identifier shall be coded as "00000000" when Protection scheme identifier is set to "0000" (i.e. Null scheme). | | | | | | | | | | | | | |
| Bits | | | | | | | | | | | | | |
| 8 | 7 | 6 | | 5 | | 4 | 3 | 2 | 1 |  |  | |
| 0 | 0 | 0 | | 0 | | 0 | 0 | 0 | 0 |  | Home network PKI value 0 | |
| 0 | 0 | 0 | | 0 | | 0 | 0 | 0 | 1 |  |  | |
| to | | | | | | | | | |  | Home network PKI value (1-254) | |
| 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | 0 |  |  | |
| 1 | 1 | 1 | | 1 | | 1 | 1 | 1 | 1 |  | Reserved | |
|  | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Scheme output (octets 12 to x)  The Scheme output field consists of a string of characters with a variable length or hexadecimal digits as specified in 3GPP TS 23.003 [4]. If Protection scheme identifier is set to "0000" (i.e. Null scheme), then the Scheme output consists of the MSIN and is coded using BCD coding with each digit of the MSIN coded over 4 bits. If the MSIN includes an odd number of digits, bits 5 to 8 of octet x shall be coded as "1111". If Protection scheme identifier is not "0000" (i.e. ECIES scheme profile A, ECIES scheme profile B or Operator-specific protection scheme), then Scheme output is coded as hexadecimal digits. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the SUCI with SUPI format set to "Network specific identifier", the SUCI NAI field contains an NAI constructed as specified in subclause 28.7.3 of 3GPP TS 23.003 [4] and encoded as UTF-8 string. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| For the 5G-S-TMSI, bits 5 to 8 of octet 4 are coded as "1111". The coding of the 5G-S-TMSI is left open for each administration. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| AMF Set ID (octet 5, octet 6 bits 7 to 8)  This field contains the binary encoding of the AMF Set ID. Bit 8 of octet 5 is the most significant bit and bit 7 of octet 6 is the least significant bit.  AMF Pointer (octet 6 bits 1 to 6)  This field contains the binary encoding of the AMF Pointer. Bit 6 of octet 6 is the most significant bit and bit 1 of octet 6 is the least significant bit.  5G-TMSI (octet 7 to 10)  Bit 8 of octet 7 is the most significant bit and bit 1 of octet 10 is the least significant bit. | | | | | | | | | | | | | |
| MAC address (octets 5 to 10)  This field contains the MAC address as defined in subclause 8 of IEEE Std 802 [43].  Bit 8 of octet 5 is the most significant bit and bit 1 of octet 10 is the least significant bit. | | | | | | | | | | | | | |
| For Type of identity "No identity", the length of mobile identity contents parameter shall be set to 1 and the bits 4-8 of octet 4 are spare and shall be coded as zero. | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| NOTE 1: This can be used when the requested identity is not available at the UE during the identification procedure.  NOTE 2: For a 3-digit Routing Indicator, e.g "567", bits 1 to 4 of octet 8 are coded as "0101", bits 5 to 8 of octet 8 are coded as "0110", bits 1 to 4 of octet 9 are coded as "0111", bits 5 to 8 of octet 9 are coded as "1111". | | | | | | | | | | | | | |

#### 9.11.3.5 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 9.11.3.5.1 and table 9.11.3.5.1.

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.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | 2 | 1 |  |
| 5GS network feature support IEI | | | | | | | | | octet 1 |
| Length of 5GS network feature support contents | | | | | | | | | octet 2 |
| MPSI | IWK N26 | EMF | | EMC | | | IMS- VoPS-N3GPP | IMS- VoPS-3GPP | octet 3 |
| 0  Spare | 5G-UP CIoT | 5G-HC-CP CIoT | N3 data | | 5G-CP CIoT | RestrictEC | MCSI | EMCN3 | octet 4 |
| 0 | 0 | 0 | 0 | | 0 | 0 | 0 | 0 |  |
| Spare | | | | | | | | | octet 5\* |

Figure 9.11.3.5.1: 5GS network feature support information element

Table 9.11.3.5.1: 5GS network feature support information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IMS voice over PS session over 3GPP access indicator (IMS-VoPS-3GPP) (octet 3, bit 1) | | | | | | | | | |
| This bit indicates the support of IMS voice over PS session over 3GPP access | | | | | | | | | |
| (see NOTE 1) | | | | | | | | | |
| Bit | | | | | | | | | |
| 1 | |  | |  | |  | |  | |
| 0 | |  | |  | |  | | IMS voice over PS session not supported over 3GPP access | |
| 1 | |  | |  | |  | | IMS voice over PS session supported over 3GPP access | |
|  | | | | | | | | | |
| IMS voice over PS session over non-3GPP access indicator (IMS-VoPS-N3GPP) (octet 3, bit 2) | | | | | | | | | |
| This bit indicates the support of IMS voice over PS session over non-3GPP access | | | | | | | | | |
| Bit | | | | | | | | | |
| 2 | |  | |  | |  | |  | |
| 0 | |  | |  | |  | | IMS voice over PS session not supported over non-3GPP access | |
| 1 | |  | |  | |  | | IMS voice over PS session supported over non-3GPP access | |
|  | | | | | | | | | |
| Emergency service support indicator for 3GPP access (EMC) (octet 3, bit 3 and bit 4) | | | | | | | | | |
| This bit indicates the support of emergency services in 5GS for 3GPP access (see NOTE 2) | | | | | | | | | |
| Bits | | | | | | | | | |
| 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 services fallback indicator for 3GPP access (EMF) (octet 3, bit 5 and bit 6) | | | | | | | | | |
| This bit indicates the support of emergency services fallback for 3GPP access (see NOTE 2) | | | | | | | | | |
| Bits | | | | | | | | | |
| 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 7) | | | | | | | | | |
| This bit indicates whether interworking without N26 interface is supported | | | | | | | | | |
| Bit | | | | | | | | | |
| 7 | |  | |  | |  | |  | |
| 0 | |  | |  | |  | | Interworking without N26 interface not supported | |
| 1 | |  | |  | |  | | Interworking without N26 interface supported | |
|  | | | | | | | | | |
| MPS indicator (MPSI) (octet 3, bit 8) | | | | | | | | | |
| This bit indicates the validity of MPS. | | | | | | | | | |
| Bit | | | | | | | | | |
| 8 | |  | |  | |  | |  | |
| 0 | |  | |  | |  | | Access identity 1 not valid | |
| 1 | |  | |  | |  | | Access identity 1 valid | |
|  | | | | | | | | | |
| Emergency service support for non-3GPP access indicator (EMCN3) (octet 4, bit 1)  This bit indicates the support of emergency services in 5GS for non-3GPP access  Bit (see NOTE 3) | | | | | | | | | |
| 1 | |  | |  | |  | |  | |
| 0 | |  | |  | |  | | Emergency services not supported over non-3GPP access | |
| 1 | |  | |  | |  | | Emergency services supported over non-3GPP access | |
|  | |  | |  | |  | |  | |
| MCS indicator (MCSI) (octet 4, bit 2) | | | | | | | | | |
| This bit indicates the validity of MCS. | | | | | | | | | |
| Bit | | | | | | | | | |
| 2 | |  | |  | |  | |  | |
| 0 | |  | |  | |  | | Access identity 2 not valid | |
| 1 | |  | |  | |  | | Access identity 2 valid | |
|  | | | | | | | | | |
| Restriction on enhanced coverage (RestrictEC) (octet 4, bit 3)  This bit indicates if the use of enhanced coverage is restricted or not. | | | | | | | | | |
| Bit  **3** | | | | | | | | | |
| 0 | |  | |  | |  | | Use of enhanced coverage is not restricted | |
| 1 | |  | |  | |  | | Use of enhanced coverage is restricted | |
|  | | | | | | | | | |
| Control plane CIoT 5GS optimization (5G-CP CIoT)  (octet 4, bit 4) | | | | | | | | | |
| This bit indicates the capability for control plane CIoT 5GS optimization | | | | | | | | | |
| Bit | | | | | | | | | |
| **4** | | | | | | | | | |
| 0 | |  | |  | |  | | Control plane CIoT 5GS optimization not supported | |
| 1 | |  | |  | |  | | Control plane CIoT 5GS optimization supported | |
|  | | | | | | | | | |
| N3 data transfer (N3 data)  (octet 4, bit 5) | | | | | | | | | |
| This bit indicates the capability for N3 data transfer. | | | | | | | | | |
| Bit | | | | | | | | | |
| **5** | | | | | | | | | |
| 0 | |  | |  | |  | | N3 data transfer supported | |
| 1 | |  | |  | |  | | N3 data transfer not supported | |
|  | | | | | | | | | |
| Header compression for control plane CIoT 5GS optimization (5G-HC-CP CIoT)  (octet 4, bit 6) | | | | | | | | | |
| This bit indicates the capability for header compression for control plane CIoT 5GS optimization | | | | | | | | | |
| Bit | | | | | | | | | |
| **6** | | | | | | | | | |
| 0 | |  | |  | |  | | Header compression for control plane CIoT 5GS optimization not supported | |
| 1 | |  | |  | |  | | Header compression for control plane CIoT 5GS optimization supported | |
|  | | | | | | | | | |
| User plane CIoT 5GS optimization (5G-UP CIoT)  (octet 4, bit 7) | | | | | | | | | |
| This bit indicates the capability for user plane CIoT 5GS optimization | | | | | | | | | |
| Bit | | | | | | | | | |
| **7** | | | | | | | | | |
| 0 | |  | |  | |  | | User plane CIoT 5GS optimization not supported | |
| 1 | |  | |  | |  | | User plane CIoT 5GS optimization supported | |
| Bits 3 to 8 in octets 4 and all bits in octet 5 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | | | | | | |
| NOTE 1: For a registration procedure over non-3GPP access, bit 1 of octet 3 is ignored.  NOTE 2: For a registration procedure over 3GPP access, bit 1 of octet 4 is ignored.  NOTE 3: For a registration procedure over non-3GPP access, bits 3 to 6 of octet 3 are ignored. | | | | | | | | | |

#### 9.11.3.6 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 9.11.3.6.1 and table 9.11.3.6.1.

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 9.11.3.6.1: 5GS registration result information element

Table 9.11.3.6.1: 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. | | | | |

#### 9.11.3.7 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 9.11.3.7.1 and table 9.11.3.7.1.

The 5GS registration type is a type 1 information element with a length of 1 octet.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS registration type IEI | | | | FOR | 5GS registration type value | | | octet 1 |

Figure 9.11.3.7.1: 5GS registration type information element

Table 9.11.3.7.1: 5GS registration type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5GS registration type value (octet 1, 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. | | | | |
|  | | | | |
| Follow-on request bit (FOR) (octet 1, bit 4) | | | | |
| Bit | | | | |
| 4 |  |  |  |  |
| 0 |  |  |  | No follow-on request pending |
| 1 |  |  |  | Follow-on request pending |

#### 9.11.3.8 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 9.11.3.8.1 and table 9.11.3.8.1.

The 5GS tracking area identity is a type 3 information element with a length of 7 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS tracking area identity IEI | | | | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC | | | | | | | | octet 5 |
| TAC (continued) | | | | | | | | octet 6 |
| TAC (continued) | | | | | | | | octet 7 |

Figure 9.11.3.8.1: 5GS tracking area identity information element

Table 9.11.3.8.1: 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 7 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. |

#### 9.11.3.9 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 9.11.3.8.1, figure 9.11.3.8.2, figure 9.11.3.9.3, figure 9.11.3.9.4 and table 9.11.3.9.1.

