# 8 Message functional definitions and contents

## 8.1 Overview

## 8.2 5GS mobility management messages

### 8.2.1 Authentication request

#### 8.2.1.1 Message definition

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

Message type: AUTHENTICATION REQUEST

Significance: dual

Direction: network to UE

Table 8.2.1.1.1: AUTHENTICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication request message identity | Message type  9.7 | M | V | 1 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | ABBA | ABBA  9.11.3.10 | M | LV | 3-n |
| 21 | Authentication parameter RAND (5G authentication challenge) | Authentication parameter RAND  9.11.3.16 | O | TV | 17 |
| 20 | Authentication parameter AUTN (5G authentication challenge) | Authentication parameter AUTN  9.11.3.15 | O | TLV | 18 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |

#### 8.2.1.2 Authentication parameter RAND

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

#### 8.2.1.3 Authentication parameter AUTN

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

#### 8.2.1.4 Void

#### 8.2.1.5 EAP message

EAP message IE is included if the AUTHENTICATION REQUEST message is used in an EAP based primary authentication and key agreement procedure.

### 8.2.2 Authentication response

#### 8.2.2.1 Message definition

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

Message type: AUTHENTICATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.2.1.1: AUTHENTICATION RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication response message identity | Message type  9.7 | M | V | 1 |
| 2D | Authentication response parameter | Authentication response parameter  9.11.3.17 | O | TLV | 18 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |

#### 8.2.2.2 Authentication response parameter

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

#### 8.2.2.3 EAP message

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

### 8.2.3 Authentication result

#### 8.2.3.1 Message definition

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

Message type: AUTHENTICATION RESULT

Significance: dual

Direction: network to UE

Table 8.2.3.1.1: AUTHENTICATION RESULT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication result message identity | Message type  9.7 | M | V | 1 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |
| 38 | ABBA | ABBA  9.11.3.10 | O | TLV | 4-n |

#### 8.2.3.2 ABBA

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

### 8.2.4 Authentication failure

#### 8.2.4.1 Message definition

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

Message type: AUTHENTICATION FAILURE

Significance: dual

Direction: UE to network

Table 8.2.4.1.1: AUTHENTICATION FAILURE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication failure message identity | Message type  9.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.11.3.2 | M | V | 1 |
| 30 | Authentication failure parameter | Authentication failure parameter  9.11.3.14 | O | TLV | 16 |

#### 8.2.4.2 Authentication failure parameter

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

### 8.2.5 Authentication reject

#### 8.2.5.1 Message definition

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

Message type: AUTHENTICATION REJECT

Significance: dual

Direction: network to UE

Table 8.2.5.1.1: AUTHENTICATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Authentication reject message identity | Message type  9.7 | M | V | 1 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |

#### 8.2.5.2 EAP message

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

### 8.2.6 Registration request

#### 8.2.6.1 Message definition

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

Message type: REGISTRATION REQUEST

Significance: dual

Direction: UE to network

Table 8.2.6.1.1: REGISTRATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended Protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Registration request message identity | Message type  9.7 | M | V | 1 |
|  | 5GS registration type | 5GS registration type  9.11.3.7 | M | V | 1/2 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
|  | 5GS mobile identity | 5GS mobile identity  9.11.3.4 | M | LV-E | 6-n |
| C- | Non-current native NAS key set identifier | NAS key set identifier  9.11.3.32 | O | TV | 1 |
| 10 | 5GMM capability | 5GMM capability  9.11.3.1 | O | TLV | 3-15 |
| 2E | UE security capability | UE security capability  9.11.3.54 | O | TLV | 4-10 |
| 2F | Requested NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-74 |
| 52 | Last visited registered TAI | 5GS tracking area identity  9.11.3.8 | O | TV | 7 |
| 17 | S1 UE network capability | S1 UE network capability  9.11.3.48 | O | TLV | 4-15 |
| 40 | Uplink data status | Uplink data status  9.11.3.57 | O | TLV | 4-34 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| B- | MICO indication | MICO indication  9.11.3.31 | O | TV | 1 |
| 2B | UE status | UE status  9.11.3.56 | O | TLV | 3 |
| 77 | Additional GUTI | 5GS mobile identity  9.11.3.4 | O | TLV-E | 14 |
| 25 | Allowed PDU session status | Allowed PDU session status  9.11.3.13 | O | TLV | 4-34 |
| 18 | UE's usage setting | UE's usage setting  9.11.3.55 | O | TLV | 3 |
| 51 | Requested DRX parameters | 5GS DRX parameters  9.11.3.2A | O | TLV | 3 |
| 70 | EPS NAS message container | EPS NAS message container  9.11.3.24 | O | TLV-E | 4-n |
| 74 | LADN indication | LADN indication  9.11.3.29 | O | TLV-E | 3-811 |
| 8- | Payload container type | Payload container type  9.11.3.40 | O | TV | 1 |
| 7B | Payload container | Payload container  9.11.3.39 | O | TLV-E | 4-65538 |
| 9- | Network slicing indication | Network slicing indication  9.11.3.36 | O | TV | 1 |
| 53 | 5GS update type | 5GS update type  9.11.3.9A | O | TLV | 3 |
| 41 | Mobile station classmark 2 | Mobile station classmark 2  9.11.3.31C | O | TLV | 5 |
| 42 | Supported codecs | Supported codec list  9.11.3.51A | O | TLV | 5-n |
| 71 | NAS message container | NAS message container  9.11.3.33 | O | TLV-E | 4-n |
| 60 | EPS bearer context status | EPS bearer context status  9.11.3.23A | O | TLV | 4 |
| 6E | Requested extended DRX parameters | Extended DRX parameters  9.11.3.26A | O | TLV | 3 |
| 6A | T3324 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 67 | UE radio capability ID | UE radio capability ID  9.11.3.68 | O | TLV | 3-n |
| 35 | Requested mapped NSSAI | Mapped NSSAI  9.11.3.31B | O | TLV | 3-42 |
| 48 | Additional information requested | Additional information requested  9.11.3.12A | O | TLV | 3 |
| 1A | Requested WUS assistance information | WUS assistance information  9.11.3.71 | O | TLV | 3-n |
| A1 | N5GC indication | N5GC indication  9.11.3.72 | O | T | 1 |

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

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

#### 8.2.6.3 5GMM capability

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

#### 8.2.6.4 UE security capability

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

#### 8.2.6.5 Requested NSSAI

This IE shall be included by the UE when performing the registration procedure if the 5GS registration type IE indicates:

a) "initial registration", according to the conditions specified in subclause 5.5.1.2.2; or

b) "mobility registration updating", according to the conditions specified in clause 5.5.1.2.2.

#### 8.2.6.6 Last visited registered TAI

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

#### 8.2.6.7 S1 UE network capability

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

#### 8.2.6.8 Uplink data status

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

#### 8.2.6.9 PDU session status

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

#### 8.2.6.10 MICO indication

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

#### 8.2.6.11 UE status

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

#### 8.2.6.12 Additional GUTI

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

#### 8.2.6.13 Allowed PDU session status

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

#### 8.2.6.14 UE's usage setting

This IE shall be included if the UE supports IMS voice.

#### 8.2.6.15 Requested DRX parameters

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

#### 8.2.6.16 EPS NAS message container

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

#### 8.2.6.17 LADN indication

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

#### 8.2.6.17A Payload container type

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

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

#### 8.2.6.18 Payload container

This IE shall be included if the UE has one or more stored UE policy sections identified by a UPSI with the PLMN ID part indicating the HPLMN or the selected PLMN for the registration procedure for mobility and periodic registration update due to inter-system change from S1 mode to N1 mode of a UE operating in the single-registration mode or for the registration procedure for initial registration.

#### 8.2.6.19 Network slicing indication

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

#### 8.2.6.20 5GS update type

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

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

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

c) the UE requests CIoT 5GS optimizations.

#### 8.2.6.21 NAS message container

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

#### 8.2.6.22 Requested extended DRX parameters

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

#### 8.2.6.23 EPS bearer context status

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

#### 8.2.6.24 T3324 value

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

#### 8.2.6.25 Mobile station classmark 2

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

#### 8.2.6.26 Supported codecs

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

#### 8.2.6.27 UE radio capability ID

This IE shall be included if the UE is not in NB-N1 mode, the UE supports RACS and the UE needs to signal a UE radio capability ID to the network.

#### 8.2.6.28 Requested mapped NSSAI

This IE shall be included by the UE when the UE has a PDN connection or a PDU session to transfer to visited PLMN associated only with an S-NSSAI that is applicable in the HPLMN as specified in clause 5.5.1.3.2.

#### 8.2.6.29 Additional information requested

The UE shall include this IE if the UE supports ciphered broadcast assistance data and the UE needs to obtain new ciphering keys for ciphered broadcast assistance data.

#### 8.2.6.30 Requested WUS assistance information

The UE may include this IE if the UE supports WUS assistance information and the UE does not have any emergency PDU sessions.

#### 8.2.6.31 Negotiated WUS assistance information

The network shall include the Negotiated WUS assistance information IE if:

- the UE supports WUS assistance information;

- the AMF supports and accepts the use of WUS assistance information; and

- the UE does not have any emergency PDU sessions.

#### 8.2.6.32 N5GC indication

This IE shall be included in the REGISTRATION REQUEST message when the W-AGF is acting on behalf of an N5GC device.

### 8.2.7 Registration accept

#### 8.2.7.1 Message definition

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

Message type: REGISTRATION ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.7.1.1: REGISTRATION ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Registration accept message identity | Message type  9.7 | M | V | 1 |
|  | 5GS registration result | 5GS registration result  9.11.3.6 | M | LV | 2 |
| 77 | 5G-GUTI | 5GS mobile identity  9.11.3.4 | O | TLV-E | 14 |
| 4A | Equivalent PLMNs | PLMN list  9.11.3.45 | O | TLV | 5-47 |
| 54 | TAI list | 5GS tracking area identity list  9.11.3.9 | O | TLV | 9-114 |
| 15 | Allowed NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-74 |
| 11 | Rejected NSSAI | Rejected NSSAI  9.11.3.46 | O | TLV | 4-42 |
| 31 | Configured NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-146 |
| 21 | 5GS network feature support | 5GS network feature support  9.11.3.5 | O | TLV | 3-5 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| 26 | PDU session reactivation result | PDU session reactivation result  9.11.3.42 | O | TLV | 4-34 |
| 72 | PDU session reactivation result error cause | PDU session reactivation result error cause  9.11.3.43 | O | TLV-E | 5-515 |
| 79 | LADN information | LADN information  9.11.3.30 | O | TLV-E | 12-1715 |
| B- | MICO indication | MICO indication  9.11.3.31 | O | TV | 1 |
| 9- | Network slicing indication | Network slicing indication  9.11.3.36 | O | TV | 1 |
| 27 | Service area list | Service area list  9.11.3.49 | O | TLV | 6-114 |
| 5E | T3512 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 5D | Non-3GPP de-registration timer value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 16 | T3502 value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 34 | Emergency number list | Emergency number list  9.11.3.23 | O | TLV | 5-50 |
| 7A | Extended emergency number list | Extended emergency number list  9.11.3.26 | O | TLV-E | 7-65538 |
| 73 | SOR transparent container | SOR transparent container  9.11.3.51 | O | TLV-E | 20-n |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| A- | NSSAI inclusion mode | NSSAI inclusion mode  9.11.3.37A | O | TV | 1 |
| 76 | Operator-defined access category definitions | Operator-defined access category definitions  9.11.3.38 | O | TLV-E | 3-n |
| 51 | Negotiated DRX parameters | 5GS DRX parameters  9.11.3.2A | O | TLV | 3 |
| D- | Non-3GPP NW policies | Non-3GPP NW provided policies  9.11.3.36A | O | TV | 1 |
| 60 | EPS bearer context status | EPS bearer context status  9.11.3.23A | O | TLV | 4 |
| 6E | Negotiated extended DRX parameters | Extended DRX parameters  9.11.3.26A | O | TLV | 3 |
| 6C | T3447 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 6B | T3448 value | GPRS timer 3  9.11.2.4 | O | TLV | 3 |
| 6A | T3324 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 67 | UE radio capability ID | UE radio capability ID  9.11.3.68 | O | TLV | 3-n |
| 68 | UE radio capability ID deletion indication | UE radio capability ID deletion indication  9.11.3.69 | O | TV | 1 |
| 39 | Pending NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-74 |
| 74 | Ciphering key data | Ciphering key data  9.11.3.18C | O | TLV-E | x-n |
| 75 | CAG information list | CAG information list  9.11.3.18A | O | TLV-E | 3-n |
| 1B | Truncated 5G-S-TMSI configuration | Truncated 5G-S-TMSI configuration  9.11.3.70 | O | TLV | 3 |
| 1C | Negotiated WUS assistance information | WUS assistance information  9.11.3.71 | O | TLV | 3-n |

Editor's note [WI: 5G\_eLCS, CR#1705]: The Ciphering key data IE includes positioning SIBs that are still being discussed in RAN2 for Rel-16. The minimum and maximum length for this IE will need to be calculated and added to table 8.2.7.1.1 after RAN2 agreements for Rel-16.

#### 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:

1) the requested NSSAI was not included in the REGISTRATION REQUEST message or none of the requested NSSAI are allowed; and

2) the network has one or more subscribed S-NSSAIs marked as default which are not subject to network slice-specific authentication and authorization that are available.

#### 8.2.7.6 Rejected NSSAI

The network may include this IE to inform the UE of one or more 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 or SNPN.

#### 8.2.7.8 5GS network feature support

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

#### 8.2.7.9 PDU session status

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

#### 8.2.7.10 PDU session reactivation result

This IE shall be included:

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

- if the Allowed PDU session status IE is included in the REGISTRATION REQUEST message and there is at least one PDU session indicated in the Allowed PDU session status IE for which the user-plane resources can be re-established over 3GPP access.

#### 8.2.7.11 PDU session reactivation result error cause

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

#### 8.2.7.12 LADN information

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

#### 8.2.7.13 MICO indication

The network shall include the MICO indication IE if:

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

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

#### 8.2.7.14 Network slicing indication

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

#### 8.2.7.15 Service area list

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

#### 8.2.7.16 T3512 value

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

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

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

#### 8.2.7.18 T3502 value

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

#### 8.2.7.19 Emergency number list

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

#### 8.2.7.20 Extended emergency number list

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

#### 8.2.7.21 SOR transparent container

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

#### 8.2.7.22 EAP message

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

#### 8.2.7.23 NSSAI inclusion mode

This IE shall be included if required by operatory policy.

#### 8.2.7.24 Operator-defined access category definitions

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

#### 8.2.7.25 Negotiated DRX parameters

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

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

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

This IE is included if the network needs to indicate whether emergency numbers provided via non-3GPP access can be used to initiate UE detected emergency calls (see 3GPP TS 24.302 [16]). If this IE is not included then the UE shall interpret this as a receipt of an information element with all bits of the value part coded as zero.

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

#### 8.2.7.27 Negotiated extended DRX parameters

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

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

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

#### 8.2.7.28 T3447 value

The network may include T3447 value IE if:

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

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

#### 8.2.7.29 T3448 value

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

#### 8.2.7.30 T3324 value

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

#### 8.2.7.31 EPS bearer context status

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

#### 8.2.7.32 UE radio capability ID

This IE may be included if the UE is not in NB-N1 mode, both the UE and the network support RACS and the network needs to assign a network-assigned UE radio capability ID to the UE.

#### 8.2.7.33 UE radio capability ID deletion indication

This IE may be included if the UE is not in NB-N1 mode, both the UE and the network support RACS and the network needs to trigger the UE to delete all network-assigned UE radio capability IDs stored at the UE for the serving PLMN or SNPN.

#### 8.2.7.34 Pending NSSAI

The network may include this IE to inform the UE of one or more S-NSSAIs that are pending as the network slice-specific authentication and authorization procedure is not completed.

#### 8.2.7.35 Ciphering key data

This IE is included if the network needs to send ciphering key data to the UE for ciphered broadcast assistance data.

#### 8.2.7.36 CAG information list

This IE may be included to assign a new "CAG information list" to the UE or delete the "CAG information list" at the UE side.

#### 8.2.7.37 Truncated 5G-S-TMSI configuration

The network shall include this IE if:

- the UE is in NB-N1 mode;

- the UE requests "control plane CIoT 5GS optimization" in the 5GS update type IE of REGISTRATION REQUEST message;

- the AMF decides to accept the requested CIoT 5GS optimization; and

- the network is configured to provide the truncated 5G-S-TMSI configuration for control plane CIoT 5GS optimizations.

### 8.2.8 Registration complete

#### 8.2.8.1 Message definition

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

Message type: REGISTRATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.8.1.1: REGISTRATION COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Registration complete message identity | Message type  9.7 | M | V | 1 |
| 73 | SOR transparent container | SOR transparent container  9.11.3.51 | O | TLV-E | 20 |

#### 8.2.8.2 SOR transparent container

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

### 8.2.9 Registration reject

#### 8.2.9.1 Message definition

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

Message type: REGISTRATION REJECT

Significance: dual

Direction: network to UE

Table 8.2.9.1.1: REGISTRATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Registration reject message identity | Message type  9.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.11.3.2 | M | V | 1 |
| 5F | T3346 value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 16 | T3502 value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 69 | Rejected NSSAI | Rejected NSSAI  9.11.3.46 | O | TLV | 4-42 |

#### 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.

#### 8.2.9.5 Rejected NSSAI

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

### 8.2.10 UL NAS transport

#### 8.2.10.1 Message definition

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

Message type: UL NAS TRANSPORT

Significance: dual

Direction: UE to network

Table 8.2.10.1.1: UL NAS TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | UL NAS TRANSPORT message identity | Message type  9.7 | M | V | 1 |
|  | Payload container type | Payload container type  9.11.3.40 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Payload container | Payload container  9.11.3.39 | M | LV-E | 3-65537 |
| 12 | PDU session ID | PDU session identity 2  9.11.3.41 | C | TV | 2 |
| 59 | Old PDU session ID | PDU session identity 2  9.11.3.41 | O | TV | 2 |
| 8 | Request type | Request type  9.11.3.47 | O | TV | 1 |
| 22 | S-NSSAI | S-NSSAI  9.11.2.8 | O | TLV | 3-10 |
| 25 | DNN | DNN  9.11.2.1B | O | TLV | 3-102 |
| 24 | Additional information | Additional information  9.11.2.1 | O | TLV | 3-n |
| A- | MA PDU session information | MA PDU session information  9.11.3.31A | O | TV | 1 |
| F- | Release assistance indication | Release assistance indication  9.11.3.46A | O | TV | 1 |

#### 8.2.10.2 PDU session ID

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

#### 8.2.10.3 Old PDU session ID

The UE shall include this IE if the UL NAS TRANSPORT message transports a PDU SESSION ESTABLISHMENT REQUEST message upon receiving the PDU SESSION MODIFICATION COMMAND message with the 5GSM cause IE set to #39 "reactivation requested" and the Payload container type IE is set to "N1 SM information".

#### 8.2.10.4 Request type

The UE shall include this IE when the PDU session ID IE is included and the Payload container IE contains the PDU SESSION ESTABLISHMENT REQUEST message or the PDU SESSION MODIFICATION REQUEST which is not initiated to indicate a change of 3GPP PS data off UE status associated to a PDU session.

#### 8.2.10.5 S-NSSAI

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

#### 8.2.10.6 DNN

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

#### 8.2.10.7 Additional information

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

#### 8.2.10.8 MA PDU session information

The UE may include this IE if the Request type IE is included and is not set to "initial emergency request " or "existing emergency PDU session" in the UL NAS TRANSPORT message.

#### 8.2.10.9 Release assistance indication

The UE may include this IE to inform the network whether:

- no further uplink and no further downlink data transmission is expected; or

- only a single downlink data transmission (e.g. acknowledgement or response to uplink data) and no further uplink data transmission subsequent to the uplink data transmission is expected.

### 8.2.11 DL NAS transport

#### 8.2.11.1 Message definition

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

Message type: DL NAS TRANSPORT

Significance: dual

Direction: network to UE

Table 8.2.11.1.1: DL NAS TRANSPORT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | DL NAS TRANSPORT message identity | Message type  9.7 | M | V | 1 |
|  | Payload container type | Payload container type  9.11.3.40 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Payload container | Payload container  9.11.3.39 | M | LV-E | 3-65537 |
| 12 | PDU session ID | PDU session identity 2  9.11.3.41 | C | TV | 2 |
| 24 | Additional information | Additional information  9.11.2.1 | O | TLV | 3-n |
| 58 | 5GMM cause | 5GMM cause  9.11.3.2 | O | TV | 2 |
| 37 | Back-off timer value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |

#### 8.2.11.2 PDU session ID

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

#### 8.2.11.3 Additional information

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

#### 8.2.11.4 5GMM cause

The AMF shall include this IE when the Payload container IE contains an uplink payload which was not forwarded and the Payload container type IE is not set to "Multiple payloads".

#### 8.2.11.5 Back-off timer value

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

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

#### 8.2.12.1 Message definition

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

Message type: DEREGISTRATION REQUEST

Significance: dual

Direction: UE to network

Table 8.2.12.1.1: DEREGISTRATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | De-registration request message identity | Message type  9.7 | M | V | 1 |
|  | De-registration type | De-registration type  9.11.3.20 | M | V | 1/2 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
|  | 5GS mobile identity | 5GS mobile identity  9.11.3.4 | M | LV-E | 6-n |

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

#### 8.2.13.1 Message definition

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

Message type: DEREGISTRATION ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.13.1.1: DEREGISTRATION ACCEPT message content

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

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

#### 8.2.14.1 Message definition

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

Message type: DEREGISTRATION REQUEST

Significance: dual

Direction: network to UE

Table 8.2.14.1.1: DEREGISTRATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | De-registration request message identity | Message type  9.7 | M | V | 1 |
|  | De-registration type | De-registration type  9.11.3.20 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
| 58 | 5GMM cause | 5GMM cause  9.11.3.2 | O | TV | 2 |
| 5F | T3346 value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 6D | Rejected NSSAI | Rejected NSSAI  9.11.3.46 | O | TLV | 4-42 |

#### 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.

#### 8.2.14.4 Rejected NSSAI

The AMF may include this IE to inform the UE of one or more S-NSSAIs that were rejected by the network due to network slice-specific authentication and authorization failure or revocation as specified in subclause 4.6.2.4.

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

#### 8.2.15.1 Message definition

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

Message type: DEREGISTRATION ACCEPT

Significance: dual

Direction: UE to network

Table 8.2.15.1.1.1: DEREGISTRATION ACCEPT message content

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

### 8.2.16 Service request

#### 8.2.16.1 Message definition

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

Message type: SERVICE REQUEST

Significance: dual

Direction: UE to network

Table 8.2.16.1.1: SERVICE REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Service request message identity | Message type  9.7 | M | V | 1 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
|  | Service type | Service type  9.11.3.50 | M | V | 1/2 |
|  | 5G-S-TMSI | 5GS mobile identity  9.11.3.4 | M | LV-E | 9 |
| 40 | Uplink data status | Uplink data status  9.11.3.57 | O | TLV | 4-34 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| 25 | Allowed PDU session status | Allowed PDU session status  9.11.3.13 | O | TLV | 4-34 |
| 71 | NAS message container | NAS message container  9.11.3.33 | O | TLV-E | 4-n |

#### 8.2.16.2 Uplink data status

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

#### 8.2.16.3 PDU session status

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

#### 8.2.16.4 Allowed PDU session status

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

#### 8.2.16.5 NAS message container

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

### 8.2.17 Service accept

#### 8.2.17.1 Message definition

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

Message type: SERVICE ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.17.1.1: SERVICE ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Service accept message identity | Message type  9.7 | M | V | 1 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| 26 | PDU session reactivation result | PDU session reactivation result  9.11.3.42 | O | TLV | 4-34 |
| 72 | PDU session reactivation result error cause | PDU session reactivation result error cause  9.11.3.43 | O | TLV-E | 5-515 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 6B | T3448 value | GPRS timer 3  9.11.2.4 | O | TLV | 3 |

#### 8.2.17.2 PDU session status

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

#### 8.2.17.3 PDU session reactivation result

This IE shall be included:

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

- if the Allowed PDU session status IE is included in the SERVICE REQUEST message and there is at least one PDU session indicated in the Allowed PDU session status IE for which user-plane resources can be re-established over 3GPP access.

