# 8 Message functional definitions and contents

## 8.1 Overview

## 8.2 5GS mobility management messages

### 8.2.1 Authentication request

#### 8.2.1.1 Message definition

The AUTHENTICATION REQUEST message is sent by the AMF to the UE to initiate authentication of the UE identity. See table 8.2.1.1.1.

Message type: AUTHENTICATION REQUEST

Significance: dual

Direction: network to UE

Table 8.2.1.1.1: AUTHENTICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication request message identity | Message type  9.7 | M | V | 1 |
|  | ngKSI | NAS key set identifier  9.10.3.29 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
| 21 | Authentication parameter RAND (5G authentication challenge) | Authentication parameter RAND  9.10.3.13 | O | TV | 17 |
| 20 | Authentication parameter AUTN (5G authentication challenge) | Authentication parameter AUTN  9.10.3.14 | O | TLV | 18 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |

#### 8.2.1.2 Authentication parameter RAND

Authentication parameter RAND IE is included if the AUTHENTICATION REQUEST message is used in a 5G AKA authentication procedure.

#### 8.2.1.3 Authentication parameter AUTN

Authentication parameter AUTN IE is included if the AUTHENTICATION REQUEST message is used in a 5G AKA authentication procedure.

#### 8.2.1.4 EAP message

EAP message IE is included if the AUTHENTICATION REQUEST message is used in an EAP authentication procedure.

### 8.2.2 Authentication response

#### 8.2.2.1 Message definition

The AUTHENTICATION RESPONSE message is sent by the UE to the AMF to deliver a calculated authentication response to the network. See table 8.2.2.1.1.

Message type: AUTHENTICATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.2.1.1: AUTHENTICATION RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication response message identity | Message type  9.7 | M | V | 1 |
| 2D | Authentication response parameter | Authentication response parameter  9.10.3.15 | O | TLV | 6-18 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |

#### 8.2.2.2 Authentication response parameter

This IE is included if the message is sent in a 5G AKA based primary authentication and key agreement procedure.

#### 8.2.2.3 EAP message

EAP message IE is included if the EAP message received in a related AUTHENTICATION REQUEST message was an EAP-request.

### 8.2.3 Authentication result

#### 8.2.3.1 Message definition

The AUTHENTICATION RESULT message is sent by the AMF to the UE to provide result of EAP authentication of the UE identity. See table 8.2.3.1.1.

Message type: AUTHENTICATION RESULT

Significance: dual

Direction: network to UE

Table 8.2.3.1.1: AUTHENTICATION RESULT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication result message identity | Message type  9.7 | M | V | 1 |
|  | ngKSI | NAS key set identifier  9.10.3.29 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | EAP message | EAP message  9.10.2.2 | M | LV-E | 6-1502 |

### 8.2.4 Authentication failure

#### 8.2.4.1 Message definition

The AUTHENTICATION FAILURE message is sent by the UE to the AMF to indicate that authentication of the network has failed. See table 8.2.4.1.1.

Message type: AUTHENTICATION FAILURE

Significance: dual

Direction: UE to network

Table 8.2.4.1.1: AUTHENTICATION FAILURE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication failure message identity | Message type  9.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.10.3.2 | M | V | 1 |
| 30 | Authentication failure parameter | Authentication failure parameter  9.10.3.12 | O | TLV | 16 |

#### 8.2.4.2 Authentication failure parameter

This IE shall be included in a 5G AKA based primary authentication and key agreement procedure if and only if the 5GMM cause was #21 "synch failure". It shall include the response to the authentication challenge from the USIM, which is made up of the AUTS parameter (see 3GPP TS 33.501 [24]).

### 8.2.5 Authentication reject

#### 8.2.5.1 Message definition

The AUTHENTICATION REJECT message is sent by the AMF to the UE to indicate that the authentication procedure has failed and that the UE shall abort all activities. See table 8.2.5.1.1.

Message type: AUTHENTICATION REJECT

Significance: dual

Direction: network to UE

Table 8.2.5.1.1: AUTHENTICATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication reject message identity | Message type  9.7 | M | V | 1 |

### 8.2.6 Registration request

#### 8.2.6.1 Message definition

The REGISTRATION REQUEST message is sent by the UE to the AMF. See table 8.2.6.1.1.

Message type: REGISTRATION REQUEST

Significance: dual

Direction: UE to network

Table 8.2.6.1.1: REGISTRATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended Protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Registration request message identity | Message type  9.7 | M | V | 1 |
|  | 5GS registration type | 5GS registration type  9.10.3.7 | M | LV | 2 |
|  | ngKSI | NAS key set identifier  9.10.3.29 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | 5GS mobile identity | 5GS mobile identity  9.10.3.4 | M | LV | 5-TBD |
| C- | Non-current native NAS key set identifier | NAS key set identifier  9.10.3.29 | O | TV | 1 |
| 10 | 5GMM capability | 5GMM capability  9.10.3.1 | O | TLV | 3-15 |
| 2E | UE security capability | UE security capability  9.10.3.49 | O | TLV | 4-6 |
| 2F | Requested NSSAI | NSSAI  9.10.3.34 | O | TLV | 4-74 |
| 52 | Last visited registered TAI | 5GS tracking area identity  9.10.3.8 | O | TV | 7 |
| 65 | S1 UE network capability | S1 UE network capability  9.10.3.44 | O | TLV | 4-15 |
| 40 | Uplink data status | Uplink data status  9.10.2.53 | O | TLV | 4-34 |
| 50 | PDU session status | PDU session status  9.10.3.40 | O | TLV | 4-34 |
| B- | MICO indication | MICO indication  9.10.3.28 | O | TV | 1 |
| 2B | UE status | UE status  9.10.3.52 | O | TLV | 3 |
| 2C | Additional GUTI | 5GS mobile identity  9.10.3.4 | O | TLV | TBD |
| 25 | Allowed PDU session status | Allowed PDU session status  9.10.3.11 | O | TLV | 4-34 |
| 60 | UE's usage setting | UE's usage setting  9.10.3.51 | O | TLV | 3 |
| TBD | Requested DRX parameters | DRX parameters  9.10.3.20 | O | TBD | TBD |
| 7C | EPS NAS message container | EPS NAS message container  9.10.3.22 | O | TLV-E | TBD |
| 77 | Payload container | Payload container  9.10.3.35 | O | TLV-E | 4-65538 |

Editor's note: The content of the REGISTRATION REQUEST message when a limited set of IEs including those needed to establish security in the initial message when it has no NAS security context is FFS.

#### 8.2.6.2 Non-current native NAS key set identifier

The UE shall include this IE if the UE has a valid non-current native 5G NAS security context when the UE performs a inter-system change from S1 mode to N1 mode in 5GMM-CONNECTED mode and the UE uses a mapped 5G NAS security context to protect the REGISTRATION REQUEST message.

#### 8.2.6.3 5GMM capability

The UE shall include this IE, unless the UE performs a periodic registration updating procedure.

#### 8.2.6.4 UE security capability

The UE shall include this IE, unless the UE performs a periodic registration updating procedure.

#### 8.2.6.5 Requested NSSAI

This IE shall be included by the UE when performing the registration procedure if:

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

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

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

#### 8.2.6.6 Last visited registered TAI

This IE shall be included if the UE holds a valid last visited registered TAI.

#### 8.2.6.7 S1 UE network capability

A UE supporting S1 mode shall include this IE, unless the UE performs a periodic registration updating procedure.

#### 8.2.6.8 Uplink data status

This IE shall be included if the UE has uplink user data pending to be sent.

#### 8.2.6.9 PDU session status

This IE shall be included if the UE wants to indicate the PDU sessions associated with the access type the message is sent over that are active within the UE.

#### 8.2.6.10 MICO indication

The UE may include this IE to request the use of MICO mode.

#### 8.2.6.11 UE status

This IE shall be included if the UE in single-registration mode performs the registration procedure due to inter-system change from S1 mode to N1 mode or if the UE in dual-registration mode and EMM state EMM-REGISTERED performs initial registration.

#### 8.2.6.12 Additional GUTI

This IE shall be included if the UE performs the registration procedure due to inter-system change from S1 mode to N1 mode, the UE operates in single-registration mode and the UE has a 5G-GUTI.

#### 8.2.6.13 Allowed PDU session status

This IE shall be included if the REGISTRATION REQUEST message is sent as a response to paging with the access type indicating non-3GPP access and the UE wants to indicate the user-plane resources of PDU session(s) associated with non-3GPP access allowed to be re-established over 3GPP access.

#### 8.2.6.14 UE's usage setting

This IE shall be included if the UE is configured to support IMS voice.

#### 8.2.6.15 Requested DRX parameters

If the UE wants to use or change the UE specific DRX parameters, the UE shall include the Requested DRX parameters IE in the REGISTRATION REQUEST message.

#### 8.2.6.16 EPS NAS message container

The UE operating in the single-registration mode shall include this information element if the UE performs mobility from S1 mode to N1 mode. The content of this message container is the complete integrity protected TRACKING AREA UPATE REQUEST message, using EPS NAS security context.

#### 8.2.6.17 Allowed PDU session status

This IE shall be included if the REGISTRATION REQUEST message is sent as a response to paging with the access type indicating non-3GPP access and the UE wants to indicate the user-plane resources of PDU session(s) associated with non-3GPP access allowed to be re-established over 3GPP access.

#### 8.2.6.18 Payload container

This IE shall be included if the UE has one or more stored UE policy sections for the registration procedure for mobility and periodic registration update due to inter-system change from S1 mode to N1 mode of a UE operating in the single-registration mode or for the registration procedure for initial registration.

### 8.2.7 Registration accept

#### 8.2.7.1 Message definition

The REGISTRATION ACCEPT message is sent by the AMF to the UE. See table 8.2.7.1.1.

Message type: REGISTRATION ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.7.1.1: REGISTRATION ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Registration accept message identity | Message type  9.7 | M | V | 1 |
|  | 5GS registration result | 5GS registration result  9.10.3.6 | M | LV | 2 |
| 2C | 5G-GUTI | 5GS mobile identity  9.10.3.4 | O | TLV | 13 |
| 4A | Equivalent PLMNs | PLMN list  9.10.3.41 | O | TLV | 5-47 |
| 54 | TAI list | 5GS tracking area identity list  9.10.3.9 | O | TLV | 9-114 |
| 70 | Allowed NSSAI | NSSAI  9.10.3.34 | O | TLV | 4-74 |
| 11 | Rejected NSSAI | Rejected NSSAI  9.10.3.42 | O | TLV | 4-42 |
| 31 | Configured NSSAI | NSSAI  9.10.3.34 | O | TLV | 4-146 |
| 64 | 5GS network feature support | 5GS network feature support  9.10.3.5 | O | TLV | 3-5 |
| 50 | PDU session status | PDU session status  9.10.3.40 | O | TLV | 4-34 |
| 26 | PDU session reactivation result | PDU session reactivation result  9.10.3.38 | O | TLV | 4-32 |
| 7E | PDU session reactivation result error cause | PDU session reactivation result error cause  9.10.3.39 | O | TLV-E | 5-515 |
| 79 | LADN information | LADN information  9.10.3.27 | O | TLV-E | 12-1707 |
| B- | MICO indication | MICO indication  9.10.3.28 | O | TV | 1 |
| 27 | Service area list | Service area list  9.10.3.45 | O | TLV | 6-114 |
| 5E | T3512 value | GPRS timer 3  9.10.2.5 | O | TLV | 3 |
| 5D | Non-3GPP de-registration timer value | GPRS timer 2  9.10.2.4 | O | TLV | 3 |
| 16 | T3502 value | GPRS timer 2  9.10.2.4 | O | TLV | 3 |
| 34 | Emergency number list | Emergency number list  9.10.3.21 | O | TLV | 5-50 |
| 35 | Extended emergency number list | Extended emergency number list  9.10.3.24 | O | TLV | TBD |
| TBD | Transparent container | Transparent container  9.10.3.49 | O | TBD | TBD |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |

#### 8.2.7.2 5G-GUTI

This IE may be included to assign a 5G-GUTI to a UE.

#### 8.2.7.3 Equivalent PLMNs

This IE may be included in order to assign a new equivalent PLMNs list to a UE.

#### 8.2.7.4 TAI list

This IE may be included to assign a TAI list to a UE.

#### 8.2.7.5 Allowed NSSAI

This IE shall be included:

a) if the network allows one or more S-NSSAIs received in the requested NSSAI of the REGISTRATION REQUEST message; or

b) if the requested NSSAI was not included in the REGISTRATION REQUEST message or none of the requested NSSAI are present in the subscribed S-NSSAIs and the network has one or more subscribed S-NSSAIs marked as default that are available.

#### 8.2.7.6 Rejected NSSAI

The network may include this IE to inform the UE of the S-NSSAIs that were included in the requested NSSAI in the REGISTRATION REQUEST message but were rejected by the network.

#### 8.2.7.7 Configured NSSAI

The network may include this IE if the network needs to provide the UE with a new configured NSSAI for the current PLMN.

#### 8.2.7.8 5GS network feature support

The network may include this IE to inform the UE of the support of certain features. If this IE is not included then the UE shall interpret this as a receipt of an information element with all bits of the value part coded as zero.

#### 8.2.7.9 PDU session status

This IE shall be included if the network wants to indicate the PDU sessions associated with the access type the message is sent over that are active in the network.

#### 8.2.7.10 PDU session reactivation result

This IE shall be included:

- if the Uplink data status IE is included in the REGISTRATION REQUEST message;

- if the Allowed PDU session status IE is included in the REGISTRATION REQUEST message and there is at least one PDU session indicated in the Allowed PDU session status IE that can be reactivated over 3GPP access.

#### 8.2.7.11 PDU session reactivation result error cause

This IE may be included, if the PDU session reactivation result IE is included and there exist one or more PDU sessions for which the user-plane resources cannot be re-established, to indicate the cause of failure to re-establish the user-plane resources

#### 8.2.7.12 LADN information

The network shall include this IE if there are valid LADN service area(s) for the subscribed DNN(s) of the UE in the current registration area.

#### 8.2.7.13 MICO indication

The network shall include the MICO indication IE if:

a)- the UE included the MICO indication IE in the REGISTRATION REQUEST message; and

b) the network supports and accepts the use of MICO mode.

#### 8.2.7.14 Service area list

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

#### 8.2.7.15 T3512 value

The AMF shall include this IE during the initial registration procedure over 3GPP access. The AMF may include this IE during the mobility and periodic registration update procedure over 3GPP access.

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

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

#### 8.2.7.17 T3502 value

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

#### 8.2.7.18 Emergency number list

This IE may be sent by the network. If this IE is sent, the contents of this IE indicates a list of emergency numbers valid within the same country as in the cell on which this IE is received.

#### 8.2.7.19 Extended emergency number list

This IE may be sent by the network. If this IE is sent, the contents of this IE indicates a list of emergency numbers (with URN information) valid within the same country as in the cell on which this IE is received.

#### 8.2.7.20 Transparent container

This IE may be sent by the network. If this IE is sent, the contents of this IE includes the list of preferred PLMN/access technology combinations (or HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided') (see 3GPP TS 23.122 [5] annex C) and optional acknowledgement request.

#### 8.2.7.21 EAP message

EAP message IE is included if the REGISTRATION ACCEPT message is sent as part of registration for emergency services and is used to convey EAP-failure message.

### 8.2.8 Registration complete

#### 8.2.8.1 Message definition

The REGISTRATION COMPLETE message is sent by the UE to the AMF. See table 8.2.8.1.1.

Message type: REGISTRATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.8.1.1: REGISTRATION COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Registration complete message identity | Message type  9.6 | M | V | 1 |
| TBD | Transparent container | Transparent container  9.10.3.49 | O | TBD | TBD |

#### 8.2.8.2 Transparent container

This IE may be sent by the UE. If this IE is sent, the contents of this IE indicates the UE acknowledgement of successful reception of the transparent container IE in the REGISTRATION ACCEPT message.

### 8.2.9 Registration reject

#### 8.2.9.1 Message definition

The REGISTRATION REJECT message is sent by the AMF to the UE. See table 8.2.9.1.1.

Message type: REGISTRATION REJECT

Significance: dual

Direction: network to UE

Table 8.2.9.1.1: REGISTRATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Registration reject message identity | Message type  9.6 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.10.3.2 | M | V | 1 |
| 5F | T3346 value | GPRS timer 2  9.10.2.4 | O | TLV | 3 |
| 16 | T3502 value | GPRS timer 2  9.10.2.4 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |

#### 8.2.9.2 T3346 value

The AMF may include this IE when the general NAS level mobility management congestion control is active

#### 8.2.9.3 T3502 value

This IE may be included to indicate a value for timer T3502 during the initial registration.

#### 8.2.9.4 EAP message

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

### 8.2.10 UL NAS transport

#### 8.2.10.1 Message definition

The UL NAS TRANSPORT message transports message payload and associated information to the AMF. See table 8.2.10.1.1.

Message type: UL NAS TRANSPORT

Significance: dual

Direction: UE to network

Table 8.2.10.1.1: UL NAS TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | UL NAS TRANSPORT message identity | Message type  9.7 | M | V | 1 |
|  | Payload container type | Payload container type  9.10.3.36 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Payload container | Payload container  9.10.3.35 | M | LV-E | 3-65537 |
| 70 | PDU session ID | PDU session identity 2  9.10.3.37 | C | TV | 2 |
| 61 | Old PDU session ID | PDU session identity 2  9.10.3.37 | O | TV | 2 |
| 8- | Request type | Request type  9.10.3.43 | O | TV | 1 |
| 22 | S-NSSAI | S-NSSAI  9.10.2.6 | O | TLV | 3-10 |
| 25 | DNN | DNN  9.10.3.19 | O | TLV | 3-102 |
| 24 | Additional information | Additional information  9.10.2.1 | O | TLV | 3-n |

#### 8.2.10.2 PDU session ID

The UE shall include this IE when the Payload container type IE is set to "N1 SM information".

#### 8.2.10.3 Old PDU session ID

The UE shall include this IE if the UL NAS TRANSPORT message transports a PDU SESSION ESTABLISHMENT REQUEST message upon receiving the PDU SESSION MODIFICATION COMMAND message with the 5GSM cause IE set to #39 "reactivation requested".

#### 8.2.10.4 Request type

The UE shall include this IE when the PDU session ID IE is included and the Payload container IE contains the PDU SESSION ESTABLISHMENT REQUEST message.

#### 8.2.10.5 S-NSSAI

The UE may include this IE when the Request type IE is set to "initial request".

#### 8.2.10.6 DNN

The UE may include this IE when the Request type IE is set to "initial request".

#### 8.2.10.7 Additional information

The UE may include this IE when the Payload container type IE is set to "LTE Positioning Protocol (LPP) message container".

### 8.2.11 DL NAS transport

#### 8.2.11.1 Message definition

The DL NAS TRANSPORT message transports message payload and associated information to the UE. See table 8.2.11.1.1.

Message type: DL NAS TRANSPORT

Significance: dual

Direction: network to UE

Table 8.2.11.1.1: DL NAS TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | DL NAS TRANSPORT message identity | Message type  9.7 | M | V | 1 |
|  | Payload container type | Payload container type  9.10.3.36 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Payload container | Payload container  9.10.3.35 | M | LV-E | 3-65537 |
| 70 | PDU session ID | PDU session identity 2  9.10.3.37 | C | TV | 2 |
| 24 | Additional information | Additional information  9.10.2.1 | O | TLV | 3-n |
| 58 | 5GMM cause | 5GMM cause  9.10.3.2 | O | TV | 2 |
| 37 | Back-off timer value | GPRS timer 3  9.10.2.5 | O | TLV | 3 |

#### 8.2.11.2 PDU session ID

The AMF shall include this IE when the Payload container type IE is set to "N1 SM information".

#### 8.2.11.3 Additional information

The AMF may include this IE when the Payload container type IE is set to "LTE Positioning Protocol (LPP) message container".

#### 8.2.11.4 5GMM cause

The AMF shall include this IE when the Payload container IE contains an uplink payload which was not forwarded.

#### 8.2.11.5 Back-off timer value

The AMF shall include this IE when the Payload container IE contains an uplink 5GSM message which was not forwarded due to DNN based congestion control, S-NSSAI and DNN based congestion control or S-NSSAI only based congestion control.

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

#### 8.2.12.1 Message definition

The DEREGISTRATION REQUEST message is sent by the UE to the AMF. See table 8.2.12.1.1.

Message type: DEREGISTRATION REQUEST

Significance: dual

Direction: UE to network

Table 8.2.12.1.1: DEREGISTRATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | De-registration request message identity | Message type  9.7 | M | V | 1 |
|  | De-registration type | De-registration type  9.10.3.18 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | 5GS mobile identity | 5GS mobile identity  9.10.3.4 | M | TLV | TBD |

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

#### 8.2.13.1 Message definition

The DEREGISTRATION ACCEPT message is sent by the AMF to the UE. See table 8.2.13.1.1.

Message type: DEREGISTRATION ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.13.1.1: DEREGISTRATION ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | De-registration accept message identity | Message type  9.7 | M | V | 1 |

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

#### 8.2.14.1 Message definition

The DEREGISTRATION REQUEST message is sent by the AMF to the UE. See table 8.2.14.1.1.

Message type: DEREGISTRATION REQUEST

Significance: dual

Direction: network to UE

Table 8.2.14.1.1: DEREGISTRATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | De-registration request message identity | Message type  9.7 | M | V | 1 |
|  | De-registration type | De-registration type  9.10.3.18 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
| 58 | 5GMM cause | 5GMM cause  9.10.3.2 | O | TV | 2 |
| 5F | T3346 value | GPRS timer 2  9.10.2.4 | O | TLV | 3 |

#### 8.2.14.2 5GMM cause

This information element is included if a 5GMM cause is provided.

#### 8.2.14.3 T3346 value

The AMF may include this IE when the general NAS level mobility management congestion control is active.

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

#### 8.2.15.1 Message definition

The DEREGISTRATION ACCEPT message is sent by the UE to the AMF. See table 8.2.15.1.1.

Message type: DEREGISTRATION ACCEPT

Significance: dual

Direction: UE to network

Table 8.2.15.1.1.1: DEREGISTRATION ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | De-registration accept message identity | Message type  9.7 | M | V | 1 |

### 8.2.16 Service request

#### 8.2.16.1 Message definition

The SERVICE REQUEST message is sent by the UE to the AMF in order to request the establishment of an N1 NAS signalling connection and/or to request the establishment of user-plane resources for PDU sessions which are activated without user-plane resources. See table 8.2.16.1.1.

Message type: SERVICE REQUEST

Significance: dual

Direction: UE to network

Table 8.2.16.1.1: SERVICE REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Service request message identity | Message type  9.7 | M | V | 1 |
|  | ngKSI | NAS key set identifier  9.10.3.29 | M | V | 1/2 |
|  | Service type | Service type  9.10.3.46 | M | V | 1/2 |
|  | 5G-S-TMSI | 5GS mobile identity  9.10.3.4 | M | LV | 6 |
| 40 | Uplink data status | Uplink data status  9.10.3.53 | O | TLV | 4-34 |
| 50 | PDU session status | PDU session status  9.10.3.40 | O | TLV | 4-34 |
| 25 | Allowed PDU session status | Allowed PDU session status  9.10.3.11 | O | TLV | 4-34 |

#### 8.2.16.2 Uplink data status

This IE shall be included if the UE has uplink user data pending to be sent.

#### 8.2.16.3 PDU session status

This IE shall be included if the UE wants to indicate the PDU sessions associated with the access type the message is sent over that are active within the UE.

#### 8.2.16.4 Allowed PDU session status

This IE shall be included if the SERVICE REQUEST message is sent as a response to paging or notification via 3GPP access for PDU session(s) associated with non-3GPP access and the UE wants to indicate the user-plane resources of PDU session(s) associated with non-3GPP access allowed to be re-established over 3GPP access or if there is no PDU session(s) for which the UE allows the user-plane resources to be re-established over 3GPP access.

### 8.2.17 Service accept

#### 8.2.17.1 Message definition

The SERVICE ACCEPT message is sent by the AMF to the UE in order to accept the service request procedure. See table 8.2.17.1.1.

Message type: SERVICE ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.17.1.1: SERVICE ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Service accept message identity | Message type  9.7 | M | V | 1 |
| 50 | PDU session status | PDU session status  9.10.3.40 | O | TLV | 4-34 |
| 26 | PDU session reactivation result | PDU session reactivation result  9.10.3.38 | O | TLV | 4-32 |
| 7E | PDU session reactivation result error cause | PDU session reactivation result error cause  9.10.3.39 | O | TLV-E | 5-515 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |

#### 8.2.17.2 PDU session status

This IE shall be included if the network wants to indicate the PDU sessions associated with the access type the message is sent over that are active within the network.

#### 8.2.17.3 PDU session reactivation result

This IE shall be included:

- if the Uplink data status IE is included in the SERVICE REQUEST message;

- if the Allowed PDU session status IE is included in the SERVICE REQUEST message and there is at least one PDU session indicated in the Allowed PDU session status IE that can be reactivated over 3GPP access.

#### 8.2.17.4 PDU session reactivation result error cause

This IE may be included if the PDU session reactivation result IE is included and there exist one or more PDU sessions for which the user-plane resources cannot be re-established, to indicate the cause of failure to re-establish the user-plane resources.

#### 8.2.17.5 EAP message

EAP message IE is included if the SERVICE ACCEPT message is sent to a UE registered for emergency services and is used to convey EAP-failure message.

### 8.2.18 Service reject

#### 8.2.18.1 Message definition

The SERVICE REJECT message is sent by the AMF to the UE in order to reject the service request procedure. See table 8.2.18.1.1.

Message type: SERVICE REJECT

Significance: dual

Direction: network to UE

Table 8.2.18.1.1: SERVICE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Service reject message identity | Message type  9.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.10.3.2 | M | V | 1 |
| 50 | PDU session status | PDU session status  9.10.3.40 | O | TLV | 4-34 |
| 5F | T3346 value | GPRS timer 2  9.10.24 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |

#### 8.2.18.2 PDU session status

This IE shall be included if the network wants to indicate the PDU sessions associated with the access type the message is sent over that are active within the network.

#### 8.2.18.3 T3346 value

The AMF may include this IE when the general NAS level mobility management congestion control is active.

#### 8.2.18.4 EAP message

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

### 8.2.19 Configuration update command

#### 8.2.19.1 Message definition

The CONFIGURATION UPDATE COMMAND message is sent by the AMF to the UE. See table 8.2.19.1.1.