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.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS tracking area identity list IEI | | | | | | | | octet 1 |
| Length of 5GS tracking area identity list contents | | | | | | | | octet 2 |
| Partial tracking area identity list 1 | | | | | | | | octet 3  octet i |
| Partial tracking area identity list 2 | | | | | | | | octet i+1\*  octet l\* |
| … | | | | | | | | octet l+1\*  octet m\* |
| Partial tracking area identity list p | | | | | | | | octet m+1\*  octet n\* |

Figure 9.11.3.9.1: 5GS tracking area identity list information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 0  Spare | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC 1 | | | | | | | | octet 5 |
| TAC 1 (continued) | | | | | | | | octet 6 |
| TAC 1 (continued) | | | | | | | | octet 7 |
| … | | | | | | | | … |
| … | | | | | | | | … |
| TAC k | | | | | | | | octet 3k+2\* |
| TAC k (continued) | | | | | | | | octet 3k+3\* |
| TAC k (continued) | | | | | | | | octet 3k+4\* |

Figure 9.11.3.9.2: Partial tracking area identity list – type of list = "00"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 0  Spare | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC 1 | | | | | | | | octet 5 |
| TAC 1 (continued) | | | | | | | | octet 6 |
| TAC 1 (continued) | | | | | | | | octet 7 |

Figure 9.11.3.9.3: Partial tracking area identity list – type of list = "01"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 0  Spare | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC 1 | | | | | | | | octet 5 |
| TAC 1 (continued) | | | | | | | | octet 6 |
| TAC 1 (continued) | | | | | | | | octet 7 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 8\* |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 9\* |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 10\* |
| TAC 2 | | | | | | | | octet 11\* |
| TAC 2 (continued) | | | | | | | | octet 12\* |
| TAC 2 (continued) | | | | | | | | octet 13\* |
| … | | | | | | | |  |
| … | | | | | | | |  |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 6k-4\* |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 6k-3\* |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 6k-2\* |
| TAC k | | | | | | | | octet 6k-1\* |
| TAC k (continued) | | | | | | | | octet 6k\* |
| TAC k (continued) | | | | | | | | octet 6k+1\* |

Figure 9.11.3.9.4: Partial tracking area identity list – type of list = "10"

Table 9.11.3.9.1: 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". | | | | | |

#### 9.11.3.9A 5GS update type

The purpose of the 5GS update type IE is to allow the UE to provide additional information to the network when performing a registration procedure.

The 5GS update type information element is coded as shown in figure 9.11.3.9A.1 and table 9.11.3.9A.1.

The 5GS update type is a type 4 information element.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | 3 | | 2 | | 1 | |  | |
| 5GS update type IEI | | | | | | | | | | | | | | | octet 1 | |
| Length of 5GS update type | | | | | | | | | | | | | | | octet 2 | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | PNB-CIoT | | | NG-RAN-RCU | | SMS requested | | octet 3 | |

Figure 9.11.3.9A.1: 5GS update type information element

Table 9.11.3.9A.1: 5GS update type information element

|  |  |  |  |
| --- | --- | --- | --- |
| SMS over NAS transport requested (SMS requested) (octet 3, bit 1) | | | |
| Bit | | | |
| 1 |  |  | |
| 0 |  | SMS over NAS not supported | |
| 1 |  | SMS over NAS supported | |
|  | | | |
| NG-RAN Radio Capability Update (NG-RAN-RCU) (octet 3, bit 2) | | | |
| Bits | | | |
| 2 |  |  | |
| 0 |  | NG-RAN radio capability update not needed | |
| 1 |  | NG-RAN radio capability update needed | |
|  | | | |
| Preferred CIoT network behaviour (PNB-CIoT) (octet 3, bits 3 and 4) | | |
|  | | |
| Bit | | |
| 4 | 3 |  |
| 0 | 0 | no additional information |
| 0 | 1 | control plane CIoT 5GS optimization |
| 1 | 0 | user plane CIoT 5GS optimization |
| 1 | 1 | reserved |
|  | | |
| Bits 5 to 8 of octet 3 are spare and shall be coded as zero. | | | |

#### 9.11.3.10 ABBA

The purpose of the ABBA information element is to enable the bidding down protection of security features.

The ABBA information element is coded as shown in figure 9.11.3.10.1 and table 9.11.3.10.1.

The ABBA is a type 4 information element with a minimum length of 4 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| ABBA IEI | | | | | | | | octet 1 |
| Length of ABBA contents | | | | | | | | octet 2 |
| ABBA contents | | | | | | | | octet 3  octet n |

Figure 9.11.3.10.1: ABBA information element

Table 9.11.3.10.1: ABBA information element

|  |
| --- |
| ABBA contents (octet 3-n):  indicate set of security features defined for 5GS as described in 3GPP TS 33.501 [24]. |
| NOTE 1: If the UE receives the ABBA IE with a length that is set to a value of 2 and with a value of 0000H, the UE shall use the length and the contents of the ABBA IE as received from the network.  NOTE 2: If the UE receives the ABBA IE with a length that is set to a value larger than 2 or with a value that is different from 0000H, the UE shall use the length and the contents of the ABBA IE as received from the network. |

#### 9.11.3.11 Access type

The purpose of the access typeinformation 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 typeis a type 1 information element.

The access typeinformation element is coded as shown in figure 9.11.3.11.1 and table 9.11.3.11.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Access type  IEI | | | | 0  spare | | Access type | | octet 1 |

Figure 9.11.3.11.1: Access type information element

Table 9.11.3.11.1: 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. | | | | |

#### 9.11.3.12 Additional 5G security information

The purpose of the Additional 5G security information information element is to provide the UE with additional security parameters (e.g. horizontal derivation parameter) or to request the UE to retransmit an initial NAS message during a security mode control procedure as defined in 3GPP TS 33.501 [24]. The UE uses these parameters for completion of security mode control procedure.

The Additional 5G security parameters information element is coded as shown in figure 9.11.3.12.1 and table 9.11.3.12.1.

The Additional 5G security parameters is a type 4 information element with a length of 3 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| Additional 5G security parameters IEI | | | | | | | | | | | | | | | | octet 1 | |
| Length of Additional 5G security parameters contents | | | | | | | | | | | | | | | | octet 2 | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | RINMR | | HDP | | octet 3 | |

Figure 9.11.3.12.1: Additional 5G security parameters information element

Table 9.11.3.12.1: Additional 5G security parameters information element

|  |  |  |
| --- | --- | --- |
| Horizontal derivation parameter (HDP) (octet 3, bit 1) | | |
| 0 |  | KAMF derivation is not required |
| 1 |  | KAMF derivation is required |
|  | | |
| Retransmission of initial NAS message request (octet 3, bit 2) | | |
| 0 |  | Retransmission of the initial NAS message not requested |
| 1 |  | Retransmission of the initial NAS message requested |
|  | | |
| Bits 3 to 8 of octet 3 are spare and shall be coded as zero. | | |

#### 9.11.3.13 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 9.11.3.13.1 and table 9.11.3.13.1.

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 9.11.3.13.1: Allowed PDU session status information element

Table 9.11.3.13.1: 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 for which the user-plane resources can be re-established over 3GPP access, all bits in PSI(1) – 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. |

#### 9.11.3.14 Authentication failure parameter

See subclause 10.5.3.2.2 in 3GPP TS 24.008 [12].

#### 9.11.3.15 Authentication parameter AUTN

See subclause 10.5.3.1.1 in 3GPP TS 24.008 [12].

#### 9.11.3.16 Authentication parameter RAND

See subclause 10.5.3.1 in 3GPP TS 24.008 [12].

#### 9.11.3.17 Authentication response parameter

See subclause 9.9.3.4 in 3GPP TS 24.301 [15].

#### 9.11.3.18 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 9.11.3.18.1 and table 9.11.3.18.1.

The Configuration update indication is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Configuration update indication IEI | | | | 0  Spare | 0  Spare | RED | ACK | octet 1 |

Figure 9.11.3.18.1: Configuration update indication

Table 9.11.3.18.1: Configuration update indication

|  |  |
| --- | --- |
| Acknowledgement (ACK) (octet 1, bit 1) | |
| Bit | |
| 1 |  |
| 0 | acknowledgement not requested |
| 1 | acknowledgement requested |
|  |  |
| Registration requested (RED) (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, | |

#### 9.11.3.19 Daylight saving time

See subclause 10.5.3.12 in 3GPP TS 24.008 [12].

#### 9.11.3.20 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 9.11.3.20.1 and table 9.11.3.20.1.

The De-registration type is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| De-registration type  IEI | | | | Switch  off | Re-registration required | Access type | | octet 1 |

Figure 9.11.3.20.1: Deregistration type information element

Table 9.11.3.20.1: 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. | | | | |

#### 9.11.3.21 Void

#### 9.11.3.22 Void

#### 9.11.3.23 Emergency number list

See subclause 10.5.3.13 in 3GPP TS 24.008 [12].

#### 9.11.3.24 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 9.11.3.24.1 and table 9.11.3.24.1.

The EPS NAS message container is a type 6 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| EPS NAS message container IEI | | | | | | | | octet 1 |
| Length of EPS NAS message container contents | | | | | | | | octet 2  octet 3 |
| EPS NAS message container | | | | | | | | octet 4  octet n |

Figure 9.11.3.24.1: EPS NAS message container information element

Table 9.11.3.24.1: 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]. |

#### 9.11.3.25 EPS NAS security algorithms

See subclause 9.9.3.23 in 3GPP TS 24.301 [15].

#### 9.11.3.26 Extended emergency number list

See subclause 9.9.3.37A in 3GPP TS 24.301 [15].

#### 9.11.3.27 Void

#### 9.11.3.28 IMEISV request

See subclause 10.5.5.10 in 3GPP TS 24.008 [12].

#### 9.11.3.29 LADN indication

The purpose of the LADN indication information element is to request the network for LADN information for specific LADN DNN(s) or to indicate a request for LADN information.

The LADN indication information element is coded as shown in figure 9.11.3.29.1 and table 9.11.3.29.1.

The LADN indication is a type 6 information element with a minimum length of 3 octets and a maximum length of 811 octets.

The LADN indication information element can contain a minimum of 0 and a maximum of 8 different LADN DNN values.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| LADN indication IEI | | | | | | | | octet 1 |
| Length of LADN indication contents | | | | | | | | octet 2  octet 3 |
| LADN DNN value 1 | | | | | | | | octet 4\*  octet a\* |
| LADN DNN value 2 | | | | | | | | octet a+1\*  octet b\* |
| … | | | | | | | | octet b+1\*  octet g\* |
| LADN DNN value n | | | | | | | | octet g+1\*  octet h\* |

Figure 9.11.3.29.1: LADN indication information element

Table 9.11.3.29.1: LADN indication information element

|  |
| --- |
| Value part of the LADN indication information element (octet 4 to h):  The value part of the LADN indication information element consists of zero or more LADN DNN values. If the LADN indication information element conveys more than 8 LADN DNN values in this information element, the network shall consider the first 8 LADN DNN values and ignore the remaining octets of the information element.  LADN DNN value:  LADN DNN value is coded as the length and value part of DNN information element as specified in subclause 9.11.2.1A starting with the second octet. |

#### 9.11.3.30 LADN information

The purpose of the LADN information information element is to provide the UE with 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 9.11.3.30.1, figure 9.11.3.30.2 and table 9.11.3.30.1.