#### 8.2.17.4 PDU session reactivation result error cause

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

#### 8.2.17.5 EAP message

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

#### 8.2.17.6 T3448 value

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

### 8.2.18 Service reject

#### 8.2.18.1 Message definition

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

Message type: SERVICE REJECT

Significance: dual

Direction: network to UE

Table 8.2.18.1.1: SERVICE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Service reject message identity | Message type  9.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.11.3.2 | M | V | 1 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| 5F | T3346 value | GPRS timer 2  9.11.2.4 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 6B | T3448 value | GPRS timer 3  9.11.2.4 | O | TLV | 3 |

#### 8.2.18.2 PDU session status

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

#### 8.2.18.3 T3346 value

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

#### 8.2.18.4 EAP message

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

#### 8.2.18.5 T3448 value

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

### 8.2.19 Configuration update command

#### 8.2.19.1 Message definition

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

Message type: CONFIGURATION UPDATE COMMAND

Significance: dual

Direction: network to UE

Table 8.2.19.1.1: CONFIGURATION UPDATE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Configuration update command message identity | Message type  9.7 | M | V | 1 |
| D- | Configuration update indication | Configuration update indication  9.11.3.18 | O | TV | 1 |
| 77 | 5G-GUTI | 5GS mobile identity  9.11.3.4 | O | TLV-E | 14 |
| 54 | TAI list | 5GS tracking area identity list  9.11.3.9 | O | TLV | 9-114 |
| 15 | Allowed NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-74 |
| 27 | Service area list | Service area list  9.11.3.49 | O | TLV | 6-114 |
| 43 | Full name for network | Network name  9.11.3.35 | O | TLV | 3-n |
| 45 | Short name for network | Network name  9.11.3.35 | O | TLV | 3-n |
| 46 | Local time zone | Time zone  9.11.3.52 | O | TV | 2 |
| 47 | Universal time and local time zone | Time zone and time  9.11.3.53 | O | TV | 8 |
| 49 | Network daylight saving time | Daylight saving time  9.11.3.19 | O | TLV | 3 |
| 79 | LADN information | LADN information  9.11.3.30 | O | TLV-E | 3-1715 |
| B- | MICO indication | MICO indication  9.11.3.31 | O | TV | 1 |
| 9- | Network slicing indication | Network slicing indication  9.11.3.36 | O | TV | 1 |
| 31 | Configured NSSAI | NSSAI  9.11.3.37 | O | TLV | 4-146 |
| 11 | Rejected NSSAI | Rejected NSSAI  9.11.3.46 | O | TLV | 4-42 |
| 76 | Operator-defined access category definitions | Operator-defined access category definitions  9.11.3.38 | O | TLV-E | 3-n |
| F- | SMS indication | SMS indication  9.11.3.50A | O | TV | 1 |
| 6C | T3447 value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 75 | CAG information list | CAG information list  9.11.3.18A | O | TLV-E | 3-n |
| 67 | UE radio capability ID | UE radio capability ID  9.11.3.68 | O | TLV | 3-n |
| 68 | UE radio capability ID deletion indication | UE radio capability ID deletion indication  9.11.3.69 | O | TV | 1 |
| 44 | 5GS registration result | 5GS registration result  9.11.3.6 | O | TLV | 3 |
| 1B | Truncated 5G-S-TMSI configuration | Truncated 5G-S-TMSI configuration  9.11.3.70 | O | TLV | 3 |

#### 8.2.19.2 Configuration update indication

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

#### 8.2.19.3 5G-GUTI

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

#### 8.2.19.4 TAI list

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

#### 8.2.19.5 Allowed NSSAI

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

#### 8.2.19.6 Service area list

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

#### 8.2.19.7 Full name for network

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

#### 8.2.19.8 Short name for network

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

#### 8.2.19.9 Local time zone

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

#### 8.2.19.10 Universal time and local time zone

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

#### 8.2.19.11 Network daylight saving time

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

#### 8.2.19.12 LADN information

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

#### 8.2.19.13 MICO indication

This IE may be included to request the UE to re-negotiate MICO mode.

#### 8.2.19.14 Network slicing indication

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

#### 8.2.19.15 Configured NSSAI

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

#### 8.2.19.16 Rejected NSSAI

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

#### 8.2.19.17 Operator-defined access category definitions

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

#### 8.2.19.18 SMS indication

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

#### 8.2.19.19 T3447 value

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

#### 8.2.19.20 CAG information list

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

#### 8.2.19.21 UE radio capability ID

This IE may be included if the UE is not in NB-N1 mode, both the UE and the network support RACS and the network needs to assign a network-assigned UE radio capability ID to the UE.

#### 8.2.19.22 UE radio capability ID deletion indication

This IE may be included if the UE is not in NB-N1 mode, both the UE and the network support RACS and the network needs to trigger the UE to delete all network-assigned UE radio capability IDs stored at the UE for the serving PLMN or serving SNPN.

#### 8.2.19.23 5GS registration result

This IE shall be included if the network wants to indicate to the UE that the UE is registered for emergency services.

#### 8.2.19.24 Truncated 5G-S-TMSI configuration

This IE may be included to provide a new truncated 5G-S-TMSI configuration to the UE in NB-N1 mode if the network is configured to provide the truncated 5G-S-TMSI configuration for control plane CIoT 5GS optimizations.

### 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 |

#### 8.2.20.2 Void

### 8.2.21 Identity request

#### 8.2.21.1 Message definition

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

Message type: IDENTITY REQUEST

Significance: dual

Direction: AMF to UE

Table 8.2.21.1.1: IDENTITY REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Identity request message identity | Message type  9.7 | M | V | 1 |
|  | Identity type | 5GS identity type  9.11.3.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |

### 8.2.22 Identity response

#### 8.2.22.1 Message definition

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

Message type: IDENTITY RESPONSE

Significance: dual

Direction: UE to AMF

Table 8.2.22.1.1: IDENTITY RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Identity response message identity | Message type  9.7 | M | V | 1 |
|  | Mobile identity | 5GS mobile identity  9.11.3.4 | M | LV-E | 3-n |

### 8.2.23 Notification

#### 8.2.23.1 Message definition

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

Message type: NOTIFICATION

Significance: dual

Direction: network to UE

Table 8.2.23.1.1: NOTIFICATION message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Notification message identity | Message type  9.7 | M | V | 1 |
|  | Access type | Access type  9.11.2.1A | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |

### 8.2.24 Notification response

#### 8.2.24.1 Message definition

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

Message type: NOTIFICATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.2341.1: NOTIFICATION RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Notification response message identity | Message type  9.7 | M | V | 1 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |

#### 8.2.24.2 PDU session status

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

### 8.2.25 Security mode command

#### 8.2.25.1 Message definition

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

Message type: SECURITY MODE COMMAND

Significance: dual

Direction: network to UE

Table 8.2.25.1.1: SECURITY MODE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Security mode command message identity | Message type  9.7 | M | V | 1 |
|  | Selected NAS security algorithms | NAS security algorithms  9.11.3.34 | M | V | 1 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Replayed UE security capabilities | UE security capability  9.11.3.54 | M | LV | 3-9 |
| E- | IMEISV request | IMEISV request  9.11.3.28 | O | TV | 1 |
| 57 | Selected EPS NAS security algorithms | EPS NAS security algorithms  9.11.3.25 | O | TV | 2 |
| 36 | Additional 5G security information | Additional 5G security information  9.11.3.12 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 38 | ABBA | ABBA  9.11.3.10 | O | TLV | 4-n |
| 19 | Replayed S1 UE security capabilities | S1 UE security capability  9.11.3.48A | O | TLV | 4-7 |

#### 8.2.25.2 IMEISV request

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

#### 8.2.25.3 Void

#### 8.2.25.4 Selected EPS NAS security algorithms

This IE shall be included if the AMF supports N26 interface and the UE set the S1 mode bit to "S1 mode supported" in the 5GMM capability IE of the REGISTRATION REQUEST message.

#### 8.2.25.5 Additional 5G security information

The network shall include this IE if:

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

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

#### 8.2.25.6 EAP message

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

#### 8.2.25.7 ABBA

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

#### 8.2.25.8 Replayed S1 UE security capabilities

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

### 8.2.26 Security mode complete

#### 8.2.26.1 Message definition

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

Message type: SECURITY MODE COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.26.1.1: SECURITY MODE COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Security mode complete message identity | Message type  9.6 | M | V | 1 |
| 77 | IMEISV | 5GS mobile identity  9.11.3.4 | O | TLV-E | 12 |
| 71 | NAS message container | NAS message container  9.11.3.33 | O | TLV-E | 4-n |
| 78 | non-IMEISV PEI | 5GS mobile identity  9.11.3.4 | O | TLV-E | 7-n |

#### 8.2.26.2 IMEISV

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

#### 8.2.26.3 NAS message container

The UE shall include this information element:

a) if during an ongoing registration procedure or service request procedure, the AMF included the Additional 5G security information with the RINMR bit set to "Retransmission of the initial NAS message requested" in the SECURITY MODE COMMAND message as described in 3GPP TS 33.501 [24]; and

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

#### 8.2.26.4 non-IMEISV PEI

The 5G-RG or the W-AGF acting on behalf of the FN-RG (or on behalf of the N5GC device) shall include this information element, if the IMEISV was requested within the corresponding SECURITY MODE COMMAND message, the IMEISV is not available but MAC address is available.

The UE shall include this information element, if the IMEISV was requested within the corresponding SECURITY MODE COMMAND message, the IMEISV is not available but EUI-64 is available.

### 8.2.27 Security mode reject

#### 8.6.27.1 Message definition

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

Message type: SECURITY MODE REJECT

Significance: dual

Direction: UE to network

Table 8.2.27.1.1: SECURITY MODE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Security mode reject message identity | Message type  9.6 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.11.3.2 | M | V | 1 |

### 8.2.28 Security protected 5GS NAS message

#### 8.2.28.1 Message definition

This message is sent by the UE or the network to transfer a plain 5GS NAS message together with the sequence number and the message authentication code protecting the message. See table 8.2.28.1.1.

Message type: SECURITY PROTECTED 5GS NAS MESSAGE

Significance: dual

Direction: both

Table 8.2.28.1.1: SECURITY PROTECTED 5GS NAS MESSAGE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | Message authentication code | Message authentication code  9.8 | M | V | 4 |
|  | Sequence number | Sequence number  9.10 | M | V | 1 |
|  | Plain 5GS NAS message | Plain 5GS NAS message  9.9 | M | V | 3-n |

### 8.2.29 5GMM status

#### 8.2.29.1 Message definition

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

Message type: 5GMM STATUS

Significance: local

Direction: both

Table 8.2.29.1.1: 5GMM STATUS message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | Security header type | Security header type  9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1/2 |
|  | 5GMM STATUS message identity | Message type  9.7 | M | V | 1 |
|  | 5GMM cause | 5GMM cause  9.11.3.2 | M | V | 1 |

### 8.2.30 Control Plane Service request

#### 8.2.30.1 Message definition

The CONTROL PLANE SERVICE REQUEST message is sent by the UE to the AMF when the UE is using 5GS services with control plane CIoT 5GS optimization. See table 8.2.30.1.1.

Message type: CONTROL PLANE SERVICE REQUEST

Significance: dual

Direction: UE to network

Table 8.2.30.1.1: CONTROL PLANE 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 |
|  | Control plane service request message identity | Message type  9.7 | M | V | 1 |
|  | Control plane service type | Control plane service type  9.11.3.18D | M | V | 1/2 |
|  | ngKSI | NAS key set identifier  9.11.3.32 | M | V | 1/2 |
| 6F | CIoT small data container | CIoT small data container  9.11.3.18B | O | TLV | 4-257 |
| 8- | Payload container type | Payload container type  9.11.3.40 | O | TV | 1 |
| 7B | Payload container | Payload container  9.11.3.39 | O | TLV-E | 4-65538 |
| 12 | PDU session ID | PDU session identity 2  9.11.3.41 | C | TV | 2 |
| 50 | PDU session status | PDU session status  9.11.3.44 | O | TLV | 4-34 |
| F- | Release assistance indication | Release assistance indication  9.11.3.46A | O | TV | 1 |
| 40 | Uplink data status | Uplink data status  9.11.3.57 | O | TLV | 4-34 |
| 71 | NAS message container | NAS message container  9.11.3.33 | O | TLV-E | 4-n |
| 24 | Additional information | Additional information  9.11.2.1 | O | TLV | 3-n |

Editor's note: Whether other optimizations besides using a new EPD can be used in order to further reduce the message header of the message is FFS.

Editor's note: Whether Control plane service type IE can be removed is FFS.

#### 8.2.30.2 CIoT small data container

This IE shall be included if the UE needs to send uplink small user data, SMS or location services message or uplink SMS that is not more than 254 bytes, and there is no other optional IE to be sent.

NOTE: When the UE determines to use the CIoT small data container IE to send uplink data in this message, there is no other optional IEs in this message.

#### 8.2.30.3 Payload container type

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

#### 8.2.30.4 Payload container

This IE shall be included if the UE needs to send uplink CIoT user data, SMS or location services message.

#### 8.2.30.5 PDU session ID

The UE shall include this IE when the Payload container type IE is set to "CIoT user data container".

#### 8.2.30.6 PDU session status

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

#### 8.2.30.7 Release assistance indication

The UE may include this IE to inform the network whether:

- no further uplink and no further downlink data transmission is expected; or

- only a single downlink data transmission (e.g. acknowledgement or response to uplink data) and no further uplink data transmission subsequent to the uplink data transmission is expected.

#### 8.2.30.8 Uplink data status

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

#### 8.2.30.9 NAS message container

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

#### 8.2.30.10 Additional information

The UE may include this IE when the Payload container type IE is set to "Location services message container".

### 8.2.31 Network slice-specific authentication command

#### 8.2.31.1 Message definition

The NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message is sent by the AMF to the UE for authentication of the upper layers of the UE. See table 8.2.31.1.1.

Message type: NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND

Significance: dual

Direction: network to UE

Table 8.2.31.1.1: NETWORK SLICE-SPECIFIC AUTHENTICATION 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 |
|  | NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message identity | Message type  9.7 | M | V | 1 |
|  | S-NSSAI | S-NSSAI  9.11.2.8 | M | LV | 2-5 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |

### 8.2.32 Network slice-specific authentication complete

#### 8.2.32.1 Message definition

The NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message is sent by the UE to the AMF in response to the NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message and indicates acceptance of the NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message. See table 8.2.32.1.1.

Message type: NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.2.32.1.1: NETWORK SLICE-SPECIFIC AUTHENTICATION 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 |
|  | Spare half octet | Spare half octet  9.5 | M | V | 1 |
|  | NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message identity | Message type  9.7 | M | V | 1 |
|  | S-NSSAI | S-NSSAI  9.11.2.8 | M | LV | 2-5 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |

### 8.2.33 Network slice-specific authentication result

#### 8.2.33.1 Message definition

The NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message is sent by the AMF to the UE for indicating the result of the network slice-specific authentication and authorization procedure. See table 8.2.33.1.1.

Message type: NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT

Significance: dual

Direction: network to UE

Table 8.2.33.1.1: NETWORK SLICE-SPECIFIC 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 |
|  | NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message identity | Message type  9.7 | M | V | 1 |
|  | S-NSSAI | S-NSSAI  9.11.2.8 | M | LV | 2-5 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |

## 8.3 5GS session management messages

### 8.3.1 PDU session establishment request

#### 8.3.1.1 Message definition

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

Message type: PDU SESSION ESTABLISHMENT REQUEST

Significance: dual

Direction: UE to network

Table 8.3.1.1.1: PDU SESSION ESTABLISHMENT REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION ESTABLISHMENT REQUEST message identity | Message type  9.7 | M | V | 1 |
|  | Integrity protection maximum data rate | Integrity protection maximum data rate  9.11.4.7 | M | V | 2 |
| 9- | PDU session type | PDU session type  9.11.4.11 | O | TV | 1 |
| A- | SSC mode | SSC mode  9.11.4.16 | O | TV | 1 |
| 28 | 5GSM capability | 5GSM capability  9.11.4.1 | O | TLV | 3-15 |
| 55 | Maximum number of supported packet filters | Maximum number of supported packet filters  9.11.4.9 | O | TV | 3 |
| B- | Always-on PDU session requested | Always-on PDU session requested  9.11.4.4 | O | TV | 1 |
| 39 | SM PDU DN request container | SM PDU DN request container  9.11.4.15 | O | TLV | 3-255 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 66 | Header compression configuration | Header compression configuration  9.11.4.24 | O | TLV | 5-257 |
| 6E | DS-TT Ethernet port MAC address | DS-TT Ethernet port MAC address  9.11.4.25 | O | TLV | 8 |
| 6F | UE-DS-TT residence time | UE-DS-TT residence time  9.11.4.26 | O | TLV | 10 |
| 7C | Port management information container | Port management information container  9.11.4.27 | O | TLV-E | 4-65538 |

#### 8.3.1.2 PDU session type

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

#### 8.3.1.3 SSC mode

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

#### 8.3.1.4 Maximum number of supported packet filters

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

#### 8.3.1.5 5GSM capability

This IE is included in the message when the UE requests to establish a new PDU session or to transfer an existing PDN connection and any of the 5GSM capabilities supported by the UE is relevant for the PDU session.

#### 8.3.1.6 Void

#### 8.3.1.7 Always-on PDU session requested

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

#### 8.3.1.8 SM PDU DN request container

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

#### 8.3.1.9 Extended protocol configuration options

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

#### 8.3.1.10 Header compression configuration

The UE shall include the Header compression configuration IE if:

- the PDU session type value of the PDU session type IE is set to "IPv4", "IPv6", "IPv4v6", or "Ethernet";

- the UE indicates "Control Plane CIoT 5GS optimization supported" and "Header compression for control plane CIoT 5GS optimization supported" in the 5GMM capability IE of the REGISTRATION REQUEST message; and

- the network indicates "Control plane CIoT 5GS optimization supported" and "Header compression for control plane CIoT 5GS optimization supported" in the 5GS network support feature IE of the REGISTRATION ACCEPT message.

#### 8.3.1.11 DS-TT Ethernet port MAC address

This IE shall be included in the message if the UE supports transfer of port management information containers and the UE requests to establish a new PDU session of "Ethernet" PDU session type.

#### 8.3.1.12 UE-DS-TT residence time

This IE shall be included in the message if:

a) the UE supports transfer of port management information containers;

b) the UE requests to establish a new PDU session of "Ethernet" PDU session type; and

c) the UE-DS-TT residence time is available at the UE.

#### 8.3.1.13 Port management information container

This IE shall be included in the message if the UE supports transfer of port management information containers and the UE requests to establish a new PDU session of "Ethernet" PDU session type.

### 8.3.2 PDU session establishment accept

#### 8.3.2.1 Message definition

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

Message type: PDU SESSION ESTABLISHMENT ACCEPT

Significance: dual

Direction: network to UE

Table 8.3.2.1.1: PDU SESSION ESTABLISHMENT ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION ESTABLISHMENT ACCEPT message identity | Message type  9.7 | M | V | 1 |
|  | Selected PDU session type | PDU session type  9.11.4.11 | M | V | 1/2 |
|  | Selected SSC mode | SSC mode  9.11.4.16 | M | V | 1/2 |
|  | Authorized QoS rules | QoS rules  9.11.4.13 | M | LV-E | 6-65538 |
|  | Session AMBR | Session-AMBR  9.11.4.14 | M | LV | 7 |
| 59 | 5GSM cause | 5GSM cause  9.11.4.2 | O | TV | 2 |
| 29 | PDU address | PDU address  9.11.4.10 | O | TLV | 7, 11 or 15 |
| 56 | RQ timer value | GPRS timer  9.11.2.3 | O | TV | 2 |
| 22 | S-NSSAI | S-NSSAI  9.11.2.8 | O | TLV | 3-10 |
| 8- | Always-on PDU session indication | Always-on PDU session indication  9.11.4.3 | O | TV | 1 |
| 75 | Mapped EPS bearer contexts | Mapped EPS bearer contexts  9.11.4.8 | O | TLV-E | 7-65538 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 79 | Authorized QoS flow descriptions | QoS flow descriptions  9.11.4.12 | O | TLV-E | 6-65538 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 25 | DNN | DNN  9.11.2.1B | O | TLV | 3-102 |
| 17 | 5GSM network feature support | 5GSM network feature support  9.11.4.18 | O | TLV | 3-15 |
| 18 | Serving PLMN rate control | Serving PLMN rate control  9.11.4.20 | O | TLV | 4 |
| 77 | ATSSS container | ATSSS container  9.11.4.22 | O | TLV-E | 3-65538 |
| C- | Control plane only indication | Control plane only indication  9.11.4.23 | O | TV | 1 |
| 66 | Header compression configuration | Header compression configuration  9.11.4.24 | O | TLV | 5-257 |

#### 8.3.2.2 5GSM cause

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

#### 8.3.2.3 PDU address

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

#### 8.3.2.4 RQ timer value

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

#### 8.3.2.5 S-NSSAI

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

#### 8.3.2.6 Always-on PDU session indication

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

#### 8.3.2.7 Mapped EPS bearer contexts

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

#### 8.3.2.8 EAP message

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

#### 8.3.2.9 Authorized QoS flow descriptions

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

#### 8.3.2.10 Extended protocol configuration options

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

#### 8.3.2.11 DNN

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

#### 8.3.2.12 5GSM network feature support

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

#### 8.3.2.13 Void

#### 8.3.2.14 Serving PLMN rate control

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

#### 8.3.2.15 ATSSS container

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

#### 8.3.2.16 Control plane only indication

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

#### 8.3.2.17 Header compression configuration

The SMF may include the Header compression configuration IE if:

- the network accepts an IP or Ethernet PDU session type; and

- control plane CIoT 5GS optimization is selected.

### 8.3.3 PDU session establishment reject

#### 8.3.3.1 Message definition

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

Message type: PDU SESSION ESTABLISHMENT REJECT

Significance: dual

Direction: network to UE

Table 8.3.3.1.1: PDU SESSION ESTABLISHMENT REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION ESTABLISHMENT REJECT message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.11.4.2 | M | V | 1 |
| 37 | Back-off timer value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| F- | Allowed SSC mode | Allowed SSC mode  9.11.4.5 | O | TV | 1 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 1D | Re-attempt indicator | Re-attempt indicator  9.11.4.17 | O | TLV | 3 |
| 61 | 5GSM congestion re-attempt indicator | 5GSM congestion re-attempt indicator  9.11.4.21 | O | TLV | 3 |

#### 8.3.3.2 Back-off timer value

The network may include this IE if the 5GSM cause is not #28 "unknown PDU session type", #39 "reactivation requested", #46 "out of LADN service area", #50 "PDU session type IPv4 only allowed", #51 "PDU session type IPv6 only allowed", #54 "PDU session does not exist", #57 "PDU session type IPv4v6 only allowed", #58 "PDU session type Unstructured only allowed", #61 "PDU session type Ethernet only allowed", or #68 "not supported SSC mode", to request a minimum time interval before procedure retry is allowed.

#### 8.3.3.3 Allowed SSC mode

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

#### 8.3.3.4 EAP message

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

#### 8.3.3.5 Extended protocol configuration options

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

#### 8.3.3.6 Re-attempt indicator

The network may include this IE if the network includes the Back-off timer value IE and the 5GSM cause value is not #26 "insufficient resources", #28 "unknown PDU session type", #39 "reactivation requested", #46 "out of LADN service area", #54 "PDU session does not exist", #67 "insufficient resources for specific slice and DNN", #68 "not supported SSC mode", or #69 "insufficient resources for specific slice".

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

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

### 8.3.4 PDU session authentication command

#### 8.3.4.1 Message definition

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

Message type: PDU SESSION AUTHENTICATION COMMAND

Significance: dual

Direction: network to UE

Table 8.3.4.1.1: PDU SESSION AUTHENTICATION COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION AUTHENTICATION COMMAND message identity | Message type  9.7 | M | V | 1 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.4.2 Extended protocol configuration options

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

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

### 8.3.5 PDU session authentication complete

#### 8.3.5.1 Message definition

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

Message type: PDU SESSION AUTHENTICATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.5.1.1: PDU SESSION AUTHENTICATION COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION AUTHENTICATION COMPLETE message identity | Message type  9.7 | M | V | 1 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.5.2 Extended protocol configuration options

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

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

### 8.3.6 PDU session authentication result

#### 8.3.6.1 Message definition

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

Message type: PDU SESSION AUTHENTICATION RESULT

Significance: dual

Direction: network to UE

Table 8.3.6.1.1: PDU SESSION AUTHENTICATION RESULT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION AUTHENTICATION RESULT message identity | Message type  9.7 | M | V | 1 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.6.2 EAP message

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

#### 8.3.6.3 Extended protocol configuration options

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

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

### 8.3.7 PDU session modification request

#### 8.3.7.1 Message definition

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

Message type: PDU SESSION MODIFICATION REQUEST

Significance: dual

Direction: UE to network

Table 8.3.7.1.1: PDU SESSION MODIFICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION REQUEST message identity | Message type  9.7 | M | V | 1 |
| 28 | 5GSM capability | 5GSM capability  9.11.4.1 | O | TLV | 3-15 |
| 59 | 5GSM cause | 5GSM cause  9.11.4.2 | O | TV | 2 |
| 55 | Maximum number of supported packet filters | Maximum number of supported packet filters  9.11.4.9 | O | TV | 3 |
| B- | Always-on PDU session requested | Always-on PDU session requested  9.11.4.4 | O | TV | 1 |
| 13 | Integrity protection maximum data rate | Integrity protection maximum data rate  9.11.4.7 | O | TV | 3 |
| 7A | Requested QoS rules | QoS rules  9.11.4.13 | O | TLV-E | 7-65538 |
| 79 | Requested QoS flow descriptions | QoS flow descriptions  9.11.4.12 | O | TLV-E | 6-65538 |
| 75 | Mapped EPS bearer contexts | Mapped EPS bearer contexts  9.11.4.8 | O | TLV-E | 7-65538 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 7C | Port management information container | Port management information container  9.11.4.27 | O | TLV-E | 3-65538 |
| 66 | Header compression configuration | Header compression configuration  9.11.4.24 | O | TLV | 5-257 |

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

#### 8.3.7.2 5GSM capability

This IE is included in the message:

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

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

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

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

#### 8.3.7.3 5GSM cause

This IE is included in the message to indicate the reason for the deletion of one or more non-default QoS rules, QoS flow descriptions or mapped EPS bearer contexts.