Message type: CONFIGURATION UPDATE COMMAND

Significance: dual

Direction: network to UE

Table 8.2.19.1.1: CONFIGURATION UPDATE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Configuration update command message identity | Message type  9.7 | M | V | 1 |
| D- | Configuration update indication | Configuration update indication  9.10.3.16 | O | TV | 1 |
| 2C | 5G-GUTI | 5GS mobile identity  9.10.3.4 | O | TLV | 13 |
| 54 | TAI list | 5GS tracking area identity list  9.10.3.9 | O | TLV | 9-114 |
| 70 | Allowed NSSAI | NSSAI  9.10.3.34 | O | TLV | 4-74 |
| 27 | Service area list | Service area list  9.10.3.45 | O | TLV | 6-114 |
| 43 | Full name for network | Network name  9.10.3.33 | O | TLV | 3-n |
| 45 | Short name for network | Network name  9.10.3.33 | O | TLV | 3-n |
| 46 | Local time zone | Time zone  9.10.3.47 | O | TV | 2 |
| 47 | Universal time and local time zone | Time zone and time  9.10.3.48 | O | TV | 8 |
| 49 | Network daylight saving time | Daylight saving time  9.10.3.17 | O | TLV | 3 |
| 79 | LADN information | LADN information  9.10.3.27 | O | TLV-E | 3-1707 |
| B- | MICO indication | MICO indication  9.10.3.28 | O | TV | 1 |
| 31 | Configured NSSAI | NSSAI  9.10.3.34 | O | TLV | 4-146 |
| 11 | Rejected NSSAI | Rejected NSSAI  9.10.3.42 | O | TLV | 4-42 |

#### 8.2.19.2 Configuration update indication

The AMF shall include this IE if the AMF wants to request an acknowledgement or a registration procedure from the UE.

#### 8.2.19.3 5G-GUTI

This IE may be included to assign a new 5G GUTI to the UE.

#### 8.2.19.4 TAI list

This IE may be included to assign a new TAI list to the UE.

#### 8.2.19.5 Allowed NSSAI

This IE may be included to assign a new allowed NSSAI to the UE.

#### 8.2.19.6 Service area list

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

#### 8.2.19.7 Full name for network

This IE may be included to assign a new full name for network to the UE.

#### 8.2.19.8 Short name for network

This IE may be included to assign a new short name for network to the UE.

#### 8.2.19.9 Local time zone

This IE may be included to assign a new local time zone to the UE.

#### 8.2.19.10 Universal time and local time zone

This IE may be included to assign new universal time and local time zone to the UE.

#### 8.2.19.11 Network daylight saving time

This IE may be included to assign new network daylight saving time to the UE.

#### 8.2.19.12 LADN information

This IE may be included to assign new LADN information to the UE or delete the LADN information at the UE side.

#### 8.2.19.13 MICO indication

This IE may be included to assign a new MICO indication to the UE.

#### 8.2.19.14 Configured NSSAI

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

#### 8.2.19.15 Rejected NSSAI

The network may include this IE to inform the UE of the S-NSSAIs that were previously sent to the UE in the allowed NSSAI, but are now rejected by the network.

### 8.2.20 Configuration update complete

#### 8.2.20.1 Message definition

The CONFIGURATION UPDATE COMPLETE message is sent by the UE to the AMF. See table 8.2.20.1.1.

Message type: CONFIGURATION UPDATE COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.20.1.1: CONFIGURATION UPDATE COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Configuration update complete message identity | Message type  9.7 | M | V | 1 |

### 8.2.21 Identity request

#### 8.2.21.1 Message definition

The IDENTITY REQUEST message is sent by the AMF to the UE to request the UE to provide specified identity. See table 8.2.21.1.1

Message type: IDENTITY REQUEST

Significance: dual

Direction: AMF to UE

Table 8.2.21.1.1: IDENTITY REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Identity request message identity | Message type  9.7 | M | V | 1 |
|  | Identity type | 5GS identity type  9.10.3.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |

### 8.2.22 Identity response

#### 8.2.22.1 Message definition

The IDENTITY RESPONSE message is sent by the UE to the AMF to provide the requested identity. See table 8.2.22.1.

Message type: IDENTITY RESPONSE

Significance: dual

Direction: UE to AMF

Table 8.2.22.1.1: IDENTITY RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Identity response message identity | Message type  9.7 | M | V | 1 |
|  | Mobile identity | 5GS mobile identity  9.10.3.4 | M | LV | 2-TBD |

### 8.2.23 Notification

#### 8.2.23.1 Message definition

The NOTIFICATION message is sent by the AMF to the UE to notify the UE to initiate a service request procedure. See table 8.2.23.1.1.

Message type: NOTIFICATION

Significance: dual

Direction: network to UE

Table 8.2.23.1.1: NOTIFICATION message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Notification message identity | Message type  9.7 | M | V | 1 |
|  | Access type | Access type  9.10.3.10 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |

### 8.2.24 Notification response

#### 8.2.24.1 Message definition

The NOTIFICATION RESPONSE message is sent by the UE to the AMF to notify the failure to initiate the service request procedure as a response of notification. See table 8.2.24.1.1.

Message type: NOTIFICATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.2341.1: NOTIFICATION RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Notification response message identity | Message type  9.7 | M | V | 1 |
| 50 | PDU session status | PDU session status  9.10.3.40 | O | TLV | 4-34 |

#### 8.2.24.2 PDU session status

This information element shall be included if the UE wants to indicate over non-3GPP access type the PDU sessions associated with the 3GPP access type that are active within the UE.

### 8.2.25 Security mode command

#### 8.2.25.1 Message definition

The SECURITY MODE COMMAND message is sent by the AMF to the UE to establish NAS signalling security. See table 8.2.25.1.1.

Message type: SECURITY MODE COMMAND

Significance: dual

Direction: network to UE

Table 8.2.25.1.1: SECURITY MODE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Security mode command message identity | Message type  9.7 | M | V | 1 |
|  | Selected NAS security algorithms | NAS security algorithms  9.10.3.32 | M | V | 1 |
|  | ngKSI | NAS key set identifier  9.10.3.29 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Replayed UE security capabilities | UE security capability  9.10.3.50 | M | LV | 3-5 |
| E- | IMEISV request | IMEISV request  9.10.3.26 | O | TV | 1 |
| 4F | HashAMF | HashAMF  9.10.3.25 | O | TV | 9 |
| 57 | Selected EPS NAS security algorithms | EPS NAS security algorithms  9.10.3.23 | O | TV | 2 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7 |

#### 8.2.25.2 IMEISV request

The AMF may include this information element to request the UE to send its IMEISV with the corresponding SECURITY MODE COMPLETE message.

#### 8.2.25.3 HashAMF

The AMF shall include this information element when the AMF is initiating a SECURITY MODE COMMAND during a registration procedure and the REGISTRATION REQUEST message did not successfully pass the integrity check at the AMF.

#### 8.2.25.4 Selected EPS NAS security algorithms

This IE shall be included if the AMF does not support interworking procedures without N26 interface and the UE set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message.

#### 8.2.25.5 EAP message

This IE is included when the EAP Success message is sent as part of the EAP-based primary authentication and key agreement procedure, as specified in subclause 5.4.1.2.

### 8.2.26 Security mode complete

#### 8.2.26.1 Message definition

The SECURITY MODE COMPLETE message is sent by the UE to the AMF in response to a SECURITY MODE COMMAND message. See table 8.2.26.1.1.

Message type: SECURITY MODE COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.26.1.1: SECURITY MODE COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Security mode complete message identity | Message type  9.6 | M | V | 1 |
| 2C | IMEISV | 5G mobile identity  9.10.3.4 | O | TLV | 11 |
| 7D | NAS message container | NAS message container  9.10.3.31 | O | TLV-E | 3-n |

#### 8.2.26.2 IMEISV

The UE shall include this information element, if the IMEISV was requested within the corresponding SECURITY MODE COMMAND message.

#### 8.2.26.3 NAS message container

The UE shall include this information element:

a) if during an ongoing registration procedure, the AMF included HASHAMF in the SECURITY MODE COMMAND message and HASHAMF has a different value from the hash value locally calculated at the UE as described in 3GPP TS 33.501 [24]; and

b) when the UE has sent an initial NAS message with a limited set of IEs before the SECURITY MODE COMMAND message was received and the UE needs to include the complete initial NAS message in the SECURITY MODE COMPLETE message, as described in 3GPP TS 33.501 [24].

### 8.2.27 Security mode reject

#### 8.6.27.1 Message definition

The SECURITY MODE REJECT message is sent by the UE to the AMF to indicate that the corresponding security mode command has been rejected. See table 8.2.27.1.1.

Message type: SECURITY MODE REJECT

Significance: dual

Direction: UE to network

Table 8.2.27.1.1: SECURITY MODE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Security mode reject message identity | Message type  9.6 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.10.3.2 | M | V | 1 |

### 8.2.28 Security protected 5GS NAS message

#### 8.2.28.1 Message definition

This message is sent by the UE or the network to transfer a NAS message together with the sequence number and the message authentication code protecting the message. See table 8.2.28.1.1.

Message type: SECURITY PROTECTED 5GS NAS MESSAGE

Significance: dual

Direction: both

Table 8.2.28.1.1: SECURITY PROTECTED 5GS NAS MESSAGE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.4 | M | V | 1/2 |
|  | Message authentication code | Message authentication code  9.8 | M | V | 4 |
|  | Sequence number | Sequence number  9.9 | M | V | 1 |
|  | NAS message | NAS message  9.10.3.30 | M | V | 3-n |

### 8.2.29 5GMM status

#### 8.2.29.1 Message definition

The 5GMM STATUS message is sent by the UE or by the AMF at any time to report certain error conditions. See table 8.2.28.1.1.

Message type: 5GMM STATUS

Significance: local

Direction: both

Table 8.2.29.1.1: 5GMM STATUS message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | 5GMM STATUS message identity | Message type  9.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.10.3.2 | M | V | 2 |

## 8.3 5GS session management messages

### 8.3.1 PDU session establishment request

#### 8.3.1.1 Message definition

The PDU SESSION ESTABLISHMENT REQUEST message is sent by the UE to the SMF to initiate establishment of a PDU session. See table 8.3.1.1.1.

Message type: PDU SESSION ESTABLISHMENT REQUEST

Significance: dual

Direction: UE to network

Table 8.3.1.1.1: PDU SESSION ESTABLISHMENT REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION ESTABLISHMENT REQUEST message identity | Message type  9.7 | M | V | 1 |
| 9- | PDU session type | PDU session type  9.10.4.8 | O | TV | 1 |
| A- | SSC mode | SSC mode  9.10.4.12 | O | TV | 1 |
| 28 | 5GSM capability | 5GSM capability  9.10.4.1 | O | TLV | 3-15 |
| 55 | Maximum number of supported packet filters | Maximum number of supported packet filters  9.10.4.6 | O | TV | 3 |
| TBD | SM PDU DN request container | SM PDU DN request container  9.10.4.11 | O | TBD | TBD |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.1.2 PDU session type

This IE is included in the message when the UE requests to establish a new PDU session with a DN and requests a PDU session type.

#### 8.3.1.3 SSC mode

This IE is included in the message when the UE requests to establish a new PDU session with a DN and requests an SSC mode.

#### 8.3.1.4 Maximum number of supported packet filters

This IE shall be included in the message when the selected PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet" and the UE can support more than 16 packet filters for this PDU session.

#### 8.3.1.5 5GSM capability

This IE is included in the message when the UE requests to establish a new PDU session of "IPv4", "IPv6", "IPv4v6" or "Ethernet" PDU session type and the UE supports Reflective QoS, or establish a new PDU session of "IPv6" or "IPv4v6" PDU session type and the UE supports acting as a type C host as specified in IETF RFC 4191 [36].

#### 8.3.1.6 SM PDU DN request container

This IE is included in the message when the UE requests to establish a new PDU session with a DN and needs to provide information for the PDU session authentication and authorization by the external DN.

#### 8.3.1.7 Extended protocol configuration options

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

### 8.3.2 PDU session establishment accept

#### 8.3.2.1 Message definition

The PDU SESSION ESTABLISHMENT ACCEPT message is sent by the SMF to the UE in response to PDU SESSION ESTABLISHMENT REQUEST message and indicates successful establishment of a PDU session. See table 8.3.2.1.1.

Message type: PDU SESSION ESTABLISHMENT ACCEPT

Significance: dual

Direction: network to UE

Table 8.3.2.1.1: PDU SESSION ESTABLISHMENT ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION ESTABLISHMENT ACCEPT message identity | Message type  9.7 | M | V | 1 |
|  | Selected PDU session type | PDU session type  9.10.4.8 | M | V | 1/2 |
|  | Selected SSC mode | SSC mode  9.10.4.12 | M | V | 1/2 |
|  | DNN | DNN  9.10.3.19 | M | LV | 2-TBD |
|  | Authorized QoS rules | QoS rules  9.10.4.9 | M | LV-E | 7-65538 |
|  | Session AMBR | Session-AMBR  9.10.4.10 | M | LV | TBD |
| 59 | 5GSM cause | 5GSM cause  9.10.4.2 | O | TV | 2 |
| 29 | PDU address | PDU address  9.10.4.7 | O | TLV | 7, 11 or 15 |
| 56 | RQ timer value | GPRS timer  9.10.2.3 | O | TV | 2 |
| 22 | S-NSSAI | S-NSSAI  9.10.2.6 | O | TLV | 3-10 |
| 7F | Mapped EPS bearer contexts | Mapped EPS bearer contexts  9.10.4.6 | O | TLV-E | 7-65538 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.2.2 5GSM cause

This IE is included when the selected PDU session type is different from the PDU session type requested by the UE.

#### 8.3.2.3 PDU address

This IE is included when the selected PDU session type is "IPv4", "IPv6" or "IPv4v6".

#### 8.3.2.4 RQ timer value

This IE is included when the network wants to provide the RQ timer value.

#### 8.3.2.5 S-NSSAI

This IE shall be included in the message when the SMF received from the AMF an S-NSSAI together with the PDU SESSION ESTABLISHMENT REQUEST message, and the PDU session is a non-emergency PDU session.

#### 8.3.2.6 Mapped EPS bearer contexts

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

#### 8.3.2.7 EAP message

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

#### 8.3.2.8 Extended protocol configuration options

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

### 8.3.3 PDU session establishment reject

#### 8.3.3.1 Message definition

The PDU SESSION ESTABLISHMENT REJECT message is sent by the SMF to the UE in response to PDU SESSION ESTABLISHMENT REQUEST message and indicates unsuccessful establishment of a PDU session. See table 8.3.3.1.1.

Message type: PDU SESSION ESTABLISHMENT REJECT

Significance: dual

Direction: network to UE

Table 8.3.3.1.1: PDU SESSION ESTABLISHMENT REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION ESTABLISHMENT REJECT message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.10.4.2 | M | V | 1 |
| 37 | Back-off timer value | GPRS timer 3  9.10.2.5 | O | TLV | 3 |
| F- | Allowed SSC mode | Allowed SSC mode  9.10.4.3 | O | TV | 1 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.3.2 Back-off timer value

The network may include this IE to request a minimum time interval before procedure retry is allowed.

#### 8.3.3.3 Allowed SSC mode

This IE is included when the network rejects the PDU SESSION ESTABLISHMENT REQUEST with cause #68 "not supported SSC mode.

#### 8.3.3.4 EAP message

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

#### 8.3.3.5 Extended protocol configuration options

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

### 8.3.4 PDU session authentication command

#### 8.3.4.1 Message definition

The PDU SESSION AUTHENTICATION COMMAND message is sent by the SMF to the UE for authentication of the UE establishing the PDU session or of the UE participating in the PDU session. See table 8.3.4.1.1.

Message type: PDU SESSION AUTHENTICATION COMMAND

Significance: dual

Direction: network to UE

Table 8.3.4.1.1: PDU SESSION AUTHENTICATION COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION AUTHENTICATION COMMAND message identity | Message type  9.7 | M | V | 1 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.4.2 EAP message

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

#### 8.3.4.3 Extended protocol configuration options

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

### 8.3.5 PDU session authentication complete

#### 8.3.5.1 Message definition

The PDU SESSION AUTHENTICATION COMPLETE message is sent by the UE to the SMF in response to the PDU SESSION AUTHENTICATION COMMAND message and indicates acceptance of the PDU SESSION AUTHENTICATION COMMAND message. See table 8.3.5.1.1.

Message type: PDU SESSION AUTHENTICATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.5.1.1: PDU SESSION AUTHENTICATION COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION AUTHENTICATION COMPLETE message identity | Message type  9.7 | M | V | 1 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.5.2 EAP message

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

#### 8.3.5.3 Extended protocol configuration options

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

### 8.3.6 PDU session authentication result

#### 8.3.6.1 Message definition

The PDU SESSION AUTHENTICATION RESULT message is sent by the SMF to the UE for indication of successful result of authentication of the UE participating in the PDU session. See table 8.3.6.1.1.

Message type: PDU SESSION AUTHENTICATION RESULT

Significance: dual

Direction: network to UE

Table 8.3.6.1.1: PDU SESSION AUTHENTICATION RESULT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION AUTHENTICATION RESULT message identity | Message type  9.7 | M | V | 1 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.6.2 EAP message

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

#### 8.3.6.3 Extended protocol configuration options

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

### 8.3.7 PDU session modification request

#### 8.3.7.1 Message definition

The PDU SESSION MODIFICATION REQUEST message is sent by the UE to the SMF to request a modification of a PDU session. See table 8.3.7.1.1.

Message type: PDU SESSION MODIFICATION REQUEST

Significance: dual

Direction: UE to network

Table 8.3.7.1.1: PDU SESSION MODIFICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION REQUEST message identity | Message type  9.7 | M | V | 1 |
| 28 | 5GSM capability | 5GSM capability  9.10.4.1 | O | TLV | 3-15 |
| 55 | Maximum number of supported packet filters | Maximum number of supported packet filters  9.10.4.6 | O | TV | 3 |
| 7A | Requested QoS rules | QoS rules  9.10.4.9 | O | TLV-E | 3-65538 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.7.2 5GSM capability

This IE is included in the message after inter-system change from S1 mode to N1 mode:

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

b) if the PDU session is of "IPv6" or "IPv4v6" PDU session type, and the UE supports acting as a type C host as specified in IETF RFC 4191 [36].

#### 8.3.7.3 Maximum number of supported packet filters

This IE shall be included in the message when the selected PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet", the UE can support more than 16 packet filters for this PDU session, and the UE is sending the message after an inter-system change from S1 mode to N1 mode.

#### 8.3.7.4 Requested QoS rules

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

#### 8.3.7.5 Extended protocol configuration options

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

### 8.3.8 PDU session modification reject

#### 8.3.8.1 Message definition

The PDU SESSION MODIFICATION REJECT message is sent by the SMF to the UE to indicate rejection of the PDU SESSION MODIFICATION REQUEST. See table 8.3.8.1.1.

Message type: PDU SESSION MODIFICATION REJECT

Significance: dual

Direction: network to UE

Table 8.3.8.1.1: PDU SESSION MODIFICATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION REJECT message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.10.4.2 | M | V | 1 |
| 37 | Back-off timer value | GPRS timer 3  9.10.2.5 | O | TLV | 3 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.8.2 Back-off timer value

The network may include this IE to request a minimum time interval before procedure retry is allowed.

#### 8.3.8.3 Extended protocol configuration options

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

### 8.3.9 PDU session modification command

#### 8.3.9.1 Message definition

The PDU SESSION MODIFICATION COMMAND message is sent by the SMF to the UE to indicate a modification of a PDU session. See table 8.3.9.1.1

Message type: PDU SESSION MODIFICATION COMMAND

Significance: dual

Direction: network to UE

Table 8.3.9.1.1: PDU SESSION MODIFICATION COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION COMMAND message identity | Message type  9.7 | M | V | 1 |
| 59 | 5GSM cause | 5GSM cause  9.10.4.2 | O | TV | 2 |
| 2A | Session AMBR | Session-AMBR  9.10.4.10 | O | TLV | 8 |
| 56 | RQ timer value | GPRS timer  9.10.2.3 | O | TV | 2 |
| 7A | Authorized QoS rules | QoS rules  9.10.4.9 | O | TLV-E | 7-65538 |
| 7F | Mapped EPS bearer contexts | Mapped EPS bearer contexts  9.10.4.5 | O | TLV-E | 7-65538 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.9.2 5GSM cause

This IE is included when the network performs the PDU session anchor relocation for SSC mode 3.

#### 8.3.9.3 Session-AMBR

This IE is included when the session-AMBR of the PDU session is modified.

#### 8.3.9.4 RQ timer value

This IE is included when the network wants to provide the RQ timer value.

#### 8.3.9.5 Authorized QoS rules

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

#### 8.3.9.6 Mapped EPS bearer contexts

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

#### 8.3.9.7 Extended protocol configuration options

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

### 8.3.10 PDU session modification complete

#### 8.3.10.1 Message definition

The PDU SESSION MODIFICATION COMPLETE message is sent by the UE to the SMF in response to the PDU SESSION MODIFICATION COMMAND message and indicates an acceptance of the PDU SESSION MODIFICATION COMMAND message. See table 8.3.10.1.1.

Message type: PDU SESSION MODIFICATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.10.1.1: PDU SESSION MODIFICATION COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION COMPLETE message identity | Message type  9.7 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.10.2 Extended protocol configuration options

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

### 8.3.11 PDU session modification command reject

#### 8.3.11.1 Message definition

The PDU SESSION MODIFICATION COMMAND REJECT message is sent by the UE to the SMF to indicate rejection of the PDU SESSION MODIFICATION COMMAND message. See table 8.3.11.1.1.

Message type: PDU SESSION MODIFICATION COMMAND REJECT

Significance: dual

Direction: UE to network

Table 8.3.11.1.1: PDU SESSION MODIFICATION COMMAND REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION COMMAND REJECT message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.10.4.2 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.11.2 Extended protocol configuration options

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

### 8.3.12 PDU session release request

#### 8.3.12.1 Message definition

The PDU SESSION RELEASE REQUEST message is sent by the UE to the SMF to request a release of a PDU session. See table 8.3.12.1.1.

Message type: PDU SESSION RELEASE REQUEST

Significance: dual

Direction: UE to network

Table 8.3.12.1.1: PDU SESSION RELEASE REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION RELEASE REQUEST message identity | Message type  9.7 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.12.2 Extended protocol configuration options

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

### 8.3.13 PDU session release reject

#### 8.3.13.1 Message definition

The PDU SESSION RELEASE REJECT message is sent by the SMF to the UE to indicate rejection of request a release of a PDU session. See table 8.3.13.1.1.

Message type: PDU SESSION RELEASE REJECT

Significance: dual

Direction: network to UE

Table 8.3.13.1.1: PDU SESSION RELEASE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU RELEASE REJECT message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.10.4.2 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.13.2 Extended protocol configuration options

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

### 8.3.14 PDU session release command

#### 8.3.14.1 Message definition

The PDU SESSION RELEASE COMMAND message is sent by the SMF to the UE to indicate a release of a PDU session. See table 8.3.14.1.1.

Message type: PDU SESSION RELEASE COMMAND

Significance: dual

Direction: network to UE

Table 8.3.14.1.1: PDU SESSION RELEASE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION RELEASE COMMAND message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.10.4.2 | M | V | 1 |
| 37 | Back-off timer value | GPRS timer 3  9.10.2.5 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.10.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.14.2 Back-off timer value

The network may include this IE to request a minimum time interval before procedure retry is allowed.

#### 8.3.14.3 EAP message

This IE is included when the external DN performs re-authentication and re-authorization of the UE using EAP and it completes unsuccessfully.

#### 8.3.14.4 Extended protocol configuration options

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

### 8.3.15 PDU session release complete

#### 8.3.15.1 Message definition

The PDU SESSION RELEASE COMPLETE message is sent by the UE to the SMF in response to the PDU SESSION RELEASE COMMAND message and indicates an acceptance of a release of the PDU session. See table 8.3.15.1.1.

Message type: PDU SESSION RELEASE COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.15.1.1: PDU SESSION RELEASE COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION RELEASE COMPLETE message identity | Message type  9.7 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.10.4.4 | O | TLV-E | 4-65538 |

#### 8.3.15.2 Extended protocol configuration options

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

### 8.3.16 5GSM status

#### 8.3.16.1 Message definition

The 5GSM STATUS message is sent by the SMF or the UE to pass information on the status of the indicated PDU session and report certain error conditions. See table 8.3.16.1.1.

Message type: 5GSM STATUS

Significance: dual

Direction: both

Table 8.3.16.1.1: 5GSM STATUS message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | 5GSM STATUS message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.10.4.2 | M | V | 1 |

# 9 General message format and information elements coding

## 9.1 Overview

Within the protocols defined in the present document, every 5GS NAS message is a standard L3 message as defined in 3GPP TS 24.007 [11]. This means that the message consists of the following parts:

1) if the message is a plain 5GS NAS message:

a) extended protocol discriminator;

b) security header type or PDU session identity;

c) procedure transaction identity;

d) message type;

e) other information elements, as required.

2) if the message is a security protected 5GS NAS message:

a) extended protocol discriminator;

b) security header type;

c) message authentication code;

d) sequence number;

e) plain 5GS NAS message, as defined in item 1

The organization of a plain 5GS NAS message is illustrated in the example shown in figure .9.1.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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: 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 9.1.2: General message organization example for a security protected 5GS NAS message

Unless specified otherwise in the message descriptions of clause 8 and clause 9, a particular information element shall not be present more than once in a given message.

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

## 9.2 Extended protocol discriminator

Bits 1 to 8 of the first octet of every 5GS NAS message contain the Extended protocol discriminator (EPD) IE. The EPD and its use are defined in 3GPP TS 24.007 [11]. The extended protocol discriminator in the header (see 3GPP TS 24.007 [11]) of a security protected 5GS NAS message is encoded as "5GS mobility management messages".

## 9.3 Security header type

Bits 1 to 4 of the second octet of every 5GMM message contain the Security header type IE. This IE includes control information related to the security protection of a 5GMM message. The total size of the Security header type IE is 4 bits.

The Security header type IE can take the values shown in table 9.3.1.

Table 9.3.1: Security header type

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security header type (octet 1) | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | Plain 5GS NAS message, not security protected |
|  |  |  |  |  |
|  |  |  |  | Security protected 5GS NAS message: |
| 0 | 0 | 0 | 1 | Integrity protected |
| 0 | 0 | 1 | 0 | Integrity protected and ciphered |
| 0 | 0 | 1 | 1 | Integrity protected with new 5G NAS security context (NOTE 1) |
| 0 | 1 | 0 | 0 | Integrity protected and ciphered with new 5G NAS security context (NOTE 2) |
|  |  |  |  |  |
| All other values are reserved. | | | | |
|  | | | | |
| NOTE 1: This codepoint may be used only for a SECURITY MODE COMMAND message.  NOTE 2: This codepoint may be used only for a SECURITY MODE COMPLETE message. | | | | |

An 5GMM message received with the security header type encoded as 0000 shall be treated as not security protected, plain 5GS NAS message. A protocol entity sending a not security protected 5GMM message shall send the message as plain 5GS NAS message and encode the security header type as 0000.