The LADN information is a type 6 information element with a minimum length of 3 octets and a maximum length of 1715 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 5GS tracking area identity list.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| LADN information IEI | | | | | | | | octet 1 |
| Length of LADN information contents | | | | | | | | octet 2  octet 3 |
| LADN 1 | | | | | | | | octet 4  octet a |
| LADN 2 | | | | | | | | octet a+1\*  octet b\* |
| … | | | | | | | | octet b+1\*  octet g\* |
| LADN n | | | | | | | | octet g+1\*  octet h\* |

Figure 9.11.3.30.1: LADN information information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Length of DNN value | | | | | | | | octet 4 |
| DNN value | | | | | | | | octet 5  octet m |
| 5GS tracking area identity list | | | | | | | | octet m+1  octet a |

Figure 9.11.3.30.2: LADN

Table 9.11.3.30.1: LADN information information element

|  |
| --- |
| Value part of the LADN information information element (octet 4 to octet h)  The value part of the LADN information information element consists of one or several LADNs. Each LADN (e.g. octet 4 to octet a) consists one DNN value and one 5GS tracking area identity list. The length of each LADN is determined by the length of DNN value field and the length of 5GS tracking area identity list field.  The UE shall store the complete list as 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.  DNN value (octet 5 to octet m):  DNN value field is coded as DNN value part of DNN information element as specified in subclause 9.11.2.1A starting with the third octet. |
| 5GS tracking area identity list (octet m+1 to octet a): |
| 5GS tracking area identity list field is coded as the length and the value part of the 5GS Tracking area identity list information element as specified in subclause 9.11.3.9 starting with the second octet. |

#### 9.11.3.31 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 9.11.3.31.1 and table 9.11.3.31.1.

The MICO indication is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| MICO indication IEI | | | | 0  Spare | 0  Spare | SPRTI | RAAI | octet 1 |

Figure 9.11.3.31.1: MICO indication

Table 9.11.3.31.1: MICO indication

|  |  |  |  |
| --- | --- | --- | --- |
| Registration Area Allocation Indication (RAAI) (octet 1, bit 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. | | | |
| Strictly Periodic Registration Timer Indication (SPRTI) (octet 1, bit 2) | | | | |
|  | | | | |
| In the network to UE and the UE to network direction: | | | | |
| Bit | | | | |
| 2 | |  | | | |
| 0 | | strictly periodic registration timer not supported | | | |
| 1 | | strictly periodic registration timer supported | | | |
|  | | | |
| Bits 3 and 4 are spare and shall be coded as zero.  NOTE: In the network to UE direction in the CONFIGURATION UPDATE COMMAND message, bit 1 shall be coded as zero. | | | |

#### 9.11.3.32 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 9.11.3.32.1 and table 9.11.3.32.1.

The NAS key set identifier is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NAS key set identifier IEI | | | | TSC | NAS key set identifier | | | octet 1 |

Figure 9.11.3.32.1: NAS key set identifier information element

Table 9.11.3.32.1: NAS key set identifier information element

|  |  |  |  |
| --- | --- | --- | --- |
| Type of security context flag (TSC) (octet 1) | | | |
|  | | | |
| Bit | | | |
| 4 |  |  |  |
| 0 |  |  | native security context (for KSIAMF) |
| 1 |  |  | mapped security context (for KSIASME) |
|  | | | |
| TSC does not apply for NAS key set identifier value "111". | | | |
|  | | | |
| NAS key set identifier (octet 1) | | | |
|  | | | |
| Bits | | | |
| 3 | 2 | 1 |  |
| 0 | 0 | 0 |  |
| through | | | possible values for the NAS key set identifier |
| 1 | 1 | 0 |  |
|  |  |  |  |
| 1 | 1 | 1 | no key is available (UE to network); |
|  |  |  | reserved (network to UE) |

#### 9.11.3.33 NAS message container

The purpose of the NAS message container IE is to encapsulate a plain 5GS NAS message.

The NAS message container information element is coded as shown in figure 9.11.3.33.1 and table 9.11.3.33.1.

The NAS message container is a type 6 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NAS message container IEI | | | | | | | | octet 1 |
| Length of NAS message container contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
|  | | | | | | | | octet 4 |
| NAS message container contents | | | | | | | |  |
|  | | | | | | | | octet n |

Figure 9.11.3.33.1: NAS message container information element

Table 9.11.3.33.1: 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. |

#### 9.11.3.34 NAS security algorithms

The purpose of the NAS security algorithms information element is to indicate the 5G algorithms to be used for ciphering and integrity protection.

The NAS security algorithms information element is coded as shown in figure 9.11.3.34.1 and table 9.11.3.34.1.

The NAS security algorithms is a type 3 information element with a length of 2 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NAS security algorithms IEI | | | | | | | | octet 1 |
| Type of ciphering algorithm | | | | Type of integrity protection algorithm | | | | octet 2 |

Figure 9.11.3.34.1: NAS security algorithms information element

Table 9.11.3.34.1: 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 | 5G integrity algorithm 5G-IA0 (null integrity protection algorithm) |
| 0 | 0 | 0 | 1 | 5G integrity algorithm 128-5G-IA1 |
| 0 | 0 | 1 | 0 | 5G integrity algorithm 128-5G-IA2 |
| 0 | 0 | 1 | 1 | 5G integrity algorithm 128-5G-IA3 |
| 0 | 1 | 0 | 0 | 5G integrity algorithm 5G-IA4 |
| 0 | 1 | 0 | 1 | 5G integrity algorithm 5G-IA5 |
| 0 | 1 | 1 | 0 | 5G integrity algorithm 5G-IA6 |
| 0 | 1 | 1 | 1 | 5G 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 | 5G encryption algorithm 5G-EA0 (null ciphering algorithm) |
| 0 | 0 | 0 | 1 | 5G encryption algorithm 128-5G-EA1 |
| 0 | 0 | 1 | 0 | 5G encryption algorithm 128-5G-EA2 |
| 0 | 0 | 1 | 1 | 5G encryption algorithm 128-5G-EA3 |
| 0 | 1 | 0 | 0 | 5G encryption algorithm 5G-EA4 |
| 0 | 1 | 0 | 1 | 5G encryption algorithm 5G-EA5 |
| 0 | 1 | 1 | 0 | 5G encryption algorithm 5G-EA6 |
| 0 | 1 | 1 | 1 | 5G encryption algorithm 5G-EA7 |
|  | | | | |
| All other values are reserved. | | | | |

#### 9.11.3.35 Network name

See subclause 10.5.3.5a in 3GPP TS 24.008 [12].

#### 9.11.3.36 Network slicing indication

The purpose of the Network slicing indication information element is to indicate additional information associated with network slicing in the generic UE configuration update procedure and the registration procedure, other than the user's configured NSSAI, allowed NSSAI and rejected NSSAI information.

The Network slicing indication information element is coded as shown in figure 9.11.3.36.1 and table 9.11.3.36.1.

The Network slicing indication is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Network slicing indication IEI | | | | 0  Spare | 0  Spare | DCNI | NSSCI | octet 1 |

Figure 9.11.3.36.1: Network slicing indication

Table 9.11.3.36.1: Network slicing indication

|  |  |  |  |
| --- | --- | --- | --- |
| Network slicing subscription change indication (NSSCI) (octet 1, bit 1) | | | |
| Bit | | | |
| 1 | |  | | |
| 0 | | Network slicing subscription not changed | |
| 1 | | Network slicing subscription changed | |
|  | | | |
| Default configured NSSAI indication (DCNI) (octet 1, bit 2) | | | | |
| Bit | | | | |
| 2 | |  | | |
| 0 | | Requested NSSAI not created from default configured NSSAI | | |
| 1 | | Requested NSSAI created from default configured NSSAI | | |
|  | | | | |
| In the UE to network direction bit 1 is spare. The UE shall set this bit to zero.  In the network to UE direction bit 2 is spare. The network shall set this bit to zero.  Bits 3 and 4 are spare and shall be coded as zero. | | | |

#### 9.11.3.37 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 9.11.3.37.1 and table 9.11.3.37.1.

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: More than one S-NSSAIs in an NSSAI can have the same SST values, and optionally same SD values, which are associated with different mapped HPLMN SST values and optionally mapped HPLMN SD values.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NSSAI IEI | | | | | | | | octet 1 |
| Length of NSSAI contents | | | | | | | | octet 2 |
| S-NSSAI value 1 | | | | | | | | octet 3  octet m |
| S-NSSAI value 2 | | | | | | | | octet m+1\*  octet n\* |
| … | | | | | | | | octet n+1\*  octet u\* |
| S-NSSAI value n | | | | | | | | octet u+1\*  octet v\* |

Figure 9.11.3.37.1: NSSAI information element

Table 9.11.3.37.1: 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 S-NSSAI.  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 9.11.2.8 starting with the second octet. |

#### 9.11.3.37A NSSAI inclusion mode

The purpose of the NSSAI inclusion mode information element is to indicate the NSSAI inclusion mode in which the UE shall operate.

The NSSAI inclusion mode is a type 1 information element.

The NSSAI inclusion modeinformation element is coded as shown in figure 9.11.3.37A.1 and table 9.11.3.37A.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| NSSAI inclusion mode  IEI | | | | 0  spare | 0  spare | NSSAI inclusion mode | | octet 1 |

Figure 9.11.3.37A.1: NSSAI inclusion mode information element

Table 9.11.3.37A.1: NSSAI inclusion mode information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| NSSAI inclusion mode (octet 1, bit 1 to bit 2) | | | | |
|  | | | | |
| Bits | | | | | |
| 2 | 1 |  |  |  | |
| 0 | 0 |  |  | NSSAI inclusion mode A | |
| 0 | 1 |  |  | NSSAI inclusion mode B | |
| 1 | 0 |  |  | NSSAI inclusion mode C | |
| 1 | 1 |  |  | NSSAI inclusion mode D | |

#### 9.11.3.38 Operator-defined access category definitions

The purpose of the Operator-defined access category definitions information element is to provide the UE with the operator-defined access category definitions or to delete the operator-defined access category definitions at the UE.

The Operator-defined access category definitions information element is coded as shown in figure 9.11.3.38.1, figure 9.11.3.38.2 and table 9.11.3.38.1.

The Operator-defined access category definitions is a type 6 information element with a minimum length of 3 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Operator-defined access category definitions IEI | | | | | | | | octet 1 |
| Length of operator-defined access category definitions contents | | | | | | | | octet 2  octet 3 |
| Operator-defined access category definition 1 | | | | | | | | octet 4  octet a |
| Operator-defined access category definition 2 | | | | | | | | octet a+1\*  octet b\* |
| … | | | | | | | | octet b+1\*  octet g\* |
| Operator-defined access category definition 1 n | | | | | | | | octet g+1\*  octet h\* |

Figure 9.11.3.38.1: Operator-defined access category definitions information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Length of operator-defined access category definition contents | | | | | | | | octet 4 |
| Precedence value | | | | | | | | octet 5 |
| PSAC | 0  Spare | 0  Spare | Operator-defined access category number | | | | | octet 6 |
| Length of criteria | | | | | | | | octet 7 |
| Criteria | | | | | | | | octet 8  octet a-1 |
| 0  Spare | 0  Spare | 0  Spare | Standardized access category | | | | | octet a\* |