#### 8.3.7.4 Maximum number of supported packet filters

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

#### 8.3.7.5 Always-on PDU session requested

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

#### 8.3.7.6 Integrity protection maximum data rate

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

#### 8.3.7.7 Requested QoS rules

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

#### 8.3.7.8 Requested QoS flow descriptions

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

#### 8.3.7.9 Extended protocol configuration options

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

#### 8.3.7.10 Mapped EPS bearer contexts

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

#### 8.3.7.11 Port management information container

This IE shall be included when the UE needs to convey a port management information container.

#### 8.3.7.12 Header compression configuration

This IE is included in the message if the UE wishes to re-negotiate header compression configuration associated to a PDU session and both the UE and the network supports Control plane CIoT 5GS optimization and header compression.

### 8.3.8 PDU session modification reject

#### 8.3.8.1 Message definition

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

Message type: PDU SESSION MODIFICATION REJECT

Significance: dual

Direction: network to UE

Table 8.3.8.1.1: PDU SESSION MODIFICATION REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION REJECT message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.11.4.2 | M | V | 1 |
| 37 | Back-off timer value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 1D | Re-attempt indicator | Re-attempt indicator  9.11.4.17 | O | TLV | 3 |
| 61 | 5GSM congestion re-attempt indicator | 5GSM congestion re-attempt indicator  9.11.4.21 | O | TLV | 3 |

#### 8.3.8.2 Back-off timer value

The network may include this IE if the 5GSM cause is not #46 "out of LADN service area", to request a minimum time interval before procedure retry is allowed.

#### 8.3.8.3 Extended protocol configuration options

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

#### 8.3.8.4 Re-attempt indicator

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

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

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

### 8.3.9 PDU session modification command

#### 8.3.9.1 Message definition

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

Message type: PDU SESSION MODIFICATION COMMAND

Significance: dual

Direction: network to UE

Table 8.3.9.1.1: PDU SESSION MODIFICATION COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION COMMAND message identity | Message type  9.7 | M | V | 1 |
| 59 | 5GSM cause | 5GSM cause  9.11.4.2 | O | TV | 2 |
| 2A | Session AMBR | Session-AMBR  9.11.4.14 | O | TLV | 8 |
| 56 | RQ timer value | GPRS timer  9.11.2.3 | O | TV | 2 |
| 8- | Always-on PDU session indication | Always-on PDU session indication  9.11.4.3 | O | TV | 1 |
| 7A | Authorized QoS rules | QoS rules  9.11.4.13 | O | TLV-E | 7-65538 |
| 75 | Mapped EPS bearer contexts | Mapped EPS bearer contexts  9.11.4.8 | O | TLV-E | 7-65538 |
| 79 | Authorized QoS flow descriptions | QoS flow descriptions  9.11.4.12 | O | TLV-E | 6-65538 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 77 | ATSSS container | ATSSS container  9.11.4.22 | O | TLV-E | 3-65538 |
| 66 | Header compression configuration | Header compression configuration  9.11.4.24 | O | TLV | 5-257 |
| 7C | Port management information container | Port management information container  9.11.4.27 | O | TLV-E | 3-65538 |
| 1E | Serving PLMN rate control | Serving PLMN rate control  9.11.4.20 | O | TLV | 4 |

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

#### 8.3.9.2 5GSM cause

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

#### 8.3.9.3 Session-AMBR

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

#### 8.3.9.4 RQ timer value

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

#### 8.3.9.5 Always-on PDU session indication

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

#### 8.3.9.6 Authorized QoS rules

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

#### 8.3.9.7 Mapped EPS bearer contexts

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

#### 8.3.9.8 Authorized QoS flow descriptions

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

#### 8.3.9.9 Extended protocol configuration options

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

#### 8.3.9.10 Void

#### 8.3.9.11 ATSSS container

The IE is included in the message when the network needs to indicate that the ATSSS parameters of the MA PDU session are modified.

#### 8.3.9.12 Header compression configuration

This IE is included in the message if the network wishes to re-negotiate header compression configuration associated to a PDU session and both the UE and the network support Control plane CIoT 5GS optimization and header compression.

#### 8.3.9.13 Port management information container

This IE shall be included when the network needs to convey a port management information container.

#### 8.3.9.14 Serving PLMN rate control

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

### 8.3.10 PDU session modification complete

#### 8.3.10.1 Message definition

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

Message type: PDU SESSION MODIFICATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.10.1.1: PDU SESSION MODIFICATION COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION COMPLETE message identity | Message type  9.7 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 7C | Port management information container | Port management information container  9.11.4.27 | O | TLV-E | 3-65538 |

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

#### 8.3.10.2 Extended protocol configuration options

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

#### 8.3.10.3 Port management information container

This IE shall be included when the UE needs to convey a port management information container.

### 8.3.11 PDU session modification command reject

#### 8.3.11.1 Message definition

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

Message type: PDU SESSION MODIFICATION COMMAND REJECT

Significance: dual

Direction: UE to network

Table 8.3.11.1.1: PDU SESSION MODIFICATION COMMAND REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION MODIFICATION COMMAND REJECT message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.11.4.2 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.11.2 Extended protocol configuration options

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

### 8.3.12 PDU session release request

#### 8.3.12.1 Message definition

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

Message type: PDU SESSION RELEASE REQUEST

Significance: dual

Direction: UE to network

Table 8.3.12.1.1: PDU SESSION RELEASE REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION RELEASE REQUEST message identity | Message type  9.7 | M | V | 1 |
| 59 | 5GSM cause | 5GSM cause  9.11.4.2 | O | TV | 2 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.12.2 5GSM cause

This IE is included in the message to indicate the reason for releasing the PDU session.

#### 8.3.12.3 Extended protocol configuration options

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

### 8.3.13 PDU session release reject

#### 8.3.13.1 Message definition

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

Message type: PDU SESSION RELEASE REJECT

Significance: dual

Direction: network to UE

Table 8.3.13.1.1: PDU SESSION RELEASE REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION RELEASE REJECT message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.11.4.2 | M | V | 1 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.13.2 Extended protocol configuration options

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

### 8.3.14 PDU session release command

#### 8.3.14.1 Message definition

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

Message type: PDU SESSION RELEASE COMMAND

Significance: dual

Direction: network to UE

Table 8.3.14.1.1: PDU SESSION RELEASE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION RELEASE COMMAND message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.11.4.2 | M | V | 1 |
| 37 | Back-off timer value | GPRS timer 3  9.11.2.5 | O | TLV | 3 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 7-1503 |
| 61 | 5GSM congestion re-attempt indicator | 5GSM congestion re-attempt indicator  9.11.4.21 | O | TLV | 3 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| D- | Access type | Access type  9.11.2.1A | O | TV | 1 |

#### 8.3.14.2 Back-off timer value

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

#### 8.3.14.3 EAP message

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

#### 8.3.14.4 Extended protocol configuration options

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

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

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

#### 8.3.14.6 Access type

This IE is included in the message when the network releases user-plane reources of an MA PDU session specifically over either 3GPP access or non-3GPP access.

### 8.3.15 PDU session release complete

#### 8.3.15.1 Message definition

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

Message type: PDU SESSION RELEASE COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.15.1.1: PDU SESSION RELEASE COMPLETE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | PDU SESSION RELEASE COMPLETE message identity | Message type  9.7 | M | V | 1 |
| 59 | 5GSM cause | 5GSM cause  9.11.4.2 | O | TV | 2 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |

#### 8.3.15.2 5GSM cause

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

#### 8.3.15.3 Extended protocol configuration options

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

### 8.3.16 5GSM status

#### 8.3.16.1 Message definition

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

Message type: 5GSM STATUS

Significance: dual

Direction: both

Table 8.3.16.1.1: 5GSM STATUS message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator  9.2 | M | V | 1 |
|  | PDU session ID | PDU session identity  9.4 | M | V | 1 |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | 5GSM STATUS message identity | Message type  9.7 | M | V | 1 |
|  | 5GSM cause | 5GSM cause  9.11.4.2 | M | V | 1 |

# 9 General message format and information elements coding

## 9.1 Overview

### 9.1.1 NAS message format

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

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

a) extended protocol discriminator;

b) security header type associated with a half spare octet or PDU session identity;

c) procedure transaction identity;

d) message type;

e) other information elements, as required.

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

a) extended protocol discriminator;

b) security header type associated with a half spare octet;

c) message authentication code;

d) sequence number;

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

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

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

Figure 9.1.1.1: General message organization example for a plain 5GS NAS message

The PDU session identity and the procedure transaction identity are only used in messages with extended protocol discriminator 5GS session management. Octet 2a with the procedure transaction identity shall only be included in these messages.

The organization of a security protected 5GS NAS message is illustrated in the example shown in figure 9.1.2.

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

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

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

### 9.1.2 Field format and mapping

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

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

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

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

Figure 9.1.2.1: Field mapping convention

## 9.2 Extended protocol discriminator

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

## 9.3 Security header type

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

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

Table 9.3.1: Security header type

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

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

## 9.4 PDU session identity

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

## 9.5 Spare half octet

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

## 9.6 Procedure transaction identity

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

## 9.7 Message type

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

Table 9.7.1: Message types for 5GS mobility management

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

Table 9.7.2: Message types for 5GS session management

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

## 9.8 Message authentication code

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

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

The usage of MAC is specified in subclause 4.4.3.3.

## 9.9 Plain 5GS NAS message

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

## 9.10 Sequence number

This IE includes the NAS message sequence number (SN) which consists of the eight least significant bits of the NAS COUNT for a SECURITY PROTECTED 5GS NAS MESSAGE message.

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

The usage of SN is specified in subclause 4.4.3.

## 9.11 Other information elements

### 9.11.1 General

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

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

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

The definitions of information elements which are:

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

b) used by access stratum protocols; or

c) sent to upper layers

are described in subclause 9.11.2.

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

### 9.11.2 Common information elements

#### 9.11.2.1 Additional information

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

The Additional information information element is coded as shown in figure 9.11.2.1.1 and table 9.11.2.1.1.

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

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

Figure 9.11.2.1.1: Additional information information element

Table 9.11.2.1.1 : Additional information information element

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

#### 9.11.2.1A Access type

The purpose of the access typeinformation element is to indicate the access type over which the signalling or user data is pending to be sent to the UE.

The access typeis a type 1 information element.

The access typeinformation element is coded as shown in figure 9.11.2.1A.1 and table 9.11.2.1A.1.

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

Figure 9.11.2.1A.1: Access type information element

Table 9.11.2.1A.1: Access type information element

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

#### 9.11.2.1B DNN

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

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

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

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

Figure 9.11.2.1B.1: DNN information element

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

#### 9.11.2.2 EAP message

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

The EAP message information element is coded as shown in figure 9.11.2.2.1 and table 9.11.2.2.1.

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

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

Figure 9.11.2.2.1: EAP message information element

Table 9.11.2.2.1: EAP message information element

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

#### 9.11.2.3 GPRS timer

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

#### 9.11.2.4 GPRS timer 2

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

#### 9.11.2.5 GPRS timer 3

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

#### 9.11.2.6 Intra N1 mode NAS transparent container

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

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

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

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

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

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

Figure 9.11.2.6.1: Intra N1 mode NAS transparent container information element

Table 9.11.2.6.1: Intra N1 mode NAS transparent container information element

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

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

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

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

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

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

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

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

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

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

#### 9.11.2.8 S-NSSAI

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

The S-NSSAI information element is coded as shown in figure 9.11.2.8.1 and table 9.11.2.8.1.

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

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

Figure 9.11.2.8.1: S-NSSAI information element

Table 9.11.2.8.1: S-NSSAI information element

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Length of S-NSSAI contents (octet 2) | | | | | | | | |
|  | | | | | | | | |
| This field indicates the length of the included S-NSSAI contents, and it can have the following values. Depending on the value of the length field the following S-NSSAI contents are included: | | | | | | | | |
| Bits | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | SST |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | SST and mapped HPLMN SST |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | SST and SD |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | SST, SD and mapped HPLMN SST |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | SST, SD, mapped HPLMN SST and mapped HPLMN SD |
| All other values are reserved. | | | | | | | | |
| Slice/service type (SST) (octet 3) | | | | | | | | |
| This field contains the 8 bit SST value. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. If this IE is included during the network slice-specific authentication and authorization procedure, this field contains the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of the HPLMN. | | | | | | | | |
| Slice differentiator (SD) (octet 4 to octet 6)  This field contains the 24 bit SD value. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. If this IE is included during the network slice-specific authentication and authorization procedure, this field contains the 24 bit SD value of an S-NSSAI in the S-NSSAI(s) of the HPLMN. | | | | | | | | |
| If the SST encoded in octet 3 is not associated with a valid SD value, and the sender needs to include a mapped HPLMN SST (octet 7) and a mapped HPLMN SD (octets 8 to 10), then the sender shall set the SD value (octets 4 to 6) to "no SD value associated with the SST". | | | | | | | | |
|  | | | | | | | | |
| mapped HPLMN Slice/service type (SST) (octet 7) | | | | | | | | |
| This field contains the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SST value is mapped. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. | | | | | | | | |
| mapped HPLMN Slice differentiator (SD) (octet 8 to octet 10)  This field contains the 24 bit SD value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SD value is mapped. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. | | | | | | | | |
| NOTE 1: Octet 3 shall always be included.  NOTE 2: If the octet 4 is included, then octet 5 and octet 6 shall be included.  NOTE 3: If the octet 7 is included, then octets 8, 9, and 10 may be included.  NOTE 4: If the octet 8 is included, then octet 9 and octet 10 shall be included.  NOTE 5: If only HPLMN S-NSSAI is included, then octets 7 to 10 shall not be included. | | | | | | | | |

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

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

The S1 mode to N1 mode NAS transparent container information element is coded as shown in figure 9.11.2.9.1 and table 9.11.2.9.1.

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

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

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

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

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

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

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

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

#### 9.11.3.1 5GMM capability

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

The 5GMM capability information element is coded as shown in figure 9.11.3.1.1 and table 9.11.3.1.1.

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GMM capability IEI | octet 1 | | | | | | | |
| Length of 5GMM capability contents | octet 2 | | | | | | | |
| SGC | 5G-HC-CP CIoT | N3 data | 5G-CP CIoT | RestrictEC | LPP | HO attach | S1 mode | octet 3 |
| RACS | NSSAA | 5G-LCS | V2XCNPC5 | V2XCEPC5 | V2X | 5G-UP CIoT | 5GSRVCC | octet 4\* |
| 0 | 0 | 0 | 0 | 0 | 0 | WUSA | CAG | Octet 5\* |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | octet 6\*-15\* |
| Spare |  | | | | | | | |

Figure 9.11.3.1.1: 5GMM capability information element

Table 9.11.3.1.1: 5GMM capability information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| EPC NAS supported (S1 mode) (octet 3, bit 1) | | | | |
| 0 |  |  |  | S1 mode not supported |
| 1 |  |  |  | S1 mode supported |
|  | | | | |
| ATTACH REQUEST message containing PDN CONNECTIVITY REQUEST message for handover support (HO attach) (octet 3, bit 2) | | | | |
| 0 |  |  |  | ATTACH REQUEST message containing PDN CONNECTIVITY REQUEST message with request type set to "handover" or "handover of emergency bearer services" to transfer PDU session from N1 mode to S1 mode not supported |
| 1 |  |  |  | ATTACH REQUEST message containing PDN CONNECTIVITY REQUEST message with request type set to "handover" or "handover of emergency bearer services" to transfer PDU session from N1 mode to S1 mode supported |
|  | | | | |
| LTE Positioning Protocol (LPP) capability (octet 3, bit 3) | | | | |
| 0 |  |  |  | LPP in N1 mode not supported |
| 1 |  |  |  | LPP in N1 mode supported (see 3GPP TS 36.355 [26]) |
|  | | | | |
| Restriction on use of enhanced coverage support (RestrictEC) (octet 3, bit 4)  This bit indicates the capability to support restriction on use of enhanced coverage. | | | | |
| 0 |  |  |  | Restriction on use of enhanced coverage not supported |
| 1 |  |  |  | Restriction on use of enhanced coverage supported |
| Control plane CIoT 5GS optimization (5G-CP CIoT) (octet 3, bit 5)  This bit indicates the capability for control plane CIoT 5GS optimization. | | | | |
| 0 |  |  |  | Control plane CIoT 5GS optimization not supported |
| 1 |  |  |  | Control plane CIoT 5GS optimization supported |
| N3 data transfer (N3 data) (octet 3, bit 6)  This bit indicates the capability for N3 data transfer. | | | | |
| 0 |  |  |  | N3 data transfer supported |
| 1 |  |  |  | N3 data transfer not supported |
| Header compression for control plane CIoT 5GS optimization (5G-HC-CP CIoT) (octet 3, bit 7)  This bit indicates the capability for header compression for control plane CIoT 5GS optimization. | | | | |
| 0 |  |  |  | Header compression for control plane CIoT 5GS optimization not supported |
| 1 |  |  |  | Header compression for control plane CIoT 5GS optimization supported |
|  | | | | |
| Service gap control (SGC) (octet 3, bit 8) | | | | |
| 0 |  |  |  | service gap control not supported |
| 1 |  |  |  | service gap control supported |
|  | | | | |
| 5G-SRVCC from NG-RAN to UTRAN (5GSRVCC) capability (octet 4, bit 1) | | | | |
| 0 |  |  |  | 5G-SRVCC from NG-RAN to UTRAN not supported |
| 1 |  |  |  | 5G-SRVCC from NG-RAN to UTRAN supported (see 3GPP TS 23.216 [6A]) |
| User plane CIoT 5GS optimization (5G-UP CIoT) (octet 4, bit 2)  This bit indicates the capability for user plane CIoT 5GS optimization. | | | | |
| 0 |  |  |  | User plane CIoT 5GS optimization not supported |
| 1 |  |  |  | User plane CIoT 5GS optimization supported |
|  | | | | |
| V2X capability (V2X) (octet 4, bit 3) | | | | |
| This bit indicates the capability for V2X, as specified in 3GPP TS 24.587 [19B].  Bit | | | | |
| 3 |  |  |  |  |
| 0 |  |  |  | V2X not supported |
| 1 |  |  |  | V2X supported |
|  | | | | |
| V2X communication over E-UTRA-PC5 capability (V2XCEPC5) (octet 4, bit 4) | | | | |
| This bit indicates the capability for V2X communication over E-UTRA-PC5, as specified in 3GPP TS 24.587 [19B]. | | | | |
| Bit | | | | |
| 4 |  |  |  |  |
| 0 |  |  |  | V2X communication over E-UTRA-PC5 not supported |
| 1 |  |  |  | V2X communication over E-UTRA-PC5 supported |
|  | | | | |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | V2X communication over NR-PC5 capability (V2XCNPC5) (octet 4, bit 5) | | | | | | This bit indicates the capability for V2X communication over NR-PC5, as specified in 3GPP TS 24.587 [19B]. | | | | | | Bit | | | | | | 5 |  |  |  |  | | 0 |  |  |  | V2X communication over NR-PC5 not supported | | 1 |  |  |  | V2X communication over NR-PC5 supported | |  | | | | | | | | | |
| Location Services (5G-LCS) notification mechanisms capability (octet 4, bit 6) | | | | |
| 0 |  |  |  | LCS notification mechanisms not supported |
| 1 |  |  |  | LCS notification mechanisms supported (see 3GPP TS 23.273 [6B]) |
| Network slice-specific authentication and authorization (NSSAA) (octet 4, bit 7)  This bit indicates the capability to support network slice-specific authentication and authorization. | | | | |
| 0 |  |  |  | Network slice-specific authentication and authorization not supported |
| 1 |  |  |  | Network slice-specific authentication and authorization supported |
|  | | | | |
| Radio capability signalling optimisation (RACS) capability (octet 4, bit 8) | | | | |
| 0 |  |  |  | RACS not supported |
| 1 |  |  |  | RACS supported |
|  | | | | |
| Closed Access Group (CAG) capability (octet 5, bit 1) | | | | |
| 0 |  |  |  | CAG not supported |
| 1 |  |  |  | CAG supported |
|  | | | | |
|  | | | | |
| WUS assistance (WUSA) information reception capability (octet 5, bit 2) | | | | |
| 0 |  |  |  | WUS assistance information reception not supported |
| 1 |  |  |  | WUS assistance information reception supported |
|  | | | | |
| bits 3-8 in octet 5 and bits in octets 6 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | |

#### 9.11.3.2 5GMM cause

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

The 5GMM cause information element is coded as shown in figure 9.11.3.2.1 and table 9.11.3.2.1.

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

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

Figure 9.11.3.2.1: 5GMM cause information element

Table 9.11.3.2.1: 5GMM cause information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cause value (octet 2) | | | | | | | | | |
|  | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |  | Illegal UE |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |  | PEI not accepted |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |  | Illegal ME |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |  | 5GS services not allowed |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |  | UE identity cannot be derived by the network |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |  | Implicitly de-registered |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |  | PLMN not allowed |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |  | Tracking area not allowed |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |  | Roaming not allowed in this tracking area |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |  | No suitable cells in tracking area |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |  | MAC failure |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |  | Synch failure |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |  | Congestion |
| 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |  | UE security capabilities mismatch |
| 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |  | Security mode rejected, unspecified |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |  | Non-5G authentication unacceptable |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |  | N1 mode not allowed |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |  | Restricted service area |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |  | Redirection to EPC required |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |  | LADN not available |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 |  | No network slices available |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |  | Maximum number of PDU sessions reached |
| 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |  | Insufficient resources for specific slice and DNN |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |  | Insufficient resources for specific slice |
| 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |  | ngKSI already in use |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |  | Non-3GPP access to 5GCN not allowed |
| 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |  | Serving network not authorized |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |  | Temporarily not authorized for this SNPN |
| 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |  | Permanently not authorized for this SNPN |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |  | Not authorized for this CAG or authorized for CAG cells only |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 |  | Wireline access area not allowed |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |  | Payload was not forwarded |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |  | DNN not supported or not subscribed in the slice |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |  | Insufficient user-plane resources for the PDU session |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |  | Semantically incorrect message |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |  | Invalid mandatory information |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |  | Message type non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |  | Message type not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |  | Information element non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |  | Conditional IE error |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |  | Message not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |  | Protocol error, unspecified |
|  |  |  |  |  |  |  |  |  |  |
| Any other value received by the mobile station shall be treated as 0110 1111, "protocol error, unspecified". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified". | | | | | | | | | |

#### 9.11.3.2A 5GS DRX parameters

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

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

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

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

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

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

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

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

#### 9.11.3.3 5GS identity type

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

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

The 5GS identity type information element is coded as shown in figure 9.11.3.3.1 and table 9.11.3.3.1.

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

Figure 9.11.3.3.1: 5GS identity type information element

Table 9.11.3.3.1: 5GS identity type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of identity (octet 1) | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 1 |  | SUCI |
| 0 | 1 | 0 |  | 5G-GUTI |
| 0 | 1 | 1 |  | IMEI |
| 1 | 0 | 0 |  | 5G-S-TMSI |
| 1 | 0 | 1 |  | IMEISV |
| 1 | 1 | 0 |  | MAC address |
| 1 | 1 | 1 |  | EUI-64 |
|  | | | | |
| All other values are unused and shall be interpreted as "SUCI", if received by the UE. | | | | |

#### 9.11.3.4 5GS mobile identity

The purpose of the 5GS mobile identity information element is to provide either the SUCI, the 5G-GUTI, the IMEI, the IMEISV, the 5G-S-TMSI, the MAC address or the EUI-64.