## 9.4 PDU session identity

Bits 1 to 8 of the second octet of every 5GSM message contain the PDU session identity IE. The PDU session identity and its use to identify a message flow are defined in 3GPP TS 24.007 [11].

## 9.5 Spare half octet

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

## 9.6 Procedure transaction identity

Bits 1 to 8 of the third octet of every 5GSM message contain the procedure transaction identity. The procedure transaction identity and its use are defined in 3GPP TS 24.007 [11].

## 9.7 Message type

The Message type IE and its use are defined in 3GPP TS 24.007 [11]. Tables 9.7.1 and 9.7.2 define the value part of the message type IE used in the 5GS mobility management protocol and 5GS session management protocol.

Table 9.7.1: Message types for 5GS mobility management

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bits | | | | | | | |  |  |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | - | - | - | - | - | - |  | 5GS mobility management messages |
|  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |  | Registration request |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |  | Registration accept |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |  | Registration complete |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |  | Registration reject |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |  | Deregistration request (UE originating) |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |  | Deregistration accept (UE originating) |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |  | Deregistration request (UE terminated) |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |  | Deregistration accept (UE terminated) |
|  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |  | Service request |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |  | Service reject |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |  | Service accept |
|  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |  | Configuration update command |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |  | Configuration update complete |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |  | Authentication request |
| 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |  | Authentication response |
| 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 |  | Authentication reject |
| 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |  | Authentication failure |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |  | Authentication result |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |  | Identity request |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |  | Identity response |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |  | Security mode command |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |  | Security mode complete |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |  | Security mode reject |
|  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |  | 5GMM status |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |  | Notification |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |  | Notification response |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 |  | UL NAS transport |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |  | DL NAS transport |
|  |  |  |  |  |  |  |  |  |  |

Table 9.7.2: Message types for 5GS session management

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bits | | | | | | | |  |  |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 1 | 1 | - | - | - | - | - | - |  | 5GS session management messages |
|  |  |  |  |  |  |  |  |  |  |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |  | PDU session establishment request |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |  | PDU session establishment accept |
| 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |  | PDU session establishment reject |
|  |  |  |  |  |  |  |  |  |  |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |  | PDU session authentication command |
| 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |  | PDU session authentication complete |
| 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |  | PDU session authentication result |
|  |  |  |  |  |  |  |  |  |  |
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |  | PDU session modification request |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |  | PDU session modification reject |
| 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |  | PDU session modification command |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |  | PDU session modification complete |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |  | PDU session modification command reject |
|  |  |  |  |  |  |  |  |  |  |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |  | PDU session release request |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |  | PDU session release reject |
| 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |  | PDU session release command |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |  | PDU session release complete |
|  |  |  |  |  |  |  |  |  |  |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |  | 5GSM status |
|  |  |  |  |  |  |  |  |  |  |

## 9.8 Message authentication code

The message authentication code (MAC) information element contains the integrity protection information for the message. The MAC IE shall be included in the security protected 5GS NAS message if a valid 5G NAS security context exists and security functions are started.

Editor's note: The usage of MAC is FFS.

## 9.9 Sequence number

This IE includes the NAS message sequence number (SN) which consists of the eight least significant bits of the NAS COUNT for a security protected 5GS NAS message. The usage of SN is specified in subclause 4.4.3.

## 9.10 Other information elements

### 9.10.1 General

### 9.10.2 Common information elements

#### 9.10.2.1 Additional information

The purpose of the Additional information information element is to provide additional information to upper layers in relation to the NAS transport mechanism.

The Additional information information element is coded as shown in figure 9.10.2.1.1 and table 9.10.2.1.1.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.2.1.1: Additional information information element

Table 9.10.2.1.1 : Additional information information element

|  |
| --- |
| Additional information value (octet 3 to octet n) |
|  |
| The coding of the additional information value is dependent on the LCS application. |

#### 9.10.2.2 EAP message

The purpose of the EAP message information element is to transport an EAP message as specified in IETF RFC 3748 [34].

The EAP message information element is coded as shown in figure 9.10.2.2.1 and table 9.10.2.2.1.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.2.2.1: EAP message information element

Table 9.10.2.2.1: EAP message information element

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

#### 9.10.2.3 GPRS timer

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

#### 9.10.2.4 GPRS timer 2

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

#### 9.10.2.5 GPRS timer 3

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

#### 9.10.2.6 S-NSSAI

The purpose of the S-NSSAI information element is to identify a network slice.

The S-NSSAI information element is coded as shown in figure 9.8.2.6.1 and table 9.8.2.6.1.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 configured SST | | | | | | | | octet 7\* |
| Mapped configured SD | | | | | | | | octet 8\*  octet 10\* |

Figure 9.10.2.6.1: S-NSSAI information element

Table 9.10.2.6.1: S-NSSAI information element

|  |
| --- |
| Slice/service type (SST) (octet 3) |
| This field contains the 8 bit SST value. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. |
| Slice differentiator (SD) (octet 4 to octet 6)  This field contains the 24 bit SD value. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. |
| mapped configured Slice/service type (SST) (octet 7) |
| This field contains the 8 bit SST value of an S-NSSAI in the configured NSSAI for the HPLMN to which the SST value is mapped. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. |
| mapped configured Slice differentiator (SD) (octet 8 to octet 10)  This field contains the 24 bit SD value of an S-NSSAI in the configured NSSAI for the HPLMN to which the SD value is mapped. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. |
| NOTE 1: Octet 3 shall always be included.  NOTE 2: If the octet 4 is included, then octet 5 and octet 6 shall be included.  NOTE 3: If the octet 7 is included, then octets 8, 9, and 10 may be included.  NOTE 4: If the octet 8 is included, then octet 9 and octet 10 shall be included. |

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

The purpose of the S1 mode to N1 mode NAS transparent container information element is to provide the UE with parameters that enable the UE to create a mapped 5G NAS security context and take this context into use after inter-system change to N1 mode in 5GMM-CONNECTED mode.

The S1 mode to N1 mode NAS transparent container information element is coded as shown in figure 9.10.2.7.1 and table 9.0.2.7.1.

The S1 mode to N1 mode NAS transparent container is a type 4 information element with a minimum length of 10 octets and a maximum length of 12 octets.

Octets 11 and 12 are optional. If octet 11 is included, then also octet 12 shall be included.

The value part of the S1 mode to N1 mode NAS transparent container information element is included in specific information elements within some RRC messages sent to the UE.

NOTE: For these cases the coding of the information element identifier and length information of RRC is defined in 3GPP TS 38.331 [30].

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| NAS count | | | | TSC | Key set identifier in 5G | | | octet 8 |
|  |  |  |  |  |  | | |  |
|  | | | |
| 5G UE security capability | | | | | | | | octet 9  octet 10 |
| EPS UE security capability | | | | | | | | octet 11\*  octet 12\* |

Figure 9.10.2.7.1: S1 mode to N1 mode NAS transparent container information element

Table 9.10.2.7.1: S1 mode to N1 mode NAS transparent container information element

|  |
| --- |
| Message authentication code (octet 2 to 5) |
|  |
| This field is coded as the Message authentication code information element (see subclause 9.8.3.28). |
|  |
| Type of integrity protection algorithm (octet 6, bit 1 to 4) and type of ciphering algorithm (octet 6, bit 5 to 8) |
|  |
| These fields are coded as the type of integrity protection algorithm and type of ciphering algorithm in the NAS security algorithms information element (see subclause 9.8.3.32). |
|  |
| NAS count (octet 7, bits 5 to 8) |
|  |
| This field is coded as the 4 LSB of the Sequence number information element (see subclause 9.8.3.48) |
|  |
| Key set identifier in 5G (octet 7, bit 1 to 3) and type of security context flag (TSC) (octet 7, bit 4) |
|  |
| These fields are coded as the NAS key set identifier and type of security context flag in the NAS key set identifier information element (see subclause 9.8.3.29). |
|  |
| 5G UE security capability (octets 9 to 10) |
|  |
| This field is coded as octets 3 and 4 of the UE security capability information element (see subclause 9.8.3.57). |
|  |
| EPS UE security capability (octets 11 to 12) |
|  |
| This field is coded as octets 5 and 6 of the UE security capability information element (see subclause 9.8.3.57). |

### 9.10.3 5GS mobility management (5GMM) information elements

#### 9.10.3.1 5GMM capability

The purpose of the 5GMM capability information element is to provide the network with information concerning aspects of the UE related to the 5GCN or interworking with the EPS. The contents might affect the manner in which the network handles the operation of the UE.

The 5GMM capability information element is coded as shown in figure 9.10.3.1.1 and table 9.10.3.1.1.

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| 5GMM capability IEI | | | | | | | | | | | | | | | | octet 1 | |
| Length of 5GMM capability contents | | | | | | | | | | | | | | | | octet 2 | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | HO attach | | S1 mode | | octet 3 | |
| 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | octet 4\* -15\* | |
| Spare | | | | | | | | | | | | | | | |

Figure 9.10.3.1.1: 5GMM capability information element

Table 9.10.3.1.1: 5GMM capability information element

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| EPC NAS supported (S1 mode) (octet 3, bit 1) | | | | | | | | | | | |
| 0 | | |  | |  | |  | | S1 mode not supported | | |
| 1 | | |  | |  | |  | | S1 mode supported | | |
|  | | | | | | | | | | | |
| Attach request message containing PDN connectivity request with request type handover to transfer PDU session from N1 mode to S1 mode supported (HO attach) (octet 3, bit 2) | | | | | | | | | | | |
| 0 | | | |  | |  | |  | | Attach request message containing PDN connectivity request with request type handover to transfer PDU session from N1 mode to S1 mode not supported | |
| 1 | | | |  | |  | |  | | Attach request message containing PDN connectivity request with request type handover to transfer PDU session from N1 mode to S1 mode supported | |
| All other bits in octet 3 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | | | | | | | | |

#### 9.10.3.2 5GMM cause

The purpose of the 5GMM cause information element is to indicate the reason why a 5GMM request from the UE is rejected by the network.

The 5GMM cause information element is coded as shown in figure 9.10.3.1.2 and table 9.10.3.1.2.

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

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

Figure 9.10.3.1.2: 5GMM cause information element

Table 9.10.3.1.2 : 5GMM cause information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cause value (octet 2) | | | | | | | | | |
|  | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |  | Illegal UE |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |  | PEI not accepted |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |  | Illegal ME |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |  | 5GS services not allowed |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |  | Implicitly de-registered |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |  | PLMN not allowed |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |  | Tracking area not allowed |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |  | Roaming not allowed in this tracking area |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |  | Synch failure |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |  | N1 mode not allowed |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |  | Restricted service area |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |  | LADN not available |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |  | Insufficient resources for specific slice and DNN |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |  | Insufficient resources for specific slice |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |  | Payload was not forwarded |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |  | Semantically incorrect message |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |  | Invalid mandatory information |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |  | Message type non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |  | Message type not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |  | Information element non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |  | Conditional IE error |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |  | Message not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |  | Protocol error, unspecified |
|  |  |  |  |  |  |  |  |  |  |
| Any other value received by the mobile station shall be treated as 0110 1111, "protocol error, unspecified". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified". | | | | | | | | | |

#### 9.10.3.3 5GS identity type

The purpose of the 5GS identity type information element is to specify which identity is requested.

The 5GS identity type is a type 1 information element.

The 5GS identity type information element is coded as shown in figure 9.10.3.3.1 and table 9.0.3.3.1.

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

Figure 9.10.3.3.1: 5GS identity type information element

Table 9.10.3.3.1: 5GS identity type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of identity (octet 1) | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 1 |  | SUCI |
| 1 | 1 | 0 |  | 5G-GUTI |
| 0 | 1 | 1 |  | IMEI |
| 1 | 0 | 0 |  | 5G-S-TMSI |
| 1 | 0 | 1 |  | IMEISV |
|  | | | | |
| All other values are interpreted as SUCI by this version of the protocol. | | | | |

#### 9.10.3.4 5GS mobile identity

The purpose of the 5GS mobile identity information element is to provide either the SUCI, the 5G-GUTI, the IMEI, the IMEISV or the 5G-S-TMSI.

The 5GS mobile identity information element is coded as shown in figures 9.10.3.4.1, 9.10.3.4.2, 9.10.3.4.3 and 9.10.3.4.4, and table 9.10.3.4.1.

The 5GS mobile identity is a type 4 information element with a minimum length of 3 octets and a maximum length of TBD octets.

Editor’s note: The maximum length of 5GS mobile identity is TBD and will be updated based on CT4 specification.

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

Figure 9.10.3.4.1: 5GS mobile identity information element for type of identity "5G-GUTI"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2 |
| Identity digit 1 | | | | odd/  even  indic | Type of identity | | | octet 3 |
| Identity digit p+1 | | | | Identity digit p | | | | octet 4\* |

Figure 9.10.3.4.2: 5GS mobile identity information element for type of identity "SUCI" or "IMEI" or "IMEISV"

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 |
| Length of 5GS mobile identity contents | | | | | | | | octet 2 |
| 1 | 1 | 1 | 1 | odd/  even  indic | Type of identity | | | octet 3 |
| AMF Set ID | | | | AMF Pointer | | | | octet 4 |
| 5G-TMSI | | | | | | | | octet 5 |
| 5G-TMSI (continued) | | | | | | | | octet 6 |
| 5G-TMSI (continued) | | | | | | | | octet 7 |
| 5G-TMSI (continued) | | | | | | | | octet 8 |

Figure 9.10.3.4.3: 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 |
| Identity digit 1 | | | | odd/  even  indic | Type of identity | | | octet 3 |

Figure 9.10.3.4.4: 5GS mobile identity information element for type of identity "No identity"

Table 9.10.3.4.1: 5GS mobile identity information element

|  |  |  |  |
| --- | --- | --- | --- |
| Type of identity (octet 3)  Bits | | | |
| 3 | 2 | 1 |  |
| 0 | 0 | 0 | No identity (NOTE) |
| 0 | 0 | 1 | SUCI |
| 1 | 1 | 0 | 5G-GUTI |
| 0 | 1 | 1 | IMEI |
| 1 | 0 | 0 | 5G-S-TMSI |
| 1 | 0 | 1 | IMEISVI |
| All other values are reserved. | | | |
|  | | | |
| Odd/even indication (octet 3)  Bit | | | |
| 4 |  |  |  |
| 0 |  |  | even number of identity digits and also when the GUTI or 5G-TMSI is used |
| 1 |  |  | odd number of identity digits |
|  | | | |
| Identity digits (octet 4 etc.)  For the SUCI, this field is coded using BCD coding. If the number of identity digits is even then bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". | | | |
|  | | | |
| For the 5G-GUTI, then bits 5 to 8 of octet 3 are coded as "1111", octet 4 through 6 contain the MCC and MNC values as specified below, and bit 8 of octet 7 is the most significant bit and bit 1 of the last octet the least significant bit for the subsequent fields. The required fields for the 5G-GUTI are as defined in 3GPP TS 23.003 [4]. | | | |
| MCC, Mobile country code (octet 4, octet 5 bits 1 to 4)  The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | | | |
|  | | | |
| MNC, Mobile network code (octet 5 bits 5 to 8, octet 6)  The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 5 shall be coded as "1111".  The contents of the MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12]. | | | |
|  | | | |
| For the IMEI, this field is coded using BCD coding. The format of the IMEI is described in 3GPP TS 23.003 [4]. | | | |
|  | | | |
| For the IMEISV, this field is coded using BCD coding. Bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". The format of the IMEISV is described in 3GPP TS 23.003 [4]. | | | |
|  | | | |
| For the 5G-S-TMSI, bits 5 to 8 of octet 3 are coded as "1111" and bit 8 of octet 4 is the most significant bit and bit 1 of the last octet is the least significant bit. The coding of the 5G-S-TMSI is left open for each administration. | | | |
|  | | | |
| For Type of identity "No identity", the identity digit bits shall be encoded with all 0s and the length of mobile identity contents parameter shall be set to 1. | | | |
|  | | | |
| NOTE: This can be used when the requested identity is not available at the UE during the identification procedure. | | | |

#### 9.10.3.5 5GS network feature support

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

The 5GS network feature support information element is coded as shown in figure 9.10.3.5.1 and table 9.10.3.5.1.

The 5GS network feature support is a type 4 information element with a minimum length of 3 octets and a maximum length of 5 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | | | | | octet 3 | | |
| 0 | | | 0 | | | 0 | | 0 | | | 0 | | 0 | | | 0 | | 0 | | |  | | |
| Spare | | | | | | | | | | | | | | | | | | | | | octet 4\*- 5\* | | |

Figure 9.10.3.5.1: 5GS network feature support information element

Table 9.10.3.5.1: 5GS network feature support information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IMS voice over PS session indicator (IMS VoPS) (octet 3, bit1 and bit 2) | | | | |
| This bit indicates the support of IMS voice via 5GS | | | | |
| Bit | | | | |
| 2 | 1 |  |  |  |
| 0 | 0 |  |  | IMS voice over PS session not supported |
| 0 | 1 |  |  | IMS voice over PS session supported over 3GPP access |
| 1 | 0 |  |  | IMS voice over PS session supported over non-3GPP access |
| 1 | 1 |  |  | reserved |
|  | | | | |
| Emergency service support indicator (EMC) (octet 3, bit 3 and bit 4) | | | | |
| This bit indicates the support of emergency services in 5GS | | | | |
| Bit | | | | |
| 4 | 3 |  |  |  |
| 0 | 0 |  |  | Emergency services not supported |
| 0 | 1 |  |  | Emergency services supported in NR connected to 5GCN only |
| 1 | 0 |  |  | Emergency services supported in E-UTRA connected to 5GCN only |
| 1 | 1 |  |  | Emergency services supported in NR connected to 5GCN and E-UTRA connected to 5GCN |
|  | | | | |
| Emergency service fallback indicator (EMF) (octet 3, bit 5 and bit 6) | | | | |
| This bit indicates the support of emergency services fallback | | | | |
| Bit | | | | |
| 6 | 5 |  |  |  |
| 0 | 0 |  |  | Emergency services fallback not supported |
| 0 | 1 |  |  | Emergency services fallback supported in NR connected to 5GCN only |
| 1 | 0 |  |  | Emergency services fallback supported in E-UTRA connected to 5GCN only |
| 1 | 1 |  |  | Emergency services fallback supported in NR connected to 5GCN and E-UTRA connected to 5GCN |
|  | | | | |
| Interworking without N26 interface indicator (IWK N26) (octet 3, bit 6) | | | | |
| This bit indicates whether the network supports interworking procedure without N26 interface | | | | |
| Bit | | | | |
| 7 |  |  |  |  |
| 0 |  |  |  | Interworking without N26 not supported |
| 1 |  |  |  | Interworking without N26 supported |
|  | | | | |
| MPS indicator (MPSI) (octet 3, bit 7) | | | | |
| This bit indicates the support of MPS in the RPLMN or equivalent PLMN. | | | | |
| Bit | | | | |
| 0 |  |  |  | Access identity 1 not valid in RPLMN or equivalent PLMN |
| 1 |  |  |  | Access identity 1 valid in RPLMN or equivalent PLMN |
|  | | | | |
| All bits in octets 4 to 5 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | |

#### 9.10.3.6 5GS registration result

The purpose of the 5GS registration result information element is to specify the result of a registration procedure.

The 5GS registration result information element is coded as shown in figure 9.10.3.6.1 and table 9.10.3.6.1.

The 5GS registration result is a type 4 information element with a length of 3 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | 2 | 1 | |  | |
| 5GS registration result IEI | | | | | | | | | | | | | | octet 1 | |
| Length of 5GS registration result contents | | | | | | | | | | | | | | octet 2 | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | SMS allowed | | 5GS registration result value | | | | octet 3 | |

Figure 9.10.3.6.1: 5GS registration result information element

Table 9.10.3.6.1: 5GS registration result information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5GS registration result value (octet 3, bits 1 to 3) | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 1 |  | 3GPP access |
| 0 | 1 | 0 |  | Non-3GPP access |
| 0 | 1 | 1 |  | 3GPP access and non-3GPP access |
| 1 | 1 | 1 |  | reserved |
|  | | | | |
| All other values are unused and shall be treated as "3GPP access", if received by the UE. | | | | |
|  | | | | |
| SMS over NAS transport allowed (SMS allowed) (octet 3, bit 4) | | | | |
| Bit | | | | |
| 4 |  |  |  |  |
| 0 |  |  |  | SMS over NAS not allowed |
| 1 |  |  |  | SMS over NAS allowed |
|  | | | | |
| Bits 5 to 8 of octet 3 are spare and shall be coded as zero. | | | | |

#### 9.10.3.7 5GS registration type

The purpose of the 5GS registration type information element is to indicate the type of the requested registration.

The 5GS registration type information element is coded as shown in figure 9.10.3.7.1 and table 9.10.3.7.1.

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | 2 | 1 | |  | |
| 5GS registration type IEI | | | | | | | | | | | | | | octet 1 | |
| Length of 5GS registration type contents | | | | | | | | | | | | | | octet 2 | |
| 0  Spare | | 0  Spare | | 0  Spare | | FOR | | SMS requested | | 5GS registration type value | | | | octet 3 | |

Figure 9.10.3.7.1: 5GS registration type information element

Table 9.10.3.7.1: 5GS registration type information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5GS registration type value (octet 3, bits 1 to 3) | | | | | | | | |
| Bits | | | | | | | | |
| 3 | | 2 | | 1 |  |  | | |
| 0 | | 0 | | 1 |  | initial registration | | |
| 0 | | 1 | | 0 |  | mobility registration updating | | |
| 0 | | 1 | | 1 |  | periodic registration updating | | |
| 1 | | 0 | | 0 |  | emergency registration | | |
| 1 | | 1 | | 1 |  | reserved | | |
|  | | | | | | | | |
| All other values are unused and shall be interpreted as "initial registration", if received by the network. | | | | | | | | |
|  | | | | | | | | |
| SMS over NAS transport requested (SMS requested) (octet 3, bit 4) | | | | | | | |
|  | | | | | | | |
| Bit | | | | | | | |
| 4 | |  | |  | | | | |
| 0 | |  | | SMS over NAS not supported | | | | |
| 1 | |  | | SMS over NAS supported | | | | |
|  | | | | | | | |
| Follow-on request bit (FOR) (octet 3, bit 5) | | | | | | | | |
| Bit | | | | | | | | |
| 5 | |  | |  |  |  | | |
| 0 | |  | |  |  | No follow-on request pending | | |
| 1 | |  | |  |  | Follow-on request pending | | |
|  | | | | | | | | |
| Bits 6 to 8 of octet 3 are spare and shall be coded as zero. | | | | | | | | |

#### 9.10.3.8 5GS tracking area identity

The purpose of the 5GS tracking area identity information element is to provide an unambiguous identification of tracking areas within the area covered by the 5GS.

The 5GS tracking area identity information element is coded as shown in figure 9.10.3.8.1 and table 9.10.3.8.1.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.8.1: 5GS tracking area identity information element

Table 9.10.3.8.1: 5GS tracking area identity information element

|  |
| --- |
| MCC, Mobile country code (octets 2 and 3)  The MCC field is coded as in ITU-T Rec. E212 [39], annex A.  If the TAI is deleted the MCC and MNC shall take the value from the deleted TAI.  In abnormal cases, the MCC stored in the UE can contain elements not in the set {0, 1 ... 9}. In such cases the UE should transmit the stored values using full hexadecimal encoding. When receiving such an MCC, the network shall treat the TAI as deleted.  MNC, Mobile network code (octet 3 bits 5 to 8, octet 4)  The coding of this field is the responsibility of each administration, but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. For PCS 1900 for NA, Federal regulation mandates that a 3-digit MNC shall be used. However, a network operator may decide to use only two digits in the MNC in the TAI over the radio interface. In this case, bits 5 to 8 of octet 3 shall be coded as "1111". Mobile equipment shall accept a TAI coded in such a way.  In abnormal cases, the MNC stored in the UE can have:  - digit 1 or 2 not in the set {0, 1 ... 9}, or  - digit 3 not in the set {0, 1 ... 9, F} hex.  In such cases the UE shall transmit the stored values using full hexadecimal encoding. When receiving such an MNC, the network shall treat the TAI as deleted.  The same handling shall apply for the network, if a 3-digit MNC is sent by the UE to a network using only a 2-digit MNC.  TAC, Tracking area code (octets 5 to 7)  In the TAC field bit 8 of octet 5 is the most significant bit and bit 1 of octet 6 the least significant bit.  The coding of the tracking area code is the responsibility of each administration except that two values are used to mark the TAC, and hence the TAI, as deleted. Coding using full hexadecimal representation may be used. The tracking area code consists of 3 octets.  If a TAI has to be deleted, then all bits of the tracking area code shall be set to one with the exception of the least significant bit which shall be set to zero. If a USIM is inserted in a mobile equipment with the tracking area code containing all zeros, then the mobile equipment shall recognise this TAC as part of a deleted TAI. |

#### 9.10.3.9 5GS tracking area identity list

The purpose of the 5GS tracking area identity list information element is to transfer a list of tracking areas from the network to the UE.

The coding of the information element allows combining different types of lists. The lists of type "00" and "01" allow a more compact encoding, when the different TAIs are sharing the PLMN identity.

The 5GS tracking area identity list information element is coded as shown in figure 9.10.3.8.1, figure 9.10.3.8.2, figure 9.10.3.9.3, figure 9.10.3.9.4 and table 9.10.3.9.1.