Figure 9.11.3.38.2: Operator-defined access category definition

Table 9.11.3.38.1: Operator-defined access category definitions information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Value part of the Operator-defined access category definitions information element (octet 3 to h)  The value part of the Operator-defined access category definitions information element consists of zero or several operator-defined access category definition fields. Each operator-defined access category definition field is coded as described in figure 9.11.3.38.2. The length of each operator-defined access category definition field is determined by the length of operator-defined access category definition contents field. | | | | | | | | | |
| Operator-defined access category definition (octet 4 to octet a): | | | | | | | | | |
| Precedence value (octet 5) | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  | Precedence value 0 |
| to | | | | | | | |  |  |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |  | Precedence value 255 |
|  | | | | | | | | | |
| Operator-defined access category number (bits 5 to 1 of octet 6) | | | | | | | | | |
| Bits | | | | | | | | | |
| 5 | 4 | 3 | 2 | 1 |  | | |  | |
| 0 | 0 | 0 | 0 | 0 |  | | | Access category number 32 | |
| to | | | | |  | | |  | |
| 1 | 1 | 1 | 1 | 1 |  | | | Access category number 63 | |
|  | | | | | | | | | |
| Presence of standardized access category (PSAC) (bit 8 of octet 6) | | | | | | | | | |
| PSAC field indicates whether the standardized access category field is present or absent. | | | | | | | | | |
| Bit | | | | | | | | | |
| 8 |  |  | | | | | | | |
| 0 | | Standardized access category field is not included | | | | | | | |
| 1 | | Standardized access category field is included | | | | | | | |
|  | | | | | | | | | |
| Length of criteria (octet 7) | | | | | | | | | |
| Length of criteria field indicates binary coded length of the criteria field. | | | | | | | | | |
|  | | | | | | | | | |
| Criteria (octets 8 to octet a-1) | | | | | | | | | |
| The criteria field contains one or more criteria components fields. Each criteria component field shall be encoded as a sequence of a one octet criteria type field and zero or more octets criteria value field. The criteria type field shall be transmitted first. | | | | | | | | | |
|  | | | | | | | | | |
| Criteria type | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  | DNN type |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |  | OS id + OS App Id type |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |  | S-NSSAI type |
| All other values are reserved. | | | | | | | | | |
|  | | | | | | | | | |
| For "DNN type", the criteria value field shall be encoded as a sequence of one octet DNN length-value pair count field and one or more DNN length-value pair fields. The DNN length-value pair count field indicates the number of included DNN length-value pair fields. Each DNN length-value pair field is coded as a sequence of one octet DNN value length field and a DNN value field. The DNN value length field indicates the length in octets of the DNN value field. The DNN value field contains an APN as specified in 3GPP TS 23.003 [4]. | | | | | | | | | |
|  | | | | | | | | | |
| For "OS Id + OS App Id type", the criteria value field shall be encoded as a sequence of one octet app id value count field and one or more app id value fields. The app id value count field indicates the number of included app id value fields. Each app id value field is coded as a sequence of a sixteen octet OS id value field, one octet OS app id value length field and an OS app id value field. The OS app id value length field indicates the length in octets of the OS app id value field. The OS id value field contains a Universally Unique IDentifier (UUID) as specified in IETF RFC 4122 [35A]. The OS app id value field contains an OS specific application identifier. Coding of the OS app id value field is outside the scope of the present document. | | | | | | | | | |
|  | | | | | | | | | |
| For "S-NSSAI type", the criteria value field shall be encoded as a sequence of one octet S-NSSAI length-value pair count field and one or more S-NSSAI length-value value fields. The S-NSSAI length-value pair count field indicates the number of included S-NSSAI length-value pair fields. Each S-NSSAI length-value pair field is coded as a sequence of one octet S-NSSAI value length field and an S-NSSAI value field. The S-NSSAI value length field indicates the length in octets of the S-NSSAI value field. The S-NSSAI value field contains one octet SST field optionally followed by three octets SD field. The SST field contains a SST. The SD field contains an SD. SST and SD are specified in 3GPP TS 23.003 [4]. | | | | | | | | | |
|  | | | | | | | | | |
| Standardized access category (bits 5 to 1 of octet a) | | | | | | | | | |
| Standardized access category field indicates the access category number of the standardized access category that is used in combination with the access identities to determine the establishment cause. | | | | | | | | | |
| Bits | | | | | | | | | |
| 5 | 4 | 3 | 2 | 1 |  | | |  | |
| 0 | 0 | 0 | 0 | 0 |  | | | Access category number 0 | |
| to | | | | |  | | |  | |
| 0 | 0 | 1 | 1 | 1 |  | | | Access category number 7 | |
| All other values are reserved. | | | | | | | | | |

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

#### 9.11.3.39 Payload container

The purpose of the Payload container information element is to transport one or multiple payloads. If multiple payloads are transported, the associated information of each payload are also transported together with the payload.

The Payload container information element is coded as shown in figure 9.11.3.39.1, figure 9.11.3.39.2, figure 9.11.3.39.3, figure 9.11.3.39.4 and table 9.11.3.39.1.

The Payload container is a type 6 information element with a minimum length of 4 octets and a maximum length of 65538 octets.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
| Payload container IEI | | | | | | | | | | octet 1 |
| Length of payload container contents | | | | | | | | | | octet 2 |
|  | | | | | | | | | | octet 3 |
|  | | | | | | | | | | octet 4 |
| Payload container contents | | | | | | | | | |  |
|  | | | | | | | | | | octet n |

Figure 9.11.3.39.1: Payload container information element

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |  | |
| Number of entries | | | | | | | | | octet 4 | |
| Payload container entry 1 | | | | | | | | | octet 5  octet x2 | |
| Payload container entry 2 | | | | | | | | | octet x2+1  octet x3 | |
| …… | | | | | | | | | … | |
| Payload container entry i | | | | | | | | | octet xi +1  octet n | |

Figure 9.11.3.39.2: Payload container contents with Payload container type "Multiple payloads"

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | 2 | 1 | |  | |
| Length of Payload container entry | | | | | | | | | | octet xi +1  octet xi +2 | |
| Number of optional IEs | | | | | Payload container type | | | | | octet xi +3 | |
| Optional IE 1 | | | | | | | | | | octet xi +4  octet y2 | |
| Optional IE 2 | | | | | | | | | | octet y2+1  octet y3 | |
| … | | | | | | | | | |  | |
| Optional IE j | | | | | | | | | | octet yj+1  octet z | |
| Payload container entry contents | | | | | | | | | | octet z+1  octet n | |

Figure 9.11.3.39.3: Payload container entry

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |  | |
| Type of optional IE | | | | | | | | | octet xi +4 | |
| Length of optional IE | | | | | | | | | octet xi +5 | |
| Value of optional IE | | | | | | | | | octet xi +6  octet y2 | |

Figure 9.11.3.39.4: Optional IE

Table 9.11.3.39.1: Payload container information element

|  |  |  |
| --- | --- | --- |
| Payload container contents (octet 4 to octet n); max value of 65535 octets | | |
| If the payload container type is set to "SOR transparent container" and is included in the DL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the SOR transparent container IE (see subclause 9.11.3.51) for SOR data type is set to value "0" except that the first three octets are not included.  If the payload container type is set to "SOR transparent container" and is included in the UL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the SOR transparent container IE (see subclause 9.11.3.51) for SOR data type is set to value "1" except that the first three octets are not included.  If the payload container type is set to "UE parameters update transparent container" and is included in the DL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the UE parameters update transparent container IE (see subclause 9.11.3.53A) for UE parameters update data type is set to value "0" except that the first three octets are not included.  If the payload container type is set to "UE parameters update transparent container" and is included in the UL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the UE parameters update transparent container IE (see subclause 9.11.3.53A) for UE parameters update data type is set to value "1" except that the first three octets are not included.  If the payload container type is set to "SMS", the payload container contents contain an SMS message (i.e. CP-DATA, CP-ACK or CP-ERROR) as defined in subclause 7.2 in 3GPP TS 24.011 [13].  The coding of Payload container contents is dependent on the particular application.  If the payload container type is set to "Multiple payloads", the number of entries field represents the total number of payload container entries, and the payload container entry contents field is coded as a list of payload container entry according to figure 9.11.3.39.2, with each payload container entry is coded according to figure 9.11.3.39.3 and figure 9.11.3.39.4. | | |
| Payload container entry  For each payload container entry, the payload container type field represents the payload container type value as described in subclause 9.11.3.40, the coding of payload container contents field is dependent on the particular application, and the number of optional IEs field represents the total number of optional IEs associated with the payload container entry contents field in the payload container entry. The error handlings for optional IEs specified in subclauses 7.6.1, 7.6.3 and 7.7.1 shall apply to the optional IEs included in the payload container entry. | | |
| Optional IEs  Type of optional IE (octet xi +4)  This field contains the IEI of the optional IE.  Length of optional IE (octet xi+5)  This field indicates binary coded length of the value of the optional IE entry.  Value of optional IE (octet xi+6 to octet y2)  This field contains the value of the optional IE entry with the value part of the referred information element based on following optional IE reference. If the Request type is included, the value part of the Request type shall be encoded in the bits 1 to 4 and bits 5 to 8 shall be coded as zero. | | |
| IEI | Optional IE name | Optional IE reference |
| 12 | PDU session ID | PDU session identity 2 (see subclause 9.11.3.41) |
| 24 | Additional information | Additional information (see subclause 9.11.2.1) |
| 58 | 5GMM cause | 5GMM cause (see subclause 9.11.3.2) |
| 37 | Back-off timer value | GPRS timer 3 (see subclause 9.11.2.5) |
| 59 | Old PDU session ID | PDU session identity (see subclause 2 9.11.3.41) |
| 80 | Request type | Request type (see subclause 9.11.3.47) |
| 22 | S-NSSAI | S-NSSAI (see subclause 9.11.2.8) |
| 25 | DNN | DNN (see subclause 9.11.2.1A) |
|  | | |
|  | | |
|  | | |
|  | | |
|  | | |
|  | | |

#### 9.11.3.40 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 type information element is coded as shown in figure 9.11.3.40.1 and table 9.11.3.40.1.

The Payload container type is a type 1 information element.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | 6 | 5 | 4 | | 3 | 2 | 1 |  | |
| Payload container type  IEI | | | | | Payload container type value | | | | | octet 1 | |

Figure 9.11.3.40.1: Payload container type information element

Table 9.11.3.40.1: Payload container type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Payload container type value (octet 1) | | | | |
| 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 | SOR transparent container |
| 0 | 1 | 0 | 1 | UE policy container |
| 0 | 1 | 1 | 0 | UE parameters update transparent container |
| 1 | 1 | 1 | 1 | Multiple payloads |
|  | | | | |
| All other values are reserved. | | | | |
|  | | | | |
| NOTE: The value "Multiple payloads" is only used when the Payload container contents in figure 9.11.3.39.1 contains multiple payloads as shown in figure 9.11.3.39.2. | | | | |

#### 9.11.3.41 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 9.11.3.41.1 and table 9.11.3.41.1.

The PDU session identity 2 is a type 3 information element with a length of 2 octets .

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PDU session identity 2 IEI | | | | | | | | octet 1 |
| PDU session identity 2 value | | | | | | | | octet 2 |

Figure 9.11.3.41.1: PDU session identity 2 information element

Table 9.11.3.41.1: 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] . |

#### 9.11.3.42 PDU session reactivation result

The purpose of the PDU session reactivation result information element is to indicate the result of establishments of user-plane resources of PDU sessions.

The PDU session reactivation result information element is coded as shown in figure 9.11.3.42.1 and table 9.11.3.42.1.

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 | | Spare | | | | | | | | | | | | | | | | octet 5\* -34\* |

Figure 9.11.3.42.1: PDU session reactivation result information element

Table 9.11.3.42.1: 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 establishment of user-plane resources of the PDU session was not requested in the Uplink data status IE or establishment of user-plane resources of the PDU session was not allowed in the Allowed PDU session status IE or establishment of user-plane resource of the PDU session is successful.  1 indicates either establishment of user-plane resources of the PDU session was requested in the Uplink data status IE but establishment of user-plane resource of the PDU session is not successful or indicates establishment of user-plane resources of the PDU session was allowed in the Allowed PDU session status IE but establishment of user-plane resource of the PDU session 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. |

#### 9.11.3.43 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 establish the user-plane resources.

The PDU session reactivation result error cause information element is coded as shown in figure 9.11.3.43.1 and table 9.11.3.43.1.

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 9.11.3.43.1: PDU session reactivation result error cause information element

Table 9.11.3.43.1: 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 9.11.3.2). |

#### 9.11.3.44 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 9.11.3.44.1 and table 9.11.3.44.1.

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\*- |
| spare | | | | | | | | 34\* |

Figure 9.11.3.44.1: PDU session status information element

Table 9.11.3.44.1: 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. |

#### 9.11.3.45 PLMN list

See subclause 10.5.1.13 in 3GPP TS 24.008 [12].

#### 9.11.3.46 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 9.11.3.46.1, figure 9.11.3.46.2 and table 9.11.3.46.1.

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.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Rejected NSSAI IEI | | | | | | | | octet 1 |
| Length of Rejected NSSAI contents | | | | | | | | octet 2 |
| Rejected S-NSSAI 1 | | | | | | | | octet 3  octet m |
| Rejected S-NSSAI 2 | | | | | | | | octet m+1\*  octet n\* |
| … | | | | | | | | octet n+1\*  octet u\* |
| Rejected S-NSSAI n | | | | | | | | octet u+1\*  octet v\* |

Figure 9.11.3.46.1: Rejected NSSAI information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Length of rejected S-NSSAI | | | | Cause value | | | | octet 1 |
| SST | | | | | | | | octet 2 |
| SD | | | | | | | | octet 3\*  octet 5\* |

Figure 9.11.3.46.2: Rejected S-NSSAI

Table 9.11.3.46.1: 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. | | | | | |

#### 9.11.3.47 Request type

The purpose of the Request type information element is to indicate the type of the 5GSM message.

The Request type information element is coded as shown in figure 9.11.3.47.1 and table 9.11.3.47.1.