The 5GS mobile identity information element is coded as shown in figures 9.11.3.4.1, 9.11.3.4.2, 9.11.3.4.3, 9.11.3.4.4, 9.11.3.4.5, 9.11.3.4.6, 9.11.3.4.8 and 9.11.3.4.7, and table 9.11.3.4.1.

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

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

Figure 9.11.3.4.1: 5GS mobile identity information element for type of identity "5G-GUTI"

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

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

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

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

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

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

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

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

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

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

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

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

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

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |  |
| 5GS mobile identity IEI | | | | | | | | octet 1 | |
| Length of 5GS mobile identity contents | | | | | | | | octet 2  octet 3 | |
| 0  spare | 0  spare | 0  spare | 0  spare | 0  spare | Type of identity | | | octet 4 | |
| EUI-64 | | | | | | | | octet 5  octet 12 | |

Figure 9.11.3.4.8: 5GS mobile identity information element for type of identity "EUI-64"

Table 9.11.3.4.1: 5GS mobile identity information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Type of identity (octet 4)  Bits | | | | | | | | | |
| 3 | 2 | 1 |  | | | | | | |
| 0 | 0 | 0 | No identity (see NOTE 1) | | | | | | |
| 0 | 0 | 1 | SUCI | | | | | | |
| 0 | 1 | 0 | 5G-GUTI | | | | | | |
| 0 | 1 | 1 | IMEI | | | | | | |
| 1 | 0 | 0 | 5G-S-TMSI | | | | | | |
| 1 | 0 | 1 | IMEISV | | | | | | |
| 1 | 1 | 0 | MAC address | | | | | | |
| 1 | 1 | 1 | EUI-64 | | | | | | |
| All other values are reserved. | | | | | | | | | |
|  | | | | | | | | | |
| Odd/even indication (octet 4)  Bit | | | | | | | | | |
| 4 |  |  |  | | | | | | |
| 0 |  |  | even number of identity digits | | | | | | |
| 1 |  |  | odd number of identity digits | | | | | | |
|  | | | | | | | | | |
| For the 5G-GUTI, then bits 5 to 8 of octet 4 are coded as "1111", octet 5 through 7 contain the MCC and MNC values as specified below, octet 8 through 10 contain the AMF Region ID, the AMF Set ID and the AMF Pointer values and octet 11 through 14 contain the 5G-TMSI as defined in 3GPP TS 23.003 [4]. | | | | | | | | | |
| MCC, Mobile country code (octet 5, octet 6 bits 1 to 4)  The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | | | | | | | | | |
| MNC, Mobile network code (octet 6 bits 5 to 8, octet 7)  The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 6 shall be coded as "1111".  The contents of the MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12]. | | | | | | | | | |
|  | | | | | | | | | |
| AMF Region ID (octet 8)  This field contains the binary encoding of the AMF Region ID. Bit 8 of octet 7 is the most significant bit and bit 1 of octet 7 is the least significant bit.  AMF Set ID (octet 9, octet 10 bits 7 to 8)  This field contains the binary encoding of the AMF Set ID. Bit 8 of octet 9 is the most significant bit and bit 7 of octet 10 is the least significant bit.  AMF Pointer (octet 10 bits 1 to 6)  This field contains the binary encoding of the AMF Pointer. Bit 6 of octet 9 is the most significant bit and bit 1 of octet 9 is the least significant bit.  5G-TMSI (octet 11 to 14)  Bit 8 of octet 11 is the most significant bit and bit 1 of octet 14 is the least significant bit. | | | | | | | | | |
|  | | | | | | | | | |
| Identity digit (octet 4 bits 5 to 8, octet 5 etc.) | | | | | | | | | |
| For the IMEI, Identity digit field is coded using BCD coding. If the number of identity digits is even then bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". The format of the IMEI is described in 3GPP TS 23.003 [4]. | | | | | | | | | |
|  | | | | | | | | | |
| For the IMEISV, Identity digit field is coded using BCD coding. Bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". The format of the IMEISV is described in 3GPP TS 23.003 [4]. | | | | | | | | | |
|  | | | | | | | | | |
| For the SUCI, bit 8 of octet 4 is spare and shall be coded as zero. Bits 5-7 of octet 4 contain the SUPI format and are coded as shown below. | | | | | | | | | |
| SUPI format (octet 4, bits 5-7)  Bits | | | | | | | | | |
| 7 | 6 | 5 |  |  | | | | | |
| 0 | 0 | 0 |  | IMSI | | | | | |
| 0 | 0 | 1 |  | Network specific identifier | | | | | |
| 0 | 1 | 0 |  | GCI | | | | | |
| 0 | 1 | 1 |  | GLI | | | | | |
| All other values are interpreted as IMSI by this version of the protocol. | | | | | | | | | |
|  | | | | | | | | | |
| For the SUCI with SUPI format "IMSI", octets 5 through 7 contain the MCC and MNC values as specified below. For subsequent fields, bit 8 of octet 8 is the most significant bit and bit 1 of the last octet the least significant bit. The required fields for the SUCI are as defined in 3GPP TS 23.003 [4]. | | | | | | | | | |
| MCC, Mobile country code (octet 5, octet 6 bits 1 to 4)  The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | | | | | | | | | |
| MNC, Mobile network code (octet 6 bits 5 to 8, octet 7)  The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 6 shall be coded as "1111".  The contents of the MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12]. | | | | | | | | | |
|  | | | | | | | | | |
| Routing indicator (octets 8-9)  Routing Indicator shall consist of 1 to 4 digits. The coding of this field is the responsibility of home network operator but BCD coding shall be used. If a network operator decides to assign less than 4 digits to Routing Indicator, the remaining digits shall be coded as "1111" to fill the 4 digits coding of Routing Indicator (see NOTE 2). If no Routing Indicator is configured in the USIM, the UE shall code bits 1 to 4 of octet 8 of the Routing Indicator as "0000" and the remaining digits as “1111". | | | | | | | | | |
|  | | | | | | | | | |
| Protection scheme identifier (octet 10 bits 1 to 4) | | | | | | | | | |
| Bits | | | | | | | | | |
|  | | | | | | | | | |
| 4 | 3 | 2 | 1 |  | | | | | |
| 0 | 0 | 0 | 0 | Null scheme | | | | | |
| 0 | 0 | 0 | 1 | ECIES scheme profile A | | | | | |
| 0 | 0 | 1 | 0 | ECIES scheme profile B | | | | | |
| 0 | 0 | 1 | 1 |  | | | | | |
| to | Reserved | | | | | | | | |
| 1 | 0 | 1 | 1 |  | | | | | |
| 1 | 1 | 0 | 0 |  | | | | | |
| to | Operator-specific protection scheme | | | | | | | | |
| 1 | 1 | 1 | 1 |  | | | | | |
|  | | | | | | | | | |
| Bits 5-8 of octet 10 are spare and shall be coded as zero. | | | | | | | | | |
|  | | | | | | | | | |
| Home network public key identifier (octet 10) | | | | | | | | | |
| The Home network public key identifier (PKI) field is coded as defined in 3GPP TS 23.003 [4]. Home network public key identifier shall be coded as "00000000" when Protection scheme identifier is set to "0000" (i.e. Null scheme). | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  | Home network PKI value 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |  |  |
| to |  | Home network PKI value (1-254) | | | | | | | |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 |  |  |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |  | Reserved |
|  | | | | | | | | | |
|  | | | | | | | | | |
| Scheme output (octets 12 to x)  The Scheme output field consists of a string of characters with a variable length or hexadecimal digits as specified in 3GPP TS 23.003 [4]. If Protection scheme identifier is set to "0000" (i.e. Null scheme), then the Scheme output consists of the MSIN and is coded using BCD coding with each digit of the MSIN coded over 4 bits. If the MSIN includes an odd number of digits, bits 5 to 8 of octet x shall be coded as "1111". If Protection scheme identifier is not "0000" (i.e. ECIES scheme profile A, ECIES scheme profile B or Operator-specific protection scheme), then Scheme output is coded as hexadecimal digits. | | | | | | | | | |
|  | | | | | | | | | |
| For the SUCI with SUPI format set to "Network specific identifier", the SUCI NAI field contains an NAI constructed as specified in subclause 28.7.3 of 3GPP TS 23.003 [4] and encoded as UTF-8 string. | | | | | | | | | |
|  | | | | | | | | | |
| For the SUCI with SUPI format set to "GCI", the SUCI NAI field contains an NAI constructed as specified in subclause 28.15.5 of 3GPP TS 23.003 [4] and encoded as UTF-8 string. | | | | | | | | | |
|  | | | | | | | | | |
| For the SUCI with SUPI format set to "GLI", the SUCI NAI field contains an NAI constructed as specified in subclause 28.16.5 of 3GPP TS 23.003 [4] and encoded as UTF-8 string. | | | | | | | | | |
|  | | | | | | | | | |
| For the 5G-S-TMSI, bits 5 to 8 of octet 4 are coded as "1111". The coding of the 5G-S-TMSI is left open for each administration. | | | | | | | | | |
|  | | | | | | | | | |
| AMF Set ID (octet 5, octet 6 bits 7 to 8)  This field contains the binary encoding of the AMF Set ID. Bit 8 of octet 5 is the most significant bit and bit 7 of octet 6 is the least significant bit.  AMF Pointer (octet 6 bits 1 to 6)  This field contains the binary encoding of the AMF Pointer. Bit 6 of octet 6 is the most significant bit and bit 1 of octet 6 is the least significant bit.  5G-TMSI (octet 7 to 10)  Bit 8 of octet 7 is the most significant bit and bit 1 of octet 10 is the least significant bit. | | | | | | | | | |
| MAC address (octets 5 to 10)  This field contains the MAC address as defined in subclause 8 of IEEE Std 802 [43].  Bit 8 of octet 5 is the most significant bit and bit 1 of octet 10 is the least significant bit.  EUI-64 (octets 5 to12)  This field contains an EUI-64 as defined in [48].  Bit 8 of octet 5 is the most significant bit and bit 1 of octet 10 is the least significant bit. | | | | | | | | | |
| MAC address usage restriction indication (MAURI) (octet 4 bit 4) | | | | | | | | | |
| Bit | | | | | | | | | |
| 4 |  |  |  |  | | | | | |
| 0 |  |  |  | No restrictions | | | | | |
| 1 |  |  |  | MAC address is not usable as an equipment identifier | | | | | |
|  | | | | | | | | | |
| For Type of identity "No identity", the length of mobile identity contents parameter shall be set to 1 and the bits 4-8 of octet 4 are spare and shall be coded as zero. | | | | | | | | | |
|  | | | | | | | | | |
| NOTE 1: This can be used when the requested identity is not available at the UE during the identification procedure.  NOTE 2: For a 3-digit Routing Indicator, e.g "567", bits 1 to 4 of octet 8 are coded as "0101", bits 5 to 8 of octet 8 are coded as "0110", bits 1 to 4 of octet 9 are coded as "0111", bits 5 to 8 of octet 9 are coded as "1111". | | | | | | | | | |

#### 9.11.3.5 5GS network feature support

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

The 5GS network feature support information element is coded as shown in figure 9.11.3.5.1 and table 9.11.3.5.1.

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

If the network does not include octet 4 as defined in figure 9.11.3.5.1 in the present version of the protocol, then the UE shall interpret this as a receipt of an information element with all bits of octet 4 coded as zero.

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

Figure 9.11.3.5.1: 5GS network feature support information element

Table 9.11.3.5.1: 5GS network feature support information element

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

#### 9.11.3.6 5GS registration result

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

The 5GS registration result information element is coded as shown in figure 9.11.3.6.1 and table 9.11.3.6.1.

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

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

Figure 9.11.3.6.1: 5GS registration result information element

Table 9.11.3.6.1: 5GS registration result information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5GS registration result value (octet 3, bits 1 to 3) (NOTE) | | | | |
| 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) (NOTE) | | | | |
| Bit | | | | |
| 4 |  |  |  |  |
| 0 |  |  |  | SMS over NAS not allowed |
| 1 |  |  |  | SMS over NAS allowed |
|  | | | | |
| Network slice-specific authentication and authorization is to be performed (NSSAA to be performed) (octet 3, bit 5) (NOTE) | | | | |
| Bit | | | | |
| 5 |  |  |  |  |
| 0 |  |  |  | Network slice-specific authentication and authorization is not to be performed |
| 1 |  |  |  | Network slice-specific authentication and authorization is to be performed |
|  | | | | |
| Emergency registered (octet 3, bit 6) | | | | |
| Bit | | | | |
| 6 |  |  |  |  |
| 0 |  |  |  | Not registered for emergency services |
| 1 |  |  |  | Registered for emergency services |
|  | | | | |
|  | | | | |
| Bits 7 to 8 of octet 3 are spare and shall be coded as zero. | | | | |
| NOTE: All bits other than bit 6 in octet 3 shall be ignored by the UE when the 5GS registration result IE is received in the CONFIGURATION UPDATE COMMAND message | | | | |

#### 9.11.3.7 5GS registration type

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

The 5GS registration type information element is coded as shown in figure 9.11.3.7.1 and table 9.11.3.7.1.

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

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

Figure 9.11.3.7.1: 5GS registration type information element

Table 9.11.3.7.1: 5GS registration type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5GS registration type value (octet 1, bits 1 to 3) | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 1 |  | initial registration |
| 0 | 1 | 0 |  | mobility registration updating |
| 0 | 1 | 1 |  | periodic registration updating |
| 1 | 0 | 0 |  | emergency registration |
| 1 | 1 | 1 |  | reserved |
|  | | | | |
| All other values are unused and shall be interpreted as "initial registration", if received by the network. | | | | |
|  | | | | |
| Follow-on request bit (FOR) (octet 1, bit 4) | | | | |
| Bit | | | | |
| 4 |  |  |  |  |
| 0 |  |  |  | No follow-on request pending |
| 1 |  |  |  | Follow-on request pending |

#### 9.11.3.8 5GS tracking area identity

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

The 5GS tracking area identity information element is coded as shown in figure 9.11.3.8.1 and table 9.11.3.8.1.

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

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

Figure 9.11.3.8.1: 5GS tracking area identity information element

Table 9.11.3.8.1: 5GS tracking area identity information element

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

#### 9.11.3.9 5GS tracking area identity list

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

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

The 5GS tracking area identity list information element is coded as shown in figure 9.11.3.8.1, figure 9.11.3.8.2, figure 9.11.3.9.3, figure 9.11.3.9.4 and table 9.11.3.9.1.

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

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

Figure 9.11.3.9.1: 5GS tracking area identity list information element

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

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

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

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

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

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

Table 9.11.3.9.1: Tracking area identity list information element

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

#### 9.11.3.9A 5GS update type

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

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

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

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

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

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

|  |  |  |
| --- | --- | --- |
| SMS over NAS transport requested (SMS requested) (octet 3, bit 1) | | |
| Bit | | |
| 1 |  |  |
| 0 |  | SMS over NAS not supported |
| 1 |  | SMS over NAS supported |
|  | | |
| NG-RAN Radio Capability Update (NG-RAN-RCU) (octet 3, bit 2) | | |
| Bit | | |
| 2 |  |  |
| 0 |  | NG-RAN radio capability update not needed |
| 1 |  | NG-RAN radio capability update needed |
|  | | |
| 5GS Preferred CIoT network behaviour (5GS PNB-CIoT) (octet 3, bits 3 and 4) | | |
|  | | |
| Bits | | |
| 4 | 3 |  |
| 0 | 0 | no additional information |
| 0 | 1 | control plane CIoT 5GS optimization |
| 1 | 0 | user plane CIoT 5GS optimization |
| 1 | 1 | reserved |
|  | | |
| EPS Preferred CIoT network behaviour (EPS-PNB-CIoT) (octet 3, bits 5 and 6) | | |
|  | | |
| Bits   |  |  |  | | --- | --- | --- | | 6 | 5 |  | | | |
| |  |  |  | | --- | --- | --- | | 0 | 0 | no additional information | | 0 | 1 | control plane CIoT EPS optimization | | 1 | 0 | user plane CIoT EPS optimization | | 1 | 1 | reserved | | | |
|  | | |
|  | | |
| Bits 7 to 8 of octet 3 are spare and shall be coded as zero. | | |

#### 9.11.3.10 ABBA

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

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

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

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

Figure 9.11.3.10.1: ABBA information element

Table 9.11.3.10.1: ABBA information element

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

#### 9.11.3.11 Void

#### 9.11.3.12 Additional 5G security information

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

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

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

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

Figure 9.11.3.12.1: Additional 5G security information information element

Table 9.11.3.12.1: Additional 5G security information information element

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

#### 9.11.3.12A Additional information requested

The purpose of the Additional information requested information element is to enable the UE to request ciphering keys for deciphering of ciphered broadcast assistance data.

The Additional information requested information element is coded as shown in figure 9.11.3.12A.1 and table 9.11.3.12A.1.

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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
| Additional information requested IEI | | | | | | | | | octet 1 |
| Length of additional information requested contents | | | | | | | | | octet 2 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | CipherKey | octet 3 | |
| Spare | | | | | | |

Figure 9.11.3.12A.1: Additional information requested information element

Table 9.11.3.12A.1: Additional information requested information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ciphering keys for ciphered broadcast assistance data (CipherKey) (octet 3, bit 1) | | | | |
| Bit | | | | |
| 1 |  |  |  |  |
| 0 |  |  |  | ciphering keys for ciphered broadcast assistance data not requested |
| 1 |  |  |  | ciphering keys for ciphered broadcast assistance data requested |
|  | | | | |
| Bits 8 to 2 of octet 3 are spare and shall be coded as zero. | | | | |

#### 9.11.3.13 Allowed PDU session status

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

The Allowed PDU session status information element is coded as shown in figure 9.11.3.13.1 and table 9.11.3.13.1.

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

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

Figure 9.11.3.13.1: Allowed PDU session status information element

Table 9.11.3.13.1: Allowed PDU session status information element

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

#### 9.11.3.14 Authentication failure parameter

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

#### 9.11.3.15 Authentication parameter AUTN

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

#### 9.11.3.16 Authentication parameter RAND

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

#### 9.11.3.17 Authentication response parameter

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

#### 9.11.3.18 Configuration update indication

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

The Configuration update indication information element is coded as shown in figure 9.11.3.18.1 and table 9.11.3.18.1.

The Configuration update indication is a type 1 information element.

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

Figure 9.11.3.18.1: Configuration update indication

Table 9.11.3.18.1: Configuration update indication

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

#### 9.11.3.18A CAG information list

The purpose of the CAG information list information element is to provide "CAG information list" or to delete the "CAG information list" at the UE.

The CAG information list information element is coded as shown in figures 9.11.3.18A.1 and 9.11.3.18A.2 and table 9.11.3.18A.1.

The CAG information list is a type 6 information element, with a minimum length of 3 octets.

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

Figure 9.11.3.18A.1: CAG information list information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
| Length of entry contents | | | | | | | | octet q | |
| MCC digit 2 | | | | MCC digit 1 | | | | | octet q+1 |
| MNC digit 3 | | | | MCC digit 3 | | | | | octet q+2 |
| MNC digit 2 | | | | MNC digit 1 | | | | | octet q+3 |
| 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | CAG  only | octet q+4 | |
| CAG-ID 1 | | | | | | | | octet q+5\*  octet q+8\* | |
| CAG-ID 2 | | | | | | | | octet q+9\*  octet q+12\* | |
| … | | | | | | | | octet q+13\*  octet q+4m\* | |
| CAG-ID n | | | | | | | | octet q+4m+1\*  octet q+4m+4\* | |

Figure 9.11.3.18A.2: Entry n

Table 9.11.3.18A.1: CAG information list information element

|  |  |
| --- | --- |
| MCC, Mobile country code (octet q+1 and bits 1 to 4 octet q+2)  The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. | |
|  | |
| MNC, Mobile network code (bits 5 to 8 of octet q+2 and octet q+3)  The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 6 shall be coded as "1111". | |
|  | |
| The contents of the MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12]. | |
|  | |
| Indication that the UE is only allowed to access 5GS via CAG cells (CAGonly) (bit 1 of octet q+4) | |
| Bit | |
| 1 |  |
| 0 | "Indication that the UE is only allowed to access 5GS via CAG cells" is not set (i.e. the UE is allowed to access 5GS via non-CAG cells) |
| 1 | "Indication that the UE is only allowed to access 5GS via CAG cells" is set (i.e. the UE is not allowed to access 5GS via non-CAG cells) |
|  | |
| CAG-ID m (octet q+4m+1 to octet q+4m+4)  This field contains the 32 bit CAG-ID. The coding of the CAG-ID is defined as the CAG-Identifier in 3GPP TS 23.003 [4]. | |

#### 9.11.3.18B CIoT small data container

This information element is used to encapsulate the CIoT user data, SMS, or location services message with a size that is not more than 254 octets between the UE and the AMF when the UE is using control plane CIoT 5GS optimization. The CIoT small data container information element is coded as shown in figure 9.11.3.18B.1, figure 9.11.3.18B.2, figure 9.11.3.18B.3, figure 9.11.3.18B.4 and table 9.11.3.18B.1.

The CIoT small data container is a type 4 information element with a minimum length of 4 octets and a maximum length of 257 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| CIoT small data container IEI | | | | | | | | octet 1 |
| Length of CIoT small data container contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
| CIoT small data container contents | | | | | | | |  |
|  | | | | | | | | octet 257 |

Figure 9.11.3.18B.1: CIoT small data container information element

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | | 2 | 1 |  | | |
| Data type | | | | DDX | | | PDU session identity | | | | | octet 3 |
| Data contents | | | | | | | | | | | octet 4  octet 257 | |

Figure 9.11.3.18B.2: CIoT small data container contents

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | | 2 | | 1 | |  | | |
| Data type | | | | DDX | | | 0  Spare | | 0  Spare | | 0  Spare | | octet 3 | |
| Length of additional information | | | | | | | | | | | | | | octet 4 |
| Additional information | | | | | | | | | | | | | | octet 5\*  octet m\* |
| Data contents | | | | | | | | | | | | | | octet m+1  octet n |

Figure 9.11.3.18B.3: CIoT small data container contents for Data type "Location services message container"

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | | 2 | 1 |  | | |
| Data type | | | |  | | | Spare | | | | | octet 3 |
| Data contents | | | | | | | | | | | octet 4  octet n | |

Figure 9.11.3.18B.4: CIoT small data container contents for Data type "SMS"

Table 9.11.3.18B.1: CIoT small data container information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CIoT small data container contents (octet 3 to octet 257) | | | | |
|  | | | | |
| These octets include user data to be delivered between UE and AMF. | | | | |
|  | | | | |
| Data type (octet 3, bits 6 to 8)  Bits | | | | |
| 8 | 7 | 6 |  |  |
| 0 | 0 | 0 |  | Control plane user data |
| 0 | 0 | 1 |  | SMS |
| 0 | 1 | 0 |  | Location services message container |
|  | | | | |
| All other values are spare. | | | | |
|  | | | | |
| When the Data type is "Control plane user data ", the PDU session identity and Downlink data expected (DDX) fields are encoded as follows: | | | | |
|  | | | | |
| PDU session identity (octet 3, bits 1 to 4)  Bit | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 0 |  | No PDU session identity assigned |
| 0 | 0 | 1 |  | PDU session identity value 1 |
| 0 | 1 | 0 |  | PDU session identity value 2 |
| 0 | 1 | 1 |  | PDU session identity value 3 |
| 1 | 0 | 0 |  | PDU session identity value 4 |
| 1 | 0 | 1 |  | PDU session identity value 5 |
| 1 | 1 | 0 |  | PDU session identity value 6 |
| 1 | 1 | 1 |  | PDU session identity value 7 |
|  | | | | |
|  | | | | |
| Downlink data expected (DDX) (octet 3, bits 5 to 6) | | | | |
| Bits | | | | |
| 5 | 4 |  | | |
| 0 | 0 | No information available | | |
| 0 | 1 | No further uplink and no further downlink data transmission subsequent to the uplink data transmission is expected | | |
| 1 | 0 | Only a single downlink data transmission and no further uplink data transmission subsequent to the uplink data transmission is expected | | |
| 1 | 1 | reserved | | |
|  | | | | |
| NOTE: The DDX field is only used in the UE to network direction. | | | | |
|  | | | | |
| Data contents (octet 4 to octet 257)  This field contains the control plane user data. | | | | |
|  | | | | |
| When the Data type is "SMS", Bits 1 to 5 of octet 3 are spare and shall be coded as zero. | | | | |
| Data contents (octet 4 to octet 257)  This field contains an SMS message.  When the Data type is "Location services message container":  Downlink data expected (DDX) (octet 3, bits 5 to 4)  This field is encoded as described above for the case when the Data type is "Control plane user data".  Bits 3 to 1 of octet 3 are spare and shall be encoded as zero.  Length of Additional information (octet 4) (see NOTE)  Indicates the length, in octets, of the Additional information field.  Additional information (octets 5 to m)  Contains additional information if provided by the upper layer location services application.  Data contents (octets m+1 to n)  Contains the location services message payload. | | | | |
|  | | | | |
| NOTE: The Length of Additional information shall be set to zero if the upper layer location service application does not provide routing information. | | | | |

#### 9.11.3.18C Ciphering key data

The purpose of the Ciphering key data information element is to transfer a list of ciphering data sets from the network to the UE for deciphering of ciphered assistance data.