The 5GS tracking area identity list is a type 4 information element, with a minimum length of 9 octets and a maximum length of 114 octets. The list can contain a maximum of 16 different tracking area identities.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.9.1: 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 9.10.3.9.2: 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 9.10.3.9.3: 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 9.10.3.9.4: Partial tracking area identity list – type of list = "10"

Table 9.10.3.9.1: Tracking area identity list information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Value part of the Tracking area identity list information element (octets 3 to n) | | | | | |
|  | | | | | |
| The value part of the Tracking area identity list information element consists of one or several partial tracking area identity lists. The length of each partial tracking area identity list can be determined from the 'type of list' field and the 'number of elements' field in the first octet of the partial tracking area identity list. | | | | | |
| The UE shall store the complete list received. If more than 16 TAIs are included in this information element, the UE shall store the first 16 TAIs and ignore the remaining octets of the information element. | | | | | |
|  | | | | | |
|  | | | | | |
| Partial tracking area identity list: | | | | | |
|  | | | | | |
| Type of list (octet 1) | | | | | |
| Bits | | | | | |
| 7 | 6 |  | | | |
| 0 | 0 | list of TACs belonging to one PLMN, with non-consecutive TAC values | | | |
| 0 | 1 | list of TACs belonging to one PLMN, with consecutive TAC values | | | |
| 1 | 0 | list of TAIs belonging to different PLMNs (see NOTE) | | | |
|  | | | | | |
| All other values are reserved. | | | | | |
|  | | | | | |
| Number of elements (octet 1) | | | | | |
| Bits | | | | | |
| 5 | 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | 0 | 1 element |
| 0 | 0 | 0 | 0 | 1 | 2 elements |
| 0 | 0 | 0 | 1 | 0 | 3 elements |
| … | | | | |  |
| 0 | 1 | 1 | 0 | 1 | 14 elements |
| 0 | 1 | 1 | 1 | 0 | 15 elements |
| 0 | 1 | 1 | 1 | 1 | 16 elements |
|  | | | | | |
| All other values are unused and shall be interpreted as 16, if received by the UE. | | | | | |
|  | | | | | |
| Bit 8 of octet 1 is spare and shall be coded as zero. | | | | | |
|  | | | | | |
|  | | | | | |
| For type of list = "00" and number of elements = k: | | | | | |
|  | | | | | |
| octet 2 to 4 contain the MCC+MNC, and | | | | | |
| for j = 1, …, k: | | | | | |
| octets 3j+2 to 3j+4 contain the TAC of the j-th TAI belonging to the partial list, | | | | | |
|  | | | | | |
| For type of list = "01" and number of elements = k: | | | | | |
|  | | | | | |
| octet 2 to 4 contain the MCC+MNC, and | | | | | |
| octets 5 to 7 contain the TAC of the first TAI belonging to the partial list. | | | | | |
| The TAC values of the other k-1 TAIs are TAC+1, TAC+2, …, TAC+k-1. | | | | | |
|  | | | | | |
| For type of list = "10" and number of elements = k: | | | | | |
|  | | | | | |
| for j = 1, …, k. | | | | | |
| octets 6j-4 to 6j-2 contain the MCC+MNC, and | | | | | |
| octets 6j-1 to 6j+1 contain the TAC of the j-th TAI belonging to the partial list. | | | | | |
|  | | | | | |
|  | | | | | |
| MCC, Mobile country code | | | | | |
|  | | | | | |
| The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | | | | | |
|  | | | | | |
| MNC, Mobile network code | | | | | |
|  | | | | | |
| The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111". | | | | | |
|  | | | | | |
| TAC, Tracking area code | | | | | |
|  | | | | | |
| In the TAC field bit 8 of the first octet is the most significant bit and bit 1 of third octet the least significant bit. | | | | | |
| The coding of the tracking area code is the responsibility of each administration. Coding using full hexadecimal representation may be used. The tracking area code consists of 3 octets. | | | | | |
|  | | | | | |
| NOTE: If the "list of TAIs belonging to different PLMNs" is used, the PLMNs included in the list need to be present in the list of "equivalent PLMNs". | | | | | |

#### 9.10.3.10 Access type

The purpose of the access 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 9.10.3.10.1 and table 9.10.3.10.1.

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

Figure 9.10.3.10.1: Access type information element

Table 9.10.3.10.1: Access type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Access type value (octet 1, bit 1 to bit 2) | | | | |
|  | | | | |
| Bits | | | | | |
| 2 | 1 |  |  |  | |
| 0 | 1 |  |  | 3GPP access | |
| 1 | 0 |  |  | Non-3GPP access | |
|  | | | | |
| All other values are reserved. | | | | |
|  | | | | |

#### 9.10.3.11 Allowed PDU session status

The purpose of the Allowed PDU session status information element is to indicate to the network user-plane resources of PDU sessions associated with non-3GPP access that are allowed to be re-established over 3GPP access or if there is no PDU session(s) for which the UE allows the user-plane resources to be re-established over 3GPP access..

The Allowed PDU session status information element is coded as shown in figure 9.10.3.11.1 and table 9.10.3.11.1.

The Allowed PDU session status is a type 4 information element with minimum length of 4 octets and maximum length of 34 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed PDU session status IEI | | | | | | | | octet 1 |
| Length of Allowed PDU session status contents | | | | | | | | octet 2 |
| PSI  (7) | PSI  (6) | PSI  (5) | PSI  (4) | PSI  (3) | PSI  (2) | PSI  (1) | PSI  (0) | octet 3 |
| PSI  (15) | PSI  (14) | PSI  (13) | PSI  (12) | PSI  (11) | PSI  (10) | PSI  (9) | PSI  (8) | octet 4 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  |
| Spare | | | | | | | | octet 5\* -34\* |

Figure 9.10.3.11.1: Allowed PDU session status information element

Table 9.10.3.11.1: Allowed PDU session status information element

|  |
| --- |
| PSI(x) shall be coded as follows:  PSI(0):  Bit 1octet 3 is spare and shall be coded as zero.  PSI(1) – PSI(15):  0 indicates that the user-plane resources of corresponding PDU session is not allowed to be re-established over 3GPP access.  1 indicates that the user-plane resources of corresponding PDU session can be re-established over 3GPP access.  If there is no PDU session that can be re-established over 3GPP access, all bits in PSI(5) – PSI(15) shall be coded as zero.  All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element. |

#### 9.10.3.12 Authentication failure parameter

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

#### 9.10.3.13 Authentication parameter AUTN

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

Editor's note: The format of the Authentication parameter AUTN IE in 3GPP TS 24.008 [12] is TLV with a length of 18 octets.

#### 9.10.3.14 Authentication parameter RAND

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

Editor's note: The format of the Authentication parameter RAND IE in 3GPP TS 24.008 [12] is TV with a length of 17 octets.

#### 9.10.3.15 Authentication response parameter

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

#### 9.10.3.16 Configuration update indication

The purpose of the Configuration update indication information element is to indicate the additional information associated with the generic UE configuration update procedure.

The Configuration update indication information element is coded as shown in figure 9.10.3.16.1 and table 9.10.3.16.1.

The Configuration update indication is a type 1 information element.

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

Figure 9.10.3.16.1: Configuration update indication

Table 9.10.3.16.1: Configuration update indication

|  |  |
| --- | --- |
| Acknowledgement (ACK) value (octet 1, bit 1) | |
| Bit | |
| 1 |  |
| 0 | acknowledgement not requested |
| 1 | acknowledgement requested |
|  |  |
| Registration requested (RED) value (octet 1, bit 2) | |
| Bit | |
| 2 |  |
| 0 | registration not requested |
| 1 | registration requested |
|  | |
| Bits 3 and 4 are spare and shall be coded as zero, | |

#### 9.10.3.17 Daylight saving time

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

#### 9.10.3.18 De-registration type

The purpose of the De-registration type information element is to indicate the type of de-registration.

The De-registration type information element is coded as shown in figure 9.10.3.18.1 and table 9.10.3.18.1.

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

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

Figure 9.10.3.18.1: Deregistration type information element

Table 9.10.3.18.1: Deregistration type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Switch off (octet 1, bit 4) | | | | |
| In the UE to network direction: | | | | |
| Bit | | | | |
| 4 |  |  |  |  |
| 0 |  |  |  | Normal de-registration |
| 1 |  |  |  | Switch off |
|  | | | | |
| In the network to UE direction bit 4 is spare. The network shall set this bit to zero. | | | | |
|  | | | | |
| Re-registration required (octet 1, bit 3) | | | | |
|  | | | | |
| In the network to UE direction: | | | | |
| Bit | | | | |
| 3 |  |  |  |  |
| 0 |  |  |  | re-registration not required |
| 1 |  |  |  | re-registration required |
|  | | | | |
| In the UE to network direction bit 3 is spare. The UE shall set this bit to zero. | | | | |
|  | | | | |
| Access type (octet 1,bit 2, bit 1) | | | | |
| Bit | | | | |
| 2 | 1 |  |  |  |
| 0 | 1 |  |  | 3GPP access |
| 1 | 0 |  |  | Non-3GPP access |
| 1 | 1 |  |  | 3GPP access and non-3GPP access |
|  | | | | |
| All other values are reserved. | | | | |

#### 9.10.3.19 DNN

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

The DNN information element is coded as shown in figure 9.10.3.19.1.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.19.1: DNN information element

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

#### 9.10.3.20 DRX parameters

Editor's note: The DRX parameters need to be defined by RAN WGs.

#### 9.10.3.21 Emergency number list

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

#### 9.10.3.22 EPS NAS message container

The purpose of the EPS NAS message container information element is to transport an EPS NAS message as specified in 3GPP TS 24.301 [15].

The EPS NAS message container information element is coded as shown in figure 9.10.3.22.1 and table 9.10.3.22.1.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.22.1: EPS NAS message container information element

Table 9.10.3.22.1: EPS NAS message container information element

|  |
| --- |
| EPS NAS message container (octet 4 to n) |
| An EPS NAS message as specified in 3GPP TS 24.301 [15]. |

#### 9.10.3.23 EPS NAS security algorithms

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

#### 9.10.3.24 Extended emergency number list

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

#### 9.10.3.25 HashAMF

The purpose of the HashAMF information element is to transfer a 64-bit hash value to the UE so the UE can check the AMF calculated value against the value locally calculated by the UE to determine whether the REGISTRATION REQUEST message sent by the UE has been modified.

The HashAMF information element is coded as shown in figure 9.10.3.25.1 and table 9.10.3.25.1.

The HashAMF is a type 3 information element with a length of 9 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| HashAMF IEI | | | | | | | | octet 1 |
| HashAMF value | | | | | | | | octet 2  octet 9 |

Figure 9.10.3.25.1: HashAMF information element

Table 9.10.3.25.1: HashAMF information element

|  |
| --- |
| HashAMF value (octet 2 to 9) |
|  |
| This field contains the binary representation of the HashAMF. Bit 8 of octet 2 represents the most significant bit of the HashAMF and bit 1 of octet 9 the least significant bit. |

#### 9.10.3.26 IMEISV request

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

#### 9.10.3.27 LADN information

The purpose of the LADN information information element is to provide the UE the LADN service area for each available LADN in the current registration area or to delete the LADN information at the UE.

The LADN information information element is coded as shown in figure 9.10.3.27.1, figure 9.10.3.27.2 and table 9.10.3.27.1.

The LADN information is a type 6 information element with a minimum length of 3 octets and a maximum length of 1707 octets.

The LADN information information element can contain a minimum of 0 and a maximum of 8 different LADNs each including a DNN and a tracking area identity lists.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.27.1: LADN information information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Length of DNN value | | | | | | | | octet 1 |
| DNN value | | | | | | | | octet 2  octet a |
| Tracking area identity list contents | | | | | | | | octet a+1  octet b |

Figure 9.10.3.27.2: LADN

Table 9.10.3.27.1: LADN information information element

|  |
| --- |
| Value part of the LADN information information element (octet 3 to h)  The value part of the LADN information information element consists of one or several LADNs. Each LADN consists one DNN value and one Tracking area identity list contents. The length of each LADN is determined by the length of DNN value and the length of Tracking area identity list contents.  The UE shall store the complete list received. If more than 8 LADNs are included in this information element, the UE shall store the first 8 LADNs and ignore the remaining octets of the information element.  LADN (octet 4 to octet a):  DNN value is coded as DNN value part of DNN information element as specified in subclause 9.8.3.15 starting with the third octet. |
| Tracking area identity list contents (octet a+1 to octet b): |
| Tracking area identity list contents is coded as the value part of the Tracking area identity list information element as specified in subclause 9.8.3.8 starting with the third octet. |

#### 9.10.3.28 MICO indication

The purpose of the MICO indication information element is to indicate the use of MICO mode or the re-negotiation of MICO mode.

The MICO indication information element is coded as shown in figure 9.10.3.28.1 and table 9.10.3.28.1.

The MICO indication is a type 1 information element.

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

Figure 9.10.3.28.1: MICO indication

Table 9.10.3.28.1: MICO indication

|  |  |
| --- | --- |
| Registration Area Allocation Indication (RAAI) (octet 1) | |
|  | |
| In the network to UE direction: | |
| Bit | |
| 1 |  | |
| 0 | all PLMN registration area not allocated |
| 1 | all PLMN registration area allocated |
| In the UE to network direction bit 1 is spare. The UE shall set this bit to zero. | |
| Bits 2, 3 and 4 are spare and shall be coded as zero, | |

#### 9.10.3.29 NAS key set identifier

The NAS key set identifier is allocated by the network.

The NAS key set identifier information element is coded as shown in figure 9.10.3.29.1 and table 9.10.3.29.1.

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

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

Figure 9.10.3.29.1: NAS key set identifier information element

Table 9.10.3.29.1: NAS key set identifier information element

|  |  |  |  |
| --- | --- | --- | --- |
| Type of security context flag (TSC) (octet 1) | | | |
|  | | | |
| Bit | | | |
| 4 |  |  |  |
| 0 |  |  | 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) |

#### 9.10.3.30 NAS message

This IE includes a complete plain 5GS NAS message as specified in subclause 8.2. The SECURITY PROTECTED 5GS NAS MESSAGE message is not a plain 5GS NAS message and shall not be included in this IE.

#### 9.10.3.31 NAS message container

The purpose of the NAS message container IE is to encapsulate a NAS message without NAS security header.

The NAS message container information element is coded as shown in figure 9.10.3.31.1 and table 9.10.3.31.1.

The NAS message container is a type 6 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.31.1: NAS message container information element

Table 9.10.3.31.1: NAS message container information element

|  |
| --- |
| NAS message container contents (octet 4 to octet n); Max value of 65535 octets |
|  |
| This IE can contain a REGISTRATION REQUEST message as defined in subclause 5.5.1, or a SERVICE REQUEST message as defined in subclause 5.6.1. |

#### 9.10.3.32 NAS security algorithms

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

The NAS security algorithms information element is coded as shown in figure 9.10.3.32.1 and table 9.10.3.32.1.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.32.1: NAS security algorithms information element

Table 9.10.3.32.1: NAS security algorithms information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of integrity protection algorithm (octet 2, bit 1 to 3) | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | 5GS integrity algorithm 5G-IA0 (null integrity protection algorithm) |
| 0 | 0 | 0 | 1 | 5GS integrity algorithm 128-5G-IA1 |
| 0 | 0 | 1 | 0 | 5GS integrity algorithm 128-5G-IA2 |
| 0 | 0 | 1 | 1 | 5GS integrity algorithm 128-5G-IA3 |
| 0 | 1 | 0 | 0 | 5GS integrity algorithm 5G-IA4 |
| 0 | 1 | 0 | 1 | 5GS integrity algorithm 5G-IA5 |
| 0 | 1 | 1 | 0 | 5GS integrity algorithm 5G-IA6 |
| 0 | 1 | 1 | 1 | 5GS integrity algorithm 5G-IA7 |
|  | | | | |
| All other values are reserved. | | | | |
|  | | | | |
| Type of ciphering algorithm (octet 2, bit 5 to 7) | | | | |
| Bits | | | | |
| 8 | 7 | 6 | 5 |  |
| 0 | 0 | 0 | 0 | 5GS encryption algorithm 5G-EA0 (null ciphering algorithm) |
| 0 | 0 | 0 | 1 | 5GS encryption algorithm 128-5G-EA1 |
| 0 | 0 | 1 | 0 | 5GS encryption algorithm 128-5G-EA2 |
| 0 | 0 | 1 | 1 | 5GS encryption algorithm 128-5G-EA3 |
| 0 | 1 | 0 | 0 | 5GS encryption algorithm 5G-EA4 |
| 0 | 1 | 0 | 1 | 5GS encryption algorithm 5G-EA5 |
| 0 | 1 | 1 | 0 | 5GS encryption algorithm 5G-EA6 |
| 0 | 1 | 1 | 1 | 5GS encryption algorithm 5G-EA7 |
|  | | | | |
| All other values are reserved. | | | | |
|  | | | | |

#### 9.10.3.33 Network name

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

#### 9.10.3.34 NSSAI

The purpose of the NSSAI information element is to identify a collection of S-NSSAIs

The NSSAI information element is coded as shown in figure 9.10.3.34.1 and table 9.10.3.34.1.

The NSSAI is a type 4 information element with a minimum length of 4 octets and a maximum length of 146 octets.

NOTE 1: The number of S-NSSAI values in a requested NSSAI or allowed NSSAI cannot exceed eight.

NOTE 2: The number of S-NSSAI values in a configured NSSAI cannot exceed sixteen.

NOTE 3: An NSSAI can include more than one S-NSSAIs with same SST values, and optionally same SD values, which are associated with different mapped SST values and optionally mapped SD values.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.34.1: NSSAI information element

Table 9.10.3.34.1: NSSAI information element

|  |
| --- |
| Value part of the NSSAI information element (octet 3 to v)  The value part of the NSSAI information element consists of one or more S-NSSAI values. Each S-NSSAI value consists of one S-NSSAI and optionally one mapped configured S-NSSAI from the configured NSSAI for the HPLMN.  If the recipient of this information element is the UE, the UE shall store the complete list received. If the NSSAI information element conveys an allowed NSSAI and more than 8 S-NSSAI values are included in this information element, the UE shall store the first 8 S-NSSAI values and ignore the remaining octets of the information element.  If the NSSAI information element conveys a configured NSSAI and more than 16 S-NSSAI values are included in this information element, the UE shall store the first 16 S-NSSAI values and ignore the remaining octets of the information element.  S-NSSAI value:  S-NSSAI value is coded as the length and value part of S-NSSAI information element as specified in subclause 9.8.2.6 starting with the second octet. |

#### 9.10.3.35 Payload container

The purpose of the Payload container information element is to transport a payload.

The Payload container information element is coded as shown in figure 9.10.3.35.1 and table 9.10.3.35.1.

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.35.1: Payload container information element

Table 9.10.3.35.1: Payload container information element

|  |
| --- |
| Payload container contents (octet 4 to octet n); max value of 65535 octets |
| The coding of Payload container contents is dependent on the particular application. |

#### 9.10.3.36 Payload container type

The purpose of the Payload container type information element indicates type of payload included in the payload container information element.

The Payload container information element is coded as shown in figure 9.10.3.36.1 and table 9.10.3.36.1.

The Payload container is a type 1 information element with a length of half octet.

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

Figure 9.10.3.36.1: Payload container information element

Table 9.10.3.36.1: Payload container information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Payload container type value (octet 1, bit 1 to bit 4) | | | | | | | | | |
| Bits | | | | | | | | | |
| 4 | | 3 | | 2 | | 1 | |  | |
| 0 | | 0 | | 0 | | 1 | | N1 SM information | |
| 0 | | 0 | | 1 | | 0 | | SMS | |
| 0 | | 0 | | 1 | | 1 | | LTE Positioning Protocol (LPP) message container | |
| 0 | | 1 | | 0 | | 0 | | Transparent container | |
| 0 | | 1 | | 0 | | 1 | | UE policy container | |
|  | | | | | | | | | |
| All other values are reserved. | | | | | | | | | |

#### 9.10.3.37 PDU session identity 2

The purpose of the PDU session identity 2 information element is to indicate the identity of a PDU session in a 5GMM message.

The PDU session identity 2 information element is coded as shown in figure 9.10.3.37.1 and table 9.10.3.37.1.

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

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

Figure 9.10.3.37.1: PDU session identity 2 information element

Table 9.10.3.37.1: PDU session identity 2 information element

|  |
| --- |
| PDU session identity 2 value (octet 2)  The coding of the DU session identity 2 value is identical to the coding of the PDU session identity value as defined in 3GPP TS 24.007 [11] . |

#### 9.10.3.38 PDU session reactivation result

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

The PDU session reactivation result information element is coded as shown in figure 9.10.3.38.1 and table 9.10.3.38.1.

The PDU session reactivation result is a type 4 information element with minimum length of 4 octets and maximum length of 34 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PDU session reactivation result IEI | | | | | | | | octet 1 |
| Length of PDU session reactivation result | | | | | | | | octet 2 |
| PSI  (7) | PSI  (6) | PSI  (5) | PSI  (4) | PSI  (3) | PSI  (2) | PSI  (1) | PSI  (0) | octet 3 |
| PSI  (15) | PSI  (14) | PSI  (13) | PSI  (12) | PSI  (11) | PSI  (10) | PSI  (9) | PSI  (8) | octet 4 |
| |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | Spare | | | | | | | | | | | | | | | | octet 5\* -34\* |

Figure 9.10.3.38.1: PDU session reactivation result information element

Table 9.10.3.38.1: PDU session reactivation result information element

|  |
| --- |
| PSI(x) shall be coded as follows:  PSI(0):  Bit 0 of octet 3 is spare and shall be coded as zero.  PSI(1) – PSI(15):  0 indicates PDU session user-plane resource reactivation was not requested in the Uplink data status IE or was not allowed to be reactivated in the Allowed PDU session status IE or user-plane resource reactivation is successful.  1 indicates either PDU session reactivation was requested in the Uplink data status IE but user-plane resource reactivation is not successful or indicates PDU session was allowed to be reactivated in the Allowed PDU session status IE but user-plane resource reactivation is either not performed or not successful.  All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element. |

#### 9.10.3.39 PDU session reactivation result error cause

The purpose of the PDU session reactivation result error cause information element is to indicate error causes for PDU session ID(s) where there was a failure to activate the user-plane resources.

The PDU session reactivation result error cause information element is coded as shown in figure 9.10.3.39.1 and table 9.10.3.39.1.

The PDU session reactivation result error cause is a type 6 information element with a minimum length of 5 octets and a maximum length of 515 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PDU session reactivation result error cause IEI | | | | | | | | octet 1 |
| Length of PDU session reactivation result error cause | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
| PDU session ID | | | | | | | | octet 4 |
| cause value | | | | | | | | octet 5 |
|  | | | | | | | |  |
| …. | | | | | | | |  |
|  | | | | | | | |  |
| PDU session ID | | | | | | | | octet 514\* |
| cause value | | | | | | | | octet 515\* |

Figure 9.10.3.39.1: PDU session reactivation result error cause information element

Table 9.10.3.39.1: PDU session reactivation result error cause information element

|  |
| --- |
| PDU session ID is coded same as PDU session ID IE (see subclause 9.4).  The cause value is coded same as second octet of 5GMM cause information element (see subclause 9.10.3.2). |

#### 9.10.3.40 PDU session status

The purpose of the PDU session status information element is to indicate the state of each PDU session that can be identified by a PDU session identity.

The PDU session status information element is coded as shown in figure 9.10.3.40.1 and table 9.10.3.40.1.

The PDU session status information element is a type 4 information element with minimum length of 4 octets and a maximum length of 34 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PDU session status IEI | | | | | | | | octet 1 |
| Length of PDU session status contents | | | | | | | | octet 2 |
| PSI  (7) | PSI  (6) | PSI  (5) | PSI  (4) | PSI  (3) | PSI  (2) | PSI  (1) | PSI  (0) | octet 3 |
| PSI  (15) | PSI  (14) | PSI  (13) | PSI  (12) | PSI  (11) | PSI  (10) | PSI  (9) | PSI  (8) | octet 4 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | octet 5\*- |
| spare | | | | | | | | 34\* |

Figure 9.10.3.40.1: PDU session status information element

Table 9.10.3.40.1: PDU session status information element

|  |
| --- |
| PSI(x) shall be coded as follows:  PSI(0):  Bit 1 of octet 3 is spare and shall be coded as zero.  PSI(1) – PSI(15):  0 indicates that the 5GSM state of the corresponding PDU session is PDU SESSION INACTIVE.  1 indicates that the 5GSM state of the corresponding PDU session is not PDU SESSION INACTIVE  All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element. |

#### 9.10.3.41 PLMN list

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

#### 9.10.3.42 Rejected NSSAI

The purpose of the Rejected NSSAI information element is to identify a collection of rejected S-NSSAIs

The Rejected NSSAI information element is coded as shown in figure 9.10.3.42.1, figure 9.10.3.42.2 and table 9.10.3.42.1.

The Rejected NSSAI is a type 4 information element with a minimum length of 4 octets and a maximum length of 42 octets.

NOTE: The number of rejected S-NSSAI(s) cannot exceed eight.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.42.1: 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 9.10.3.42.2: Rejected S-NSSAI

Table 9.10.3.42.1: Rejected NSSAI information element

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Value part of the Rejected NSSAI information element (octet 3 to v)  The value part of the Rejected NSSAI information element consists of one or more rejected S-NSSAIs. Each rejected S-NSSAI consists of one S-NSSAI and an associated cause value. The length of each rejected S-NSSAI can be determined by the 'length of rejected S-NSSAI' field in the first octet of the rejected S-NSSAI.  The UE shall store the complete list received. If more than 8 rejected S-NSSAIs are included in this information element, the UE shall store the first 8 rejected S-NSSAIs and ignore the remaining octets of the information element.  Rejected S-NSSAI: | | | | | | | |
| Cause value (octet 1) | | | | | | | |
| Bits | | | | | | | |
| 4 | 3 | 2 | 1 |  | | | |
| 0 | 0 | 0 | 0 | S-NSSAI not available in the current PLMN | | | |
| 0 | 0 | 0 | 1 | S-NSSAI not available in the current registration area | | | |
|  | | | | | | | |
| All other values are reserved. | | | | | | | |
| Slice/service type (SST) (octet 2)  This field contains the 8 bit SST value. The coding of the SST value part is defined in 3GPP TS 23.003 [4].  Slice differentiator (SD) (octet 3 to octet 5)  This field contains the 24 bit SD value. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. | | | | | | | |
| NOTE: If octet 3 is included, then octet 4 and octet 5 shall be included. | | | | | | | |

#### 9.10.3.43 Request type

The purpose of the Request type information element is to indicate type of the PDU session establishment.

The Request type information element is coded as shown in figure 9.10.3.43.1 and table 9.10.3.43.1.

The Request type is a type 1 information element.

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

Figure 9.10.3.43.1: Request type information element

Table 9.10.3.43.1: Request type information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Request type value (octet 1, bit 1 to bit 4) | | | | | |
|  | | | | | |
| Bits | | | | | |
| 3 | | 2 | 1 |  |  |
| 0 | | 0 | 1 |  | initial request |
| 0 | | 1 | 0 |  | existing PDU session |
| 0 | | 1 | 1 |  | initial emergency request |
| 1 | | 0 | 0 |  | existing emergency PDU session |
| 1 | | 1 | 1 |  | reserved |
| All other values are unused and shall be interpreted as "initial request", if received by the network. | | | | | |

#### 9.10.3.44 S1 UE network capability

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

#### 9.10.3.45 Service area list

The purpose of the Service area list information element is to transfer a list of allowed tracking areas for an allowed area or a list of non-allowed tracking areas for a non-allowed area from the network to the UE.

The coding of the information element allows combining different types of lists. The lists of type "00" and "01" allow a more compact encoding, when the different TAIs are sharing the PLMN identity. The lists of type "11" indicate all TAIs in the PLMN are allowed area.