The Request type is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Request type IEI | | | | 0  spare | Request type value | | | octet 1 |

Figure 9.11.3.47.1: Request type information element

Table 9.11.3.47.1: 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 | 0 | 1 |  | modification request |
| 1 | 1 | 0 |  | MA PDU request (NOTE) |
| 1 | 1 | 1 |  | reserved |
| All other values are unused and shall be interpreted as "initial request", if received by the network. | | | | |
| NOTE: This value shall be interpreted as "initial request", if received by a network not supporting MA PDU sessions. | | | | |

#### 9.11.3.48 S1 UE network capability

See subclause 9.9.3.34 in 3GPP TS 24.301 [15].

#### 9.11.3.48A S1 UE security capability

See subclause 9.9.3.36 in 3GPP TS 24.301 [15].

#### 9.11.3.49 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 of the PLMNs in the registration area are allowed area.

The Service area list information element is coded as shown in figure 9.11.3.49.1, figure 9.11.3.49.2, figure 9.11.3.49.3, figure 9.11.3.49.4, figure 9.11.3.49.5 and table 9.11.3.49.1.

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.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Service area list IEI | | | | | | | | octet 1 |
| Length of service area list contents | | | | | | | | octet 2 |
| Partial service area list 1 | | | | | | | | octet 3  octet i |
| Partial service area list 2 | | | | | | | | octet i+1\*  octet l\* |
| … | | | | | | | | octet l+1\*  octet m\* |
| Partial service area list p | | | | | | | | octet m+1\*  octet n\* |

Figure 9.11.3.49.1: Service area list information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed type | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC 1 | | | | | | | | octet 5 |
| TAC 1 (continued) | | | | | | | | octet 6 |
| TAC 1 (continued) | | | | | | | | octet 7 |
| … | | | | | | | | … |
| TAC k | | | | | | | | octet 3k+2\* |
| TAC k (continued) | | | | | | | | octet 3k+3\* |
| TAC k (continued) | | | | | | | | octet 3k+4\* |

Figure 9.11.3.49.2: Partial service area list – type of list = "00"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed type | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC 1 | | | | | | | | octet 5 |
| TAC 1 (continued) | | | | | | | | octet 6 |
| TAC 1 (continued) | | | | | | | | octet 7 |

Figure 9.11.3.49.3: Partial service area list – type of list = "01"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed type | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |
| TAC 1 | | | | | | | | octet 5 |
| TAC 1 (continued) | | | | | | | | octet 6 |
| TAC 1 (continued) | | | | | | | | octet 7 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 8\* |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 9\* |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 10\* |
| TAC 2 | | | | | | | | octet 11\* |
| TAC 2 (continued) | | | | | | | | octet 12\* |
| TAC 2 (continued) | | | | | | | | octet 13\* |
| … | | | | | | | |  |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 6k-4\* |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 6k-3\* |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 6k-2\* |
| TAC k | | | | | | | | octet 6k\*-1 |
| TAC k (continued) | | | | | | | | octet 6k\* |
| TAC k (continued) | | | | | | | | octet 6k+1\* |

Figure 9.11.3.49.4: Partial service area list – type of list = "10"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed type | Type of list | | Number of elements | | | | | octet 1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet 2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet 3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet 4 |

Figure 9.11.3.49.5: Partial service area list – type of list = "11"

Table 9.11.3.49.1: 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. | | | | | |
| The "Allowed type" fields in all the partial service area lists shall have the same value. 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 PLMNs in the registration area 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 |
| to | | | | |  |
| 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 | | | | | |
| containing the MCC+MNC can be ignored.  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. | | | | | |

#### 9.11.3.50 Service type

The purpose of the service typeinformation element is to specify the purpose of the service request procedure.

The service typeis a type 1 information element.

The service typeinformation element is coded as shown in figure 9.11.3.50.1 and table 9.11.3.50.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Service type  IEI | | | | Service type value | | | | octet 1 |

Figure 9.11.3.50.1: Service type information element

Table 9.11.3.50.1: 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 | elevated signalling |
| 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. | | | | |

#### 9.11.3.50A SMS indication

The purpose of the SMS indication information element is to indicate that the ability for the UE to use SMS over NAS has changed.

The SMS indication information element is coded as shown in figure 9.11.3.50A.1 and table 9.11.3.50A.1.

The SMS indication is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| SMS indication IEI | | | | 0  Spare | 0  Spare | 0  Spare | SAI | octet 1 |

Figure 9.11.3.50A.1: SMS indication

Table 9.11.3.50A.1: SMS indication

|  |  |  |
| --- | --- | --- |
| SMS availability indication (SAI) (octet 1) | | |
|  | | |
| Bit | | |
| 1 | |  |
| 0 | SMS over NAS not available | |
| 1 | SMS over NAS available | |
|  |  | |
| Bits 2, 3 and 4 are spare and shall be coded as zero, | | |

#### 9.11.3.51 SOR transparent container

The purpose of the SOR transparent container information element in the REGISTRATION ACCEPT message is to provide 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. The purpose of the SOR transparent container information element in the REGISTRATION COMPLETE message is to indicate the UE acknowledgement of successful reception of the SOR transparent container IE in the REGISTRATION ACCEPT message.

NOTE: When used in NAS transport procedure, the contents of the SOR transparent container information element in the Payload container IE of the DL NAS TRANSPORT message are used to provide the list of preferred PLMN/access technology combinations and optional acknowledgement request, and the contents of the SOR transparent container information element in the Payload container IE of the UL NAS TRANSPORT message are used to indicate the UE acknowledgement of successful reception of the SOR transparent container IE in the DL NAS TRANSPORT message.

The SOR transparent container information element is coded as shown in figure 9.11.3.51.1, figure 9.11.3.51.2, figure 9.11.3.51.3, figure 9.11.3.51.4, figure 9.11.3.51.5, figure 9.11.3.51.6 and table 9.11.3.51.1.

The SOR transparent container is a type 6 information element with a minimum length of 20 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| SOR transparent container IEI | | | | | | | | octet 1 |
| Length of SOR transparent container contents | | | | | | | | octet 2  octet 3 |
| SOR header | | | | | | | | octet 4 |
| SOR-MAC-IAUSF | | | | | | | | octet 5-20 |
| CounterSOR | | | | | | | | octet 21-22 |
| Secured packet | | | | | | | | octet 23\* - n\* |

Figure 9.11.3.51.1: SOR transparent container information element for list type with value "0" and SOR data type with value "0"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| SOR transparent container IEI | | | | | | | | octet 1 |
| Length of SOR transparent container contents | | | | | | | | octet 2  octet 3 |
| SOR header | | | | | | | | octet 4 |
| SOR-MAC-IAUSF | | | | | | | | octet 5-20 |
| CounterSOR | | | | | | | | octet 21-22 |
| PLMN ID and access technology list | | | | | | | | octet 23\*-102\* |

Figure 9.11.3.51.2: SOR transparent container information element for list type with value "1" and SOR data type with value "0"

|  |  |
| --- | --- |
| PLMN ID 1 | octet 23\*- 25\* |
| access technology identifier 1 | octet 26\*- 27\* |
| … |  |
| PLMN ID n | octet 98\*-100\* |
| access technology identifier n | octet 101\*-102\* |

Figure 9.11.3.51.3: PLMN ID and access technology list

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| SOR transparent container IEI | | | | | | | | octet 1 |
| Length of SOR transparent container contents | | | | | | | | octet 2  octet 3 |
| SOR header | | | | | | | | octet 4 |
| SOR-MAC-IUE | | | | | | | | octet 5 - 20 |

Figure 9.11.3.51.4: SOR transparent container information element for SOR data type with value "1"

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | ACK | | List type | | List indication | | SOR data type | | octet 4 | |

Figure 9.11.3.51.5: SOR header for SOR data type with value "0"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | SOR data type | octet 4 |

Figure 9.11.3.51.6: SOR header for SOR data type with value "1"

Table 9.11.3.51.1: SOR transparent container information element

|  |  |
| --- | --- |
| SOR-MAC-IAUSF, SOR-MAC-IUE and CounterSOR are coded as specified in 3GPP TS 33.501 [24] | |
|  | |
| SOR data type (octet 4, bit 1) | |
| 0 | The SOR transparent container carries steering of roaming information. |
| 1 | The SOR transparent container carries acknowledgement of successful reception of the steering of roaming information. |
|  | |
| List indication value (octet 4, bit 2) | |
| 0 | 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' |
| 1 | list of preferred PLMN/access technology combinations is provided |
|  | |
| List type (octet 4, bit 3) | |
| 0 | The list type is a secured packet. |
| 1 | The list type is a "PLMN ID and access technology list". |
|  |  |
| Acknowledgement (ACK) value (octet 4, bit 4) | |
| 0 | acknowledgement not requested |
| 1 | acknowledgement requested |
|  | |
| The secure packet is coded as specified in 3GPP TS 31.115 [22B]. | |
|  | |
| The PLMN ID and access technology list consists of PLMN ID and access technology identifier and are coded as specified in 3GPP TS 31.102 [22] subclause 4.2.5. The PLMN ID and access technology identifier are provided in decreasing order of priority, i.e. PLMN ID 1 indicates highest priority and PLMN ID n indicates lowest priority. | |

#### 9.11.3.52 Time zone

See subclause 10.5.3.8 in 3GPP TS 24.008 [12].

#### 9.11.3.53 Time zone and time

See subclause 10.5.3.9 in 3GPP TS 24.008 [12].

#### 9.11.3.53A UE parameters update transparent container

The purpose of the UE parameters update transparent container when sent from the network to the UE is to provide UE parameters update data, optional acknowledgement request and optional re-registration request. The purpose of the UE parameters update transparent container when sent from the UE to the network is to indicate the UE acknowledgement of successful reception of the UE parameters update transparent container.

The UE parameters update transparent container information element is coded as shown in figure 9.11.3.53A.1, figure 9.11.3.53A.2, figure 9.11.3.53A.3, figure 9.11.3.53A.4, figure 9.11.3.53A.5, figure 9.11.3.53A.6, figure 9.11.3.53A.7 and table 9.11.3.53A.1.

The UE parameters update transparent container is a type 6 information element with a minimum length of 20 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE parameters update transparent container IEI | | | | | | | | octet 1 |
| Length of UE parameters update transparent container contents | | | | | | | | octet 2  octet 3 |
| UE parameters update header | | | | | | | | octet 4 |
| UPU-MAC-IAUSF | | | | | | | | octet 5-20 |
| CounterUPU | | | | | | | | octet 21-22 |
| UE parameters update list | | | | | | | | octet 23\* - n\* |

Figure 9.11.3.53A.1: UE parameters update transparent container information element for UE parameters update data type with value "0"

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | 3 | 2 | 1 | |  | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | UE parameters update data set 1 type | | | | | octet 23\* | |
| Length of UE parameters update data set 1 | | | | | | | | | | | | | octet 24\*-  25\* | |
| UE parameters update data set 1 | | | | | | | | | | | | | octet 26\*-  x\* | |
| … | | | | | | | | | | | | |  | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | UE parameters update data set n type | | | | | octet y\* | |
| Length of UE parameters update data set n | | | | | | | | | | | | | octet y+1\*-  y+2\* | |
| UE parameters update data set n | | | | | | | | | | | | | octet y+3\*-  n\* | |

Figure 9.11.3.53A.2: UE parameters update list

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Secured packet | | | | | | | | octet a\* - a+z\* |

Figure 9.11.3.53A.3: UE parameters update data set for UE parameters update data set type with value "00000001"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Default configured NSSAI | | | | | | | | octet b\* -  c\* |

Figure 9.11.3.53A.4: UE parameters update data set for UE parameters update data set type with value "00000010"

|  |  |
| --- | --- |
| UE parameters update transparent container IEI | octet 1 |
| Length of UE parameters update transparent container contents | octet 2  octet 3 |
| UE parameters update header | octet 4 |
| UPU-MAC-IUE | octet 5 - 20 |

Figure 9.11.3.53A.5: UE parameters update transparent container information element for UE parameters update data type with value "1"

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | REG | | ACK | | UPU data type | | octet 4 | |

Figure 9.11.3.53A.6: UE parameters update header for UE parameters update data type with value "0"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | UPU data type | octet 4 |

Figure 9.11.3.53A.7: UE parameters update header for UE parameters update data type with value "1"

Table 9.11.3.53A.1: UE parameters update transparent container information element

|  |  |
| --- | --- |
| UPU-MAC-IAUSF, UPU-MAC-IUE and CounterUPU are coded as specified in 3GPP TS 33.501 [24] | |
|  | |
| UPU data type (octet 4, bit 1) | |
| 0 | The UE parameters update transparent container carries a UE parameters update list |
| 1 | The UE parameters update transparent container carries an acknowledgement of successful reception of a UE parameters update list |
|  | |
| Acknowledgement (ACK) value (octet 4, bit 2) | |
| 0 | acknowledgement not requested |
| 1 | acknowledgement requested |
|  | |
| Re-registration (REG) value (octet 4, bit 3) | |
| 0 | re-registrationt not requested |
| 1 | re-registration requested |
|  | |
| UE parameters update data set type | |
| Bits  4 3 2 1 | |
| 0 0 0 1 Routing indicator update data | |
| 0 0 1 0 Default configured NSSAI update data | |
|  | |
| All other values are reserved | |
|  | |
| The secured packet is coded as specified in 3GPP TS 31.115 [22B]. | |
|  | |
| The default configured NSSAI is encoded as the value part of the NSSAI IE (see subclause 9.11.3.37). | |

#### 9.11.3.54 UE security capability

The UE security capability information element is used by the UE and by the network to indicate which security algorithms are supported by the UE in N1 mode for NAS security as well as which security algorithms are supported over NR and E-UTRA connected to 5GCN for AS security.