The Ciphering key data information element is coded as shown in figure 9.11.3.18C.1, figure 9.11.3.18C.2 and table 9.11.3.18C.1.

The Ciphering key data is a type 6 information element, with a minimum length of m octets and a maximum length of n octets. The list can contain a maximum of 16 ciphering data sets.

Editor's note [WI: 5G\_eLCS, CR#1705]: The positioning SIBs included in figure 9.11.3.18C.2 and table 9.11.3.18C.1 include positioning SIBs defined in TS 36.331 and TS 36.355 for E-UTRAN in Rel-15 plus new positioning SIBs for NG-RAN being discussed in RAN2 for Rel-16. The positioning SIBs in figure 9.11.3.18C.2 and table 9.11.3.18C.1 will need to be aligned later with RAN2 agreements for Rel-16. At that time, the minimum and maximum octet lengths x and n can also be calculated and included.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |  |
| Ciphering key data IEI | | | | | | | | octet 1 | |
| Length of ciphering key data contents | | | | | | | | octet 2  octet 3 | |
| Ciphering data set 1 | | | | | | | | octet 4  octet i | |
| Ciphering data set 2 | | | | | | | | octet i+1\*  octet l\* | |
| … | | | | | | | | octet l+1\*  octet m\* | |
| Ciphering data set p | | | | | | | | octet m+1\*  octet n\* | |

Figure 9.11.3.18C.1: Ciphering key data information element

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | 2 | 1 | |  | |
| Ciphering set ID | | | | | | | | | | octet 1  octet 2 | |
| Ciphering key | | | | | | | | | | octet 3  octet 18 | |
| 0 | 0 | 0 | c0 length | | | | | | | octet 19 | |
| Spare | | |  |
| c0 | | | | | | | | | | octet 20  octet k | |
| 0 | 0 | 0 | 0 | | E-UTRA posSIB length | | | | | octet k+1 | |
| Spare | | | |  | | | | |  | | |
| PosSIBType1-1 | PosSIBType1-2 | PosSIBType1-3 | PosSIBType1-4 | | PosSIBType1-5 | PosSIBType1-6 | PosSIBType1-7 | PosSIBType1-8 | | octet k+2  octet k+3  octet p | |
| PosSIBType2-1 | PosSIBType2-2 | PosSIBType2-3 | PosSIBType2-4 | | PosSIBType2-5 | PosSIBType2-6 | PosSIBType2-7 | PosSIBType2-8 | |
| PosSIBType2-9 | PosSIBType2-10 | PosSIBType2-11 | PosSIBType2-12 | | PosSIBType2-13 | PosSIBType2-14 | PosSIBType2-15 | PosSIBType2-16 | |
| PosSIBType2-17 | PosSIBType2-18 | PosSIBType2-19 | PosSIBType2-20 | | PosSIBType2-21 | PosSIBType2-22 | PosSIBType2-23 | PosSIBType3-1 | |
| 0 | 0 | 0 | 0 | | NR posSIB length | | | | | octet p+1 | |
| Spare | | | |  | | | | |  | | |
| PosSIBType1-1 | PosSIBType1-2 | PosSIBType1-3 | PosSIBType1-4 | | PosSIBType1-5 | PosSIBType1-6 | PosSIBType1-7 | PosSIBType1-8 | | octet p+2  octet p+3  octet q | |
| PosSIBType2-1 | PosSIBType2-2 | PosSIBType2-3 | PosSIBType2-4 | | PosSIBType2-5 | PosSIBType2-6 | PosSIBType2-7 | PosSIBType2-8 | |
| PosSIBType2-9 | PosSIBType2-10 | PosSIBType2-11 | PosSIBType2-12 | | PosSIBType2-13 | PosSIBType2-14 | PosSIBType2-15 | PosSIBType2-16 | |
| PosSIBType2-17 | PosSIBType2-18 | PosSIBType2-19 | PosSIBType2-20 | | PosSIBType2-21 | PosSIBType2-22 | PosSIBType2-23 | PosSIBType3-2 | |
| PosSIBType3-3 | PosSIBType3-4 | 0  Spare | 0  Spare | | 0  Spare | 0  Spare | 0  Spare | 0  Spare | |
| Validity start time | | | | | | | | | | octet q+1  octe q+5 | |
| Validity duration | | | | | | | | | | octet q+6  octet q+7 | |
| TAIs list | | | | | | | | | | octet q+8  octet r | |

Figure 9.11.3.18C.2: Ciphering data set

Table 9.11.3.18C.1: Ciphering key data information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Value part of the Ciphering key data information element (octets 4 to n) | | | | |
|  | | | | |
| The value part of the Ciphering key data information element consists of one or several ciphering data sets. | | | | |
| The UE shall store the complete list received. If more than 16 ciphering data sets are included in this information element, the UE shall store the first 16 ciphering data sets and ignore the remaining octets of the information element. | | | | |
|  | | | | |
|  | | | | |
| Ciphering data set: | | | | |
|  | | | | |
| Ciphering set ID (octets 1 to 2) | | | | |
|  | | | | |
| This field contains the binary encoding of the ID identifying the ciphering set. | | | | |
|  | | | | |
| Ciphering key (octets 3 to octet 18) | | | | |
|  | | | | |
| This field contains the 128 bit ciphering key. | | | | |
|  | | | | |
| c0 length (octet 19, bits 5 to 1)  This field contains the binary encoding of the length, in octets, of the c0 counter. The maximum value for the length of the c0 counter is 16 octets. | | | | |
|  | | | | |
| Bits 8 to 6 of octect 19 are spare and shall be coded as zero. | | | | |
|  | | | | |
|  | | | | |
| c0 (octets 20 to k) | | | | |
|  | | | | |
| This field contains the binary encoding of the c0 counter. | | | | |
|  | | | | |
|  | | | | |
| E-UTRA posSIB length (octet k+1, bits 4 to 1)  This field contains the length in octets of the E -UTRA Positioning SIB types. A length of zero means E -UTRA Positioning SIB types are not included.  E-UTRA Positioning SIB types for which the ciphering data set is applicable (octets k+2 to p). Unassigned bits shall be ignored by a UE. Non-included bits shall be assumed to be zero by a UE. | | | | |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-1 (octet k+2, bit 8) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-1 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-1 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-2 (octet k+2, bit 7) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-2 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-2 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-3 (octet k+2, bit 6) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-3 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-3 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-4 (octet k+2, bit 5) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-4 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-4 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-5 (octet k+2, bit 4) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-5 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-5 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-6 (octet k+2, bit 3) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-6 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-6 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-7 (octet k+2, bit 2) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-7 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-7 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-8 (octet k+2, bit 1) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-8 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-8 |
|  | | | | |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-1 (octet k+3, bit 8) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-1 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-1 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-2 (octet k+3, bit 7) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-2 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-2 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-3 (octet k+3, bit 6) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-3 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-3 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-4 (octet k+3, bit 5) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-4 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-4 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-5 (octet k+3, bit 4) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-5 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-5 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-6 (octet k+3, bit 3) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-6 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-6 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-7 (octet k+3, bit 2) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-7 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-7 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-8 (octet k+3, bit 1) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-8 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-8 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-9 (octet k+4, bit 8) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-9 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-9 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-10 (octet k+4, bit 7) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-10 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-10 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-11 (octet k+4, bit 6) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-11 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-11 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-12 (octet k+4, bit 5) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-12 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-12 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-13 (octet k+4, bit 4) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-13 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-13 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-14 (octet k+4, bit 3) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-14 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-14 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-15 (octet k+4, bit 2) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-15 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-15 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-16 (octet k+4, bit 1) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-16 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-16 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-17 (octet k+5, bit 8) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-17 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-17 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-18 (octet k+5, bit 7) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-18 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-18 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-19 (octet k+5, bit 6) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-19 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-19 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-20 (octet k+5, bit 5) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-20 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-20 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-21 (octet k+5, bit 4) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-21 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-21 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-22 (octet k+5, bit 3) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-22 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-22 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-23 (octet k+5, bit 2) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-23 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-23 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 3-1 (octet k+5, bit 1) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 3-1 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 3-1 |
|  | | | | |
| Any unassigned bits shall be coded as zero. | | | | |
|  | | | | |
|  | | | | |
| NR posSIB length (octet p+1, bits 4 to 1)  This field contains the length in octets of the NR Positioning SIB types. A length of zero means NR Positioning SIB types are not included.  NR Positioning SIB types for which the ciphering data set is applicable (octets p+2 to q). Unassigned bits shall be ignored. Non-included bits shall be assumed to be zero. | | | | |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-1 (octet p+2, bit 8) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-1 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-1 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-2 (octet p+2, bit 7) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-2 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-2 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-3 (octet p+2, bit 6) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-3 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-3 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-4 (octet p+2, bit 5) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-4 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-4 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-5 (octet p+2, bit 4) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-5 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-5 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-6 (octet p+2, bit 3) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-6 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-6 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-7 (octet p+2, bit 2) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-7 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-7 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 1-8 (octet p+2, bit 1) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 1-8 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 1-8 |
|  | | | | |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-1 (octet p+3, bit 8) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-1 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-1 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-2 (octet p+3, bit 7) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-2 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-2 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-3 (octet p+3, bit 6) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-3 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-3 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-4 (octet p+3, bit 5) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-4 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-4 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-5 (octet p+3, bit 4) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-5 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-5 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-6 (octet p+3, bit 3) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-6 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-6 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-7 (octet p+3, bit 2) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-7 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-7 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-8 (octet p+3, bit 1) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-8 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-8 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-9 (octet p+4, bit 8) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-9 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-9 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-10 (octet p+4, bit 7) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-10 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-10 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-11 (octet p+4, bit 6) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-11 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-11 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-12 (octet p+4, bit 5) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-12 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-12 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-13 (octet p+4, bit 4) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-13 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-13 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-14 (octet p+4, bit 3) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-14 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-14 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-15 (octet p+4, bit 2) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-15 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-15 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-16 (octet p+4, bit 1) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-16 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-16 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-17 (octet p+5, bit 8) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-17 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-17 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-18 (octet p+5, bit 7) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-18 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-18 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-19 (octet p+5, bit 6) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-19 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-19 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-20 (octet p+5, bit 5) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-20 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-20 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-21 (octet p+5, bit 4) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-21 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-21 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-22 (octet p+5, bit 3) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-22 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-22 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 2-23 (octet p+5, bit 2) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 2-23 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 2-23 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 3-2 (octet p+5, bit 1) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 3-2 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 3-2 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 3-3 (octet p+6, bit 8) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 3-3 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 3-3 |
|  | | | | |
| Ciphering data set applicable for positioning SIB type 3-4 (octet p+6, bit 7) | | | | |
| 0 |  |  |  | Ciphering data set not applicable to positioning SIB type 3-4 |
| 1 |  |  |  | Ciphering data set applicable to positioning SIB type 3-4 |
|  | | | | |
| Any unassigned bits shall be coded as zero. | | | | |
|  | | | | |
|  | | | | |
| Validity start time (octets q+1 to q+5) | | | | |
|  | | | | |
| This field contains the UTC time when the ciphering data set becomes valid, encoded as octets 2 to 6 of the Time zone and time IE specified in 3GPP TS 24.008 [12]. | | | | |
|  | | | | |
|  | | | | |
| Validity duration (octets q+6 to q+7) | | | | |
|  | | | | |
| This field contains the duration for which the ciphering data set is valid after the validity start time, in units of minutes. | | | | |
|  | | | | |
|  | | | | |
| TAIs list (octets q+8 to r) | | | | |
|  | | | | |
| This field contains the list of tracking areas for which the ciphering data set is applicable, encoded as octets 2 to n of the Tracking area identity list IE as specified in subclause 9.11.3.9. If the TAIs list is empty (as indicated by a zero length), the ciphering data set is applicable to the entire serving PLMN. | | | | |
|  | | | | |

#### 9.11.3.18D Control plane service type

The purpose of the Control plane service type information element is to specify the purpose of the CONTROL PLANE SERVICE REQUEST message.

The Control plane service type information element is coded as shown in figure 9.11.3.18D.1 and table 9.11.3.18D.1.

The Control plane service type is a type 1 information element.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | | 3 | | 2 | 1 |  | |
| Control plane service type  IEI | | | | | 0  Spare | | Control plane service type  value | | | | octet 1 |

Figure 9.9.3.18D.1: Control plane service type information element

Table 9.9.3.18D.1: Control plane service type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control plane service type value (octet 1, bit 1 to 3) | | | | |
|  | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 0 |  | mobile originating request |
| 0 | 0 | 1 |  | mobile terminating request |
|  |  |  |  |  |
| 0 | 1 | 0 |  |  |
|  | to |  |  | unused; shall be interpreted as " mobile originating request", if received by the network. |
| 1 | 1 | 1 |  |  |
|  | | | | |
|  | | | | |

#### 9.11.3.19 Daylight saving time

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

#### 9.11.3.20 De-registration type

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

The De-registration type information element is coded as shown in figure 9.11.3.20.1 and table 9.11.3.20.1.

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

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

Figure 9.11.3.20.1: Deregistration type information element

Table 9.11.3.20.1: Deregistration type information element

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

#### 9.11.3.21 Void

#### 9.11.3.22 Void

#### 9.11.3.23 Emergency number list

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

#### 9.11.3.23A EPS bearer context status

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

#### 9.11.3.24 EPS NAS message container

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

The EPS NAS message container information element is coded as shown in figure 9.11.3.24.1 and table 9.11.3.24.1.

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

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

Figure 9.11.3.24.1: EPS NAS message container information element

Table 9.11.3.24.1: EPS NAS message container information element

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

#### 9.11.3.25 EPS NAS security algorithms

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

#### 9.11.3.26 Extended emergency number list

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

#### 9.11.3.26A Extended DRX parameters

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

#### 9.11.3.27 Void

#### 9.11.3.28 IMEISV request

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

#### 9.11.3.29 LADN indication

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

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

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

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

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

Figure 9.11.3.29.1: LADN indication information element

Table 9.11.3.29.1: LADN indication information element

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

#### 9.11.3.30 LADN information

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

The LADN information information element is coded as shown in figure 9.11.3.30.1, figure 9.11.3.30.2 and table 9.11.3.30.1.

The LADN information is a type 6 information element with a minimum length of 3 octets and a maximum length of 1715 octets.

The LADN information information element can contain a minimum of 0 and a maximum of 8 different LADNs each including a DNN and a 5GS tracking area identity list.

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

Figure 9.11.3.30.1: LADN information information element

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

Figure 9.11.3.30.2: LADN

Table 9.11.3.30.1: LADN information information element

|  |
| --- |
| Value part of the LADN information information element (octet 4 to octet h)  The value part of the LADN information information element consists of one or several LADNs. Each LADN (e.g. octet 4 to octet a) consists one DNN value and one 5GS tracking area identity list. The length of each LADN is determined by the length of DNN value field and the length of 5GS tracking area identity list field.  The UE shall store the complete list as received. If more than 8 LADNs are included in this information element, the UE shall store the first 8 LADNs and ignore the remaining octets of the information element.  DNN value (octet 5 to octet m):  DNN value field is coded as DNN value part of DNN information element as specified in subclause 9.11.2.1B starting with the third octet. |
| 5GS tracking area identity list (octet m+1 to octet a): |
| 5GS tracking area identity list field is coded as the length and the value part of the 5GS Tracking area identity list information element as specified in subclause 9.11.3.9 starting with the second octet. |

#### 9.11.3.31 MICO indication

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

The MICO indication information element is coded as shown in figure 9.11.3.31.1 and table 9.11.3.31.1.

The MICO indication is a type 1 information element.

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

Figure 9.11.3.31.1: MICO indication

Table 9.11.3.31.1: MICO indication

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

#### 9.11.3.31A MA PDU session information

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

The MA PDU session information information element is coded as shown in figure 9.11.3.31A.1 and table 9.11.3.31A.1.

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

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

Figure 9.11.3.31A.1: MA PDU session information information element

Table 9.11.3.31A.1: MA PDU session information information element

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

#### 9.11.3.31B Mapped NSSAI

The purpose of the Mapped NSSAI information element is to transfer S-NSSAI(s) applicable in the HPLMN to the visited PLMN.

The Mapped NSSAI information element is coded as shown in figure 9.11.3.31B.1, figure 9.11.3.31B.2 and table 9.11.3.31B.1.

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

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

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

Figure 9.11.3.31B.1: Mapped NSSAI information element

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

Figure 9.11.3.31B.2: Mapped S-NSSAI content

Table 9.11.3.31B.1: Mapped NSSAI information element

|  |
| --- |
| Value part of the Mapped NSSAI information element (octet 3 to v)  The value part of the Mapped NSSAI information element consists of one or more mapped S-NSSAI contents.  Mapped S-NSSAI content:  Length of S-NSSAI contents (octet 3)  Mapped HPLMN Slice/service type (SST) (octet 4)  This field contains the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SST value is mapped. The coding of the SST value part is defined in 3GPP TS 23.003 [4].  NOTE 1: Octet 4 (i.e. mapped HPLMN SST) shall always be included.  Mapped HPLMN Slice differentiator (SD) (octet 5 to octet 7)  This field contains a 24-bit SD value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SD value is mapped. The coding of the SD value part is defined in 3GPP TS 23.003 [4].  NOTE 2: If the octet 5 is included, then octet 6 and octet 7 shall be included. |

#### 9.11.3.31C Mobile station classmark 2

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

#### 9.11.3.32 NAS key set identifier

The NAS key set identifier is allocated by the network.

The NAS key set identifier information element is coded as shown in figure 9.11.3.32.1 and table 9.11.3.32.1.

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

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

Figure 9.11.3.32.1: NAS key set identifier information element

Table 9.11.3.32.1: NAS key set identifier information element

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

#### 9.11.3.33 NAS message container

The purpose of the NAS message container IE is to encapsulate a plain 5GS NAS REGISTRATION REQUEST or SERVICE REQUEST message, or to encapsulate non-cleartext IEs of a CONTROL PLANE SERVICE REQUEST message.

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

The NAS message container is a type 6 information element.

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

Figure 9.11.3.33.1: NAS message container information element

Table 9.11.3.33.1: NAS message container information element

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

#### 9.11.3.34 NAS security algorithms

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

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

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

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

Figure 9.11.3.34.1: NAS security algorithms information element

Table 9.11.3.34.1: NAS security algorithms information element

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

#### 9.11.3.35 Network name

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

#### 9.11.3.36 Network slicing indication

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

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

The Network slicing indication is a type 1 information element.

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

Figure 9.11.3.36.1: Network slicing indication

Table 9.11.3.36.1: Network slicing indication

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

#### 9.11.3.36A Non-3GPP NW provided policies

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

#### 9.11.3.37 NSSAI

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

The NSSAI information element is coded as shown in figure 9.11.3.37.1 and table 9.11.3.37.1.

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

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

NOTE 2: The number of S-NSSAI values in an allowed NSSAI or pending NSSAI cannot exceed eight.

NOTE 3: The number of S-NSSAI values in a configured NSSAI cannot exceed sixteen.

NOTE 4: More than one S-NSSAIs in an NSSAI can have the same SST values, and optionally same SD values, which are associated with different mapped HPLMN SST values and optionally mapped HPLMN SD values.

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

Figure 9.11.3.37.1: NSSAI information element

Table 9.11.3.37.1: NSSAI information element

|  |
| --- |
| Value part of the NSSAI information element (octet 3 to v)  The value part of the NSSAI information element consists of one or more S-NSSAI values. Each S-NSSAI value consists of one S-NSSAI and optionally one mapped S-NSSAI.  If the recipient of this information element is the UE, the UE shall store the complete list received. If the NSSAI information element conveys an allowed NSSAI and more than 8 S-NSSAI values are included in this information element, the UE shall store the first 8 S-NSSAI values and ignore the remaining octets of the information element.  If the NSSAI information element conveys a configured NSSAI and more than 16 S-NSSAI values are included in this information element, the UE shall store the first 16 S-NSSAI values and ignore the remaining octets of the information element.  S-NSSAI value:  S-NSSAI value is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet. |

#### 9.11.3.37A NSSAI inclusion mode

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

The NSSAI inclusion mode is a type 1 information element.

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

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

Figure 9.11.3.37A.1: NSSAI inclusion mode information element

Table 9.11.3.37A.1: NSSAI inclusion mode information element

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

#### 9.11.3.38 Operator-defined access category definitions

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

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

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

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

Figure 9.11.3.38.1: Operator-defined access category definitions information element

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

Figure 9.11.3.38.2: Operator-defined access category definition

Table 9.11.3.38.1: Operator-defined access category definitions information element

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

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

#### 9.11.3.39 Payload container

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

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

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

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

Figure 9.11.3.39.1: Payload container information element

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

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

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

Figure 9.11.3.39.3: Payload container entry

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

Figure 9.11.3.39.4: Optional IE

Table 9.11.3.39.1: Payload container information element

|  |  |  |
| --- | --- | --- |
| Payload container contents (octet 4 to octet n); max value of 65535 octets | | |
| If the payload container type is set to "SOR transparent container" and is included in the DL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the SOR transparent container IE (see subclause 9.11.3.51) for SOR data type is set to value "0" except that the first three octets are not included.  If the payload container type is set to "SOR transparent container" and is included in the UL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the SOR transparent container IE (see subclause 9.11.3.51) for SOR data type is set to value "1" except that the first three octets are not included.  If the payload container type is set to "UE parameters update transparent container" and is included in the DL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the UE parameters update transparent container IE (see subclause 9.11.3.53A) for UE parameters update data type is set to value "0" except that the first three octets are not included.  If the payload container type is set to "UE parameters update transparent container" and is included in the UL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the UE parameters update transparent container IE (see subclause 9.11.3.53A) for UE parameters update data type is set to value "1" except that the first three octets are not included.  If the payload container type is set to "SMS", the payload container contents contain an SMS message (i.e. CP-DATA, CP-ACK or CP-ERROR) as defined in subclause 7.2 in 3GPP TS 24.011 [13].  If the payload container type is set to "CIoT user data container" and is included in the UL NAS TRANSPORT, DL NAS TRANSPORT or CONTROL PLANE SERVICE REQUEST message, the payload container contents are coded the same way as the contents of the user data container IE (see subclause 9.9.4.24 in 3GPP TS 24.301 [15]) except that the first three octets are not included.  If the payload container type is set to "SMS" and is included in the CONTROL PLANE SERVICE REQUEST message, the payload container contents are coded the same way as the contents of the NAS message container IE (see subclause 9.9.3.22 in 3GPP TS 24.301 [15]) except that the first two octets are not included.  The coding of Payload container contents is dependent on the particular application.  If the payload container type is set to "Multiple payloads", the number of entries field represents the total number of payload container entries, and the payload container entry contents field is coded as a list of payload container entry according to figure 9.11.3.39.2, with each payload container entry is coded according to figure 9.11.3.39.3 and figure 9.11.3.39.4. | | |
| Payload container entry  For each payload container entry, the payload container type field represents the payload container type value as described in subclause 9.11.3.40, the coding of payload container contents field is dependent on the particular application, and the number of optional IEs field represents the total number of optional IEs associated with the payload container entry contents field in the payload container entry. The error handlings for optional IEs specified in subclauses 7.6.1, 7.6.3 and 7.7.1 shall apply to the optional IEs included in the payload container entry. | | |
| Optional IEs  Type of optional IE (octet xi +4)  This field contains the IEI of the optional IE.  Length of optional IE (octet xi+5)  This field indicates binary coded length of the value of the optional IE entry.  Value of optional IE (octet xi+6 to octet y2)  This field contains the value of the optional IE entry with the value part of the referred information element based on following optional IE reference. If the Request type is included, the value part of the Request type shall be encoded in the bits 1 to 4 and bits 5 to 8 shall be coded as zero. | | |
| IEI | Optional IE name | Optional IE reference |
| 12 | PDU session ID | PDU session identity 2 (see subclause 9.11.3.41) |
| 24 | Additional information | Additional information (see subclause 9.11.2.1) |
| 58 | 5GMM cause | 5GMM cause (see subclause 9.11.3.2) |
| 37 | Back-off timer value | GPRS timer 3 (see subclause 9.11.2.5) |
| 59 | Old PDU session ID | PDU session identity 2 (see subclause 9.11.3.41) |
| 80 | Request type | Request type (see subclause 9.11.3.47) |
| 22 | S-NSSAI | S-NSSAI (see subclause 9.11.2.8) |
| 25 | DNN | DNN (see subclause 9.11.2.1B) |
| F0 | Release assistance indication | Release assistance indication (see subclause 9.11.3.46A) |
| A0 | MA PDU session information | MA PDU session information (see subclause 9.11.3.31A) |

#### 9.11.3.40 Payload container type

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

The Payload container type information element is coded as shown in figure 9.11.3.40.1 and table 9.11.3.40.1.