The Service area list information element is coded as shown in figure 9.10.3.45.1, figure 9.10.3.45.2, figure 9.10.3.45.3, figure 9.10.3.45.4, figure 9.10.3.45.5 and table 9.10.3.45.1.

The Service area list is a type 4 information element with a minimum length of 6 octets and a maximum length of 114 octets. The list can contain a maximum of 16 different tracking area identities.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 9.10.3.45.1: 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 9.10.3.45.2: 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 9.10.3.45.3: 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 9.10.3.45.4: 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 9.10.3.45.5: Partial service area list – type of list = "11"

Table 9.10.3.45.1: Service area list information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Value part of the Service area list information element (octets 3 to n) | | | | | |
|  | | | | | |
| The value part of the Service area list information element consists of one or several partial service area lists. The length of each partial service area list can be determined from the 'type of list' field and the 'number of elements' field in the first octet of the partial service area list. | | | | | |
| For allowed type "0", TAIs contained in all partial service area lists are in the allowed area. For allowed type "1", TAIs contained in all partial service area lists are in the non-allowed area.  The UE shall store the complete list received. If more than 16 TAIs are included in this information element, the UE shall store the first 16 TAIs and ignore the remaining octets of the information element. | | | | | |
|  | | | | | |
|  | | | | | |
| Partial service area list: | | | | | |
|  | | | | | |
| Allowed type (octet 1) | | | | | |
| Bit | | | | | |
| 8 |  |  | | | |
| 0 |  | TAIs in the list are in the allowed area | | | |
| 1 |  | TAIs in the list are in the non-allowed area | | | |
|  | | | | | |
| Type of list (octet 1) | | | | | |
| Bits | | | | | |
| 7 | 6 |  | | | |
| 0 | 0 | list of TACs belonging to one PLMN, with non-consecutive TAC values | | | |
| 0 | 1 | list of TACs belonging to one PLMN, with consecutive TAC values | | | |
| 1 | 0 | list of TAIs belonging to different PLMNs (see NOTE) | | | |
| 1 | 1 | All TAIs belonging to the PLMN are in the allowed area | | | |
|  | | | | | |
| Number of elements (octet 1) | | | | | |
| Bits | | | | | |
| 5 | 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | 0 | 1 element |
| 0 | 0 | 0 | 0 | 1 | 2 elements |
| 0 | 0 | 0 | 1 | 0 | 3 elements |
| … | | | | |  |
| 0 | 1 | 1 | 0 | 1 | 14 elements |
| 0 | 1 | 1 | 1 | 0 | 15 elements |
| 0 | 1 | 1 | 1 | 1 | 16 elements |
|  | | | | | |
| All other values are unused and shall be interpreted as 16, if received by the UE. | | | | | |
|  | | | | | |
| For type of list = "00" and number of elements = k: | | | | | |
|  | | | | | |
| octets 2 to 4 contain the MCC+MNC, and | | | | | |
| for j = 1, …, k: | | | | | |
| octets 3j+2 to 3j+4 contain the TAC of the j-th TAI belonging to the partial list, | | | | | |
|  | | | | | |
| For type of list = "01" and number of elements = k: | | | | | |
|  | | | | | |
| octets 2 to 4 contain the MCC+MNC, and | | | | | |
| octets 5 to 7 contain the TAC of the first TAI belonging to the partial list. | | | | | |
| The TAC values of the other k-1 TAIs are TAC+1, TAC+2, …, TAC+k-1. | | | | | |
|  | | | | | |
| For type of list = "10" and number of elements = k: | | | | | |
|  | | | | | |
| for j = 1, …, k. | | | | | |
| octets 6j-4 to 6j-1 contain the MCC+MNC, and | | | | | |
| octets 6j-1 to 6j+1 contain the TAC of the j-th TAI belonging to the partial list. | | | | | |
|  | | | | | |
| For type of list = "11": | | | | | |
|  | | | | | |
| Allowed type shall be coded as "0" and number of elements shall be ignored, and | | | | | |
| octets 2 to 4 contain the MCC+MNC.  If allowed type is coded as "1", it shall be interpreted as "0". | | | | | |
|  | | | | | |
|  | | | | | |
| MNC, Mobile network code | | | | | |
|  | | | | | |
| The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111". | | | | | |
|  | | | | | |
| TAC, Tracking area code | | | | | |
|  | | | | | |
| In the TAC field bit 8 of the first octet is the most significant bit and bit 1 of the third octet the least significant bit. | | | | | |
| The coding of the tracking area code is the responsibility of each administration. Coding using full hexadecimal representation may be used. The tracking area code consists of 3 octets. | | | | | |
| NOTE: If the "list of TAIs belonging to different PLMNs" is used, the PLMNs included in the list need to be present in the list of equivalent PLMNs. | | | | | |

#### 9.10.3.46 Service type

The purpose of the service 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 9.10.3.46.1 and table 9.10.3.46.1.

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

Figure 9.10.3.46.1: Service type information element

Table 9.10.3.46.1: Service typeinformation element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service type value (octet 1) | | | | |
|  | | | | |
| Service type value | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | signalling |
| 0 | 0 | 0 | 1 | data |
| 0 | 0 | 1 | 0 | mobile terminated services |
| 0 | 0 | 1 | 1 | emergency services |
| 0 | 1 | 0 | 0 | emergency services fallback |
| 0 | 1 | 0 | 1 | high priority access |
| 0 | 1 | 1 | 0 | unused; shall be interpreted as "signalling", if received by the network |
| 0 | 1 | 1 | 1 | unused; shall be interpreted as "signalling", if received by the network |
| 1 | 0 | 0 | 0 | unused; shall be interpreted as "signalling", if received by the network |
| 1 | 0 | 0 | 1 | unused; shall be interpreted as "data", if received by the network |
| 1 | 0 | 1 | 0 | unused; shall be interpreted as "data", if received by the network |
| 1 | 0 | 1 | 1 | unused; shall be interpreted as "data", if received by the network |
|  | | | | |
| All other values are reserved. | | | | |
|  | | | | |

#### 9.10.3.47 Time zone

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

#### 9.10.3.48 Time zone and time

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

#### 9.10.3.49 Transparent container

Editor's note: The IE coding is FFS.

#### 9.10.3.50 UE security capability

The UE security capability information element is used by the network to indicate which security algorithms are supported by the UE in N1 mode and S1 mode for NAS security as well as which security algorithms are supported over NR and E-UTRA for AS security.

The UE security capability information element is coded as shown in figure 9.10.3.50.1 and table 9.10.3.50.1.

The UE security capability is a type 4 information element with a minimum length of 4 octets and a maximum length of 6 octets.

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

If the UE did not indicate support of any security algorithm for NAS security in S1 mode and did not indicate support of any security algorithm for AS security over E-UTRA, octets 5 and 6 shall not be included.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| UE security capability IEI | | | | | | | | | | | | | | | | octet 1 | |
| Length of UE security capability contents | | | | | | | | | | | | | | | | octet 2 | |
| 5G-EA0 | | 128-  5G-EA1 | | 128-  5G-EA2 | | 128-  5G-EA3 | | 5G-EA4 | | 5G-EA5 | | 5G-EA6 | | 5G-EA7 | | octet 3 | |
| 5G-IA0 | | 128-  5G-IA1 | | 128-  5G-IA2 | | 128-  5G-IA3 | | 5G-IA4 | | 5G-IA5 | | 5G-IA6 | | 5G-IA7 | | octet 4 | |
| EEA0 | | 128-  EEA1 | | 128-  EEA2 | | 128-  EEA3 | | EEA4 | | EEA5 | | EEA6 | | EEA7 | | octet 5\* | |
| EIA0 | | 128-  EIA1 | | 128-  EIA2 | | 128-  EIA3 | | EIA4 | | EIA5 | | EIA6 | | EIA7 | | octet 6\* | |

Figure 9.10.3.50.1: UE security capability information element

Table 9.10.3.50.1: UE security capability information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5GS encryption algorithms supported (see NOTE 1) (octet 3) | | | | | |
|  | | | | | |
| 5GS encryption algorithm 5G-EA0 supported (octet 3, bit 8) | | | | | |
| 0 | |  |  |  | 5GS encryption algorithm 5G-EA0 not supported |
| 1 | |  |  |  | 5GS encryption algorithm 5G-EA0 supported |
|  | | | | | |
| 5GS encryption algorithm 128-5G-EA1 supported (octet 3, bit 7) | | | | | |
| 0 | |  |  |  | 5GS encryption algorithm 128-5G-EA1 not supported |
| 1 | |  |  |  | 5GS encryption algorithm 128-5G-EA1 supported |
|  | | | | | |
| 5GS encryption algorithm 128-5G-EA2 supported (octet 3, bit 6) | | | | | |
| 0 | |  |  |  | 5GS encryption algorithm 128-5G-EA2 not supported |
| 1 | |  |  |  | 5GS encryption algorithm 128-5G-EA2 supported |
|  | | | | | |
| 5GS encryption algorithm 128-5G-EA3 supported (octet 3, bit 5) | | | | | |
| 0 | |  |  |  | 5GS encryption algorithm 128-5G-EA31 not supported |
| 1 | |  |  |  | 5GS encryption algorithm 128-5G-EA3 supported |
|  | | | | | |
| 5GS encryption algorithm 5G-EA4 supported (octet 3, bit 4) | | | | | |
| 0 | |  |  |  | 5GS encryption algorithm 5G-EA4 not supported |
| 1 | |  |  |  | 5GS encryption algorithm 5G-EA4 supported |
|  | | | | | |
| 5GS encryption algorithm 5G-EA5 supported (octet 3, bit 3) | | | | | |
| 0 | |  |  |  | 5GS encryption algorithm 5G-EA5 not supported |
| 1 | |  |  |  | 5GS encryption algorithm 5G-EA5 supported |
|  | | | | | |
| 5GS encryption algorithm 5G-EA6 supported (octet 3, bit 2) | | | | | |
| 0 | |  |  |  | 5GS encryption algorithm 5G-EA6 not supported |
| 1 | |  |  |  | 5GS encryption algorithm 5G-EA6 supported |
|  | | | | | |
| 5GS encryption algorithm 5G-EA7 supported (octet 3, bit 1) | | | | | |
| 0 | |  |  |  | 5GS encryption algorithm 5G-EA7 not supported |
| 1 | |  |  |  | 5GS encryption algorithm 5G-EA7 supported |
|  | | | | | |
| 5GS integrity algorithms supported (see NOTE 2) (octet 4) | | | | | |
|  | | | | | |
| 5GS integrity algorithm 5G-IA0 supported (octet 4, bit 8) | | | | | |
| 0 | |  |  |  | 5GS integrity algorithm 5G-IA0 not supported |
| 1 | |  |  |  | 5GS integrity algorithm 5G-IA0 supported |
|  | | | | | |
| 5GS integrity algorithm 128-5G-IA1 supported (octet 4, bit 7) | | | | | |
| 0 | |  |  |  | 5GS integrity algorithm 128-5G-IA1 not supported |
| 1 | |  |  |  | 5GS integrity algorithm 128-5G-IA1 supported |
|  | | | | | |
| 5GS integrity algorithm 128-5G-IA2 supported (octet 4, bit 6) | | | | | |
| 0 | |  |  |  | 5GS integrity algorithm 128-5G-IA2 not supported |
| 1 | |  |  |  | 5GS integrity algorithm 128-5G-IA2 supported |
|  | | | | | |
| 5GS integrity algorithm 128-5G-IA3 supported (octet 4, bit 5) | | | | | |
| 0 | |  |  |  | 5GS integrity algorithm 128-5G-IA3 not supported |
| 1 | |  |  |  | 5GS integrity algorithm 128-5G-IA3 supported |
|  | | | | | |
| 5GS integrity algorithm 5G-IA4 supported (octet 4, bit 4) | | | | | |
| 0 | |  |  |  | 5GS integrity algorithm 5G-IA4 not supported |
| 1 | |  |  |  | 5GS integrity algorithm 5G-IA4 supported |
|  | | | | | |
| 5GS integrity algorithm 5G-IA5 supported (octet 4, bit 3) | | | | | |
| 0 | |  |  |  | 5GS integrity algorithm 5G-IA5 not supported |
| 1 | |  |  |  | 5GS integrity algorithm 5G-IA5 supported |
|  | | | | | |
| 5GS integrity algorithm 5G-IA6supported (octet 4, bit 2) | | | | | |
| 0 | |  |  |  | 5GS integrity algorithm 5G-IA6 not supported |
| 1 | |  |  |  | 5GS integrity algorithm 5G-IA6 supported |
|  | | | | | |
| 5GS integrity algorithm 5G-IA7 supported (octet 4, bit 1) | | | | | |
| 0 | |  |  |  | 5GS integrity algorithm 5G-IA7 not supported |
| 1 | |  |  |  | 5GS integrity algorithm 5G-IA7 supported |
|  | | | | | |
| EPS encryption algorithms supported (see NOTE 3) (octet 5) | | | | | |
|  | | | | | |
| EPS encryption algorithm EEA0 supported (octet 5, bit 8) | | | | | |
| 0 | |  |  |  | EPS encryption algorithm EEA0 not supported |
| 1 | |  |  |  | EPS encryption algorithm EEA0 supported |
|  | | | | | |
| EPS encryption algorithm 128-EEA1 supported (octet 5, bit 7) | | | | | |
| 0 | |  |  |  | EPS encryption algorithm 128-EEA1 not supported |
| 1 | |  |  |  | EPS encryption algorithm 128-EEA1 supported |
|  | | | | | |
| EPS encryption algorithm 128-EEA2 supported (octet 5, bit 6) | | | | | |
| 0 | |  |  |  | EPS encryption algorithm 128-EEA2 not supported |
| 1 | |  |  |  | EPS encryption algorithm 128-EEA2 supported |
|  | | | | | |
| EPS encryption algorithm 128-EEA3 supported (octet 5, bit 5) | | | | | |
| 0 | |  |  |  | EPS encryption algorithm 128-EEA3 not supported |
| 1 | |  |  |  | EPS encryption algorithm 128-EEA3 supported |
|  | | | | | |
| EPS encryption algorithm EEA4 supported (octet 5, bit 4) | | | | | |
| 0 | |  |  |  | EPS encryption algorithm EEA4 not supported |
| 1 | |  |  |  | EPS encryption algorithm EEA4 supported |
|  | | | | | |
| EPS encryption algorithm EEA5 supported (octet 5, bit 3) | | | | | |
| 0 | |  |  |  | EPS encryption algorithm EEA5 not supported |
| 1 | |  |  |  | EPS encryption algorithm EEA5 supported |
|  | | | | | |
| EPS encryption algorithm EEA6 supported (octet 5, bit 2) | | | | | |
| 0 | |  |  |  | EPS encryption algorithm EEA6 not supported |
| 1 | |  |  |  | EPS encryption algorithm EEA6 supported |
|  | | | | | |
| EPS encryption algorithm EEA7 supported (octet 5, bit 1) | | | | | |
| 0 | |  |  |  | EPS encryption algorithm EEA7 not supported |
| 1 | |  |  |  | EPS encryption algorithm EEA7 supported |
|  | | | | | |
| EPS integrity algorithms supported (see NOTE 4) (octet 6) | | | | | |
|  | | | | | |
| EPS integrity algorithm EIA0 supported (octet 6, bit 8) | | | | | |
| 0 | |  |  |  | EPS integrity algorithm EIA0 not supported |
| 1 | |  |  |  | EPS integrity algorithm EIA0 supported |
|  | | | | | |
| EPS integrity algorithm 128-EIA1 supported (octet 6, bit 7) | | | | | |
| 0 | |  |  |  | EPS integrity algorithm 128-EIA1 not supported |
| 1 | |  |  |  | EPS integrity algorithm 128-EIA1 supported |
|  | | | | | |
| EPS integrity algorithm 128-EIA2 supported (octet 6, bit 6) | | | | | |
| 0 | |  |  |  | EPS integrity algorithm 128-EIA2 not supported |
| 1 | |  |  |  | EPS integrity algorithm 128-EIA2 supported |
|  | | | | | |
| EPS integrity algorithm 128-EIA3 supported (octet 6, bit 5) | | | | | |
| 0 | |  |  |  | EPS integrity algorithm 128-EIA3 not supported |
| 1 | |  |  |  | EPS integrity algorithm 128-EIA3 supported |
|  | | | | | |
| EPS integrity algorithm EIA4 supported (octet 6, bit 4) | | | | | |
| 0 | |  |  |  | EPS integrity algorithm EIA4 not supported |
| 1 | |  |  |  | EPS integrity algorithm EIA4 supported |
|  | | | | | |
| EPS integrity algorithm EIA5 supported (octet 6, bit 3) | | | | | |
| 0 | |  |  |  | EPS integrity algorithm EIA5 not supported |
| 1 | |  |  |  | EPS integrity algorithm EIA5 supported |
|  | | | | | |
| EPS integrity algorithm EIA6 supported (octet 6, bit 2) | | | | | |
| 0 | |  |  |  | EPS integrity algorithm EIA6 not supported |
| 1 | |  |  |  | EPS integrity algorithm EIA6 supported |
|  | | | | | |
| EPS integrity algorithm EIA7 supported (octet 6, bit 1) | | | | | |
| 0 | |  |  |  | EPS integrity algorithm EIA7 not supported |
| 1 | |  |  |  | EPS integrity algorithm EIA7 supported |
|  | | | | | |
| NOTE 1: The code points in octet 3 are used to indicate support for 5GS encryption algorithms for NAS security in N1 mode and support for 5GS encryption algorithms for AS security over NR.  NOTE 2: The code points in octet 4 are used to indicate support for 5GS integrity algorithms for NAS security in N1 mode and support for 5GS integrity algorithms for AS security over NR.  NOTE 3: The code points in octet 5 are used to indicate support for EPS encryption algorithms for NAS security in S1 mode and support for EPS encryption algorithms for AS security over E-UTRA.  NOTE 4: The code points in octet 6 are used to indicate support for EPS integrity algorithms for NAS security in S1 mode and support for EPS integrity algorithms for AS security over E-UTRA. | | | | | |

#### 9.10.3.51 UE's usage setting

The purpose of the UE's usage setting information element is to provide the network with the UE's usage setting as defined in 3GPP TS 24.301 [15]. The network uses the UE's usage setting to select the RFSP index.

The UE's usage setting information element is coded as shown in figure 9.10.3.51.1 and table 9.10.3.51.1.

The UE's usage setting is a type 4 information element with a length of 3 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| UE's usage setting IEI | | | | | | | | | | | | | | | | octet 1 | |
| Length of UE's usage setting contents | | | | | | | | | | | | | | | | octet 2 | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | UE's usage setting | | octet 3 | |

Figure 9.10.3.51.1: UE's usage setting information element

Table 9.10.3.51.1: UE's usage setting information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| UE's usage setting (octet 3, bit 1) | | | | | |
| 0 | |  |  |  | voice centric |
| 1 | |  |  |  | data centric |
|  | | | | | |
| All other bits in the octet 3 are spare and shall be coded as zero, | | | | | |

#### 9.10.3.52 UE status

The purpose of the UE status information element is to provide the network with information concerning aspects of the current UE registration status which is used for interworking with EPS.

The UE status information element is coded as shown in figure 9.10.3.52.1 and table 9.10.3.52.1.

The UE status is a type 4 information element with a length of 3 octets.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
| UE status IEI | | | | | | | | | | | | | | | | octet 1 | |
| Length of UE status contents | | | | | | | | | | | | | | | | octet 2 | |
| 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | 0  Spare | | N1 mode reg | | S1 mode reg | | octet 3 | |

Figure 9.10.3.52.1: UE status information element

Table 9.10.3.52.1: UE status information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| EMM registration status (S1 mode reg) (octet 3, bit 1) | | | | | |
| 0 | |  |  |  | UE is not in EMM-REGISTERED state |
| 1 | |  |  |  | UE is in EMM-REGISTERED state |
|  | | | | | |
| 5GMM registration status (N1 mode reg) (octet 3, bit 2) | | | | | |
| 0 | |  |  |  | UE is not in 5GMM-REGISTERED state |
| 1 | |  |  |  | UE is in 5GMM-REGISTERED state |
|  | | | | | |
| All other bits in the octet 3 are spare and shall be coded as zero. | | | | | |

#### 9.10.3.53 Uplink data status

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

The Uplink data status information element is coded as shown in figure 9.10.3.53.1 and table 9.10.3.53.1.

The Uplink data status information element is a type 4 information element with minimum length of 4 octets a maximum length of 34 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Uplink data status IEI | | | | | | | | octet 1 |
| Length of uplink data status contents | | | | | | | | octet 2 |
| PSI  (7) | PSI  (6) | PSI  (5) | PSI  (4) | PSI  (3) | PSI  (2) | PSI  (1) | PSI  (0) | octet 3 |
| PSI  (15) | PSI  (14) | PSI  (13) | PSI  (12) | PSI  (11) | PSI  (10) | PSI  (9) | PSI  (8) | octet 4 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  |
| spare | | | | | | | | octet 5\* -34\* |

Figure 9.10.3.53.1: Uplink data status information element

Table 9.10.3.53.1: Uplink data status information element

|  |
| --- |
| PSI(x) shall be coded as follows:  PSI(0):  Bit 1 of octet 3 is spare and shall be coded as zero.  PSI(1) – PSI(15):  0 indicates that no uplink data are pending for the corresponding PDU session identity.  1 indicates that uplink data are pending for the corresponding PDU session identity.  All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element. |

### 9.10.4 5GS session management (5GSM) information elements

#### 9.10.4.1 5GSM capability

The purpose of the 5GSM capability information element is to indicate UE capability related to the PDU session management.

The 5GSM capability information element is coded as shown in figure 9.10.4.1.1 and table 9.10.4.1.1.

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 | | 0  Spare | | 0  Spare | | 0  Spare | | MH6-PDU | | RqoS | | octet 3 | |
| 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | octet 4\* -15\* | |
| Spare | | | | | | | | | | | | | | | |

Figure 9.10.4.1.1: 5GSM capability information element

Table 9.10.4.1.1: 5GSM capability information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 5GSM capability value | | | | | |
| RqoS(octet 3, bit 1) | | | | | |
| This bit indicates the 5GSM capability to support reflective QoS. | | | | | |
| 0 | |  |  |  | Reflective QoS not supported |
| 1 | |  |  |  | Reflective QoS supported |
|  | | | | | |
| Multi-homed IPv6 PDU session (MH6-PDU) (octet 3, bit 2) | | | | | |
| This bit indicates the 5GSM capability for Multi-homed IPv6 PDU session. | | | | | |
| 0 | |  |  |  | Multi-homed IPv6 PDU session not supported |
| 1 | |  |  |  | Multi-homed IPv6 PDU session supported |
|  | | | | | |
| All other bits in octet 3 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | | |
|  | | | | | |

#### 9.10.4.2 5GSM cause

The purpose of the 5GSM cause information element is to indicate the reason why a 5GSM request is rejected.

The 5GSM cause information element is coded as shown in figure 9.10.4.2.1 and table 9.10.4.2.1.

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

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

Figure 9.10.4.2.1: 5GSM cause information element

Table 9.10.4.2.1: 5GSM cause information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cause value (octet 2) | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |  | Insufficient resources |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |  | Missing or unknown DNN |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |  | Unknown PDU session type |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |  | User authentication failed |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |  | Request rejected, unspecified |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |  | Service option temporarily out of order |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |  | Requested service option not subscribed |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |  | Service option temporarily out of order |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |  | PTI already in use |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |  | Regular deactivation |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |  | Reactivation requested |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |  | PDU session type IPv4 only allowed |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |  | PDU session type IPv6 only allowed |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |  | Insufficient resources for specific slice and DNN |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |  | Not supported SSC mode |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |  | Insufficient resources for specific slice |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |  | Missing or unknown DNN in a slice |
| 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |  | Invalid PTI value |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |  | Semantically incorrect message |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |  | Invalid mandatory information |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |  | Message type non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |  | Message type not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |  | Information element non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |  | Conditional IE error |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |  | Message not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |  | Protocol error, unspecified |
|  |  |  |  |  |  |  |  |  |  |
| Any other value received by the UE shall be treated as 0010 0010, "service option temporarily out of order". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified". | | | | | | | | | |

#### 9.10.4.3 Allowed SSC mode

The purpose of the Allowed SSC mode information element is to indicate the SSC modes allowed to be used by the UE for the PDU session.

The Allowed SSC mode information element is coded as shown in figure 9.10.4.3.1 and table 9.10.4.3.1.

The Allowed SSC mode is a type 1 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Allowed SSC mode IEI | | | | 0  Spare | SSC3 | SSC2 | SSC1 | octet 1 |

Figure 9.10.4.3.1: Allowed SSC mode information element

Table 9.10.4.3.1: Allowed SSC mode information element

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

#### 9.10.4.4 Extended protocol configuration options

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

#### 9.10.4.5 Mapped EPS bearer contexts

The purpose of the mapped EPS bearer contexts information element is to indicate a set of EPS contexts for a PDU session context, as described in subclause 6.1.4.1.

The mapped EPS bearer contexts information element is a type 6 information element with a minimum length of 7 octet and a maximum length of 65538 octets.