The UE security capability information element is coded as shown in figure 9.11.3.54.1 and table 9.11.3.54.1.

The UE security capability is a type 4 information element with a minimum length of 4 octets and a maximum length of 10 octets.

Octets 5 to 10 are optional. If octet 5 is included, then also octet 6 shall be included.

If the UE does not support any security algorithm for AS security over E-UTRA connected to 5GCN, it shall not include octets 5 and 6. The UE shall not include octets 7 to 10.

If the UE does not support any security algorithm for AS security over E-UTRA connected to 5GCN, and if the network includes octets 7 to 10, then the network shall also include octets 5 to 6.

If the network includes octet 7, then it shall include also octet 8. If the network includes octet 9, then it shall include also octet 10.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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\* |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  |
| Spare | | | | | | | | octet 7\* -10\* |

Figure 9.11.3.54.1: UE security capability information element

Table 9.11.3.54.1: 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-EA3 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 |
|  | | | | | |
| For the UE not supporting any security algorithm for AS security over E-UTRA connected to 5GCN, all bits in octets 5 to 10 are spare and shall be ignored, if the respective octet is received with the information element.  For the UE supporting at least one security algorithm for AS security over E-UTRA connected to 5GCN all bits in octets 7 to 10 are spare and shall be ignored, if the respective octet is received with the information element.  If the AMF receives any of the octets 7 to 10 (NOTE 5), it shall store the octets as received and include them when sending the UE security capability information element to the UE. | | | | | |
| 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 AS security over E-UTRA connected to 5GCN.  NOTE 4: The code points in octet 6 are used to indicate support for EPS integrity algorithms for AS security over E-UTRA connected to 5GCN.  NOTE 5: The AMF can receive this information element also from another AMF or MME during N1 mode to N1 mode or S1 mode to N1 mode handover preparation. | | | | | |

#### 9.11.3.55 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 9.11.3.55.1 and table 9.11.3.55.1.

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 9.11.3.55.1: UE's usage setting information element

Table 9.11.3.55.1: 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, | | | | |

#### 9.11.3.56 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 9.11.3.56.1 and table 9.11.3.56.1.

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 9.11.3.56.1: UE status information element

Table 9.11.3.56.1: 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. | | | | |

#### 9.11.3.57 Uplink data status

The purpose of the Uplink data status information element is to indicate to the network which preserved PDU sessions have uplink data pending.

The Uplink data status information element is coded as shown in figure 9.11.3.57.1 and table 9.11.3.57.1.

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 9.11.3.57.1: Uplink data status information element

Table 9.11.3.57.1: 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. |

#### 9.11.3.58 Non-3GPP NW provided policies

See subclause 10.5.5.37 in 3GPP TS 24.008 [12].

#### 9.11.3.59 EPS bearer context status

See subclause 9.9.2.1 in 3GPP TS 24.301 [15].

#### 9.11.3.60 Extended DRX parameters

See subclause 10.5.5.32 in 3GPP TS 24.008 [12].

#### 9.11.3.61 Mobile station classmark 2

See subclause 10.5.1.6 in 3GPP TS 24.008 [12].

#### 9.11.3.62 Supported codec list

See subclause 10.5.4.32 in 3GPP TS 24.008 [12].

#### 9.11.3.63 MA PDU session information

The purpose of the MA PDU session information information element is to convey the MA-related information for the PDU session.

The MA PDU session information information element is coded as shown in figure 9.11.3.63.1 and table 9.11.3.63.1.

The MA PDU session information is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| MA PDU session information IEI | | | | MA PDU session information value | | | | octet 1 |

Figure 9.11.3.63.1: MA PDU session information information element

Table 9.11.3.63.1: MA PDU session information information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| MA PDU session information value (octet 1, bit 1 to bit 4) | | | | |
|  | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 1 | MA PDU session network upgrade is allowed |
| All other values are spare. | | | | |

### 9.11.4 5GS session management (5GSM) information elements

#### 9.11.4.1 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 9.11.4.1.1 and table 9.11.4.1.1.

The 5GSM capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GSM capability IEI | | | | | | | | octet 1 |
| Length of 5GSM capability contents | | | | | | | | octet 2 |
| 0  Spare | 0  Spare | 0  Spare | MPTCP | ATS-LL | EPT-S1 | MH6-PDU | RqoS | octet 3 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | octet 4\* -15\* |
| Spare | | | | | | | |

Figure 9.11.4.1.1: 5GSM capability information element

Table 9.11.4.1.1: 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 |
|  | | | | |
| Ethernet PDN type in S1 mode (EPT-S1) (octet 3, bit 3) | | | | |
| This bit indicates UE's 5GSM capability for Ethernet PDN type in S1 mode. | | | | |
| 0 |  |  |  | Ethernet PDN type in S1 mode not supported |
| 1 |  |  |  | Ethernet PDN type in S1 mode supported |
|  | | | | |
| ATSSS Low-Layer functionality (ATS-LL) (octet 3, bit 4) | | | | |
| This bit indicates the 5GSM capability to support ATSSS Low-Layer functionality | | | | |
| 0 |  |  |  | ATSSS Low-Layer functionality not supported |
| 1 |  |  |  | ATSSS Low-Layer functionality supported |
|  | | | | |
| MPTCP functionality (MPTCP) (octet 3, bit 5) | | | | |
| This bit indicates the 5GSM capability to support MPTCP functionality | | | | |
| 0 |  |  |  | MPTCP functionality not supported |
| 1 |  |  |  | MPTCP functionality 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. | | | | |
|  | | | | |

#### 9.11.4.2 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 9.11.4.2.1 and table 9.11.4.2.1.

The 5GSM cause is a type 3 information element with 2 octets length.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GSM cause IEI | | | | | | | | octet 1 |
| Cause value | | | | | | | | octet 2 |

Figure 9.11.4.2.1: 5GSM cause information element

Table 9.11.4.2.1: 5GSM cause information element

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cause value (octet 2) | | | | | | | | | | | | | | | | | | | |
| Bits | | | | | | | | | | | | | | | | | | | |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |  | |
| 0 | | 0 | | 0 | | 0 | | 1 | | 0 | | 0 | | 0 | |  | | Operator determined barring | |
| 0 | | 0 | | 0 | | 1 | | 1 | | 0 | | 1 | | 0 | |  | | Insufficient resources | |
| 0 | | 0 | | 0 | | 1 | | 1 | | 0 | | 1 | | 1 | |  | | 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 or authorization failed | |
| 0 | | 0 | | 0 | | 1 | | 1 | | 1 | | 1 | | 1 | |  | | Request rejected, unspecified | |
| 0 | | 0 | | 1 | | 0 | | 0 | | 0 | | 0 | | 0 | |  | | Service option not supported | |
| 0 | | 0 | | 1 | | 0 | | 0 | | 0 | | 0 | | 1 | |  | | Requested service option not subscribed | |
| 0 | | 0 | | 1 | | 0 | | 0 | | 0 | | 1 | | 0 | |  | | Service option temporarily out of order | |
| 0 | | 0 | | 1 | | 0 | | 0 | | 0 | | 1 | | 1 | |  | | PTI already in use | |
| 0 | | 0 | | 1 | | 0 | | 0 | | 1 | | 0 | | 0 | |  | | Regular deactivation | |
| 0 | | 0 | | 1 | | 0 | | 0 | | 1 | | 1 | | 0 | |  | | Network failure | |
| 0 | | 0 | | 1 | | 0 | | 0 | | 1 | | 1 | | 1 | |  | | Reactivation requested | |
| 0 | | 0 | | 1 | | 0 | | 1 | | 0 | | 0 | | 1 | |  | | Semantic error in the TFT operation | |
| 0 | | 0 | | 1 | | 0 | | 1 | | 0 | | 1 | | 0 | |  | | Syntactical error in the TFT operation | |
| 0 | | 0 | | 1 | | 0 | | 1 | | 0 | | 1 | | 1 | |  | | Invalid PDU session identity | |
| 0 | | 0 | | 1 | | 0 | | 1 | | 1 | | 0 | | 0 | |  | | Semantic errors in packet filter(s) | |
| 0 | | 0 | | 1 | | 0 | | 1 | | 1 | | 0 | | 1 | |  | | Syntactical error in packet filter(s) | |
| 0 | | 0 | | 1 | | 0 | | 1 | | 1 | | 1 | | 0 | |  | | Out of LADN service area | |
| 0 | | 0 | | 1 | | 0 | | 1 | | 1 | | 1 | | 1 | |  | | PTI mismatch | |
| 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 | | 0 | | 1 | | 1 | | 0 | | 1 | | 1 | | 0 | |  | | PDU session does not exist | |
| 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 | | 0 | | 0 | | 1 | | 0 | |  | | Maximum data rate per UE for user-plane integrity protection is too low | |
| 0 | | 1 | | 0 | | 1 | | 0 | | 0 | | 1 | | 1 | |  | | Semantic error in the QoS operation | |
| 0 | | 1 | | 0 | | 1 | | 0 | | 1 | | 0 | | 0 | |  | | Syntactical error in the QoS operation | |
| 0 | | 1 | | 0 | | 1 | | 0 | | 1 | | 0 | | 1 | |  | | Invalid mapped EPS bearer identity | |
| 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". | | | | | | | | | | | | | | | | | | | |

#### 9.11.4.3 Always-on PDU session indication

The purpose of the Always-on PDU session indication information element is to indicate whether a PDU session is established as an always-on PDU session.

The Always-on PDU session indication information element is coded as shown in figure 9.11.4.3.1 and table 9.11.4.3.1.

The Always-on PDU session indication is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Always-on PDU session indication IEI | | | | 0  Spare | 0  Spare | 0  Spare | APSI | octet 1 |

**Figure 9.11.4.3.1: Always-on PDU session indication**

**Table 9.11.4.3.1: Always-on PDU session indication**

|  |  |
| --- | --- |
| Always-on PDU session indication (APSI) (octet 1) | |
|  | |
| Bit | |
| **1** |  | |
| 0 | Always-on PDU session not allowed |
| 1 | Always-on PDU session required |
|  | |
| Bits 2, 3 and 4 are spare and shall be coded as zero, | |

#### 9.11.4.4 Always-on PDU session requested

The purpose of the Always-on PDU session requested information element is to indicate whether a PDU session is requested to be established as an always-on PDU session.

The Always-on PDU session requested information element is coded as shown in figure 9.11.4.4.1 and table 9.11.4.4.1.