The Payload container type is a type 1 information element.

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

Figure 9.11.3.40.1: Payload container type information element

Table 9.11.3.40.1: Payload container type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Payload container type value (octet 1) | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 1 | N1 SM information |
| 0 | 0 | 1 | 0 | SMS |
| 0 | 0 | 1 | 1 | LTE Positioning Protocol (LPP) message container |
| 0 | 1 | 0 | 0 | SOR transparent container |
| 0 | 1 | 0 | 1 | UE policy container |
| 0 | 1 | 1 | 0 | UE parameters update transparent container |
| 0 | 1 | 1 | 1 | Location services message container (see 3GPP TS 23.273 [6B]) |
| 1 | 0 | 0 | 0 | CIoT user data container |
| 1 | 1 | 1 | 1 | Multiple payloads |
|  | | | | |
| All other values are reserved. | | | | |
|  | | | | |
| NOTE: The value "Multiple payloads" is only used when the Payload container contents in figure 9.11.3.39.1 contains multiple payloads as shown in figure 9.11.3.39.2. | | | | |

#### 9.11.3.41 PDU session identity 2

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

The PDU session identity 2 information element is coded as shown in figure 9.11.3.41.1 and table 9.11.3.41.1.

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

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

Figure 9.11.3.41.1: PDU session identity 2 information element

Table 9.11.3.41.1: PDU session identity 2 information element

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

#### 9.11.3.42 PDU session reactivation result

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

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

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

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

Figure 9.11.3.42.1: PDU session reactivation result information element

Table 9.11.3.42.1: PDU session reactivation result information element

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

#### 9.11.3.43 PDU session reactivation result error cause

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

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

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

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

Figure 9.11.3.43.1: PDU session reactivation result error cause information element

Table 9.11.3.43.1: PDU session reactivation result error cause information element

|  |
| --- |
| PDU session ID is coded same as PDU session ID IE (see subclause 9.4).  The cause value is coded same as second octet of 5GMM cause information element (see subclause 9.11.3.2). |

#### 9.11.3.44 PDU session status

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

The PDU session status information element is coded as shown in figure 9.11.3.44.1 and table 9.11.3.44.1.

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

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

Figure 9.11.3.44.1: PDU session status information element

Table 9.11.3.44.1: PDU session status information element

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

#### 9.11.3.45 PLMN list

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

#### 9.11.3.46 Rejected NSSAI

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

The Rejected NSSAI information element is coded as shown in figure 9.11.3.46.1, figure 9.11.3.46.2 and table 9.11.3.46.1.

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

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

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

Figure 9.11.3.46.1: Rejected NSSAI information element

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

Figure 9.11.3.46.2: Rejected S-NSSAI

Table 9.11.3.46.1: Rejected NSSAI information element

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

#### 9.11.3.46A Release assistance indication

See subclause 9.9.4.25 in 3GPP TS 24.301 [15].

#### 9.11.3.47 Request type

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

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

The Request type is a type 1 information element.

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

Figure 9.11.3.47.1: Request type information element

Table 9.11.3.47.1: Request type information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Request type value (octet 1, bit 1 to bit 4) | | | | |
|  | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 1 |  | initial request |
| 0 | 1 | 0 |  | existing PDU session |
| 0 | 1 | 1 |  | initial emergency request |
| 1 | 0 | 0 |  | existing emergency PDU session |
| 1 | 0 | 1 |  | modification request |
| 1 | 1 | 0 |  | MA PDU request (NOTE) |
| 1 | 1 | 1 |  | reserved |
| All other values are unused and shall be interpreted as "initial request", if received by the network. | | | | |
| NOTE: This value shall be interpreted as "initial request", if received by a network not supporting MA PDU sessions. | | | | |

#### 9.11.3.48 S1 UE network capability

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

#### 9.11.3.48A S1 UE security capability

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

#### 9.11.3.49 Service area list

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

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

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

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

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

Figure 9.11.3.49.1: Service area list information element

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

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

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

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

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

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

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

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

Table 9.11.3.49.1: Service area list information element

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

#### 9.11.3.50 Service type

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

The service typeis a type 1 information element.

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

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

Figure 9.11.3.50.1: Service type information element

Table 9.11.3.50.1: Service type information element

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

#### 9.11.3.50A SMS indication

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

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

The SMS indication is a type 1 information element.

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

Figure 9.11.3.50A.1: SMS indication

Table 9.11.3.50A.1: SMS indication

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

#### 9.11.3.51 SOR transparent container

The purpose of the SOR transparent container information element in the REGISTRATION ACCEPT message is to provide the list of preferred PLMN/access technology combinations (or HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided') (see 3GPP TS 23.122 [5] annex C) and optional acknowledgement request. The purpose of the SOR transparent container information element in the REGISTRATION COMPLETE message is to indicate the UE acknowledgement of successful reception of the SOR transparent container IE in the REGISTRATION ACCEPT message.

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

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

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

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

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

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

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

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

Figure 9.11.3.51.3: PLMN ID and access technology list

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

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

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

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

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

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

Table 9.11.3.51.1: SOR transparent container information element

|  |  |
| --- | --- |
| SOR-MAC-IAUSF, SOR-MAC-IUE and CounterSOR are coded as specified in 3GPP TS 33.501 [24] | |
|  | |
| SOR data type (octet 4, bit 1) | |
| 0 | The SOR transparent container carries steering of roaming information. |
| 1 | The SOR transparent container carries acknowledgement of successful reception of the steering of roaming information. |
|  | |
| List indication value (octet 4, bit 2) | |
| 0 | HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided' |
| 1 | list of preferred PLMN/access technology combinations is provided |
|  | |
| List type (octet 4, bit 3) | |
| 0 | The list type is a secured packet. |
| 1 | The list type is a "PLMN ID and access technology list". |
|  |  |
| Acknowledgement (ACK) value (octet 4, bit 4) | |
| 0 | acknowledgement not requested |
| 1 | acknowledgement requested |
|  | |
| The secure packet is coded as specified in 3GPP TS 31.115 [22B]. | |
|  | |
| The PLMN ID and access technology list consists of PLMN ID and access technology identifier and are coded as specified in 3GPP TS 31.102 [22] subclause 4.2.5. The PLMN ID and access technology identifier are provided in decreasing order of priority, i.e. PLMN ID 1 indicates highest priority and PLMN ID n indicates lowest priority. | |

#### 9.11.3.51A Supported codec list

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

#### 9.11.3.52 Time zone

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

#### 9.11.3.53 Time zone and time

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

#### 9.11.3.53A UE parameters update transparent container

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

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

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

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

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

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

Figure 9.11.3.53A.2: UE parameters update list

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

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

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

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

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

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

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

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

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

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

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

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

#### 9.11.3.54 UE security capability

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

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

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

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

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

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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE security capability IEI | | | | | | | | octet 1 |
| Length of UE security capability contents | | | | | | | | octet 2 |
| 5G-EA0 | 128-  5G-EA1 | 128-  5G-EA2 | 128-  5G-EA3 | 5G-EA4 | 5G-EA5 | 5G-EA6 | 5G-EA7 | octet 3 |
| 5G-IA0 | 128-  5G-IA1 | 128-  5G-IA2 | 128-  5G-IA3 | 5G-IA4 | 5G-IA5 | 5G-IA6 | 5G-IA7 | octet 4 |
| EEA0 | 128-  EEA1 | 128-  EEA2 | 128-  EEA3 | EEA4 | EEA5 | EEA6 | EEA7 | octet 5\* |
| EIA0 | 128-  EIA1 | 128-  EIA2 | 128-  EIA3 | EIA4 | EIA5 | EIA6 | EIA7 | octet 6\* |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |  |
| Spare | | | | | | | | octet 7\* -10\* |

Figure 9.11.3.54.1: UE security capability information element

Table 9.11.3.54.1: UE security capability information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5GS encryption algorithms supported (see NOTE 1) (octet 3) | | | | |
|  | | | | |
| 5GS encryption algorithm 5G-EA0 supported (octet 3, bit 8) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA0 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA0 supported |
|  | | | | |
| 5GS encryption algorithm 128-5G-EA1 supported (octet 3, bit 7) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 128-5G-EA1 not supported |
| 1 |  |  |  | 5GS encryption algorithm 128-5G-EA1 supported |
|  | | | | |
| 5GS encryption algorithm 128-5G-EA2 supported (octet 3, bit 6) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 128-5G-EA2 not supported |
| 1 |  |  |  | 5GS encryption algorithm 128-5G-EA2 supported |
|  | | | | |
| 5GS encryption algorithm 128-5G-EA3 supported (octet 3, bit 5) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 128-5G-EA3 not supported |
| 1 |  |  |  | 5GS encryption algorithm 128-5G-EA3 supported |
|  | | | | |
| 5GS encryption algorithm 5G-EA4 supported (octet 3, bit 4) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA4 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA4 supported |
|  | | | | |
| 5GS encryption algorithm 5G-EA5 supported (octet 3, bit 3) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA5 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA5 supported |
|  | | | | |
| 5GS encryption algorithm 5G-EA6 supported (octet 3, bit 2) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA6 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA6 supported |
|  | | | | |
| 5GS encryption algorithm 5G-EA7 supported (octet 3, bit 1) | | | | |
| 0 |  |  |  | 5GS encryption algorithm 5G-EA7 not supported |
| 1 |  |  |  | 5GS encryption algorithm 5G-EA7 supported |
|  | | | | |
| 5GS integrity algorithms supported (see NOTE 2) (octet 4) | | | | |
|  | | | | |
| 5GS integrity algorithm 5G-IA0 supported (octet 4, bit 8) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA0 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA0 supported |
|  | | | | |
| 5GS integrity algorithm 128-5G-IA1 supported (octet 4, bit 7) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 128-5G-IA1 not supported |
| 1 |  |  |  | 5GS integrity algorithm 128-5G-IA1 supported |
|  | | | | |
| 5GS integrity algorithm 128-5G-IA2 supported (octet 4, bit 6) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 128-5G-IA2 not supported |
| 1 |  |  |  | 5GS integrity algorithm 128-5G-IA2 supported |
|  | | | | |
| 5GS integrity algorithm 128-5G-IA3 supported (octet 4, bit 5) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 128-5G-IA3 not supported |
| 1 |  |  |  | 5GS integrity algorithm 128-5G-IA3 supported |
|  | | | | |
| 5GS integrity algorithm 5G-IA4 supported (octet 4, bit 4) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA4 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA4 supported |
|  | | | | |
| 5GS integrity algorithm 5G-IA5 supported (octet 4, bit 3) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA5 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA5 supported |
|  | | | | |
| 5GS integrity algorithm 5G-IA6supported (octet 4, bit 2) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA6 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA6 supported |
|  | | | | |
| 5GS integrity algorithm 5G-IA7 supported (octet 4, bit 1) | | | | |
| 0 |  |  |  | 5GS integrity algorithm 5G-IA7 not supported |
| 1 |  |  |  | 5GS integrity algorithm 5G-IA7 supported |
|  | | | | |
| EPS encryption algorithms supported (see NOTE 3) (octet 5) | | | | |
|  | | | | |
| EPS encryption algorithm EEA0 supported (octet 5, bit 8) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA0 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA0 supported |
|  | | | | |
| EPS encryption algorithm 128-EEA1 supported (octet 5, bit 7) | | | | |
| 0 |  |  |  | EPS encryption algorithm 128-EEA1 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA1 supported |
|  | | | | |
| EPS encryption algorithm 128-EEA2 supported (octet 5, bit 6) | | | | |
| 0 |  |  |  | EPS encryption algorithm 128-EEA2 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA2 supported |
|  | | | | |
| EPS encryption algorithm 128-EEA3 supported (octet 5, bit 5) | | | | |
| 0 |  |  |  | EPS encryption algorithm 128-EEA3 not supported |
| 1 |  |  |  | EPS encryption algorithm 128-EEA3 supported |
|  | | | | |
| EPS encryption algorithm EEA4 supported (octet 5, bit 4) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA4 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA4 supported |
|  | | | | |
| EPS encryption algorithm EEA5 supported (octet 5, bit 3) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA5 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA5 supported |
|  | | | | |
| EPS encryption algorithm EEA6 supported (octet 5, bit 2) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA6 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA6 supported |
|  | | | | |
| EPS encryption algorithm EEA7 supported (octet 5, bit 1) | | | | |
| 0 |  |  |  | EPS encryption algorithm EEA7 not supported |
| 1 |  |  |  | EPS encryption algorithm EEA7 supported |
|  | | | | |
| EPS integrity algorithms supported (see NOTE 4) (octet 6) | | | | |
|  | | | | |
| EPS integrity algorithm EIA0 supported (octet 6, bit 8) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA0 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA0 supported |
|  | | | | |
| EPS integrity algorithm 128-EIA1 supported (octet 6, bit 7) | | | | |
| 0 |  |  |  | EPS integrity algorithm 128-EIA1 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA1 supported |
|  | | | | |
| EPS integrity algorithm 128-EIA2 supported (octet 6, bit 6) | | | | |
| 0 |  |  |  | EPS integrity algorithm 128-EIA2 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA2 supported |
|  | | | | |
| EPS integrity algorithm 128-EIA3 supported (octet 6, bit 5) | | | | |
| 0 |  |  |  | EPS integrity algorithm 128-EIA3 not supported |
| 1 |  |  |  | EPS integrity algorithm 128-EIA3 supported |
|  | | | | |
| EPS integrity algorithm EIA4 supported (octet 6, bit 4) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA4 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA4 supported |
|  | | | | |
| EPS integrity algorithm EIA5 supported (octet 6, bit 3) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA5 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA5 supported |
|  | | | | |
| EPS integrity algorithm EIA6 supported (octet 6, bit 2) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA6 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA6 supported |
|  | | | | |
| EPS integrity algorithm EIA7 supported (octet 6, bit 1) | | | | |
| 0 |  |  |  | EPS integrity algorithm EIA7 not supported |
| 1 |  |  |  | EPS integrity algorithm EIA7 supported |
|  | | | | |
| For the UE not supporting any security algorithm for AS security over E-UTRA connected to 5GCN, all bits in octets 5 to 10 are spare and shall be ignored, if the respective octet is received with the information element.  For the UE supporting at least one security algorithm for AS security over E-UTRA connected to 5GCN all bits in octets 7 to 10 are spare and shall be ignored, if the respective octet is received with the information element.  If the AMF receives any of the octets 7 to 10 (NOTE 5), it shall store the octets as received and include them when sending the UE security capability information element to the UE. | | | | |
| NOTE 1: The code points in octet 3 are used to indicate support for 5GS encryption algorithms for NAS security in N1 mode and support for 5GS encryption algorithms for AS security over NR.  NOTE 2: The code points in octet 4 are used to indicate support for 5GS integrity algorithms for NAS security in N1 mode and support for 5GS integrity algorithms for AS security over NR.  NOTE 3: The code points in octet 5 are used to indicate support for EPS encryption algorithms for AS security over E-UTRA connected to 5GCN.  NOTE 4: The code points in octet 6 are used to indicate support for EPS integrity algorithms for AS security over E-UTRA connected to 5GCN.  NOTE 5: The AMF can receive this information element also from another AMF or MME during N1 mode to N1 mode or S1 mode to N1 mode handover preparation. | | | | |

#### 9.11.3.55 UE's usage setting

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

The UE's usage setting information element is coded as shown in figure 9.11.3.55.1 and table 9.11.3.55.1.

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

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

Figure 9.11.3.55.1: UE's usage setting information element

Table 9.11.3.55.1: UE's usage setting information element

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

#### 9.11.3.56 UE status

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

The UE status information element is coded as shown in figure 9.11.3.56.1 and table 9.11.3.56.1.

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

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

Figure 9.11.3.56.1: UE status information element

Table 9.11.3.56.1: UE status information element

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

#### 9.11.3.57 Uplink data status

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

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

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

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

Figure 9.11.3.57.1: Uplink data status information element

Table 9.11.3.57.1: Uplink data status information element

|  |
| --- |
| PSI(x) shall be coded as follows:  PSI(0):  Bit 1 of octet 3 is spare and shall be coded as zero.  PSI(1) – PSI(15):  0 indicates that no uplink data are pending for the corresponding PDU session identity or the PDU session is in PDU SESSION INACTIVE state or is in PDU SESSION ACTIVE state with user-plane resources already established.  1 indicates that uplink data are pending for the corresponding PDU session identity and the user-plane resources for the corresponding PDU session are not established.  All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element. |

#### 9.11.3.58 Void

#### 9.11.3.59 Void

#### 9.11.3.60 Void

#### 9.11.3.61 Void

#### 9.11.3.62 Void

#### 9.11.3.63 Void

#### 9.11.3.64 Void

#### 9.11.3.65 Void

#### 9.11.3.66 Void

#### 9.11.3.67 Void

#### 9.11.3.68 UE radio capability ID

The purpose of the UE radio capability ID information element is to carry a UE radio capability ID.

The UE radio capability ID information element is coded as shown in figure 9.11.3.68.1 and table 9.11.3.68.1.

The UE radio capability ID is a type 4 information element with a length of n octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE radio capability ID IEI | | | | | | | | octet 1 |
| Length of UE radio capability ID contents | | | | | | | | octet 2 |
| UE radio capability ID | | | | | | | | octet 3 |
| octet n |

Figure 9.11.3.68.1: UE radio capability ID information element

Table 9.11.3.68.1: UE radio capability ID information element

|  |
| --- |
| UE radio capability ID (octets 3 to n) |
| The UE radio capability ID contents contain the UE radio capability ID as specified in 3GPP TS 23.003 [4], with each hexadecimal digit coded over 4 bits, starting with the first hexadecimal digit coded in bits 4 to 1 of octet 3, the second hexadecimal digit coded in bits 8 to 5 of octet 3, and so on. If the UE radio capability ID contains an odd number of hexadecimal digits, bits 8 to 5 of the last octet (octet n) shall be coded as "1111". |
|  |

#### 9.11.3.69 UE radio capability ID deletion indication

The purpose of the UE radio capability ID deletion indication information element is to indicate to the UE that deletion of UE radio capability IDs is requested.

The UE radio capability ID deletion indication is a type 1 information element.

The UE radio capability ID deletion indication information element is coded as shown in figure 9.11.3.69.1 and table 9.11.3.69.1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | | 2 | 1 |  | |
| UE radio capability ID deletion indication  IEI | | | | 0  spare | | | Deletion request | | | | octet 1 |

Figure 9.11.3.69.1: UE radio capability ID deletion indication information element

Table 9.11.3.69.1: UE radio capability ID deletion indication information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Deletion requested (octet 1) | | | | |
| Bits | | | | |
| 3 | 2 | 1 |  |  |
| 0 | 0 | 0 |  | UE radio capability ID deletion not requested |
| 0 | 0 | 1 |  | Network-assigned UE radio capability IDs deletion requested |
|  | | | | |
| All other values are unused and shall be interpreted as "UE radio capability ID deletion not requested", if received by the UE. | | | | |

#### 9.11.3.70 Truncated 5G-S-TMSI configuration

The purpose of the Truncated 5G-S-TMSI configuration information element is to provide the size of the components of the truncated 5G-S-TMSI to the UE in NB-N1 mode to create the truncated 5G-S-TMSI.

The Truncated 5G-S-TMSI configuration information element is coded as shown in figure 9.11.3.70.1 and table 9.11.3.70.1.

The Truncated 5G-S-TMSI configuration is a type 4 information element with 3 octets length.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | 2 | 1 |  |
| Truncated 5G-S-TMSI configuration IEI | | | | | | | | | octet 1 |
| Length of Truncated 5G-S-TMSI configuration contents | | | | | | | | | octet 2 |
| Truncated AMF Set ID value | | | | Truncated AMF Pointer value | | | | | octet 3 |

Figure 9.11.3.70.1: Truncated 5G-S-TMSI configuration information element

Table 9.11.3.70.1: Truncated 5G-S-TMSI configuration information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Truncated AMF Pointer value (bits 4 to 1 of octet 3)  This field represents the size of the least significant bits of the AMF Pointer. | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | reserved |
| 0 | 0 | 0 | 1 | 1 least significant bit of the AMF Pointer |
| 0 | 0 | 1 | 0 | 2 least significant bits of the AMF Pointer |
| 0 | 0 | 1 | 1 | 3 least significant bits of the AMF Pointer |
| 0 | 1 | 0 | 0 | 4 least significant bits of the AMF Pointer |
| 0 | 1 | 0 | 1 | 5 least significant bits of the AMF Pointer |
| 0 | 1 | 1 | 0 | 6 least significant bits of the AMF Pointer |
|  | | | | |
| All other values shall be interpreted as "6 least significant bits of the AMF Pointer" by this version of the protocol. | | | | |
| Truncated AMF Set ID value (bits 8 to 5 of octet 3)  This field represents the size of the least significant bits of the AMF Set ID. | | | | |
| Bits | | | | |
| 4 | 3 | 2 | 1 |  |
| 0 | 0 | 0 | 0 | reserved |
| 0 | 0 | 0 | 1 | 1 least significant bit of the AMF Set ID |
| 0 | 0 | 1 | 0 | 2 least significant bits of the AMF Set ID |
| 0 | 0 | 1 | 1 | 3 least significant bits of the AMF Set ID |
| 0 | 1 | 0 | 0 | 4 least significant bits of the AMF Set ID |
| 0 | 1 | 0 | 1 | 5 least significant bits of the AMF Set ID |
| 0 | 1 | 1 | 0 | 6 least significant bits of the AMF Set ID |
| 0 | 1 | 1 | 1 | 7 least significant bits of the AMF Set ID |
| 1 | 0 | 0 | 0 | 8 least significant bits of the AMF Set ID |
| 1 | 0 | 0 | 1 | 9 least significant bits of the AMF Set ID |
| 1 | 0 | 1 | 0 | 10 least significant bits of the AMF Set ID |
|  | | | | |
| All other values shall be interpreted as "10 least significant bits of the AMF Set ID" by this version of the protocol. | | | | |
|  | | | | |
| NOTE: Total sum of the "Truncated AMF Set ID value" and the "Truncated AMF Pointer value" in the Truncated 5G-S-TMSI configuration IE is specified in 3GPP TS 23.003 [4] and 3GPP TS 36.300 [25B]. | | | | |

#### 9.11.3.71 WUS assistance information

See subclause 9.9.3.62 in 3GPP TS 24.301 [15].

#### 9.11.3.72 N5GC indication

The purpose of the N5GC indication information element is to indicate to the network that the registration request by the W-AGF is on behalf of an N5GC device.

The N5GC indication information element is coded as shown in figure 9.11.3.72.1.

The N5GC indication is a type 2 information element.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
| N5GC indication IEI | | | | | | | | | octet 1 |

Figure 9.11.3.72.1: N5GC indication

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

#### 9.11.4.1 5GSM capability

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

The 5GSM capability information element is coded as shown in figure 9.11.4.1.1 and table 9.11.4.1.1.