The mapped EPS bearer contextsinformation element is coded as shown in figure 9.10.4.5.1, figure 9.10.4.5.2, figure 9.10.4.5.3 and table 9.10.4.5.1.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 9.10.4.5.1: 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 | | DEB  bit | | | E bit | | Number of EPS parameters | | | | octet 7 | |
|  | | EPS parameters list | | | | | | | | | | | octet 8 |
|  | | octet u |

Figure 9.10.4.5.2: Mapped EPS bearer context

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | | EPS parameter identifier 1 | | | | | | | | | | octet 6 | |
|  | | Length of EPS parameter contents 1 | | | | | | | | | | octet 7 | |
|  | | EPS parameter contents 1 | | | | | | | | | | octet 8  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 x | |

Figure 9.10.4.5.3: EPS parameters list

Table 9.10.4.5.1: Mapped EPS bearer contexts information element

|  |
| --- |
| EPS bearer identity (octet 4)  The EPS bearer identity is used to identity the EPS bearer, and is coded as specified in subclause 9.3.2 of 3GPP TS 24.301 [15].  Operation code (bits 8 to 7 of octet 7) Bits 8 7  0 0 Reserved 0 1 Create new EPS bearer  1 0 Delete existing EPS bearer  1 1 Modify existing EPS bearer  DEB bit (bit 6 of octet 7)  The DEB bit indicates whether the EPS bearer is the default EPS bearer and it is encoded as follows:  Bit  6  0 the EPS bearer is not the default EPS bearer.  1 the EPS bearer is the default EPS bearer.  E bit (bit 5 of octet 7)  For the "create new EPS bearer" operation, the E bit is encoded as follows:  Bit 5  0 parameters list is not included  1 parameters list is included  For the "modify existing EPS bearer" operation, the E bit is encoded as follows:  Bit 5  0 previously provided parameters list extension  1 previously provided parameters list replacement  If the E bit is set to "parameters list is not included", the number of EPS parameters field has zero value. If the E bit is set to "parameters list is included", the number of EPS parameters field has non-zero value. If the E bit is set to "previously provided parameters list extension" or "previously provided parameters list replacement", the number of parameters field can have zero or non-zero value.  Number of EPS parameters (bits 4 to 1 of octet 7)  The number of EPS parameters contains the binary coding for the number of EPS parameters in the EPS parameters list field. The number of EPS parameters field is encoded in bits 5 through 1 of octet x+1 where bit 5 is the most significant and bit 1 is the least significant bit.  EPS parameters list (octets 8 to u)  The EPS parameters list contains a variable number of EPS parameters.  Each EPS parameter included in the EPS parameters list is of variable length and consists of:  - an EPS parameter identifier (1 octet);  - the length of the EPS parameter contents (1 octet); and - the EPS parameter contents itself (variable amount of octets).  The EPS parameter identifier field is used to identify each EPS parameter included in the EPS parameters list and it contains the hexadecimal coding of the EPS parameter identifier. Bit 8 of the EPS parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following EPS parameter identifiers are specified:  - 01H (Mapped EPS QoS parameters); - 02H (Mapped extended EPS QoS parameters); and  - 03H (Traffic flow template).  - 04H (APN-AMBR).  - 05H (extended APN-AMBR).  If the EPS parameters list contains an EPS parameter identifier that is not supported by the receiving entity the corresponding EPS parameter shall be discarded.  The length of EPS parameter contents field contains the binary coded representation of the length of the EPS parameter contents field. The first bit in transmission order is the most significant bit.  When the parameter identifier indicates mapped EPS QoS parameters, the length and parameter contents field are coded as specified in subclause 9.9.4.3 of 3GPP TS 24.301 [15].  When the parameter identifier indicates mapped extended EPS QoS parameters, the length and parameter contents field are coded as specified in subclause 9.9.4.30 of 3GPP TS 24.301 [15].  When the parameter identifier indicates traffic flow template, the length and parameter contents field are coded from octet 2 as shown figure 10.5.144 and table 10.5.162 of 3GPP TS 24.008 [12].  When the parameter identifier indicates APN-AMBR, the length and parameter contents field are coded as specified in subclause 9.9.4.2 of 3GPP TS 24.301 [15].  When the parameter identifier indicates Extended APN-AMBR, the length and parameter contents field are coded as specified in subclause 9.9.4.29 of 3GPP TS 24.301 [15]. |

#### 9.10.4.6 Maximum number of supported packet filters

The purpose of the Maximum number of supported packet filters information element is for the UE to indicate to the network the maximum number of packet filters, associated with signaled QoS rules, that can be supported by the UE for the PDU session that is being established, when the PDU session type "IPv4", "IPv6", "IPv4v6" or "Ethernet".

The Maximum number of supported packet filters is coded as shown in figure 9.10.4.6.1 and table 9.10.4.6.2.

The Maximum number of supported packet filters is a type 3 information element with a length of 3 octets.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |  | |
| Maximum number of supported packet filters IEI | | | | | | | | | octet 1 | |
| Maximum number of supported packet filters | | | | | | | | | octet 2 | |
| octet 3 | |

Figure 9.10.4.6.1: Maximum number of supported packet filters information element

Table 9.10.4.6.2: Maximum number of supported packet filters information element

|  |
| --- |
| Maximum number of supported packet filters (octet 2 to 3) |
| In the Maximum number of supported packet filters field bit 8 of the first octet is the most significant bit and bit 7 of second octet is the least significant bit. Bit 6 to bit 1 of the second octet are spare bits and shall be coded as zero.  The number of supported packet filters shall be in the range of 17 to 1024. |
|  |

#### 9.10.4.7 PDU address

The purpose of the PDU address information element is to assign to the UE:

- an IPv4 address associated with a PDU session;

- an interface identifier for the IPv6 link local address associated with the PDU session; or

- an IPv4 address and an interface identifier for the IPv6 link local address, associated with the PDU session.

The PDU address information element is coded as shown in figure 9.10.4.7.1 and table 9.10.4.7.1.

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 11 | |

Figure 9.10.4.7.1: PDU address information element

Table 9.10.4.7.1: PDU address information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PDU session type value (octet 3) | | | | | |
| Bits | | | | | |
| 3 | | 2 | 1 |  |  |
| 0 | | 0 | 1 |  | IPv4 |
| 0 | | 1 | 0 |  | IPv6 |
| 0 | | 1 | 1 |  | IPv4v6 |
|  | | | | | |
| All other values are reserved. | | | | | |
|  | | | | | |
| Bit 4 to 8 of octet 3 are spare and shall be coded as zero. | | | | | |
|  | | | | | |
| PDU address information (octet 4 to 15) | | | | | |
|  | | | | | |
| If the PDU session type value indicates IPv4, the PDU address information in octet 4 to octet 7 contains an IPv4 address. | | | | | |
|  | | | | | |
| If the PDU session type value indicates IPv6, the PDU address information in octet 4 to octet 11 contains an interface identifier for the IPv6 link local address. | | | | | |
|  | | | | | |
| If the PDU session type value indicates IPv4v6, the PDU address information in octet 4 to octet 11 contains an interface identifier for the IPv6 link local address and in octet 12 to octet 15 contains an IPv4 address. | | | | | |

#### 9.10.4.8 PDU session type

The purpose of the PDU session type information element is to indicate type of the PDU session.

The PDU session type information element is coded as shown in figure 9.10.4.8.1 and table 9.10.4.8.1.

The PDU session type is a type 1 information element.

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

Figure 9.10.4.8.1: PDU session type information element

Table 9.10.4.8.1: PDU session type information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| PDU session type value (octet 1, bit 1 to bit 3) | | | | | |
| Bits | | | | | |
| 3 | | 2 | 1 |  |  |
| 0 | | 0 | 1 |  | IPv4 |
| 0 | | 1 | 0 |  | IPv6 |
| 0 | | 1 | 1 |  | IPv4v6 |
| 1 | | 0 | 0 |  | Unstructured |
| 1 | | 0 | 1 |  | Ethernet |
| 1 | | 1 | 1 |  | reserved |
|  | | | | | |
| All other values are unused and shall be interpreted as "IPv4v6", if received by the UE or the network. | | | | | |

#### 9.10.4.9 QoS rules

The purpose of the QoS 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 9.10.4.9.1, figure 9.10.4.9.2, figure 9.10.4.9.3, figure 9.10.4.9.4, figure 9.10.4.9.5 and table 9.10.4.9.1.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 9.10.4.9.1: 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 z |
|  | 0  Spare | E | Number of parameters | | | | | | | | octet z+1 |
|  | Parameters list | | | | | | | | | | octet z+2\*  octet m |
|  | QoS rule precedence | | | | | | | | | | octet m+1\* |
|  | 0  Spare | 0  Spare | QoS flow identifier (QFI) | | | | | | | | octet m+2\* |

Figure 9.10.4.9.2: 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 9.10.4.9.3: 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 9.10.4.9.4: Packet filter list when the rule operation is "create new QoS rule", or "modify existing QoS rule and add packet filters" or "modify existing QoS rule and replace packet filters"

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
|  | Parameter identifier 1 | | | | | | | | octet z+2 |
|  | Length of Parameter contents 1 | | | | | | | | octet z+3 |
|  | Parameter contents 1 | | | | | | | | octet z+4  octet k |
|  | Parameter identifier 2 | | | | | | | | octet k+1 |
|  | Length of Parameter contents 2 | | | | | | | | octet k+2 |
|  | Parameter contents 2 | | | | | | | | octet k+3  octet p |
|  | … | | | | | | | | octet p+1  octet q |
|  | Parameter identifier N | | | | | | | | octet q+1 |
|  | Length of Parameter contents N | | | | | | | | octet q+2 |
|  | Parameter contents N | | | | | | | | octet q+3  octet m |

Figure 9.10.4.9.5: Parameters list

Table 9.10.4.9.1: QoS rules information element

|  |
| --- |
| QoS rule identifier (octet 4)  The QoS rule identifier field is used to identify the QoS rule.  QoS rule precedence (octet m+1)  The QoS rule precedence field is used to specify the precedence of the QoS rule among all QoS rules (both the signalled QoS rules as described in subclause 6.2.5.1.1.2 and the derived QoS rules as described in subclause 6.2.5.1.1.3) associated with the PDU session of the QoS flow. This field includes the binary coded value of the QoS rule precedence in the range from 0 to 255 (decimal). The higher the value of the QoS rule precedence field, the lower the precedence of that QoS rule is.  The value 80 (decimal) is reserved.  QoS flow identifier (QFI) (bits 6 to 1 of octet m+2)  The QoS flow identifier (QFI) field contains the QoS flow identifier.  Bits  6 5 4 3 2 1  0 0 0 0 0 0 QFI 0  to  1 1 1 1 1 1 QFI 63  DQR bit (bit 5 of octet 7)  The DQR bit indicates whether the QoS rule is the default QoS rule and it is encoded as follows:  Bit  5  0 the QoS rule is not the default QoS rule.  1 the QoS rule is the default QoS rule.  Rule operation code (bits 8 to 6 of octet 7) Bits 8 7 6  0 0 0 Reserved 0 0 1 Create new QoS rule  0 1 0 Delete existing QoS rule  0 1 1 Modify existing QoS rule and add packet filters  1 0 0 Modify existing QoS rule and replace packet filters  1 0 1 Modify existing QoS rule and delete packet filters  1 1 0 Modify existing QoS rule without modifying packet filters  1 1 1 Reserved  E bit (bit 7 of octet z+1)  For the "create new QoS rule" operation, the E bit is encoded as follows:  Bit 7  0 parameters list is not included  1 parameters list is included  For the "modify existing QoS rule and add packet filters" operation, the "modify existing QoS rule and replace packet filters", the "modify existing QoS rule and delete packet filters" operation and the "modify existing QoS rule without modifying packet filters" operation, the E bit is encoded as follows:  Bit 7  0 previously provided parameters list extension  1 previously provided parameters list replacement  If the E bit is set to "parameters list is not included", the number of parameters field has zero value. If the E bit is set to "parameters list is included", the number of parameters field has non-zero value. If the E bit is set to "previously provided parameters list extension" or "previously provided parameters list replacement", the number of parameters field can have zero or non-zero value.  Number of packet filters (bits 4 to 1 of octet 7)  The number of packet filters contains the binary coding for the number of packet filters in the packet filter list. The number of packet filters field is encoded in bits 4 through 1 of octet 7 where bit 4 is the most significant and bit 1 is the least significant bit. For the "delete existing QoS rule" operation and for the "modify existing QoS rule without modifying packet filters" operation, the number of packet filters shall be coded as 0. For the "create new QoS rule" operation and the "modify existing QoS rule and replace packet filters" operation, the number of packet filters shall be greater than or equal to 0 and less than or equal to 15. For all other operations, the number of packet filters shall be greater than 0 and less than or equal to 15.  Packet filter list (octets 8 to z)  The packet filter list contains a variable number of packet filters.  For the "delete existing QoS rule" operation, the length of QoS rule field is set to one.  For the "delete existing QoS rule" operation and the "modify existing QoS rule without modifying packet filters" operation, the packet filter list shall be empty.  For the "modify existing QoS rule and delete packet filters" operation, the packet filter list shall contain a variable number of packet filter identifiers. This number shall be derived from the coding of the number of packet filters field in octet 7.  For the "create new QoS rule" operation and for the "modify existing QoS rule and replace packet filters" operation, the packet filter list shall contain 0 or a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.  For the "modify existing QoS rule and add packet filters" operation, the packet filter list shall contain a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.  Each packet filter is of variable length and consists of  a packet filter direction (2 bits);  - a packet filter identifier (4 bits);  - the length of the packet filter contents (1 octet); and - the packet filter contents itself (variable amount of octets).  The packet filter direction field is used to indicate for what traffic direction the filter applies.  Bits  6 5  0 0 reserved  0 1 downlink only  1 0 uplink only  1 1 bidirectional (see NOTE 1)  The packet filter identifier field is used to identify each packet filter in a QoS rule. The least significant 4 bits are used.  The length of the packet filter contents field contains the binary coded representation of the length of the packet filter contents field of a packet filter. The first bit in transmission order is the most significant bit.  The packet filter contents field is of variable size and contains a variable number (at least one) of packet filter components. Each packet filter component shall be encoded as a sequence of a one octet packet filter component type identifier and a fixed length packet filter component value field. The packet filter component type identifier shall be transmitted first.  In each packet filter, there shall not be more than one occurrence of each packet filter component type. Among the "IPv4 remote address type" and "IPv6 remote address/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "IPv4 local address type" and "IPv6 local address/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "single local port type" and "local port range type" packet filter components, only one shall be present in one packet filter. Among the "single remote port type" and "remote port range type" packet filter components, only one shall be present in one packet filter. If the "match-all type" packet filter component is present in the packet filter, no other packet filter component shall be present in the packet filter and the length of the packet filter contents field shall be set to one.  The term local refers to the UE and the term remote refers to an external network entity.  Packet filter component type identifier Bits 8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 1 Match-all type 0 0 0 1 0 0 0 0 IPv4 remote address type 0 0 0 1 0 0 0 1 IPv4 local address type  0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type 0 0 1 0 0 0 1 1 IPv6 local address/prefix length type 0 0 1 1 0 0 0 0 Protocol identifier/Next header type 0 1 0 0 0 0 0 0 Single local port type 0 1 0 0 0 0 0 1 Local port range type 0 1 0 1 0 0 0 0 Single remote port type  0 1 0 1 0 0 0 1 Remote port range type 0 1 1 0 0 0 0 0 Security parameter index type 0 1 1 1 0 0 0 0 Type of service/Traffic class type 1 0 0 0 0 0 0 0 Flow label type  1 0 0 0 0 0 0 1 Destination MAC address type 1 0 0 0 0 0 1 0 Source MAC address type 1 0 0 0 0 0 1 1 802.1Q C-TAG VID type 1 0 0 0 0 1 0 0 802.1Q S-TAG VID type 1 0 0 0 0 1 0 1 802.1Q C-TAG PCP/DEI type 1 0 0 0 0 1 1 0 802.1Q S-TAG PCP/DEI type 1 0 0 0 0 1 1 1 Ethertype type  All other values are reserved.  The description and valid combinations of packet filter component type identifiers in a packet filter are defined in 3GPP TS 23.501 [8].  For "match-all type", the packet filter component shall not include the packet filter component value field.  For "IPv4 remote address type", the packet filter component value field shall be encoded as a sequence of a four octet IPv4 address field and a four octet IPv4 address mask field. The IPv4 address field shall be transmitted first.  For "IPv4 local address type", the packet filter component value field shall be encoded as defined for "IPv4 remote address type".  For "IPv6 remote address/prefix length type", the packet filter component value field shall be encoded as a sequence of a sixteen octet IPv6 address field and one octet prefix length field. The IPv6 address field shall be transmitted first.  For "IPv6 local address/prefix length type", the packet filter component value field shall be encoded as defined for "IPv6 remote address /prefix length".  For "protocol identifier/Next header type", the packet filter component value field shall be encoded as one octet which specifies the IPv4 protocol identifier or Ipv6 next header.  For "single local port type" and "single remote port type", the packet filter component value field shall be encoded as two octets which specify a port number.  For "local port range type" and "remote port range type", the packet filter component value field shall be encoded as a sequence of a two octet port range low limit field and a two octet port range high limit field. The port range low limit field shall be transmitted first.  For "security parameter index", the packet filter component value field shall be encoded as four octets which specify the IPSec security parameter index.  For "type of service/traffic class type", the packet filter component value field shall be encoded as a sequence of a one octet type-of-service/traffic class field and a one octet type-of-service/traffic class mask field. The type-of-service/traffic class field shall be transmitted first.  For "flow label type", the packet filter component value field shall be encoded as three octets which specify the IPv6 flow label. The bits 8 through 5 of the first octet shall be spare whereas the remaining 20 bits shall contain the IPv6 flow label.  For "destination MAC address type" and "source MAC address type", the packet filter component value field shall be encoded as 6 octets which specify a MAC address.  For "802.1Q C-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the customer-VLAN tag (C-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.  For "802.1Q S-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the service-VLAN tag (S-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.  For "802.1Q C-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q C-TAG PCP and DEI. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.  For "802.1Q S-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q S-TAG PCP. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.  For "ethertype type", the packet filter component value field shall be encoded as two octets which specify an ethertype.  Number of parameters (bits 6 to 1 of octet z+1)  The number of parameters field contains the binary coding for the number of parameters in the parameters list field. The number of parameters field is encoded in bits 6 through 1 of octet z+1 where bit 6 is the most significant and bit 1 is the least significant bit.  Parameters list (octets z+2 to v)  The parameters list contains a variable number of parameters.  Each parameter included in the parameters list is of variable length and consists of:  - a parameter identifier (1 octet);  - the length of the parameter contents (1 octet); and - the parameter contents itself (variable amount of octets).  The parameter identifier field is used to identify each parameter included in the parameters list and it contains the hexadecimal coding of the parameter identifier. Bit 8 of the parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following parameter identifiers are specified:  - 01H (5QI); - 02H (GFBR uplink);  - 03H (GFBR downlink);  - 04H (MFBR uplink);  - 05H (MFBR downlink);  - 06H (Averaging window); and  - 07H (EPS bearer identity).  If the parameters list contains a parameter identifier that is not supported by the receiving entity the corresponding parameter shall be discarded.  The length of parameter contents field contains the binary coded representation of the length of the parameter contents field. The first bit in transmission order is the most significant bit.  When the parameter identifier indicates 5QI, the parameter contents field contains the binary representation of 5G QoS identifier (5QI) that is one octet in length.  5QI:  Bits  8 7 6 5 4 3 2 1  In network to UE direction:  0 0 0 0 0 0 0 0 Reserved  0 0 0 0 0 0 0 1 5QI 1  0 0 0 0 0 0 1 0 5QI 2  0 0 0 0 0 0 1 1 5QI 3  0 0 0 0 0 1 0 0 5QI 4  0 0 0 0 0 1 0 1 5QI 5  0 0 0 0 0 1 1 0 5QI 6  0 0 0 0 0 1 1 1 5QI 7  0 0 0 0 1 0 0 0 5QI 8  0 0 0 0 1 0 0 1 5QI 9  0 0 0 0 1 0 1 0  to Spare  0 1 0 0 0 0 0 0  0 1 0 0 0 0 0 1 5QI 65  0 1 0 0 0 0 1 0 5QI 66  0 1 0 0 0 0 1 1  to Spare  0 1 0 0 0 1 0 0  0 1 0 0 0 1 0 1 5QI 69  0 1 0 0 0 1 1 0 5QI 70  0 1 0 0 0 1 1 1  to Spare  0 1 0 0 1 0 1 0  0 1 0 0 1 0 1 1 5QI 75  0 1 0 0 1 1 0 0  to Spare  0 1 0 0 1 1 1 0  0 1 0 0 1 1 1 1 5QI 79  0 1 0 1 0 0 0 0  to Spare  0 1 1 1 1 1 1 1  1 0 0 0 0 0 0 0  to Operator-specific 5Qis  1 1 1 1 1 1 1 0  1 1 1 1 1 1 1 1 Reserved  The network shall consider all other values not explicitly defined in this version of the protocol as unsupported.  If the UE receives a 5QI value (excluding the reserved 5QI values) that it does not understand, the UE shall choose a 5QI value from the set of 5QI values defined in this version of the protocol (see 3GPP TS 23.501 [8]) and associated with:  - GBR QoS flows, if the QoS flow includes a GFBR uplink parameter and a GFBR downlink parameter; and  - non-GBR QoS flows, if the QoS flow does not include a GFBR uplink parameter or does not include a GFBR downlink parameter.  The UE shall use this chosen 5QI value for internal operations only. The UE shall use the received 5QI value in subsequent NAS signalling procedures.  When the parameter identifier indicates "GFBR uplink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for uplink followed by two octets containing the value of the guaranteed flow bit rate for uplink.  Unit of the guaranteed flow bit rate for uplink (octet 1)  Bits  8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 0 0 value is not used  0 0 0 0 0 0 0 0 1 value is incremented in multiples of 1 Kbps  0 0 0 0 0 0 0 1 0 value is incremented in multiples of 4 Kbps  0 0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps  0 0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps  0 0 0 0 0 0 1 0 1 value is incremented in multiples of 256 Kbps  0 0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps  0 0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps  0 0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps  0 0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps  0 0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps  0 0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps  0 0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps  0 0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps  0 0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps  0 0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps  0 0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps  0 0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps  0 0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps  0 0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps  0 0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps  0 0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps  0 0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps  0 0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps  0 0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps  0 0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps  Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol.  Value of the guaranteed flow bit rate for uplink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for uplink in units defined by the unit of the guaranteed flow bit rate for uplink.  When the parameter identifier indicates "GFBR downlink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for downlink followed by two octets containing the value of the guaranteed flow bit rate for downlink.  Unit of the guaranteed flow bit rate for downlink (octet 1)  The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.  Value of the guaranteed flow bit rate for downlink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for downlink in units defined by the unit of the guaranteed flow bit rate for downlink.  When the parameter identifier indicates "MFBR uplink", the parameter contents field contains the one octet indicating the unit of the maximum flow bit rate for uplink followed by two octets containing the value of maximum flow bit rate for uplink.  Unit of the maximum flow bit rate for uplink (octet 1)  The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.  Value of the maximum flow bit rate for uplink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for uplink in units defined by the unit of the maximum flow bit rate for uplink.  When the parameter identifier indicates "MFBR downlink", the parameter contents field contains one octet indicating the unit of the maximum flow bit rate for downlink followed by two octets containing the value of the maximum flow bit rate for downlink.  Unit of the maximum flow bit rate for downlink (octet 1)  The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.  Value of the maximum flow bit rate for downlink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for downlink in units defined by the unit of the maximum flow bit rate for downlink.  When the parameter identifier indicates "averaging window", the parameter contents field contains the binary representation of the averaging window for both uplink and downlink in milliseconds and the parameter contents field is two octets in length.  When the parameter identifier indicates EPS bearer identity, the length of EPS bearer identity is one octet and parameter contents field is coded as specified in subclause 9.3.2 of 3GPP TS 24.301 [15] (see NOTE 2). The UE shall not include the EPS bearer identity parameter in any UE initiated 5GSM messages. |
| NOTE 1: A packet filter with the "bidirectional" packet filter direction is used both as a packet filter with the "downlink only" packet filter direction and a packet filter with the "uplink only" packet filter direction.  NOTE 2: The total number of EPS bearer identities included in all QoS rules of a UE cannot exceed eleven. |

#### 9.10.4.10 Session-AMBR

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

The Session-AMBR information element is coded as shown in figure 9.10.4.10.1 and table 9.10.4.10.1.

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

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

Figure 9.10.4.10.1: Session-AMBR information element

Table 9.10.4.10.1: Session-AMBR information element

|  |
| --- |
| Unit for Session-AMBR for downlink (octet 3)  0 0 0 0 0 0 0 0 value is not used  0 0 0 0 0 0 0 1 value is incremented in multiples of 1 Kbps  0 0 0 0 0 0 1 0 value is incremented in multiples of 4 Kbps  0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps  0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps  0 0 0 0 0 1 0 1 value is incremented in multiples of 256 kbps  0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps  0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps  0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps  0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps  0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps  0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps  0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps  0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps  0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps  0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps  0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps  0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps  0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps  0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps  0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps  0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps  0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps  0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps  0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps  0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps  Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol.  Session-AMBR for downlink (octets 4 and 5)  Octets 4 and 5 represent the binary coded value of PDU session aggregated maximum bit rate for downlink in units defined by octet 3.  Unit for Session-AMBR for uplink (octet 6)  The coding is identical to the unit coding defined for Session-AMBR for downlink (octet 3)  Session-AMBR for uplink (octets 7 and 8)  Octets 7 and 8 represent the binary coded value of PDU session aggregated maximum bit rate for uplink in units defined by octet 6. |

#### 9.10.4.11 SM PDU DN request container

The SM PDU DN request container contains a DN-specific identity of the UE in the network access identifier (NAI) format.

#### 9.10.4.12 SSC mode

The purpose of the SSC mode information element is to indicate SSC mode.

The SSC mode information element is coded as shown in figure 9.10.4.12.1 and table 9.10.4.12.1.

The SSC mode is a type 1 information element.

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

Figure 9.10.4.12.1: SSC mode information element

Table 9.10.4.12.1: SSC mode information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| SSC mode value (octet 1, bit 1 to bit 4) | | | | | |
| Bits | | | | | |
| 3 | | 2 | 1 |  |  |
| 0 | | 0 | 1 |  | SSC mode 1 |
| 0 | | 1 | 0 |  | SSC mode 2 |
| 0 | | 1 | 1 |  | SSC mode 3 |
| 1 | | 0 | 0 |  | unused; shall be interpreted as "SSC mode 1", if received by the network |
| 1 | | 0 | 1 |  | unused; shall be interpreted as "SSC mode 2", if received by the network |
| 1 | | 1 | 0 |  | unused; shall be interpreted as "SSC mode 3", if received by the network |
|  | | | | | |
| All other values are reserved. | | | | | |

## 9.11 3GPP specific coding information defined within present document

### 9.11.1 Serving network name (SNN)

The serving network name (SNN) is used in the network name field of the AT\_KDF\_INPUT attribute defined in IETF RFC 5448 [40].

SNN shall take the generic format of an octet string without terminating null characters.

SNN is of maximum length of 1020 octets.

SNN consists of SNN-prefix and SNN-value, delimited by a colon.

SNN-value identifies the serving PLMN.

MCC and MNC in the SNN-PLMN-ID are MCC and MNC of the serving PLMN. If the MNC of the serving PLMN has two digits, then a zero is added at the beginning.

ABNF syntax of SNN is specified in table 9.11.1.1

Table 9.11.1.1: ABNF syntax of SNN

SNN = SNN-prefix ":" SNN-value

SNN-prefix = %x35.47 ; "5G"

SNN-value = SNN-PLMN-ID

SNN-PLMN-ID = SNN-mnc-string SNN-mnc-digits "." SNN-mcc-string SNN-mcc-digits "." SNN-3gppnetwork-string "." SNN-org-string

SNN-mnc-digits = DIGIT DIGIT DIGIT ; MNC of the PLMN ID

SNN-mcc-digits = DIGIT DIGIT DIGIT ; MCC of the PLMN ID

SNN-mnc-string = %x6d.6e.63 ; "mnc" in lower case

SNN-mcc-string = %x6d.63.63 ; "mcc" in lower case

SNN-3gppnetwork-string = %x33.67.70.70.6e.65.74.77.6f.72.6b ; "3gppnetwork" in lower case

SNN-org-string = %x6f.72.67 ; "org" in lower case

NOTE: SNN-prefix allows for distinguishing of ANID specified in 3GPP TS 24.302 [16] and SNN as either of SNN or ANID can be carried in the AT\_KDF\_INPUT attribute.