The Always-on PDU session requested is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Always-on PDU session requested IEI | | | | 0  Spare | 0  Spare | 0  Spare | APSR | octet 1 |

Figure 9.11.4.4.1: Always-on PDU session requested

Table 9.11.4.4.1: Always-on PDU session requested

|  |  |
| --- | --- |
| Always-on PDU session requested (APSR) (octet 1) | |
|  | |
| Bit | |
| **1** |  |
| 0 | Always-on PDU session not requested |
| 1 | Always-on PDU session requested |
|  | |
| Bits 2, 3 and 4 are spare and shall be coded as zero, | |

#### 9.11.4.5 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 9.11.4.5.1 and table 9.11.4.5.1.

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 9.11.4.5.1: Allowed SSC mode information element

Table 9.11.4.5.1: Allowed SSC mode information element

|  |  |
| --- | --- |
| SSC1 (octet 1, bit 1) | |
| Bit | |
| 1 |  |
| 0 | SSC mode 1 not allowed |
| 1 | SSC mode 1 allowed |
|  |  |
| SSC2 (octet 1, bit 2) | |
| Bit | |
| 2 |  |
| 0 | SSC mode 2 not allowed |
| 1 | SSC mode 2 allowed |
|  |  |
| SSC3 (octet 1, bit 3) | |
| Bit | |
| 3 |  |
| 0 | SSC mode 3 not allowed |
| 1 | SSC mode 3 allowed |
|  | |
| Bit 4 is spare and shall be encoded as zero. | |

#### 9.11.4.6 Extended protocol configuration options

See subclause 10.5.6.3A in 3GPP TS 24.008 [12].

#### 9.11.4.7 Integrity protection maximum data rate

The purpose of the integrity protection maximum data rate information element is for the UE to indicate to the network the maximum data rate per UE for user-plane integrity protection for uplink and the maximum data rate per UE for user-plane integrity protection for downlink that are supported by the UE.

The integrity protection maximum data rate is coded as shown in figure 9.11.4.7.1 and table 9.11.4.7.2.

The integrity protection maximum data rate is a type 3 information element with a length of 3 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Integrity protection maximum data rate IEI | | | | | | | | octet 1 |
| Maximum data rate per UE for user-plane integrity protection for uplink | | | | | | | | octet 2 |
| Maximum data rate per UE for user-plane integrity protection for downlink | | | | | | | | octet 3 |

Figure 9.11.4.7.1: Integrity protection maximum data rate information element

Table 9.11.4.7.2: Integrity protection maximum data rate information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Maximum data rate per UE for user-plane integrity protection for uplink (octet 2) | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  | 64 kbps |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |  | Full data rate |
| All other values are spare. If received they shall be interpreted as "64 kbps". | | | | | | | | | |
|  | | | | | | | | | |
| Maximum data rate per UE for user-plane integrity protection for downlink (octet 3) | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  | 64 kbps |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |  | Full data rate |
| All other values are spare. If received they shall be interpreted as "64 kbps". | | | | | | | | | |

#### 9.11.4.8 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, 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 contextsinformation element is coded as shown in figure 9.11.4.8.1, figure 9.11.4.8.2, figure 9.11.4.8.3 and table 9.11.4.8.1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | Mapped EPS bearer contexts IEI | | | | | | | | octet 1 | |
|  | Length of Mapped EPS bearer contexts contents | | | | | | | | octet 2 | |
|  | octet 3 | |
|  | Mapped EPS bearer context 1 | | | | | | | | octet 4  octet u | |
|  | Mapped EPS bearer context 2 | | | | | | | | octet u+1  octet v | |
|  | … | | | | | | | | octet v+1  octet w | |
|  | Mapped EPS bearer context n | | | | | | | | octet w+1  octet x |

Figure 9.11.4.8.1: Mapped EPS bearer contexts

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | | 6 | 5 | | 4 | | 3 | 2 | 1 |  |
|  | EPS bearer identity | | | | | | | | | | | octet 4 |
|  | Length of Mapped EPS bearer context | | | | | | | | | | | octet 5  octet 6 |
|  | Operation code | | 0  Spare | | | E bit | | Number of EPS parameters | | | | octet 7 |
|  | EPS parameters list | | | | | | | | | | | octet 8  octet u |

Figure 9.11.4.8.2: Mapped EPS bearer context

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | EPS parameter identifier 1 | | | | | | | | octet 8 |
|  | Length of EPS parameter contents 1 | | | | | | | | octet 9 |
|  | EPS parameter contents 1 | | | | | | | | octet 10  octet h |
|  | EPS parameter identifier 2 | | | | | | | | octet h+1 |
|  | Length of EPS parameter contents 2 | | | | | | | | octet h+2 |
|  | EPS parameter contents 2 | | | | | | | | octet h+3  octet i |
|  | … | | | | | | | | octet i+1  octet j |
|  | EPS parameter identifier N | | | | | | | | octet j+1 |
|  | Length of EPS parameter contents N | | | | | | | | octet j+2 |
|  | EPS parameter contents N | | | | | | | | octet j+3  octet u |

Figure 9.11.4.8.3: EPS parameters list

Table 9.11.4.8.1: 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  Bit 6 of octet 7 is spare and shall be coded as zero.  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.  For the "create new EPS bearer" operation and "delete existing EPS bearer" operation, bit 5 of octet 7 is ignored.  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 4 through 1 of octet x+1 where bit 4 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]. |

#### 9.11.4.9 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 9.11.4.9.1 and table 9.11.4.9.1.

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 |
| Maximum number of supported packet filters (continued) | | | | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | octet 3 |

Figure 9.11.4.9.1: Maximum number of supported packet filters information element

Table 9.11.4.9.1: 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 6 of second octet is the least significant bit. Bit 5 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. |
|  |

#### 9.11.4.10 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 9.11.4.10.1 and table 9.11.4.10.1.

The PDU address is a type 4 information element with minimum length of 7 octets and a maximum length of 15 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | 2 | 1 |  |
| PDU address IEI | | | | | | | | | | | | | octet 1 |
| Length of PDU address contents | | | | | | | | | | | | | octet 2 |
| 0 | 0 | | 0 | | 0 | | 0 | | PDU session type value | | | | octet 3 |
| spare | | | | | | | | |
| PDU address information | | | | | | | | | | | | | octet 4  octet 15 |

Figure 9.11.4.10.1: PDU address information element

Table 9.11.4.10.1: 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. | | | | |

#### 9.11.4.11 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 9.11.4.11.1 and table 9.11.4.11.1.

The PDU session type is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PDU session type IEI | | | | 0  Spare | PDU session type value | | | octet 1 |

Figure 9.11.4.11.1: PDU session type information element

Table 9.11.4.11.1: 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. | | | | |

#### 9.11.4.12 QoS flow descriptions

The purpose of the QoS flow descriptions information element is to indicate a set of QoS flow descriptions to be used by the UE, where each QoS flow description is a set of parameters as described in subclause 6.2.5.1.1.4.

The QoS flow descriptions information element is a type 6 information element with a minimum length of 6 octets. The maximum length for the information element is 65538 octets.

The QoS flow descriptions information element is coded as shown in figure 9.11.4.12.1, figure 9.11.4.12.2, figure 9.11.4.12.3, figure 9.11.4.12.4, and table 9.11.4.12.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| QoS flow descriptions IEI | | | | | | | | octet 1 |
| Length of QoS flow descriptions contents | | | | | | | | octet 2  octet 3 |
| QoS flow description 1 | | | | | | | | octet 4  octet u |
| QoS flow description 2 | | | | | | | | octet u+1  octet v |
| ... | | | | | | | | octet v+1  octet w |
| QoS flow description n | | | | | | | | octet w+1  octet x |

Figure 9.11.4.12.1: QoS flow descriptions information element

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | | 6 | | 5 | | 4 | | 3 | 2 | | 1 |  |
| 0  Spare | | 0  Spare | QFI | | | | | | | | | | octet 4 |
| Operation code | | | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | 0  Spare | | octet 5 |
| 0  Spare | | E | Number of parameters | | | | | | | | | | octet 6 |
| Parameters list | | | | | | | | | | | | | octet 7\*  octet u\* |

Figure 9.11.4.12.2: QoS flow description

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Parameter 1 | | | | | | | | octet 7  octet m |
| Parameter 2 | | | | | | | | octet m+1  octet n |
| ... | | | | | | | | octet n+1  octet o |
| Parameter n | | | | | | | | octet o+1  octet u |

Figure 9.11.4.12.3: Parameters list

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Parameter identifier | | | | | | | | octet 7 |
| Length of parameter contents | | | | | | | | octet 8 |
| Parameter contents | | | | | | | | octet 9  octet m |

Figure 9.11.4.12.4: Parameter

Table 9.11.4.12.1: QoS flow descriptions information element

|  |
| --- |
| QoS flow identifier (QFI) (bits 6 to 1 of octet 4)  QFI field contains the QoS flow identifier.  Bits  6 5 4 3 2 1  0 0 0 0 0 0 no QoS flow identifier assigned  0 0 0 0 0 1 QFI 1  to  1 1 1 1 1 1 QFI 63  The network shall not set the QFI value to 0. |
| Operation code (bits 8 to 6 of octet 5)  Bits  8 7 6  0 0 1 Create new QoS flow description  0 1 0 Delete existing QoS flow description  0 1 1 Modify existing QoS flow description  All other values are reserved. |
| E bit (bit 7 of octet 6)  For the "create new QoS flow description" operation, the E bit is encoded as follows:  Bit 7  0 reserved  1 parameters list is included  For the "Delete existing QoS flow description" operation, the E bit is encoded as follows:  Bit 7  0 parameters list is not included  1 reserved  For the "modify existing QoS flow description" operation, the E bit is encoded as follows:  Bit 7  0 extension of previously provided parameters  1 replacement of all previously provided parameters  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 "extension of previously provided parameters" or "replacement of all previously provided parameters", the number of parameters field has non-zero value. If the E bit is set to "extension of previously provided parameters" and one of the parameters in the new parameters list already exists in the previously provided parameters, the parameter shall be set to the new value.  Number of parameters (bits 6 to 1 of octet 6)  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 6 where bit 6 is the most significant and bit 1 is the least significant bit.  Parameters list (octets 7 to u)  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  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 5QI 67  0 1 0 0 0 1 0 0 Spare  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 5QI 71  0 1 0 0 1 0 0 0 5QI 72  0 1 0 0 1 0 0 1 5QI 73  0 1 0 0 1 0 1 0 5QI 74  0 1 0 0 1 0 1 1 5QI 75  0 1 0 0 1 1 0 0 5QI 76  0 1 0 0 1 1 0 1  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 5QI 80  0 1 0 1 0 0 0 1 Spare  0 1 0 1 0 0 1 0 5QI 82  0 1 0 1 0 0 1 1 5QI 83  0 1 0 1 0 1 0 0 5QI 84  0 1 0 1 0 1 0 1 5QI 85  0 1 0 1 0 1 1 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 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.  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). The UE shall not include the EPS bearer identity parameter in any mobile originated 5GSM messages. |
|  |
| NOTE: The total number of EPS bearer identities included in all QoS flow descriptions of a UE cannot exceed fifteen. |

#### 9.11.4.13 QoS rules

The purpose of the QoS rulesinformation 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 rulesinformation element is coded as shown in figure 9.11.4.13.1, figure 9.11.4.13.2, figure 9.11.4.13.3, figure 9.11.4.13.4 and table 9.11.4.13.1.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | QoS rules IEI | | | | | | | | octet 1 |
|  | Length of QoS rules IE | | | | | | | | octet 2 |
|  | octet 3 |
|  | QoS rule 1 | | | | | | | | octet 4  octet u |
|  | QoS rule 2 | | | | | | | | octet u+1  octet v |
|  | … | | | | | | | | octet v+1  octet w |
|  | QoS rule n | | | | | | | | octet w+1  octet x |

Figure 9.11.4.13.1: QoS rules information element

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | | 4 | | 3 | 2 | 1 |  |
|  | QoS rule identifier | | | | | | | | | | octet 4 |
|  | Length of QoS rule | | | | | | | | | | octet 5 |
|  | octet 6 |
|  | Rule operation code | | | | DQR bit | | Number of packet filters | | | | octet 7 |
|  | Packet filter list | | | | | | | | | | octet 8\*  octet m\* |
|  | QoS rule precedence | | | | | | | | | | octet m+1\* |
|  | 0  Spare | Segregation | QoS flow identifier (QFI) | | | | | | | | octet m+2\* |