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

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

Figure 9.11.4.1.1: 5GSM capability information element

Table 9.11.4.1.1: 5GSM capability information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5GSM capability value | | | | |
| RqoS(octet 3, bit 1) | | | | |
| This bit indicates the 5GSM capability to support reflective QoS. | | | | |
| 0 |  |  |  | Reflective QoS not supported |
| 1 |  |  |  | Reflective QoS supported |
|  | | | | |
| Multi-homed IPv6 PDU session (MH6-PDU) (octet 3, bit 2) | | | | |
| This bit indicates the 5GSM capability for Multi-homed IPv6 PDU session. | | | | |
| 0 |  |  |  | Multi-homed IPv6 PDU session not supported |
| 1 |  |  |  | Multi-homed IPv6 PDU session supported |
|  | | | | |
| Ethernet PDN type in S1 mode (EPT-S1) (octet 3, bit 3) | | | | |
| This bit indicates UE's 5GSM capability for Ethernet PDN type in S1 mode. | | | | |
| 0 |  |  |  | Ethernet PDN type in S1 mode not supported |
| 1 |  |  |  | Ethernet PDN type in S1 mode supported |
|  | | | | |
| Supported ATSSS steering functionalities and steering modes (ATSSS-ST) (octet 3, bits 4 to 7) | | | | |
| These bits indicate the 5GSM capability of ATSSS steering functionalities and steering modes | | | | |
| 0 | 0 | 0 | 0 | ATSSS not supported |
| 0 | 0 | 0 | 1 | ATSSS Low-Layer functionality with any steering mode supported |
|  | | | | |
| 0 | 0 | 1 | 0 | MPTCP functionality with any steering mode and ATSSS-LL functionality with only active-standby steering mode supported |
| 0 | 0 | 1 | 1 | MPTCP functionality with any steering mode and ATSSS-LL functionality with any steering mode supported |
| All other values are reserved. | | | | |
| Transfer of port management information containers (TPMIC) (octet 3, bit 8) | | | | |
| This bit indicates the 5GSM capability to support transfer of port management information containers | | | | |
| 0 |  |  |  | Transfer of port management information containers not supported |
| 1 |  |  |  | Transfer of port management information containers supported |
|  | | | | |
| All other bits in octet 3 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | |
|  | | | | |

#### 9.11.4.2 5GSM cause

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

The 5GSM cause information element is coded as shown in figure 9.11.4.2.1 and table 9.11.4.2.1.

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

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

Figure 9.11.4.2.1: 5GSM cause information element

Table 9.11.4.2.1: 5GSM cause information element

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cause value (octet 2) | | | | | | | | | |
| Bits | | | | | | | | | |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |  | Operator determined barring |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |  | Insufficient resources |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |  | Missing or unknown DNN |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |  | Unknown PDU session type |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |  | User authentication or authorization failed |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |  | Request rejected, unspecified |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |  | Service option not supported |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 |  | Requested service option not subscribed |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 |  | Service option temporarily out of order |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |  | PTI already in use |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |  | Regular deactivation |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |  | Network failure |
| 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 |  | Reactivation requested |
| 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |  | Semantic error in the TFT operation |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |  | Syntactical error in the TFT operation |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |  | Invalid PDU session identity |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |  | Semantic errors in packet filter(s) |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 |  | Syntactical error in packet filter(s) |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |  | Out of LADN service area |
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |  | PTI mismatch |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |  | PDU session type IPv4 only allowed |
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |  | PDU session type IPv6 only allowed |
| 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |  | PDU session does not exist |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |  | PDU session type IPv4v6 only allowed |
| 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |  | PDU session type Unstructured only allowed |
| 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |  | PDU session type Ethernet 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 | 0 | 0 | 1 | 0 |  | Maximum data rate per UE for user-plane integrity protection is too low |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |  | Semantic error in the QoS operation |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |  | Syntactical error in the QoS operation |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |  | Invalid mapped EPS bearer identity |
| 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |  | Semantically incorrect message |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |  | Invalid mandatory information |
| 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |  | Message type non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |  | Message type not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |  | Information element non-existent or not implemented |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |  | Conditional IE error |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |  | Message not compatible with the protocol state |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |  | Protocol error, unspecified |
|  |  |  |  |  |  |  |  |  |  |
| Any other value received by the UE shall be treated as 0010 0010, "service option temporarily out of order". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified". | | | | | | | | | |

#### 9.11.4.3 Always-on PDU session indication

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

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

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

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

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

**Table 9.11.4.3**.1: Always-on PDU session indication

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

#### 9.11.4.4 Always-on PDU session requested

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

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

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

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

Figure 9.11.4.4.1: Always-on PDU session requested

Table 9.11.4.4.1: Always-on PDU session requested

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

#### 9.11.4.5 Allowed SSC mode

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

The Allowed SSC mode information element is coded as shown in figure 9.11.4.5.1 and table 9.11.4.5.1.

The Allowed SSC mode is a type 1 information element.

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

Figure 9.11.4.5.1: Allowed SSC mode information element

Table 9.11.4.5.1: Allowed SSC mode information element

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

#### 9.11.4.6 Extended protocol configuration options

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

#### 9.11.4.7 Integrity protection maximum data rate

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

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

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

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

Figure 9.11.4.7.1: Integrity protection maximum data rate information element

Table 9.11.4.7.2: Integrity protection maximum data rate information element

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

#### 9.11.4.8 Mapped EPS bearer contexts

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

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

The mapped EPS bearer contextsinformation element is coded as shown in figure 9.11.4.8.1, figure 9.11.4.8.2, figure 9.11.4.8.3 and table 9.11.4.8.1.

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

Figure 9.11.4.8.1: Mapped EPS bearer contexts

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

Figure 9.11.4.8.2: Mapped EPS bearer context

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

Figure 9.11.4.8.3: EPS parameters list

Table 9.11.4.8.1: Mapped EPS bearer contexts information element

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

#### 9.11.4.9 Maximum number of supported packet filters

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

The Maximum number of supported packet filters is coded as shown in figure 9.11.4.9.1 and table 9.11.4.9.1.

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | | 4 | 3 | 2 | 1 |  | |
| Maximum number of supported packet filters IEI | | | | | | | | | octet 1 | |
| Maximum number of supported packet filters | | | | | | | | | octet 2 | |
| Maximum number of supported packet filters (continued) | | | | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | | octet 3 |

Figure 9.11.4.9.1: Maximum number of supported packet filters information element

Table 9.11.4.9.1: Maximum number of supported packet filters information element

|  |
| --- |
| Maximum number of supported packet filters (octet 2 to 3) |
| In the Maximum number of supported packet filters field bit 8 of the first octet is the most significant bit and bit 6 of second octet is the least significant bit. Bit 5 to bit 1 of the second octet are spare bits and shall be coded as zero.  The number of supported packet filters shall be in the range of 17 to 1024. |
|  |

#### 9.11.4.10 PDU address

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

- an IPv4 address associated with a PDU session;

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

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

The PDU address information element is coded as shown in figure 9.11.4.10.1 and table 9.11.4.10.1.

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

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

Figure 9.11.4.10.1: PDU address information element

Table 9.11.4.10.1: PDU address information element

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

#### 9.11.4.11 PDU session type

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

The PDU session type information element is coded as shown in figure 9.11.4.11.1 and table 9.11.4.11.1.

The PDU session type is a type 1 information element.

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

Figure 9.11.4.11.1: PDU session type information element

Table 9.11.4.11.1: PDU session type information element

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

#### 9.11.4.12 QoS flow descriptions

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

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

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

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

Figure 9.11.4.12.1: QoS flow descriptions information element

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

Figure 9.11.4.12.2: QoS flow description

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

Figure 9.11.4.12.3: Parameters list

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

Figure 9.11.4.12.4: Parameter

Table 9.11.4.12.1: QoS flow descriptions information element

|  |
| --- |
| QoS flow identifier (QFI) (bits 6 to 1 of octet 4)  QFI field contains the QoS flow identifier.  Bits  6 5 4 3 2 1  0 0 0 0 0 0 no QoS flow identifier assigned  0 0 0 0 0 1 QFI 1  to  1 1 1 1 1 1 QFI 63  The network shall not set the QFI value to 0. |
| Operation code (bits 8 to 6 of octet 5)  Bits  8 7 6  0 0 1 Create new QoS flow description  0 1 0 Delete existing QoS flow description  0 1 1 Modify existing QoS flow description  All other values are reserved. |
| E bit (bit 7 of octet 6)  For the "create new QoS flow description" operation, the E bit is encoded as follows:  Bit 7  0 reserved  1 parameters list is included  For the "Delete existing QoS flow description" operation, the E bit is encoded as follows:  Bit 7  0 parameters list is not included  1 reserved  For the "modify existing QoS flow description" operation, the E bit is encoded as follows:  Bit 7  0 extension of previously provided parameters  1 replacement of all previously provided parameters  If the E bit is set to "parameters list is not included", the number of parameters field has zero value. If the E bit is set to "parameters list is included", the number of parameters field has non-zero value. If the E bit is set to "extension of previously provided parameters" or "replacement of all previously provided parameters", the number of parameters field has non-zero value. If the E bit is set to "extension of previously provided parameters" and one of the parameters in the new parameters list already exists in the previously provided parameters, the parameter shall be set to the new value.  Number of parameters (bits 6 to 1 of octet 6)  The number of parameters field contains the binary coding for the number of parameters in the parameters list field. The number of parameters field is encoded in bits 6 through 1 of octet 6 where bit 6 is the most significant and bit 1 is the least significant bit.  Parameters list (octets 7 to u)  The parameters list contains a variable number of parameters.  Each parameter included in the parameters list is of variable length and consists of:  - a parameter identifier (1 octet);  - the length of the parameter contents (1 octet); and - the parameter contents itself (variable amount of octets).  The parameter identifier field is used to identify each parameter included in the parameters list and it contains the hexadecimal coding of the parameter identifier. Bit 8 of the parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following parameter identifiers are specified:  - 01H (5QI); - 02H (GFBR uplink);  - 03H (GFBR downlink);  - 04H (MFBR uplink);  - 05H (MFBR downlink);  - 06H (Averaging window); and  - 07H (EPS bearer identity).  If the parameters list contains a parameter identifier that is not supported by the receiving entity the corresponding parameter shall be discarded.  The length of parameter contents field contains the binary coded representation of the length of the parameter contents field. The first bit in transmission order is the most significant bit.  When the parameter identifier indicates 5QI, the parameter contents field contains the binary representation of 5G QoS identifier (5QI) that is one octet in length.  5QI:  Bits  8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 0 Reserved  0 0 0 0 0 0 0 1 5QI 1  0 0 0 0 0 0 1 0 5QI 2  0 0 0 0 0 0 1 1 5QI 3  0 0 0 0 0 1 0 0 5QI 4  0 0 0 0 0 1 0 1 5QI 5  0 0 0 0 0 1 1 0 5QI 6  0 0 0 0 0 1 1 1 5QI 7  0 0 0 0 1 0 0 0 5QI 8  0 0 0 0 1 0 0 1 5QI 9  0 0 0 0 1 0 1 0  to Spare  0 1 0 0 0 0 0 0  0 1 0 0 0 0 0 1 5QI 65  0 1 0 0 0 0 1 0 5QI 66  0 1 0 0 0 0 1 1 5QI 67  0 1 0 0 0 1 0 0 Spare  0 1 0 0 0 1 0 1 5QI 69  0 1 0 0 0 1 1 0 5QI 70  0 1 0 0 0 1 1 1 5QI 71  0 1 0 0 1 0 0 0 5QI 72  0 1 0 0 1 0 0 1 5QI 73  0 1 0 0 1 0 1 0 5QI 74  0 1 0 0 1 0 1 1 5QI 75  0 1 0 0 1 1 0 0 5QI 76  0 1 0 0 1 1 0 1  to Spare  0 1 0 0 1 1 1 0  0 1 0 0 1 1 1 1 5QI 79  0 1 0 1 0 0 0 0 5QI 80  0 1 0 1 0 0 0 1 Spare  0 1 0 1 0 0 1 0 5QI 82  0 1 0 1 0 0 1 1 5QI 83  0 1 0 1 0 1 0 0 5QI 84  0 1 0 1 0 1 0 1 5QI 85  0 1 0 1 0 1 1 0 5QI 86  0 1 0 1 0 1 1 1  to Spare  0 1 1 1 1 1 1 1  1 0 0 0 0 0 0 0  to Operator-specific 5QIs  1 1 1 1 1 1 1 0  1 1 1 1 1 1 1 1 Reserved  The network shall consider all other values not explicitly defined in this version of the protocol as unsupported.  If the UE receives a 5QI value (excluding the reserved 5QI values) that it does not understand, the UE shall choose a 5QI value from the set of 5QI values defined in this version of the protocol (see 3GPP TS 23.501 [8]) and associated with:  - GBR QoS flows, if the QoS flow includes a GFBR uplink parameter and a GFBR downlink parameter; and  - non-GBR QoS flows, if the QoS flow does not include a GFBR uplink parameter or does not include a GFBR downlink parameter.  The UE shall use this chosen 5QI value for internal operations only. The UE shall use the received 5QI value in subsequent NAS signalling procedures.  When the parameter identifier indicates "GFBR uplink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for uplink followed by two octets containing the value of the guaranteed flow bit rate for uplink.  Unit of the guaranteed flow bit rate for uplink (octet 1)  Bits  8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 0 value is not used  0 0 0 0 0 0 0 1 value is incremented in multiples of 1 Kbps  0 0 0 0 0 0 1 0 value is incremented in multiples of 4 Kbps  0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps  0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps  0 0 0 0 0 1 0 1 value is incremented in multiples of 256 Kbps  0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps  0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps  0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps  0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps  0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps  0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps  0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps  0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps  0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps  0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps  0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps  0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps  0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps  0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps  0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps  0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps  0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps  0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps  0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps  0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps  Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol.  Value of the guaranteed flow bit rate for uplink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for uplink in units defined by the unit of the guaranteed flow bit rate for uplink.  When the parameter identifier indicates "GFBR downlink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for downlink followed by two octets containing the value of the guaranteed flow bit rate for downlink.  Unit of the guaranteed flow bit rate for downlink (octet 1)  The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.  Value of the guaranteed flow bit rate for downlink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for downlink in units defined by the unit of the guaranteed flow bit rate for downlink.  When the parameter identifier indicates "MFBR uplink", the parameter contents field contains the one octet indicating the unit of the maximum flow bit rate for uplink followed by two octets containing the value of maximum flow bit rate for uplink.  Unit of the maximum flow bit rate for uplink (octet 1)  The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.  Value of the maximum flow bit rate for uplink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for uplink in units defined by the unit of the maximum flow bit rate for uplink.  When the parameter identifier indicates "MFBR downlink", the parameter contents field contains one octet indicating the unit of the maximum flow bit rate for downlink followed by two octets containing the value of the maximum flow bit rate for downlink.  Unit of the maximum flow bit rate for downlink (octet 1)  The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.  Value of the maximum flow bit rate for downlink (octets 2 and 3)  Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for downlink in units defined by the unit of the maximum flow bit rate for downlink.  In this version of the protocol, for messages specified in the present document, the sending entity shall not request 0 kbps for both the maximum flow bit rate for downlink and the maximum flow bit rate for uplink at the same time. Any entity receiving a request for 0 kbps in both the maximum flow bit rate for downlink and the maximum flow bit rate for uplink shall consider that as a syntactical error (see clause 7).  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, bits 5 to 8 of the parameter contents contain the EPS bearer identity as specified in subclause 9.3.2 of 3GPP TS 24.301 [15] (see NOTE) and bits 1 to 4 of the parameter contents are spare and shall be coded as zero. The UE shall not include the EPS bearer identity parameter in any mobile originated 5GSM messages. |
|  |
| NOTE: The total number of EPS bearer identities included in all QoS flow descriptions of a UE cannot exceed fifteen. |

#### 9.11.4.13 QoS rules

The purpose of the QoS rulesinformation element is to indicate a set of QoS rules to be used by the UE, where each QoS rule is a set of parameters as described in subclause 6.2.5.1.1.2:

a) for classification and marking of uplink user traffic; and

b) for identification of a QoS flow which the network is to use for a particular downlink user traffic.

NOTE: The UE needs to be aware of a QoS flow which the network is to use for a particular downlink user traffic e.g. to determine whether a resource is available for downlink media of a media stream of an SDP media description provided by the UE in an IMS session.

The QoS rules may contain a set of packet filters consisting of zero or more packet filters for UL direction, zero or more packet filters for DL direction, zero or more packet filters for both UL and DL directions or any combinations of these. The set of packet filters determine the traffic mapping to QoS flows.

The QoS rules information element is a type 6 information element with a minimum length of 7 octets. The maximum length for the information element is 65538 octets.

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

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

Figure 9.11.4.13.1: QoS rules information element

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

Figure 9.11.4.13.2: QoS rule (u=m+2)

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

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

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

Figure 9.11.4.13.4: Packet filter list when the rule operation is "create new QoS rule", or "modify existing QoS rule and add packet filters" or "modify existing QoS rule and replace all packet filters"

Table 9.11.4.13.1: QoS rules information element

|  |
| --- |
| QoS rule identifier (octet 4)  The QoS rule identifier field is used to identify the QoS rule.  Bits  8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 0 no QoS rule identifier assigned  0 0 0 0 0 0 0 1 QRI 1  to  1 1 1 1 1 1 1 1 QRI 255  The network shall not set the QRI value to 0.  QoS rule precedence (octet m+1)  The QoS rule precedence field is used to specify the precedence of the QoS rule among all QoS rules (both the signalled QoS rules as described in subclause 6.2.5.1.1.2 and the derived QoS rules as described in subclause 6.2.5.1.1.3) associated with the PDU session of the QoS flow. This field includes the binary coded value of the QoS rule precedence in the range from 0 to 255 (decimal). The higher the value of the QoS rule precedence field, the lower the precedence of that QoS rule is. For the "delete existing QoS rule" operation, the QoS rule precedence value field shall not be included. For the "create new QoS rule" operation, the QoS rule precedence value field shall be included.  The value 80 (decimal) is reserved.  Segregation bit (bit 7 of octet m+2) (see NOTE 1)  In the UE to network direction the segregation bit indicates whether the UE is requesting the network to bind service data flows described by the QoS rule to a dedicated QoS Flow and it is encoded as follows. In the network to UE direction this bit is spare.  Bit  7  0 Segregation not requested  1 Segregation requested  QoS flow identifier (QFI) (bits 6 to 1 of octet m+2) (see NOTE 1)  The QoS flow identifier (QFI) field contains the QoS flow identifier.  Bits  6 5 4 3 2 1  0 0 0 0 0 0 no QoS flow identifier assigned  0 0 0 0 0 1 QFI 1  to  1 1 1 1 1 1 QFI 63  The network shall not set the QFI value to 0.  For the "delete existing QoS rule" operation, the QoS flow identifier value field shall not be included. For the "create new QoS rule" operation, the QoS flow identifier value field shall be included.  DQR bit (bit 5 of octet 7)  The DQR bit indicates whether the QoS rule is the default QoS rule and it is encoded as follows:  Bit  5  0 the QoS rule is not the default QoS rule.  1 the QoS rule is the default QoS rule.  Rule operation code (bits 8 to 6 of octet 7) Bits 8 7 6  0 0 0 Reserved 0 0 1 Create new QoS rule  0 1 0 Delete existing QoS rule  0 1 1 Modify existing QoS rule and add packet filters  1 0 0 Modify existing QoS rule and replace all packet filters  1 0 1 Modify existing QoS rule and delete packet filters  1 1 0 Modify existing QoS rule without modifying packet filters  1 1 1 Reserved  Number of packet filters (bits 4 to 1 of octet 7)  The number of packet filters contains the binary coding for the number of packet filters in the packet filter list. The number of packet filters field is encoded in bits 4 through 1 of octet 7 where bit 4 is the most significant and bit 1 is the least significant bit. For the "delete existing QoS rule" operation and for the "modify existing QoS rule without modifying packet filters" operation, the number of packet filters shall be coded as 0. For the "create new QoS rule" operation and the "modify existing QoS rule and replace all packet filters" operation, the number of packet filters shall be greater than or equal to 0 and less than or equal to 15. For all other operations, the number of packet filters shall be greater than 0 and less than or equal to 15.  Packet filter list (octets 8 to m)  The packet filter list contains a variable number of packet filters.  For the "delete existing QoS rule" operation, the length of QoS rule field is set to one.  For the "delete existing QoS rule" operation and the "modify existing QoS rule without modifying packet filters" operation, the packet filter list shall be empty.  For the "modify existing QoS rule and delete packet filters" operation, the packet filter list shall contain a variable number of packet filter identifiers. This number shall be derived from the coding of the number of packet filters field in octet 7.  For the "create new QoS rule" operation and for the "modify existing QoS rule and replace all packet filters" operation, the packet filter list shall contain 0 or a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.  For the "modify existing QoS rule and add packet filters" operation, the packet filter list shall contain a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.  Each packet filter is of variable length and consists of  a packet filter direction (2 bits);  - a packet filter identifier (4 bits);  - the length of the packet filter contents (1 octet); and - the packet filter contents itself (variable amount of octets).  The packet filter direction field is used to indicate for what traffic direction the filter applies.  Bits  6 5  0 0 reserved  0 1 downlink only  1 0 uplink only  1 1 bidirectional (see NOTE)  The packet filter identifier field is used to identify each packet filter in a QoS rule. The least significant 4 bits are used.  The length of the packet filter contents field contains the binary coded representation of the length of the packet filter contents field of a packet filter. The first bit in transmission order is the most significant bit.  The packet filter contents field is of variable size and contains a variable number (at least one) of packet filter components. Each packet filter component shall be encoded as a sequence of a one octet packet filter component type identifier and a fixed length packet filter component value field. The packet filter component type identifier shall be transmitted first.  In each packet filter, there shall not be more than one occurrence of each packet filter component type. Among the "IPv4 remote address type" and "IPv6 remote address/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "IPv4 local address type" and "IPv6 local address/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "single local port type" and "local port range type" packet filter components, only one shall be present in one packet filter. Among the "single remote port type" and "remote port range type" packet filter components, only one shall be present in one packet filter. If the "match-all type" packet filter component is present in the packet filter, no other packet filter component shall be present in the packet filter and the length of the packet filter contents field shall be set to one.  The term local refers to the UE and the term remote refers to an external network entity.  Packet filter component type identifier Bits 8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 1 Match-all type 0 0 0 1 0 0 0 0 IPv4 remote address type 0 0 0 1 0 0 0 1 IPv4 local address type  0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type 0 0 1 0 0 0 1 1 IPv6 local address/prefix length type 0 0 1 1 0 0 0 0 Protocol identifier/Next header type 0 1 0 0 0 0 0 0 Single local port type 0 1 0 0 0 0 0 1 Local port range type 0 1 0 1 0 0 0 0 Single remote port type  0 1 0 1 0 0 0 1 Remote port range type 0 1 1 0 0 0 0 0 Security parameter index type 0 1 1 1 0 0 0 0 Type of service/Traffic class type 1 0 0 0 0 0 0 0 Flow label type  1 0 0 0 0 0 0 1 Destination MAC address type 1 0 0 0 0 0 1 0 Source MAC address type 1 0 0 0 0 0 1 1 802.1Q C-TAG VID type 1 0 0 0 0 1 0 0 802.1Q S-TAG VID type 1 0 0 0 0 1 0 1 802.1Q C-TAG PCP/DEI type 1 0 0 0 0 1 1 0 802.1Q S-TAG PCP/DEI type 1 0 0 0 0 1 1 1 Ethertype type  All other values are reserved.  The description and valid combinations of packet filter component type identifiers in a packet filter are defined in 3GPP TS 23.501 [8].  For "match-all type", the packet filter component shall not include the packet filter component value field.  For "IPv4 remote address type", the packet filter component value field shall be encoded as a sequence of a four octet IPv4 address field and a four octet IPv4 address mask field. The IPv4 address field shall be transmitted first.  For "IPv4 local address type", the packet filter component value field shall be encoded as defined for "IPv4 remote address type".  For "IPv6 remote address/prefix length type", the packet filter component value field shall be encoded as a sequence of a sixteen octet IPv6 address field and one octet prefix length field. The IPv6 address field shall be transmitted first.  For "IPv6 local address/prefix length type", the packet filter component value field shall be encoded as defined for "IPv6 remote address /prefix length".  For "protocol identifier/Next header type", the packet filter component value field shall be encoded as one octet which specifies the IPv4 protocol identifier or Ipv6 next header.  For "single local port type" and "single remote port type", the packet filter component value field shall be encoded as two octets which specify a port number.  For "local port range type" and "remote port range type", the packet filter component value field shall be encoded as a sequence of a two octet port range low limit field and a two octet port range high limit field. The port range low limit field shall be transmitted first.  For "security parameter index", the packet filter component value field shall be encoded as four octets which specify the IPSec security parameter index.  For "type of service/traffic class type", the packet filter component value field shall be encoded as a sequence of a one octet type-of-service/traffic class field and a one octet type-of-service/traffic class mask field. The type-of-service/traffic class field shall be transmitted first.  For "flow label type", the packet filter component value field shall be encoded as three octets which specify the IPv6 flow label. The bits 8 through 5 of the first octet shall be spare whereas the remaining 20 bits shall contain the IPv6 flow label.  For "destination MAC address type" and "source MAC address type", the packet filter component value field shall be encoded as 6 octets which specify a MAC address.  For "802.1Q C-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the customer-VLAN tag (C-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.  For "802.1Q S-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the service-VLAN tag (S-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID.  For "802.1Q C-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q C-TAG PCP and DEI. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.  For "802.1Q S-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q S-TAG PCP. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI.  For "ethertype type", the packet filter component value field shall be encoded as two octets which specify an ethertype. |
| NOTE 1: Octet m+2 shall not be included without octet m+1. |

#### 9.11.4.14 Session-AMBR

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

The Session-AMBR information element is coded as shown in figure 9.11.4.14.1 and table 9.11.4.14.1.