EXAMPLE: If PLMN ID contains MCC = 234 and MNC = 15, SNN is 5G:mnc015.mcc234.3gppnetwork.org.

# 10 List of system parameters

## 10.1 General

## 10.2 Timers of 5GS mobility management

Timers of 5GS mobility management are shown in table 10.2.1 and table 10.2.2

Table 10.2.1: Timers of 5GS mobility management – UE side

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  EXPIRY |
| --- | --- | --- | --- | --- | --- |
| T3510 | 15s | 5GMM-REGISTERED-INITIATED | Transmission of REGISTRATION REQUEST message | REGISTRATION ACCEPT message received or REGISTRATION REJECT message received | Start T3511 or T3502 as specified in subclause 5.5.1.2.7 if T3510 expired during registration procedure for initial registration.  Start T3511 or T3502 as specified in subclause 5.5.1.3.6 if T3510 expired during the registration procedure for mobility and periodic registration update |
| T3502 | Default 12 min.  NOTE 1 | 5GMM-REGISTERED | At registration failure and the attempt counter is equal to 5 | Transmission of REGISTRATION REQUEST message | Initiation of the registration procedure, if still required |
| T3511 | 10s | 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION  5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE | At registration failure due to lower layer failure, T3510 timeout or registration rejected with other 5GMM cause values than those treated in subclause 5.5.1.2.5 for initial registration or subclause 5.5.1.3.5 for mobility and periodic registration | Transmission of REGISTRATION REQUEST message | Retransmission of the REGISTRATION REQUEST, if still required |
| T3512 | Default 54 min  NOTE 1 | 5GMM-REGISTERED | In 5GMM-REGISTERED, when 5GMM-CONNECTED mode is left | When entering state 5GMM-DEREGISTERED or when entering 5GMM-CONNECTED mode | Initiation of the periodic registration procedure if the UE is not registered for emergency services.  Locally deregister if the UE is registered for emergency services |
| T3516 | 30s | 5GMM-REGISTERED-INITIATED  5GMM-REGISTERED  5GMM-DEREGISTERED-INITIATED  5GMM-SERVICE-REQUEST-INITIATED | RAND and RES stored as a result of an 5G authentication challenge | SECURITY MODE COMMAND received  SERVICE REJECT received  REGISTRATION ACCEPT received  AUTHENTICATION REJECT received  AUTHENTICATION FAILURE sent  5GMM-DEREGISTERED, 5GMM-NULL or  5GMM-IDLE mode entered | Delete the stored RAND and RES |
| T3517 | 15s | 5GMM-SERVICE-REQUEST-INITIATED | Transmission of SERVICE REQUEST message | SERVICE ACCEPT message received, or  SERVICE REJECT message received | Abort the procedure |
| T3519 | 60s | 5GMM-REGISTERED-INITIATED | Transmission of IDENTITY RESPONSE message with freshly generated SUCI | REGISTRATION ACCEPT message with new 5G-GUTI received  CONFIGURATION UPDATE COMMAND message with new 5G-GUTI received | Delete stored SUCI |
| T3520 | 15s | 5GMM-REGISTERED-INITIATED  5GMM-DEREGISTERED-INITIATED  5GMM-SERVICE-REQUEST-INITIATED | Transmission of AUTHENTICATION FAILURE message with any of the 5GMM cause #20, #21 , #26 or #29 | AUTHENTICATION REQUEST message received or AUTHENTICATION REJECT message received  or  SECURITY MODE COMMAND message received  when entering 5GMM-IDLE mode  indication of transmission failure of AUTHENTICATION FAILURE message from lower layers | On first expiry, the UE should consider the network as false and follow item g of subclause 5.4.1.3.7, if the UE is not registered for emergency services.  On first expiry, the UE will follow subclause 5.4.1.3.7 under "For items c, d, e and f:", if the UE is registered for emergency services. |
| T3521 | 15s | 5GMM-DEREGISTERED-INITIATED | Transmission of DEREGISTRATION REQUEST message when de-registration procedure is not due to a "switch off" | DEREGISTRATION ACCEPT message received | Retransmission of DEREGISTRATION REQUEST message |
| T3540 | 10s | 5GMM-REGISTERED-INITIATED  5GMM-DEREGISTERED-INITIATED  5GMM-SERVICE-REQUEST-INITIATED | REGISTRATION REJECT message or DEREGISTRATION REQUEST message received with any of the 5GMM cause #7, #11, #12 or #13  SERVICE REJECT message received with any of the 5GMM cause #7, #11, #12 or #13 | N1 NAS signalling connection released  PDU sessions have been set up | Release the NAS signalling connection for the cases a) and b) as described in subclause 5.3.1.2 |
| 5GMM-DEREGISTERED  5GMM-DEREGISTERED.NORMAL-SERVICE | REGISTRATION REJECT message or SERVICE REJECT message received with the 5GMM cause #9 or #10 | N1 NAS signalling connection released | Release the NAS signalling connection for the cases c) as described in subclause 5.3.1.2 and initiation of the registration procedure as specified in subclause 5.5.1.2.2 or 5.5.1.3.2 |
| Non-3GPP de-registration timer | Default 54 min.  NOTE 1  NOTE 2 | All 5GMM state over non-3GPP access except 5GMM-DEREGISTERED over non-3GPP access | Entering 5GMM-IDLE mode over non-3GPP access | N1 NAS signalling connection over non-3GPP access established or when entering state 5GMM-DEREGISTERED over non-3GPP access | Implicitly de-register the UE for non-3GPP access on 1st expiry |
| NOTE 1: The value of this timer is provided by the network operator during the registration procedure.  NOTE 2: The default value of this timer is used if the network does not indicate a value in the REGISTRATION ACCEPT message and the UE does not have a stored value for this timer. | | | | | |

Editor's note: The exact default value of the non-3GPP de-registration timer is FFS.

Table 10.2.2: Timers of 5GS mobility management – AMF side

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  EXPIRY |
| --- | --- | --- | --- | --- | --- |
| T3550 | 6s | 5GMM-COMMON-PROCEDURE-INITIATED | Transmission of REGISTRATION ACCEPT message at initial registration.  Transmission of REGISTRATION ACCEPT message with 5G-GUTI at mobility or periodic registration | REGISTRATION COMPLETE message received | Retransmission of REGISTRATION ACCEPT message |
| T3560 | 6s | 5GMM-COMMON-PROCEDURE-INITIATED | Transmission of AUTHENTICATION REQUEST message  Transmission of SECURITY MODE COMMAND message | AUTHENTICATION RESPONSE message received  AUTHENTICATION FAILURE message received  SECURITY MODE COMPLETE message received  SECURITY MODE REJECT message received | Retransmission of AUTHENTICATION REQUEST message or SECURITY MODE COMMAND message |
| T3570 | 6s | 5GMM-COMMON-PROCEDURE-INITIATED | Transmission of IDENTITY REQUEST message | IDENTITY RESPONSE message received | Retransmission of IDENTITY REQUEST message |
| T3513 | NOTE 4 | 5GMM-REGISTERED | Paging procedure initiated | Paging procedure completed as specified in subclause 5.6.2.2.1 | Network dependent |
| T3522 | 6s | 5GMM-DEREGISTERED-INITIATED | Transmission of DEREGISTRATION REQUEST message | DEREGISTRATION ACCEPT message received | Retransmission of DEREGISTRATION REQUEST message |
| T3555 | 6s | 5GMM-REGISTERED | Transmission of CONFIGURATION UPDATE COMMAND message with Acknowledgement requested flag IE | CONFIGURATION UPDATE COMPLETE message received | Retransmission of CONFIGURATION UPDATE COMMAND message |
| T3565 | 6s | 5GMM-REGISTERED | Transmission of NOTIFICATION message | SERVICE REQUEST message received  NOTIFICATION RESPONSE message received | Retransmission of NOTIFICATION message |
| Mobile reachable timer | NOTE 1 | All except 5GMM-DEREGISTERED | Entering 5GMM-IDLE mode | N1 NAS signalling connection established | Network dependent, but typically paging is halted on 1st expiry, and start implicit de-registration timer, if the UE is not registered for emergency services.  Implicitly de-register the UE which is registered for emergency services |
| Implicit de-registration timer | NOTE 2 | All except 5GMM-DEREGISTERED | The mobile reachable timer expires while the network is in 5GMM-IDLE mode | N1 NAS signalling connection established | Implicitly detach the UE on 1st expiry |
| Non-3GPP implicit de-registration timer | NOTE 3 | All except 5GMM-DEREGISTERED | Entering 5GMM-IDLE mode over non-3GPP access | N1 NAS signalling connection over non-3GPP access established | Implicitly de-register the UE for non-3GPP access on 1s expiry |
| NOTE 1: The default value of this timer is 4 minutes greater than T3512. If the UE is registered for emergency services, the value of this timer is set equal to T3512.  NOTE 2: The value of this timer is network dependent. If MICO is activated, the default value of this timer is 4 minutes greater than T3512.  NOTE 3: The value of this timer is network dependent. The default value of this timer is 4 minutes greater than the non-3GPP de-registration timer.  NOTE 4: The value of this timer is network dependent. | | | | | |

## 10.3 Timers of 5GS session management

Timers of 5GS session management are shown in table 10.3.1 and table 10.3.2.

Table 10.3.1: Timers of 5GS session management – UE side

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  THE 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1) |
| --- | --- | --- | --- | --- | --- |
| T3580 | TBD | TBD | Transmission of PDU SESSION ESTABLISHMENT REQUEST message | PDU SESSION ESTABLISHMENT ACCEPT message received or  PDU SESSION ESTABLISHMENT REJECT message received | Retransmission of PDU SESSION ESTABLISHMENT REQUEST message |
| T3581 | TBD | TBD | Transmission of PDU SESSION MODIFICATION REQUEST message | PDU SESSION MODIFICATION COMMAND message with the same PTI is received or PDU SESSION MODIFICATION REJECT message received | Retransmission of PDU SESSION MODIFICATION REQUEST message |
| T3582 | TBD | TBD | Transmission of PDU SESSION RELEASE REQUEST message | PDU SESSION RELEASE COMMAND message with the same PTI is received or PDU SESSION RELEASE REJECT message received | Retransmission of PDU SESSION RELEASE REQUEST message |
| T3583 | Default 1 min.  NOTE 2 | PDU SESSION ACTIVE | UE creates or updates a derived QoS rule | UE deletes the derived QoS rule (see subclause 6.2.5.1.4.5) | On 1st expiry: Deletion of the derived QoS rule |
| NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.  NOTE 2: The network may provide the value of this timer applicable to the derived QoS rules of a specific PDU session as RQ timer value in the PDU SESSION ESTABLISHMENT ACCEPT message and PDU SESSION MODIFICATION COMMAND message. The maximum value of the timer is 30 min. If the network indicates a value greater than the maximum value, then the UE shall use the maximum value. | | | | | |

Table 10.3.2: Timers of 5GS session management – SMF side

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  THE 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1) |
| --- | --- | --- | --- | --- | --- |
| T3590 | TBD | TBD | Transmission of PDU SESSION AUTHENTICATION COMMAND message | PDU SESSION AUTHENTICATION COMPLETE message received | Retransmission of PDU SESSION AUTHENTICATION COMMAND message |
| T3591 | TBD | TBD | Transmission of PDU SESSION MODIFICATION COMMAND message | PDU SESSION MODIFICATION COMPLETE message received or PDU SESSION MODIFICATION COMMAND REJECT message received | Retransmission of PDU SESSION MODIFICATION COMMAND message |
| T3592 | TBD | TBD | Transmission of PDU SESSION RELEASE COMMAND message | PDU SESSION RELEASE COMPLETE message received or  N1 SM delivery skipped indication received | Retransmission of PDU SESSION RELEASE COMMAND message |
| T3593 | TBD (NOTE 2) | TBD | Reception of PDU SESSION MODIFICATION COMPLETE message for transmitted PDU SESSION MODIFICATION COMMAND message where the PDU SESSION MODIFICATION COMMAND message included 5GSM cause #39 | PDU SESSION RELEASE REQUEST message received | Network-requested PDU session release procedure performed |
| NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.  NOTE 2: If the PDU Session Address Lifetime value is sent to the UE in the PDU SESSION MODIFICATION COMMAND message then timer T3593 shall be started with the same value, otherwise it shall use a default value. | | | | | |

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

## A.1 Causes related to UE identification

Cause #3 – Illegal UE

This 5GMM cause is sent to the UE when the network refuses service to the UE either because an identity of the UE is not acceptable to the network or because the UE does not pass the authentication check.

Cause #6 – Illegal ME

This 5GMM cause is sent to the UE if the ME used is not acceptable to the network, e.g. blacklisted.

Cause #9 – UE identity cannot be derived by the network.

This 5GMM cause is sent to the UE when the network cannot derive the UE's identity from the 5G-GUTI or 5G-S-TMSI because of e.g. no matching identity/context in the network, failure to validate the UE's identity due to integrity check failure of the received message.

Cause #10 – Implicitly de-registered

This 5GMM cause is sent to the UE either if the network has implicitly de-registered the UE, e.g. after the implicit de-registration timer has expired, or if the 5GMM context data related to the subscription does not exist in the AMF e.g. because of a AMF restart, or because of a registration request for mobility or registration update is routed to a new AMF.

## A.2 Cause related to subscription options

Cause #5 – PEI not accepted

This cause is sent to the UE if the network does not accept an initial registration procedure for emergency services using a PEI.

Cause #7 – 5GS services not allowed

This 5GMM cause is sent to the UE when it is not allowed to operate 5GS services.

Cause #11 – PLMN not allowed

This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate.

Cause #12 – Tracking area not allowed

This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a tracking area where the HPLMN determines that the UE, by subscription, is not allowed to operate.

NOTE 1: If 5GMM cause #12 is sent to a roaming subscriber the subscriber is denied service even if other PLMNs are available on which registration was possible.

Cause #13 – Roaming not allowed in this tracking area

This 5GMM cause is sent to a UE which requests service, or if the network initiates a de-registration request, in a tracking area of a PLMN which by subscription offers roaming to that UE but not in that tracking area.

Cause #27 – N1 mode not allowed

This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a PLMN where the UE by subscription, is not allowed to operate in N1 mode.

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

Cause #20 – MAC failure

This 5GMM cause is sent to the network if the USIM detects that the MAC in the AUTHENTICATION REQUEST message is not fresh.

Cause #21 – Synch failure

This 5GMM cause is sent to the network if the USIM detects that the SQN in the AUTHENTICATION REQUEST message is out of range.

Cause #22 – Congestion

This 5GMM cause is sent to the UE because of congestion in the network (e.g. no channel, facility busy/congested etc.).

Cause #23 – UE security capabilities mismatch

This 5GMM cause is sent to the network if the UE detects that the UE security capability does not match the one sent back by the network.

Cause #24 – Security mode rejected, unspecified

This 5GMM cause is sent to the network if the security mode command is rejected by the UE for unspecified reasons.

Cause #26 – Non-5G authentication unacceptable

This 5GMM cause is sent to the network in N1 mode if the "separation bit" in the AMF field of AUTN is set to 0 in the AUTHENTICATION REQUEST message (see 3GPP TS 33.501 [24]).

Cause #28 – Restricted service area

This 5GMM cause is sent to the UE if it requests service in a tracking area which is a part of the UE’s non-allowed area or is not a part of the UE’s allowed area.

Cause #29 – ngKSI already in use

This 5GMM cause is sent to the network in N1 mode if the ngKSI value received in the AUTHENTICATION REQUEST message is already associated with one of the 5G security contexts stored in the UE.

Cause #43 – LADN not available

This 5GMM cause is sent to the UE if the user-plane resources of the PDU session are not activated when the UE is located outside the LADN service area.

Cause #67 – Insufficient resources for specific slice and DNN

This 5GMM cause is sent by the network to indicate that the requested service cannot be provided due to insufficient resources for specific slice and DNN.

Cause #69 – Insufficient resources for specific slice

This 5GMM cause is sent by the network to indicate that the requested service cannot be provided due to insufficient resources for specific slice.

## A.4 Causes related to invalid messages

Cause #95 – Semantically incorrect message

This 5GMM cause is used to report receipt of a message with semantically incorrect contents.

Cause #96 – Invalid mandatory information

This cause 5GMM indicates that the equipment sending this 5GMM cause has received a message with a non-semantical mandatory IE error.

Cause #97 – Message type non-existent or not implemented

This 5GMM cause indicates that the equipment sending this 5GMM cause has received a message with a message type it does not recognize either because this is a message not defined, or defined but not implemented by the equipment sending this 5GMM cause.

Cause #98 – Message type not compatible with protocol state

This 5GMM cause indicates that the equipment sending this 5GMM cause has received a message not compatible with the protocol state.

Cause #99 – Information element non-existent or not implemented

This 5GMM cause indicates that the equipment sending this 5GMM cause has received a message which includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the 5GMM cause. However, the information element is not required to be present in the message in order for the equipment sending the 5GMM cause to process the message.

Cause #100 – Conditional IE error

This 5GMM cause indicates that the equipment sending this cause has received a message with conditional IE errors.

Cause #101 – Message not compatible with protocol state

This 5GMM cause indicates that a message has been received which is incompatible with the protocol state.

Cause #111 – Protocol error, unspecified

This 5GMM cause is used to report a protocol error event only when no other 5GMM cause in the protocol error class applies.

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

## B.1 Causes related to nature of request

Cause #26 – Insufficient resources

This 5GSM cause is used by the UE or by the network to indicate that the requested service cannot be provided due to insufficient resources.

Cause #27 – Missing or unknown DNN

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN because the DNN was not included although required or if the DNN could not be resolved.

Cause #28 – Unknown PDU session type

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN because the requested PDU session type could not be recognised or is not allowed.

Cause #29 – User authentication or authorization failed

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN due to a failed user authentication or revoked by the external DN or revoked by the external packet data network.

Cause #31 – Request rejected, unspecified

This 5GSM cause is used by the network or by the UE to indicate that the requested service or operation or the request for a resource was rejected due to unspecified reasons.

Cause #34 – Service option temporarily out of order

This 5GSM cause is sent when the network cannot serve the request because of temporary outage of one or more functions required for supporting the service.

Cause #35 – PTI already in use

This 5GSM cause is used by the network to indicate that the PTI included by the UE is already in use by another active UE requested procedure for this UE.

Cause #36 – Regular deactivation

This 5GSM cause is used to indicate a regular UE or network initiated release of PDU session resources.

Cause #39 – Reactivation requested

This 5GSM cause is used by the network to request a PDU session reactivation.

Cause #43 –Invalid PDU session identity

This 5GSM cause is used by the network or the UE to indicate that the PDU session identity value provided to it is not a valid value or the PDU session context identified by the PDU session identity IE in the request or the command is not active.

Cause #50 – PDU session type IPv4 only allowed

This 5GSM cause is used by the network to indicate that only PDU session type IPv4 is allowed for the requested IP connectivity.

Cause #51 – PDU session type IPv6 only allowed

This 5GSM cause is used by the network to indicate that only PDU session type IPv6 is allowed for the requested IP connectivity.

Cause #54 –PDU session does not exist

This 5GSM cause is used by the network to indicate that the network does not have any information about the PDU session which is requested by the UE to transfer between 3GPP access and non-3GPP access or from the EPS to the 5GS.

Cause #67 – Insufficient resources for specific slice and DNN

This 5GSM cause is by the network to indicate that the requested service cannot be provided due to insufficient resources for specific slice and DNN.

Cause #68 – Not supported SSC mode

This 5GSM cause is used by the network to indicate that the requested SSC mode is not supported.

Cause #69 –Insufficient resources for specific slice

This 5GSM cause is used by the network to indicate that the requested service cannot be provided due to insufficient resources for specific slice.

Cause #70 – Missing or unknown DNN in a slice

This 5GSM cause is used by the network to indicate that the requested service was rejected by the external DN because the DNN was not included although required or if the DNN could not be resolved, in the slice.

Cause #81 – Invalid PTI value

This 5GSM cause is used by the network or UE to indicate that the PTI provided to it is unassigned or reserved.

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

Cause #95 – Semantically incorrect message

This 5GSM cause is used to report receipt of a message with semantically incorrect contents.

Cause #96 – Invalid mandatory information

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message with a non-semantical mandatory IE error.

Cause #97 – Message type non-existent or not implemented

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message with a message type it does not recognize either because this is a message not defined, or defined but not implemented by the equipment sending this 5GSM cause.

Cause #98 – Message type not compatible with protocol state

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message not compatible with the protocol state.

Cause #99 – Information element non-existent or not implemented

This 5GSM cause indicates that the equipment sending this 5GSM cause has received a message which includes information elements not recognized because the information element identifier is not defined or it is defined but not implemented by the equipment sending the 5GSM cause. However, the information element is not required to be present in the message in order for the equipment sending the 5GSM cause to process the message.

Cause #100 – Conditional IE error

This 5GSM cause indicates that the equipment sending this cause has received a message with conditional IE errors.

Cause #101 – Message not compatible with protocol state

This 5GSM cause indicates that a message has been received which is incompatible with the protocol state.

Cause #111 – Protocol error, unspecified

This 5GSM cause is used to report a protocol error event only when no other 5GSM cause in the protocol error class applies.

Annex C (normative):  
Storage of 5GMM information

The following 5GMM parameters shall be stored on the USIM if the corresponding file is present:

a) 5G-GUTI;

b) last visited registered TAI;

c) 5GS update status; and

d) 5G NAS security context parameters from a full native 5G NAS security context (see 3GPP TS 33.501 [24]).

The presence and format of corresponding files on the USIM is specified in 3GPP TS 31.102 [22].

If the corresponding file is not present on the USIM, these 5GMM parameters are stored in a non-volatile memory in the ME together with the SUPI from the USIM. These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

The following 5GMM parameters shall be stored in a non-volatile memory in the ME together with the SUPI from the USIM:

- configured NSSAI(s).

Each configured NSSAI consists of S-NSSAIs stored together with a PLMN identity, if it is associated with a PLMN. The configured NSSAI(s) can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME; else the UE shall delete the configured NSSAI(s).

If the UE is registered for emergency services, the UE shall not store the 5GMM parameters described in this annex on the USIM or in non-volatile memory. Instead the UE shall temporarily store these parameters locally in the ME and the UE shall delete these parameters when the UE is deregistered.

If the UE is configured for eCall only mode as specified in 3GPP TS 31.102 [22], the UE shall not store the 5GMM parameters described in this annex on the USIM or in non-volatile memory. Instead the UE shall temporarily store these parameters locally in the ME and the UE shall delete these parameters when the UE enters 5GMM-DEREGISTERED.eCALL-INACTIVE state, the UE is switched-off or the USIM is removed.

Annex D (normative):  
UE policy delivery protocol

## D.1 General

The PCF can provide the UE with one or more UE policies using the network-requested UE policy management procedure. The PCF provides each UE policy using one or more UE policy sections, each identified by a UE policy section identifier (UPSI). The UPSI is composed of two parts:

a) a PLMN ID part containing the PLMN ID for the PLMN of the PCF which provides the UE policies; and

b) a UE policy section code (UPSC) containing a value assigned by the PCF.

The UE processes the UE policy sections, each identified by the UPSI, received from the PCF and informs the PCF of the result.

Editor's note: How the PCF decides whether to divide a UE policy into UE policy sections needs to be specified by CT3.

The message coding rules for the messages exchanged between the UE and the PCF for UE policy delivery are specified in subclause D.4.

## D.2 Procedures

### D.2.1 Network-requested UE policy management procedure

#### D.2.1.1 General

The purpose of the network-requested UE policy management procedure is to enable the network to:

a) send one or more new UE policy sections to the UE;

b) modify one or more UE policy sections stored at the UE; or

c) delete one or more UE policy sections stored at the UE.

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

In order to initiate the network-requested UE policy management procedure, the PCF shall:

a) encode the information about the UE policy sections to be stored, modified or deleted in a UE policy section modification list IE as specified in subclause D.5.2 and include it in a MANAGE UE POLICY COMMAND message.

b) send the MANAGE UE POLICY COMMAND message to the UE via the AMF as specified in 3GPP TS 23.502 [9]; and

c) start timer T35xx (see example in figure D.2.2.1).



Figure D.2.2.1: Network-requested UE policy management procedure

Upon receipt of the MANAGE UE POLICY COMMAND message, for each instruction included in the UE policy section management list IE, the UE shall:

a) if the instruction indicates to store the UE policy section:

1) attempt to delete UE policy rules and UE policy parameters stored at the UE associated with the same UPSI as the UPSI associated with the instruction, if any; and

2) attempt to store the UE policy rules and UE policy parameters included in the UE policy section of the instruction and associate these UE policy rules and UE policy parameters with the UPSI of the instruction; and

b) if the instruction indicates to delete the UE policy section, attempt to delete UE policy rules and UE policy parameters stored at the UE associated with the same UPSI as the UPSI of the instruction, if any.

Editor's note: How the PCF indicates to the UE the operation to perform on a UE policy section is FFS, e.g. by providing an operation code, or using the UPSI.

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

If all instructions included in the UE policy section management list IE were executed successfully by the UE, the UE shall:

a) create a MANAGE UE POLICY COMPLETE message; and

b) transport the MANAGE UE POLICY COMPLETE message using the NAS transport procedure as specified in subclause 5.4.5.

Upon receipt of the MANAGE UE POLICY COMPLETE message, the PCF shall stop timer T35xx.

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

If the UE could not execute all instructions included in the UE policy section management list IE successfully, the UE shall:

a) encode the UPSI associated with the instructions which could not be executed successfully and the associated UE Policy Delivery Protocol (UPDP) cause indicating the cause of the failure in a UE policy section management result IE as specified in subclause D.5.3 and include it in a MANAGE UE POLICY COMMAND REJECT message, and

b) transport the MANAGE UE POLICY COMMAND REJECT message using the NAS transport procedure as specified in subclause 5.4.5.

Upon receipt of the MANAGE UE POLICY COMMAND REJECT message, the PCF shall stop timer T35xx.

Editor's note: Further actions at the PCF upon receiving a MODIFY UE POLICY COMMAND REJECT message from the UE need to be specified by CT3.

Upon receipt of the N15 indication that the UE is not reachable, the PCF shall stop the T35xx.