Figure 9.11.4.13.2: QoS rule (u=m+2)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 0 | 0 | 0 | 0 | Packet filter identifier 1 | | | | octet 8 |
| Spare | | | |
|  | 0 | 0 | 0 | 0 | Packet filter identifier 2 | | | | octet 9 |
| Spare | | | |
|  | … | | | | | | | |  |
|  | 0 | 0 | 0 | 0 | Packet filter identifier N | | | | octet N+7 |
| Spare | | | |

Figure 9.11.4.13.3: Packet filter list when the rule operation is "modify existing QoS rule and delete packet filters" (z=N+7)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | 0 | 0 | Packet filter direction 1 | | Packet filter identifier 1 | | | | octet 8 |
| Spare | |
|  | Length of packet filter contents 1 | | | | | | | | octet 9 |
|  | Packet filter contents 1 | | | | | | | | octet 10  octet m |
|  | 0 | 0 | Packet filter direction 2 | | Packet filter identifier 2 | | | | octet m+1 |
| Spare | |
|  | Length of packet filter contents 2 | | | | | | | | octet m+2 |
|  | Packet filter contents 2 | | | | | | | | octet m+3  octet n |
|  | … | | | | | | | | octet n+1  octet y |
|  | 0 | 0 | Packet filter direction N | | Packet filter identifier N | | | | octet y+1 |
| Spare | |
|  | Length of packet filter contents N | | | | | | | | octet y+2 |
|  | Packet filter contents N | | | | | | | | octet y+3  octet z |

Figure 9.11.4.13.4: 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 all packet filters"

Table 9.11.4.13.1: QoS rules information element

|  |
| --- |
| QoS rule identifier (octet 4)  The QoS rule identifier field is used to identify the QoS rule.  Bits  8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 0 no QoS rule identifier assigned  0 0 0 0 0 0 0 1 QRI 1  to  1 1 1 1 1 1 1 1 QRI 255  The network shall not set the QRI value to 0.  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. For the "delete existing QoS rule" operation, the QoS rule precedence value field shall not be included. For the "create new QoS rule" operation, the QoS rule precedence value field shall be included.  The value 80 (decimal) is reserved.  Segregation bit (bit 7 of octet m+2) (see NOTE 1)  In the UE to network direction the segregation bit indicates whether the UE is requesting the network to bind service data flows described by the QoS rule to a dedicated QoS Flow and it is encoded as follows. In the network to UE direction this bit is spare.  Bit  7  0 Segregation not requested  1 Segregation requested  QoS flow identifier (QFI) (bits 6 to 1 of octet m+2) (see NOTE 1)  The QoS flow identifier (QFI) field contains the QoS flow identifier.  Bits  6 5 4 3 2 1  0 0 0 0 0 0 no QoS flow identifier assigned  0 0 0 0 0 1 QFI 1  to  1 1 1 1 1 1 QFI 63  The network shall not set the QFI value to 0.  For the "delete existing QoS rule" operation, the QoS flow identifier value field shall not be included. For the "create new QoS rule" operation, the QoS flow identifier value field shall be included.  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 all 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  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 all 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 m)  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 all 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)  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. |
| NOTE 1: Octet m+2 shall not be included without octet m+1. |

#### 9.11.4.14 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 9.11.4.14.1 and table 9.11.4.14.1.

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 9.11.4.14.1: Session-AMBR information element

Table 9.11.4.14.1: 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. |

#### 9.11.4.15 SM PDU DN request container

The purpose of the SM PDU DN request container information element is to carry a DN-specific identity of the UE in the network access identifier (NAI) format.

The SM PDU DN request container information element is coded as shown in figure 9.11.4.15.1 and table 9.11.4.15.1.

The SM PDU DN request container is a type 4 information element with minimal length of 3 octets and maximum length of 255 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| SM PDU DN request container information IEI | | | | | | | | octet 1 |
| SM PDU DN request container information length | | | | | | | | octet 2 |
| DN-specific identity | | | | | | | | octets 3\*-n\* |

Figure 9.11.4.15.1: SM PDU DN request container information element

Table 9.11.4.15.1: SM PDU DN request container information element

|  |
| --- |
| DN-specific identity (octet 3 to octet n)  A DN-specific identity of the UE in the network access identifier (NAI) format according to IETF RFC 7542 [37], encoded as UTF-8 string. |

#### 9.11.4.16 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 9.11.4.16.1 and table 9.11.4.16.1.

The SSC mode is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| SSC mode IEI | | | | 0  Spare | SSC mode value | | | octet 1 |

Figure 9.11.4.16.1: SSC mode information element

Table 9.11.4.16.1: 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. | | | | | |

#### 9.11.4.17 Re-attempt indicator

The purpose of the Re-attempt indicator information element is to indicate a condition under which the UE is allowed in the current PLMN for the same DNN, to re-attempt a session management procedure (see 3GPP TS 24.301 [15]) corresponding to the 5GS session management procedure which was rejected by the network.

The Re-attempt indicator information element is coded as shown in figure 9.11.4.17.1 and table 9.11.4.17.1.

The Re-attempt indicator is a type 4 information element with a length of 3 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | 3 | 2 | 1 | |  |
| Re-attempt indicator IEI | | | | | | | | | | | | | octet 1 |
| Length of Re-attempt indicator contents | | | | | | | | | | | | | octet 2 |
| 0  Spare | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | EPLMNC | | RATC | octet 3 |

Figure 9.11.4.17.1: Re-attempt indicator

Table 9.11.4.17.1: Re-attempt indicator

|  |  |
| --- | --- |
| RATC (octet 3, bit 1) | |
| Bit | |
| 1 |  | |
| 0 | UE is allowed to re-attempt the procedure in S1 mode |
| 1 | UE is not allowed to re-attempt the procedure in S1 mode |
|  | |
| EPLMNC (octet 3, bit 2) | |
| Bit | |
| 2 |  | |
| 0 | UE is allowed to re-attempt the procedure in an equivalent PLMN |
| 1 | UE is not allowed to re-attempt the procedure in an equivalent PLMN |
|  | |
| Bits 3 to 8 of octet 3 are spare and shall be encoded as zero. | |

#### 9.11.4.18 5GSM network feature support

The purpose of the 5GSM network feature support information element is to indicate whether certain session management related features are supported by the network.

The 5GSM network feature support information element is coded as shown in figure 9.11.4.18.1 and table 9.11.4.18.1.

The 5GSM network feature support 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 |  |
| 5GSM network feature support IEI | | | | | | | | octet 1 |
| Length of 5GSM network feature support contents | | | | | | | | octet 2 |
| 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | EPT-S1 | octet 3 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | octet 4\* -15\* |
| Spare | | | | | | | |

Figure 9.11.4.18.1: 5GSM network feature support information element

Table 9.11.4.18.1: 5GSM network feature support information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5GSM network feature support contents | | | | |
| Ethernet PDN type in S1 mode (IEPT-S1) (octet 3, bit 1) | | | | |
| This bit indicates network's capability for Ethernet PDN type in S1 mode. | | | | |
| 0 |  |  |  | Ethernet PDN type in S1 mode not supported |
| 1 |  |  |  | Ethernet PDN type in 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. | | | | |
|  | | | | |

#### 9.11.4.19 Session-TMBR

The purpose of the Session-TMBR information element is to indicate the initial subscribed PDU session total maximum bit rate when a PDU session is established or to indicate the new subscribed PDU session total maximum bit rate if it is changed by the network.

The Session-TMBR information element is coded as shown in figure 9.11.4.19.1 and table 9.11.4.19.1.

The Session-TMBR is a type 4 information element with a length of 8 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Session-TMBR IEI | | | | | | | | octet 1 |
| Length of Session-TMBR contents | | | | | | | | octet 2 |
| Unit for Session-TMBR for downlink | | | | | | | | octet 3 |
| Session-TMBR for downlink | | | | | | | | octet 4-5 |
| Unit for Session-TMBR for uplink | | | | | | | | octet 6 |
| Session-TMBR for uplink | | | | | | | | octet 7-8 |

Figure 9.11.4.19.1: Session-TMBR information element

Table 9.11.4.19.1: Session-TMBR information element

|  |
| --- |
| Unit for Session-TMBR 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-TMBR 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-TMBR for uplink (octet 6)  The coding is identical to the unit coding defined for Session-TMBR for downlink (octet 3)  Session-TMBR 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. |

#### 9.11.4.20 Serving PLMN rate control

See subclause 9.9.4.28 in 3GPP TS 24.301 [13].

#### 9.11.4.21 5GSM congestion re-attempt indicator

The purpose of the 5GSM congestion re-attempt indicator information element is to indicate whether the back-off timer is applied in the registered PLMN or all PLMNs.

The 5GSM congestion re-attempt indicator information element is coded as shown in figure 9.11.4.21.1 and table 9.11.4.21.1.

The 5GSM congestion re-attempt indicator is a type 4 information element with a length of 3 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | 3 | 2 | 1 | |  |
| 5GSM congestion re-attempt indicator IEI | | | | | | | | | | | | | octet 1 |
| Length of 5GSM congestion re-attempt indicator contents | | | | | | | | | | | | | octet 2 |
| 0  Spare | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | 0  Spare | | ABO | octet 3 |

Figure 9.11.4.21.1: 5GSM congestion re-attempt indicator

Table 9.11.4.21.1: 5GSM congestion re-attempt indicator

|  |  |
| --- | --- |
| ABO (All PLMNs Back-off timer) (octet 3, bit 3) | |
| Bit | |
| 1 |  | |
| 0 | The back-off timer is applied in the registered PLMN. |
| 1 | The back-off timer is applied in all PLMNs. |
|  | |
|  | |
| Bits 2 to 8 of octet 3 are spare and shall be encoded as zero. | |

#### 9.11.4.22 ATSSS container

The purpose of the ATSSS containerinformation element is to transfer parameters associated with ATSSS.

The ATSSS container information element is coded as shown in figure 9.11.4.22.1 and table 9.11.4.22.1.

The ATSSS containeris a type 4 information element with a minimum length of 3 octets and a maximum length of 65538 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| ATSSS container IEI | | | | | | | | octet 1 |
| Length of ATSSS container contents | | | | | | | | octet 2  octet 3 |
| ATSSS container contents | | | | | | | | octet 4  octet x |

Figure 9.11.4.22.1: ATSSS container information element

Table 9.11.4.22.1: ATSSS container information element

|  |
| --- |
| ATSSS container contents are defined in 3GPP TS 24.193 [46]. |

#### 9.11.4.23 Control plane only indication

The purpose of the control plane only indication information element is to indicate that a PDU session is only for control plane CIoT 5GS optimization.

The control plane only indication information element is coded as shown in figure 9.11.4.23.1.

The control plane only indication is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Control plane only indication IEI | | | | 0  Spare | 0  Spare | 0  Spare | CPOI value | octet 1 |

Figure 9.11.4.23.1: Control plane only indication information element

Table 9.11.4.23.1: Control plane only indication information element

|  |  |
| --- | --- |
| Control plane only indication value (CPOI) (octet 1) | |
| Bit | |
| 1 |  |
| 0 | reserved |
| 1 | PDU session can be used for control plane CIoT 5GS optimization only |
|  | |
| The value 0 is reserved. If received, it shall be interpreted as if the control plane only indication IE was not included in the message. | |
| Bits 4 to 2 of octet 1 are spare and shall be all encoded as zero. | |
|  | |

## 9.12 3GPP specific coding information defined within present document

### 9.12.1 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];

- in KAUSF derivation function as specified in 3GPP TS 33.501 [24] annex A; and

- in RES\* and XRES\* derivation function as specified in 3GPP TS 33.501 [24] annex A.

SNN shall contain a UTF-8 string without terminating null characters.

SNN is of maximum length of 1020 octets.

SNN consists of SNN-service-code and SNN-network-identifier, delimited by a colon.

SNN-network-identifier 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 9.12.1.1

Table 9.12.1.1: ABNF syntax of SNN

SNN = SNN-service-code ":" SNN-network-identifier

SNN-service-code = %x35.47 ; "5G"

SNN-network-identifier = 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-service-code 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.