Editor's note: Further actions at the PCF upon receiving the N15 indication that the UE is not reachable need to be specified by CT3.

#### D.2.1.5 Abnormal cases on the network side

Editor's note: Abnormal cases are FFS.

#### D.2.1.6 Abnormal cases in the UE

Editor's note: Abnormal cases are FFS.

### D.2.2 UE-initiated UPSI list transport procedure

#### D.2.2.1 General

The purpose of the UE-initiated UPSI list transport procedure is to deliver the UPSI(s) of the UE policy section(s) stored in the UE to the PCF if the UE has one or more stored UE policy sections.

#### D.2.2.2 UE-initiated UPSI list transport procedure initiation

In order to initiate the UE-initiated UPSI list transport procedure, the UE shall create a UPSI LIST TRANSPORT message. The UE shall:

a) allocate a PTI value currently not used and set the PTI IE to the allocated PTI value; and

b) include the UPSI(s) of the UE policy section(s) available in the UE in the UPSI list IE.

The UE shall send the UPSI LIST TRANSPORT message (see example in figure D.2.2.2.1). The UE shall transport the created UPSI LIST TRANSPORT message using the registration procedure (see subclause 5.5.1).



Figure D.2.2.2.1: UE-initiated UPSI list transport procedure

#### D.2.2.3 UE-initiated UPSI list transport procedure accepted by the network

Upon receipt of the UPSI LIST TRANSPORT message, the PCF shall operate as described in 3GPP TS 23.502 [9] and 3GPP TS 29.507 [21].

#### D.2.2.4 Abnormal cases on the network side

Editor's note: Abnormal cases are FFS.

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

When the UE needs to apply ANSDP as specified in 3GPP TS 24.502 [18], the UE shall consider all UE policy parts with ANSDP contents currently stored at the UE.

When the UE needs to apply URSP as specified in 3GPP TS 24.5xx [19], the UE shall consider all UE policy parts with URSP contents currently stored at the UE.

Editor's note: The reference to 3GPP TS 24.5xx needs to be replaced with a reference to the correct TS number for UE policies in 5GS once the TS number is allocated.

## D.4 Message coding rules

Editor's note: The message coding rules for the messages exchanged between the UE and the PCF for UE policy delivery protocol are FFS.

## D.5 Message functional definition and contents

### D.5.1 Manage UE policy command

#### D.5.1.1 Message definition

The MANAGE UE POLICY COMMAND message is sent by the PCF to the UE to request the UE to manage UE policy sections. See table D.5.1.1.1

Message type: MANAGE UE POLICY COMMAND

Significance: dual

Direction: network to UE

Table D.5.1.1.1: MANAGE UE POLICY COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | PTI | Procedure transaction identity  9.6, | M | V | 1 |
|  | MANAGE UE POLICY COMMAND message identity | UE policy delivery protocol message type  D.6.1 | M | V | 1 |
|  | UE policy section management list | UE policy section management list  D.6.2 | M | LV-E | 3-65538 |

### D.5.2 Manage UE policy complete

#### D.5.2.1 Message definition

The MANAGE UE POLICY COMPLETE message is sent by the UE to the PCF to report that all received instructions have been successfully executed at the UE. See table D.5.2.1.1

Message type: MANAGE UE POLICY COMPLETE

Significance: dual

Direction: UE to network

Table D.5.2.1.1: MANAGE UE POLICY COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | PTI | Procedure transaction identity  9.6, | M | V | 1 |
|  | MANAGE UE POLICY COMPLETE message identity | UE policy delivery protocol message type  D.6.1 | M | V | 1 |

### D.5.3 Manage UE policy command reject

#### D.5.3.1 Message definition

The MANAGE UE POLICY COMMAND REJECT message is sent by the UE to the PCF to report that one or more instructions could not be successfully executed at the UE. See table D.5.3.1.1

Message type: MANAGE UE POLICY COMMAND REJECT

Significance: dual

Direction: UE to network

Table D.5.3.1.1: MANAGE UE POLICY COMMAND REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | MANAGE UE POLICY COMMAND REJECT message identity | UE policy delivery protocol message type  D.6.1. | M | V | 1 |
|  | UE policy section management result | UE policy section management result  D.6.3 | M | LV-E | 3-65538 |

### D.5.4 UPSI list transport

#### D.5.4.1 Message definition

The UPSI LIST TRANSPORT message is sent by the UE to the PCF to deliver the UPSI(s) of the UE policy section(s) stored in the UE. See table D.5.4.1.1

Message type: UPSI LIST TRANSPORT

Significance: dual

Direction: UE to network

Table D.5.4.1.1: UPSI LIST TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | UPSI LIST TRANSPORT message identity | UE policy delivery message type  D.6.1 | M | V | 1 |
|  | UPSI list | UPSI list  D.6.4 | M | TLV-E | 9-65538 |

## D.6 Information elements coding

### D.6.1 UE policy delivery protocol message type

Table D.6.1.1: UE policy delivery protocol message type

|  |
| --- |
| Bits  **8 7 6 5 4 3 2 1**  0 0 0 0 0 0 0 0 Reserved  0 0 0 0 0 0 0 1 MANAGE UE POLICY COMMAND message  0 0 0 0 0 0 1 0 MANAGE UE POLICY COMPLETE message  0 0 0 0 0 0 1 1 MANAGE UE POLICY COMMAND REJECT message  0 0 0 0 0 1 0 0 UPSI LIST TRANSPORT message  All other values are reserved |

### D.6.2 UE policy section management list

The purpose of the UE policy section management list information element is to transfer from the PCF to the UE a list of instructions to be performed at the UE for management of UE policy section stored at the UE.

The UE policy section management list information element is coded as shown in figure D.6.2.1, figure D.6.2.2, figure D.6.2.3, figure D.6.2.4, figure D.6.2.5, figure D.6.2.6, figure D.6.2.7 and table D.6.2.1.

The UE policy section management list information element has a minimum length of 15 octets and a maximum length of 65538 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE policy section management list IEI | | | | | | | | octet 1 |
| Length of UE policy section management list contents | | | | | | | | octet 2  octet 3 |
| UE policy section management list contents | | | | | | | | octet 4  octet z |

Figure D.6.2.1: UE policy section management list information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE policy section management sublist (PLMN 1) | | | | | | | | octet 4  octet a |
| UE policy section management sublist (PLMN 2) | | | | | | | | octet a+1  octet b |
| … | | | | | | | | octet b+1  …  octet c |
| UE policy section management sublist (PLMN N) | | | | | | | | octet c+1  octet z |

Figure D.6.2.2: UE policy section management list contents

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Length of UE policy section management sublist | | | | | | | | octet d  octet d+1 |
|  | | | | MCC digit 1 | | | | octet d+2 |
| MCC digit 2 | | | |
|  | | | | MCC digit 3 | | | | octet d+3 |
| MNC digit 3 | | | |
|  | | | | MNC digit 1 | | | | octet d+4 |
| MNC digit 2 | | | |
| UE policy section management sublist contents | | | | | | | | octet d+5  octet y |

Figure D.6.2.3: UE policy section management sublist

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Instruction 1 | | | | | | | | octet d+5  octet e |
| Instruction 2 | | | | | | | | octet e+1  octet f |
| … | | | | | | | | octet f+1  …  octet g |
| Instruction N | | | | | | | | octet g+1  octet e |

Figure D.6.2.4: UE policy section management sublist contents

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Instruction contents length | | | | | | | | octet d+5  octet d+6 |
| UPSC | | | | | | | | octet d+7  octet d+8 |
| UE policy section contents | | | | | | | | octet d+9  octet k |

Figure D.6.2.5: Instruction

Editor's note: How the PCF indicates to the UE the operation to perform on a UE policy section is FFS, e.g. by providing an operation code, or using the UPSI.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE policy part 1 | | | | | | | | octet l  octet m |
| UE policy part 2 | | | | | | | | octet m+1  octet n |
| … | | | | | | | | octet n+1  …  octet o |
| UE policy part N | | | | | | | | octet o+1  octet p |

Figure D.6.2.6: UE policy section contents

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE policy part contents length | | | | | | | | octet q  octet q+1 |
| 0 | 0 | 0 | 0 | UE policy part type | | | | octet q+2 |
| Spare | | | |
| UE policy part contents | | | | | | | | octet q+3  octet r |

Figure D.6.2.7: UE policy part

Table D.6.2.1: UE policy section management list information element

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Value part of the UE policy section management list information element (octets 4 to z) | | | | | |
|  | | | | | |
| The value part of the UE policy section management list information element consists of one or several UE policy section management sublists. | | | | | |
|  | | | | | |
|  | | | | | |
| UE policy section management sublist: | | | | | |
|  | | | | | |
| Length of UE policy section management sublist (octets d to d+1) | | | | | |
|  | | | | | |
| This field contains the binary encoding of the length of the UE policy section management sublist in units of octets. | | | | | |
|  | | | | | |
| MCC, Mobile country code (octet d+2, and bits 4 to 1 of octet d+3) | | | | | |
|  | | | | | |
| The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | | | | | |
|  | | | | | |
| MNC, Mobile network code (bits 8 to 5 of octet d+3, and octet d+4) | | | | | |
|  | | | | | |
| The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111". | | | | | |
|  | | | | | |
| UE policy section management sublist contents (octets d+5 to y)  The UE policy section management sublist contents consist of one or several instructions. | | | | | |
|  | | | | | |
|  | | | | | |
| Instruction: | | | | | |
|  | | | | | |
| Instruction contents length (octets d+5 to d+6) | | | | | |
|  | | | | | |
| This field contains the binary encoding of the instruction contents length in units of octets. | | | | | |
|  | | | | | |
| UPSC (octets d+7 to d+8) | | | | | |
|  | | | | | |
| This field contains the binary encoding of the UPSC. The value of the UPSC is set by the PCF. | | | | | |
|  | | | | | |
| UE policy section contents (octets d+9 to k) | | | | | |
|  | | | | | |
| The UE policy section contents consist of one or several UE policy parts. | | | | | |
|  | | | | | |
| UE policy part: | | | | | |
|  | | | | | |
| UE policy part contents length (octets q to q+1) | | | | | |
|  | | | | | |
| This field contains the binary encoding of the UE policy part contents length in units of octets. | | | | | |
|  | | | | | |
| UE policy part type (bits 4 to 1 of octet q+2) | | | | | |
| Bits | | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | Reserved |
| 0 | 0 | 0 | 1 | URSP |
| 0 | 0 | 1 | 0 | ANDSP |
| All other values are reserved. | | | | | |
|  | | | | | |
| Bits 8 to 5 of octet q+2 are spare and shall be coded as zero. | | | | | |
|  | | | | | |
| UE policy part contents | | | | | |
|  | | | | | |
| This field contains a UE policy part encoded as specified in 3GPP TS 24.5xx [19]. | | | | | |
|  | | | | | |

Editor's note: The reference to 3GPP TS 24.5xx needs to be replaced with a reference to the correct TS number for UE policies in 5GGS once the TS number is allocated.

Editor's note: How the PCF indicates to the UE the operation to perform on a UE policy section is FFS, e.g. by providing an operation code, or using the UPSI.

### D.6.3 UE policy section management result

The purpose of the UE policy section management result information element is to transfer from the UE to the PCF information about instructions for UE policy section management which the UE could not execute successfully.

The UE policy section management result information element is coded as shown in figure D.6.3.1, figure D.6.3.2, figure D.6.3.3, figure D.6.3.4, figure D.6.3.5 and table D.6.3.1.

The UE policy section management result information element has a minimum length of 10 octets and a maximum length of 65538 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE policy section management result IEI | | | | | | | | octet 1 |
| Length of UE policy section management result contents | | | | | | | | octet 2  octet 3 |
| UE policy section management result contents | | | | | | | | octet 4  octet z |

Figure D.6.3.1: UE policy section management result information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE policy section management subresult (PLMN 1) | | | | | | | | octet 4  octet a |
| UE policy section management subresult (PLMN 2) | | | | | | | | octet a+1  octet b |
| … | | | | | | | | octet b+1  …  octet c |
| UE policy section management subresult (PLMN N) | | | | | | | | octet c+1  octet z |

Figure D.6.3.2: UE policy section management result contents

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Number of results | | | | | | | | octet d |
|  | | | | MCC digit 1 | | | | octet d+1 |
| MCC digit 2 | | | |
|  | | | | MCC digit 3 | | | | octet d+2 |
| MNC digit 3 | | | |
|  | | | | MNC digit 1 | | | | octet d+3 |
| MNC digit 2 | | | |
| UE policy section management subresult contents | | | | | | | | octet d+4  octet y |

Figure D.6.3.3: UE policy section management result

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Result 1 | | | | | | | | octet d+4  octet d+6 |
| Result 2 | | | | | | | | octet d+7  octet d+9 |
| … | | | | | | | | octet d+10  …  octet e |
| Result N | | | | | | | | octet e+1  octet e+3 |

Figure D.6.3.4: UE policy section management result contents

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UPSC | | | | | | | | octet f  octet f+1 |
| Failed instruction order | | | | | | | | octet f+2  octet f+3 |
| Cause | | | | | | | | octet f+4 |

Figure D.6.3.5: Result

Table D.6.3.1: UE policy section management result information element

|  |
| --- |
| Value part of the UE policy section management result information element (octets 4 to z) |
|  |
| The value part of the UE policy section management result information element consists of one or several UE policy section management subresults. |
|  |
|  |
| UE policy section management subresult: |
|  |
| Number of results (octet d) |
|  |
| This field contains the binary encoding of number of results included in the UE policy section management subresult. |
|  |
| MCC, Mobile country code (octet d+2, and bits 4 to 1 of octet d+3) |
|  |
| The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. |
|  |
| MNC, Mobile network code (bits 8 to 5 of octet d+3, and octet d+4) |
|  |
| The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111". |
|  |
| UE policy section management subresult contents (octets d+4 to y)  The UE policy section management subresult contents consist of one or several results. Each PSI field is 2 octet long and contains the binary encoding of a PSI. |
|  |
|  |
| Result (octet f to f+3) |
|  |
| UPSC (octet f to f+1) |
|  |
| This field contains the binary encoding of the UPSC. The value of the UPSC is set by the PCF |
|  |
| Failed instruction order (octets f+2 to f+3) |
|  |
| This field contains the binary encoding of the order of the failed instruction in the UE policy section management sublist. |
|  |
| Cause (octet f+4) |
| Bits |
| **8 7 6 5 4 3 2 1**  0 1 1 0 1 1 1 1 Protocol error, unspecified  The receiving entity shall treat any other value as 0110 1111, "protocol error, unspecified". |
|  |

### D.6.4 UPSI list

The purpose of the UPSI list information element is to transfer from the UE to the PCF a list of UPSIs.

The UPSI list information element is coded as shown in figure D.6.4.1, figure D.6.4.2, and table D.6.4.1.

The UPSI list information element has a minimum length of 9 octets and a maximum length of 65538 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UPSI list IEI | | | | | | | | octet 1 |
| Length of UPSI list contents | | | | | | | | octet 2  octet 3 |
| UPSI sublist (PLMN 1) | | | | | | | | octet 4  octet a |
| UPSI sublist (PLMN 2) | | | | | | | | octet a+1\*  octet b\* |
| … | | | | | | | | octet b+1\*  octet c\* |
| UPSI sublist (PLMN N) | | | | | | | | octet c+1\*  octet z\* |

Figure D.6.4.1: UPSI list information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Length of UPSI sublist | | | | | | | | octet d  octet d+1 |
| MCC digit 2 | | | | MCC digit 1 | | | | octet d+2 |
| MNC digit 3 | | | | MCC digit 3 | | | | octet d+3 |
| MNC digit 2 | | | | MNC digit 1 | | | | octet d+4 |
| UPSC | | | | | | | | octet d+5  octet d+6 |
| UPSC | | | | | | | | octet d+7\*  octet d+8\* |
| … | | | | | | | | octet d+9\*  octet e\* |
| UPSC | | | | | | | | octet e+1\*  octet f\* |

Figure D.6.4.2: UPSI sublist

Table D.6.4.1: UPSI list information element

|  |
| --- |
| MCC, Mobile country code (octet d+2, and bits 4 to 1 of octet d+3) |
|  |
| The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. |
|  |
| MNC, Mobile network code (bits 8 to 5 of octet d+3, and octet d+4) |
|  |
| The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111". |
|  |
| UPSC (octets d+5 to d+6) |
|  |
| This field contains the binary encoding of the UPSC. The value of the UPSC is set by the PCF. |
|  |

Annex E (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Change history | | | | | | | |
| **Date** | **Meeting** | **Tdoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2017-10 | CT1#106 | C1-174182 |  |  |  | Draft skeleton provided by the rapporteur. | 0.0.0 |
| 2017-11 | CT1#106 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-174183, C1-174184, C1-174185. | 0.1.0 |
| 2017-12 | CT1#107 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-175098, C1-175313.  Corrections done by the rapporteur. | 0.2.0 |
| 2017-12 | CT1 e-mail review |  |  |  |  | Editorial corrections. | 0.2.1 |
| 2017-12 | CT1 e-mail review |  |  |  |  | Re-introduction of table in subclause 8.2.23.1 | 0.2.2 |
| 2018-02 | CT1#108 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-180663, C1-180224, C1-180046, C1-180437, C1-180438, C1-180448, C1-180307, C1-180211, C1-180316, C1-180221, C1-180281, C1-180339, C1-180361, C1-180148, C1-180415, C1-180451, C1-180453, C1-180455, C1-180459, C1-180482, C1-180483, C1-180484, C1-180619, C1-180620, C1-180623, C1-180624, C1-180627, C1-180628, C1-180664, C1-180665, C1-180668, C1-180672, C1-180673, C1-180679, C1-180680, C1-180684, C1-180707, C1-180721, C1-180725, C1-180736, C1-180737, C1-180738, C1-180739, C1-180740, C1-180741, C1-180750, C1-180751, C1-180013, C1-180311, C1-180312, C1-180197, C1-180313, C1-180283, C1-180037, C1-180041, C1-180464, C1-180465, C1-180466, C1-180469, C1-180645, C1-180646, C1-180648, C1-180688, C1-180689, C1-180690, C1-180473, C1-180720, C1-180226, C1-180632, C1-180633, C1-180635, C1-180640, C1-180669, C1-180731, C1-180732, C1-180734, C1-180735, C1-180746, C1-180209, C1-180040, C1-180015, C1-180035, C1-180198, C1-180421, C1-180487, C1-180488, C1-180490, C1-180621, C1-180622, C1-180701, C1-180162, C1-180190, C1-180604, C1-180605, C1-180606, C1-180611, C1-180614, C1-180616, C1-180704, C1-180719, C1-180722, C1-180747, C1-180755, C1-180756  Corrections done by the rapporteur. | 0.3.0 |
| 2018-02 | CT1 e-mail review |  |  |  |  | Resolution of collision among C1-180679, C1-180721 and C1-180740.  Resolution of collision among C1-180605, C1-180616 and C1-180704.  Re-implementation of parts of C1-180035, C1-180488, C1-180605, C1-180606, C1-180729 and C1-180734 as some of the proposed changes were not implemented correctly in the previous version.  Implementation of C1-180646 which was missed.  Editorial corrections.  Corrections done by the rapporteur. | 0.3.1 |
| 2018-03 | CT1#109 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-181362, C1-181377, C1-181456, C1-181457, C1-181703, C1-181748, C1-181462, C1-181786, C1-181168, C1-181269, C1-181278, C1-181307, C1-181180, C1-181279, C1-181280, C1-181281, C1-181354, C1-181283, C1-181284, C1-181287, C1-181305, C1-181352, C1-181364, C1-181365, C1-181366, C1-181399, C1-181466, C1-181467, C1-181468, C1-181470, C1-181471, C1-181473, C1-181474, C1-181477, C1-181628, C1-181629, C1-181633, C1-181661, C1-181663, C1-181666, C1-181668, C1-181670, C1-181681, C1-181682, C1-181683, C1-181684, C1-181695, C1-181696, C1-181707, C1-181713, C1-181715, C1-181716, C1-181717, C1-181718, C1-181733, C1-181734, C1-181735, C1-181736, C1-181737, C1-181738, C1-181739, C1-181740, C1-181741, C1-181747, C1-181752, C1-181764, C1-181770, C1-181771, C1-181781, C1-181782, C1-181785, C1-181182, C1-181120, C1-181121, C1-181395, C1-181480, C1-181482, C1-181484, C1-181485, C1-181486, C1-181487, C1-181488, C1-181650, C1-181651, C1-181652, C1-181678, C1-181726, C1-181751, C1-181273, C1-181274, C1-181276, C1-181277, C1-181496, C1-181784, C1-181312, C1-181357, C1-181605, C1-181606, C1-181609, C1-181645, C1-181674, C1-181675, C1-181677, C1-181679, C1-181708, C1-181710, C1-181728, C1-181613, C1-181615, C1-181680, C1-181750, C1-181618, C1-181619, C1-181779, C1-181360, C1-181636, C1-181640, C1-181643, C1-181729, C1-181730, C1-181731, C1-181732  Corrections done by the rapporteur. | 0.4.0 |
| 2018-03 | CT1 e-mail review |  |  |  |  | Re-implementation of C1-181168 and C1-181307.  Re-implementation of C1-181656 and C1-181606 so that C1-181656 is implemented first.  Reverting to the old title.  Editorial corrections of some of the implemented p-CRs as well as adding some missing parts.  Corrections done by the rapporteur. | 0.4.1 |
| 2018-03 | CT#79 | CP-180101 |  |  |  | Version 1.0.0 created for presentation to TSG CT#79 for information. | 1.0.0 |
| 2018-05 | CT1#110 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-182219, C1-182493, C1-182496, C1-182202, C1-182497, C1-182053, C1-182311, C1-182019, C1-182359, C1-182360, C1-182361, C1-182358, C1-182305, C1-182306, C1-182354, C1-182117, C1-182182, C1-182455, C1-182459, C1-182491, C1-182600, C1-182601, C1-182605, C1-182606, C1-182607, C1-182608, C1-182609, C1-182610, C1-182614, C1-182615, C1-182621, C1-182662, C1-182664, C1-182665, C1-182708, C1-182728, C1-182730, C1-182733, C1-182724, C1-182757, C1-182759, C1-182760, C1-182768, C1-182772, C1-182775, C1-182786, C1-182787, C1-182791, C1-182831, C1-182832, C1-182833, C1-182834, C1-182835, C1-183836, C1-182838, C1-182840, C1-182844, C1-182067, C1-182073, C1-182303, C1-182321, C1-182352, C1-182385, C1-182645, C1-182646, C1-182647, C1-182648, C1-182650, C1-182651, C1-182657, C1-182659, C1-182660, C1-182741, C1-182742, C1-182761, C1-182762, C1-182763, C1-182764, C1-182765, C1-182774, C1-182789, C1-182789, C1-182815, C1-182845, C1-182797, C1-182232, C1-182230, C1-182666, C1-182667, C1-182671, C1-182673, C1-182677, C1-182800, C1-182824, C1-182710, C1-182072, C1-182078, C1-182174, C1-182190, C1-182456, C1-182636, C1-182637, C1-182638, C1-182639, C1-182726, C1-182729, C1-182747, C1-182749, C1-182766, C1-182767, C1-182841, C1-182847, C1-182043, C1-182057, C1-182260, C1-182044, C1-182617, C1-182618, C1-182619, C1-182620, C1-182622, C1-182623, C1-182624, C1-182627, C1-182628, C1-182629, C1-182802, C1-182808, C1-182345, C1-182461, C1-182630  Corrections done by the rapporteur. | 1.1.0 |
| 2018-05 | CT1 e-mail review |  |  |  |  | Re-implementation of C1-182768, C1-182841, C1-182841, C1-182619, C1-182665, C1-182497, C1-182067 and C1-182078 to correct some editorials as well as adding some missing parts.  Corrections done by the rapporteur. | 1.1.1 |
| 2018-06 | CT1#111 |  |  |  |  | Implementing the following p-CRs agreed by CT1: C1-183268, C1-183109, C1-183281, C1-183517, C1-183518, C1-183519, C1-183791, C1-183115, C1-183527, C1-183812, C1-183813, C1-183141, C1-183148, C1-183406, C1-183070, C1-183207, C1-183273, C1-183276, C1-183277, C1-183415, C1-183143, C1-183146, C1-183197, C1-183260, C1-183142, C1-183151, C1-183154, C1-183225, C1-183205, C1-183223, C1-183314, C1-183278, C1-183367, C1-183279, C1-183381, C1-183399, C1-183413, C1-183467, C1-183530, C1-183532, C1-183533, C1-183534, C1-183535, C1-183538, C1-183539, C1-183715, C1-183716, C1-183717, C1-183718, C1-183720, C1-183721, C1-183737, C1-183739, C1-183741, C1-183744, C1-183745, C1-183748, C1-183749, C1-183750, C1-183751, C1-183774, C1-183775, C1-183779, C1-183780, C1-183781, C1-183809, C1-183822, C1-183824, C1-183825, C1-183826, C1-183845, C1-183858, C1-183761, C1-183147, C1-183237, C1-183329, C1-183353, C1-183378, C1-183387, C1-183401, C1-183408, C1-183499, C1-183541, C1-183542, C1-183543, C1-183545, C1-183726, C1-183756, C1-183757, C1-183758, C1-183759, C1-183762, C1-183795, C1-183796, C1-183802, C1-183827, C1-183846, C1-183847, C1-183848, C1-183211, C1-183731, C1-183784, C1-183578, C1-183585, C1-183831, C1-183861, C1-183247, C1-183562, C1-183563, C1-183798, C1-183194, C1-183238, C1-183256, C1-183528, C1-183427, C1-183706, C1-183707, C1-183709, C1-183763, C1-183766, C1-183767, C1-183768, C1-183769, C1-183770, C1-183771, C1-183772, C1-183773, C1-183785, C1-183787, C1-183788, C1-183789, C1-183799, C1-183805, C1-183816, C1-183832, C1-183834, C1-183849, C1-183850, C1-183114, C1-183457, C1-183458, C1-183510, C1-183511, C1-183512, C1-183513, C1-183515, C1-183800, C1-183806, C1-183470  Corrections done by the rapporteur. | 1.2.0 |
| 2018-06 | CT1 e-mail review |  |  |  |  | Re-implementation of C1-183535, C1-183813, C1-183408, C1-183766 and C1-183831.  Implementation of C1-183816 which was missed.  Editorial corrections of some of the implemented p-CRs.  Corrections done by the rapporteur. | 1.2.1 |
| 2018-06 | CT#80 | CP-181094 |  |  |  | Version 2.0.0 created for presentation to TSG CT#80 for approval. | 2.0.0 |
| 2018-06 | CT#80 |  |  |  |  | Version 15.0.0 created after approval | 15.0.0 |