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

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

Figure 9.11.4.14.1: Session-AMBR information element

Table 9.11.4.14.1: Session-AMBR information element

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

#### 9.11.4.15 SM PDU DN request container

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

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

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

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

Figure 9.11.4.15.1: SM PDU DN request container information element

Table 9.11.4.15.1: SM PDU DN request container information element

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

#### 9.11.4.16 SSC mode

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

The SSC mode information element is coded as shown in figure 9.11.4.16.1 and table 9.11.4.16.1.

The SSC mode is a type 1 information element.

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

Figure 9.11.4.16.1: SSC mode information element

Table 9.11.4.16.1: SSC mode information element

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

#### 9.11.4.17 Re-attempt indicator

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

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

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

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

Figure 9.11.4.17.1: Re-attempt indicator

Table 9.11.4.17.1: Re-attempt indicator

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

#### 9.11.4.18 5GSM network feature support

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

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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| 5GSM network feature support IEI | | | | | | | | octet 1 |
| Length of 5GSM network feature support contents | | | | | | | | octet 2 |
| 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | EPT-S1 | octet 3 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | octet 4\* -15\* |
| Spare | | | | | | | |

Figure 9.11.4.18.1: 5GSM network feature support information element

Table 9.11.4.18.1: 5GSM network feature support information element

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5GSM network feature support contents | | | | |
| Ethernet PDN type in S1 mode (IEPT-S1) (octet 3, bit 1) | | | | |
| This bit indicates network's capability for Ethernet PDN type in S1 mode. | | | | |
| 0 |  |  |  | Ethernet PDN type in S1 mode not supported |
| 1 |  |  |  | Ethernet PDN type in S1 mode supported |
|  | | | | |
| All other bits in octet 3 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element. | | | | |
|  | | | | |

#### 9.11.4.19 Void

#### 9.11.4.20 Serving PLMN rate control

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

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

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

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

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

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

Figure 9.11.4.21.1: 5GSM congestion re-attempt indicator

Table 9.11.4.21.1: 5GSM congestion re-attempt indicator

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

#### 9.11.4.22 ATSSS container

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

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

The ATSSS containeris a type 6 information element with a minimum length of 3 octets and a maximum length of 65538 octets.

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

Figure 9.11.4.22.1: ATSSS container information element

Table 9.11.4.22.1: ATSSS container information element

|  |
| --- |
| ATSSS container contents are defined in 3GPP TS 24.193 [13B]. |

#### 9.11.4.23 Control plane only indication

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

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

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

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

Figure 9.11.4.23.1: Control plane only indication information element

Table 9.11.4.23.1: Control plane only indication information element

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

#### 9.11.4.24 Header compression configuration

The purpose of the Header compression configuration information element is to negotiate ROHC channel setup parameters specified in IETF RFC 5795 [39B] and, optionally, provide additional header compression context setup parameters.

The Header compression configuration information element is coded as shown in figure 9.11.4.24.1 and table 9.11.4.24.1.

The Header compression configuration is a type 4 information element with a minimum length of 5 octets and a maximum length of 257 octets.

The optional Additional header compression parameters container field conveys the additional header compression context setup parameters as specified in 3GPP TS 23.501 [8] in a generic container. This field corresponds to the profile-specific information in the header of the ROHC IR packet type in IETF RFC 5795 [39B].

Editor's note: The coding of header compression configuration may be updated for the Ethernet PDU session.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | | | 3 | 2 | | 1 | |  |
| Header compression configuration IEI | | | | | | | | | | | | octet 1 |
| Length of Header compression configuration contents | | | | | | | | | | | | octet 2 |
| Spare | P0x0104 | P0x0103 | P0x0102 | | P0x0006 | P0x0004 | | P0x0003 | P0x0002 | | octet 3 | |
| MAX\_CID | | | | | | | | | | | | octet 4 |
| octet 5 |
| Additional header compression context setup parameters type | | | | | | | | | | | | octet 6\* |
| Additional header compression context setup parameters container | | | | | | | | | | | | octet 7\* |
|  |
| octet n\* |

Figure 9.11.4.24.1: Header compression configuration information element

Table 9.11.4.24.1: Header compression configuration information element

|  |
| --- |
| ROHC Profiles (octet 3)  The ROHC Profiles shall indicate which of the ROHC profiles is supported. When a particular bit is set to 1, this indicates that the corresponding profile is supported. The No Compression profile 0x0000 (see IETF RFC 5795 [39B]) shall always be supported. When all the bits are set to 0, this indicates that only the No Compression profile 0x0000 is supported.  Profile 0x0002 support indicator (see IETF RFC 3095 [33A] and IETF RFC 4815 [38A]) (octet 3 bit 1)  0 RoHC profile 0x0002 (UDP/IP) is not supported  1 RoHC profile 0x0002 (UDP/IP) is supported  Profile 0x0003 support indicator (see IETF RFC 3095 [33A] and IETF RFC 4815 [38A]) (octet 3 bit 2)  0 RoHC profile 0x0003 (ESP/IP) is not supported  1 RoHC profile 0x0003 (ESP/IP) is supported  Profile 0x0004 support indicator (see IETF RFC 3843 [34A] and IETF RFC 4815 [38A]) (octet 3 bit 3)  0 RoHC profile 0x0004 (IP) is not supported  1 RoHC profile 0x0004 (IP) is supported  Profile 0x0006 support indicator (see IETF RFC 6846 [40B]) (octet 3 bit 4)  0 RoHC profile 0x0006 (TCP/IP) is not supported  1 RoHC profile 0x0006 (TCP/IP) is supported  Profile 0x0102 support indicator (see IETF RFC 5225 [39A]) (octet 3 bit 5)  0 RoHC profile 0x0102 (UDP/IP) is not supported  1 RoHC profile 0x0102 (UDP/IP) is supported  Profile 0x0103 support indicator (see IETF RFC 5225 [39A]) (octet 3 bit 6)  0 RoHC profile 0x0103 (ESP/IP) is not supported  1 RoHC profile 0x0103 (ESP/IP) is supported  Profile 0x0104 support indicator (see IETF RFC 5225 [39A]) (octet 3 bit 7)  0 RoHC profile 0x0104 (IP) is not supported  1 RoHC profile 0x0104 (IP) is supported  Bits 8 is spare and shall be set to 0.  MAX\_CID (octet 4 and octet 5)  This is the MAX\_CID value as specified in 3GPP TS 36.323 [25]. It is encoded in binary coding with a value in the range from 1 to 16383.  Additional header compression context parameters type (octet 6).  The Additional header compression context parameters type octet indicates the profile associated with the profile-specific information in the Additional header compression context parameters container.  Bits  **8 7 6 5 4 3 2 1** Type    0 0 0 0 0 0 0 0 0x0000 (No Compression)  0 0 0 0 0 0 0 1 0x0002 (UDP/IP)  0 0 0 0 0 0 1 0 0x0003 (ESP/IP)  0 0 0 0 0 0 1 1 0x0004 (IP)  0 0 0 0 0 1 0 0 0x0006 (TCP/IP)  0 0 0 0 0 1 0 1 0x0102 (UDP/IP)  0 0 0 0 0 1 1 0 0x0103 (ESP/IP)  0 0 0 0 0 1 1 1 0x0104 (IP)  0 0 0 0 1 0 0 0 Other  0 0 0 0 1 0 0 1  to  1 1 1 1 1 1 1 1 Spare  Additional header compression context parameters container (octets 7 to n).  Additional header compression context parameters container carries the profile-specific information (see IETF RFC 5795 [39B]). The maximum size is 251 octets.  NOTE: If the Additional header compression context setup parameters container is included, then the Additional header compression context parameters type shall be included in the octet 6. |

#### 9.11.4.25 DS-TT Ethernet port MAC address

The purpose of the DS-TT Ethernet port MAC addressinformation element is to signal the MAC address of the DS-TT Ethernet port used for a PDU session of "Ethernet" PDU session type.

The DS-TT Ethernet port MAC addressinformation element is coded as shown in figure 9.11.4.25.1 and table 9.11.4.25.1.

The DS-TT Ethernet port MAC addressis a type 4 information element with a length of 8 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| DS-TT Ethernet port MAC address IEI | | | | | | | | octet 1 |
| Length of DS-TT Ethernet port MAC address contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
| DS-TT Ethernet port MAC address contents | | | | | | | |  |
|  | | | | | | | | octet 8 |

Figure 9.11.4.25.1: DS-TT Ethernet port MAC address information element

Table 9.11.4.25.1: DS-TT Ethernet port MAC address information element

|  |
| --- |
| DS-TT Ethernet port MAC address contents (octets 3 to 7)  The DS-TT Ethernet port MAC address contents consist of the binary representation of the MAC address of the DS-TT Ethernet port used for the PDU session, starting with the LSB bit of the first octet of the MAC address included in bit 1 of octet 3. |

#### 9.11.4.26 UE-DS-TT residence time

The purpose of the UE-DS-TT residence timeinformation element is to signal the time taken within the UE and DS-TT to forward a packet between the UE and the DS-TT port for a PDU session of "Ethernet" PDU session type.

The UE- DS-TT residence time information element is coded as shown in figure 9.11.4.26.1 and table 9.11.4.26.1.

The UE-DS-TT residence time is a type 4 information element with a length of 10 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| UE-DS-TT residence time IEI | | | | | | | | octet 1 |
| Length of UE-DS-TT residence time contents | | | | | | | | octet 2 |
|  | | | | | | | | octet 3 |
| UE-DS-TT residence time contents | | | | | | | |  |
|  | | | | | | | | octet 10 |

Figure 9.11.4.26.1: UE-DS-TT residence time information element

Table 9.11.4.26.1: UE-DS-TT residence time information element

|  |
| --- |
| UE-DS-TT residence time contents (octets 3 to 10)  The UE-DS-TT residence time contents contain the UE-DS-TT residence time encoded as specified for the correctionField in IEEE 1588-2008 [43B], with the LSB bit of the first octet of the UE-DS-TT residence time included in bit 1 of octet 3. If the UE-DS-TT residence time.is too big to be represented, all bits of octets 3 to 10 shall be coded as "1" except the MSB bit of octet 10. |

#### 9.11.4.27 Port management information container

The purpose of the Port management information container information element is to transport an Ethernet port management service message as specified in clause 8 of 3GPP TS 24.5xy [19D].

The Port management information container information element is coded as shown in figure 9.11.4.27.1 and table 9.11.4.27.1.

The Port management information container is a type 6 information element with a minimum length of 3 octets and a maximum length of 65538 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Port management information container IEI | | | | | | | | octet 1 |
| Length of Port management information container contents | | | | | | | | octet 2  octet 3 |
| Port management information container | | | | | | | | octet 4\*  octet n\* |

Figure 9.11.4.27.1: Port management information container information element

Table 9.11.4.27.1: EAP message information element

|  |
| --- |
| Port management information container (octet 4 to n) |
| An Ethernet port management service message as specified in clause 8 of 3GPP TS 24.5xy [19D]. |

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

### 9.12.1 Serving network name (SNN)

The serving network name (SNN) is used:

- in the Network name field of the AT\_KDF\_INPUT attribute defined in IETF RFC 5448 [40];

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

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

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

SNN is of maximum length of 1020 octets.

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

SNN-network-identifier identifies the serving PLMN or the serving SNPN.

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.

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

SNN-NID contains an NID in hexadecimal digits.

ABNF syntax of SNN is specified in table 9.12.1.1

Table 9.12.1.1: ABNF syntax of SNN

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

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

SNN-network-identifier = SNN-PLMN-ID / SNN-SNPN-ID

SNN-PLMN-ID = SNN-mnc-string SNN-mnc-digits "." SNN-mcc-string SNN-mcc-digits "." SNN-3gppnetwork-string "." SNN-org-string ; applicable when not operating in SNPN access mode.

SNN-SNPN-ID = SNN-mnc-string SNN-mnc-digits "." SNN-mcc-string SNN-mcc-digits "." SNN-3gppnetwork-string "." SNN-org-string ":" SNN-NID ; applicable when operating in SNPN access mode.

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

SNN-NID = 11SNN-hexadecimal-digit ; NID in hexadecimal digits

SNN-hexadecimal-digit = DIGIT / %x41 / %x42 / %x43 / %x44 / %x45 / %x46

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

EXAMPLE 1: In case of a PLMN, if PLMN ID contains MCC = 234 and MNC = 15, SNN is 5G:mnc015.mcc234.3gppnetwork.org.

EXAMPLE 2: In case of an SNPN, if SNPN ID contains a PLMN ID of MCC = 234 and MNC = 15 and an NID of 123456ABCDEH, SNN is 5G:mnc015.mcc234.3gppnetwork.org:123456ABCDE.

# 10 List of system parameters

## 10.1 General

The description of timers in the following tables should be considered a brief summary. The precise details are found in clauses 4 to 6, which should be considered the definitive descriptions.

## 10.2 Timers of 5GS mobility management

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

NOTE: Timer T3346 is defined in 3GPP TS 24.008 [12]. Timers T3444, T3445, T3447 and T3448 are defined in 3GPP TS 24.301 [15].

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

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  EXPIRY |
| --- | --- | --- | --- | --- | --- |
| T3502 | Default 12 min.  NOTE 1 | 5GMM-DEREGISTERED 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 |
| T3510 | 15s  NOTE 7  NOTE 8  In WB-N1/CE mode, 85s | 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 5.5.1.3.7 if T3510 expired during the registration procedure for mobility and periodic registration update |
| T3511 | 10s | 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION  5GMM-REGISTERED.ATTEMPTING-REGISTRATION-UPDATE  5GMM-REGISTERED.NORMAL-SERVICE | 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  5GMM-CONNECTED mode entered (NOTE 5) | Retransmission of the REGISTRATION REQUEST, if still required |
| T3512 | Default 54 min  NOTE 1  NOTE 2 | 5GMM-REGISTERED | In 5GMM-REGISTERED, when 5GMM-CONNECTED mode is left and if the NW does not indicate support for strictly periodic registration timer as specified in subclause 5.3.7.  If the network indicates support for strictly periodic registration timer, T3512 is started after the successful completion of registration update procedure. T3512 is restarted if it expires in 5GMM-CONNECTED mode as specified in subclause 5.3.7. | When entering state 5GMM-DEREGISTERED  When entering 5GMM-CONNECTED mode if the NW does not indicate support for strictly periodic registration timer as specified in subclause 5.3.7. | In 5GMM-IDLE mode, Initiation of the periodic registration procedure if the UE is not registered for emergency services.  In 5GMM-CONNECTED mode, restart the timer T3512.  Locally deregister if the UE is registered for emergency services |
| T3516 | 30s  NOTE 7  NOTE 8  In WB-N1/CE mode, 48s | 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  NOTE 7  NOTE 8  In WB-N1/CE mode, 61s | 5GMM-SERVICE-REQUEST-INITIATED | Transmission of SERVICE REQUEST message | (a) Indication from the lower layers that the UE has changed to S1 mode or E-UTRA connected to 5GCN for case h) in subclause 5.6.1.1; or  (b) SERVICE ACCEPT message received, or  SERVICE REJECT message received for cases other than h) in subclause 5.6.1.1 | Abort the procedure |
| T3519 | 60s  NOTE 7  NOTE 8  In WB-N1/CE mode, 90s | 5GMM-REGISTERED-INITIATED  5GMM-REGISTERED  5GMM-DEREGISTERED-INITIATED  5GMM-SERVICE-REQUEST-INITIATED (NOTE 6) | Transmission of IDENTITY RESPONSE message, REGISTRATION REQUEST message, or DEREGISTRATION REQUEST message with freshly generated SUCI | REGISTRATION ACCEPT message with new 5G-GUTI received  CONFIGURATION UPDATE COMMAND message with new 5G-GUTI received DEREGISTRATION ACCEPT message | Delete stored SUCI |
| T3520 | 15s  NOTE 7  NOTE 8  In WB-N1/CE mode, 33s | 5GMM-REGISTERED-INITIATED  5GMM-REGISTERED  5GMM-DEREGISTERED-INITIATED  5GMM-SERVICE-REQUEST-INITIATED | Transmission of AUTHENTICATION FAILURE message with any of the 5GMM cause #20, #21, #26 or #71  Transmission of AUTHENTICATION RESPONSE message with an EAP-response message after detection of an error as described in subclause 5.4.1.2.2.4 | 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 during a 5G AKA based primary authentication and key agreement procedure, 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 during a 5G AKA based primary authentication and key agreement procedure, 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.  On first expiry during an EAP based primary authentication and key agreement procedure, the UE should consider the network as false and follow item e of subclause 5.4.1.2.4.5, if the UE is not registered for emergency services.  On first expiry during an EAP based primary authentication and key agreement procedure, the UE will follow subclause 5.4.1.2.4.5 under "For item e:", if the UE is registered for emergency services |
| T3521 | 15s  NOTE 7  NOTE 8  In WB-N1/CE mode, 45s | 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 |
| T3525 | Default 60s  NOTE 3  NOTE 7  NOTE 8  In WB-N1/CE mode, default 120s | 5GMM-REGISTERED.NORMAL-SERVICE | T3517 expires and service request attempt counter is greater than or equal to 5 | When entering state other than 5GMM-REGISTERED.NORMAL-SERVICE state,  or  UE camped on a new PLMN other than the PLMN on which timer started,  or  User-plane resources established with the network | The UE may initiate service request procedure |
| T3540 | 10s | 5GMM-DEREGISTERED  5GMM-REGISTERED | REGISTRATION REJECT message or DEREGISTRATION REQUEST message received with any of the 5GMM cause #3, #6, #7, #11, #12, #13, #15, #27, #31, #62, #72, #73, #74, #75 or #76  SERVICE REJECT message received with any of the 5GMM cause #3, #6, #7, #11, #12, #13, #15, #27, #72, #73, #74, #75 or #76.  REGISTRATION ACCEPT message received as described in subclause 5.3.1.3 case b)  SERVICE ACCEPT message received as described in subclause 5.3.1.3 case f)  AUTHENTICATION REJECT message received | N1 NAS signalling connection released  PDU sessions have been set up | Release the NAS signalling connection for the cases a), b), f) and g) as described in subclause 5.3.1.3 |
| 5GMM-REGISTERED | CONFIGURATION UPDATE COMMAND message received as described in subclause 5.3.1.3 case e) | N1 NAS signalling connection released | Release the NAS signalling connection for the case e) and perform a new registration procedure as described in subclause 5.5.1.3.2 |
| 5GMM-DEREGISTERED  5GMM-DEREGISTERED.NORMAL-SERVICE  5GMM-REGISTERED.NON-ALLOWED-SERVICE | REGISTRATION REJECT message received with the 5GMM cause #9 or #10  SERVICE REJECT message received with the 5GMM cause #9, #10 or #28 | Release the NAS signalling connection for the cases c) and d) as described in subclause 5.3.1.3 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  NOTE 4 | 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.  NOTE 3: The value of this timer is UE implementation specific, with a minimum value of 60 seconds if not in NB-N1 mode and if not in WB-N1/CE mode.  NOTE 4: If the T3346 value received in the mobility management messages is greater than the value of the non-3GPP de-registration timer, the UE sets the non-3GPP de-registration timer value to be 4 minutes greater than the value of timer T3346.  NOTE 5: The conditions for which this applies are described in subclause 5.5.1.3.7.  NOTE 6: The conditions for which this applies to the 5GMM-SERVICE-REQUEST-INITIATED state are described in subclause 5.4.1.3.7 case c) and case d).  NOTE 7: In NB-N1 mode, the timer value shall be calculated as described in subclause 4.17.  NOTE 8: In WB-N1 mode, if the UE supports CE mode B and operates in either CE mode A or CE mode B, then the timer value is as described in this table for the case of WB-N1/CE mode (see subclause 4.19). | | | | | |

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

| TIMER NUM. | TIMER VALUE | STATE | CAUSE OF START | NORMAL STOP | ON  EXPIRY |
| --- | --- | --- | --- | --- | --- |
| T3513  NOTE 7  NOTE 9 | NOTE 4 | 5GMM-REGISTERED | Paging procedure initiated | Paging procedure completed as specified in subclause 5.6.2.2.1 | Network dependent |
| T3522  NOTE 6  NOTE 8 | 6s  In WB-N1/CE mode, 24s | 5GMM-DEREGISTERED-INITIATED | Transmission of DEREGISTRATION REQUEST message | DEREGISTRATION ACCEPT message received | Retransmission of DEREGISTRATION REQUEST message |
| T3550  NOTE 6  NOTE 8 | 6s  In WB-N1/CE mode, 18s | 5GMM-COMMON-PROCEDURE-INITIATED | Transmission of REGISTRATION ACCEPT message with 5G-GUTI, SOR transparent container IE, the Extended emergency number list IE, UE radio capability ID IE, UE radio capability ID deletion indication IE, Operator-defined access category definitions IE, Network slicing subscription changed indication, or new configured NSSAI and optionally new mapped S-NSSAI(s) | REGISTRATION COMPLETE message received | Retransmission of REGISTRATION ACCEPT message |
| T3555  NOTE 6  NOTE 8 | 6s  In WB-N1/CE mode, 24s | 5GMM-REGISTERED | Transmission of CONFIGURATION UPDATE COMMAND message with "acknowledgement requested" set in the Acknowldgement bit of the Configuration update indication IE | CONFIGURATION UPDATE COMPLETE message received | Retransmission of CONFIGURATION UPDATE COMMAND message |
| T3560  NOTE 6  NOTE 8 | 6s  In WB-N1/CE mode, 24s | 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 |
| T3565  NOTE 6  NOTE 8 | 6s  In WB-N1/CE mode, 24s | 5GMM-REGISTERED | Transmission of NOTIFICATION message | SERVICE REQUEST message received  NOTIFICATION RESPONSE message received  REGISTRATION REQUEST  Message received  DEREGISTRATION REQUEST message received | Retransmission of NOTIFICATION message |
| T3570  NOTE 6  NOTE 8 | 6s  In WB-N1/CE mode, 24s | 5GMM-COMMON-PROCEDURE-INITIATED | Transmission of IDENTITY REQUEST message | IDENTITY RESPONSE message received | Retransmission of IDENTITY REQUEST message |
| T3575 | 15s | 5GMM-REGISTERED | Transmission of NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message | NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message received | Retransmission of NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND message |
| Active timer | TBD | All except 5GMM-DEREGISTERED | Entering 5GMM-IDLE mode after indicating MICO mode activation to the UE with an active timer value. | N1 NAS signalling  connection established | Activate MICO mode for the UE. |
| Implicit de-registration timer | NOTE 2 | All except 5GMM-DEREGISTERED | The mobile reachable timer expires while the network is in 5GMM-IDLE mode  Entering 5GMM-IDLE mode over 3GPP access if the MICO mode is activated and strictly periodic monitoring timer is not running  The strictly periodic monitoring timer expires while the network is in 5GMM-IDLE mode | N1 NAS signalling connection established | Implicitly de-register the UE on 1st expiry |
| 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 |
| 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 |
| Strictly periodic monitoring timer | NOTE 5 | All except 5GMM-DEREGISTERED | At the successful completion of registration update procedure if strictly periodic registration timer indication is supported as specified in subclause 5.3.7. | Entering 5GMM-DEREGISTERED. | In 5GMM-IDLE mode, start implicit de-registration timer as specified in subclause 5.3.7.  In 5GMM-CONNECTED mode, Strictly periodic monitoring timer is started again as specified in subclause 5.3.7. |
| NOTE 1: The default value of this timer is 4 minutes greater than the value of timer T3512. If the UE is registered for emergency services, the value of this timer is set equal to the value of timer T3512. If the T3346 value provided in the mobility management messages is greater than the value of the timer T3512, the AMF sets the mobile reachable timer and the implicit de-registration timer such that the sum of the timer values is greater than the value of timer T3346.  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 the value of timer 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. If the T3346 value provided in the mobility management messages is greater than the value of the non-3GPP de-registration timer, the AMF sets the non-3GPP implicit de-registration timer value to be 8 minutes greater than the value of timer T3346.  NOTE 4: The value of this timer is network dependent.  NOTE 5: The value of this timer is the same as the value of timer T3512.  NOTE 6: In NB-N1 mode, the timer value shall be calculated as described in subclause 4.17.  NOTE 7: In NB-N1 mode, the timer value shall be calculated by using an NAS timer value which is network dependent.  NOTE 8: In WB-N1 mode, if the UE supports CE mode B and operates in either CE mode A or CE mode B, then the timer value is as described in this table for the case of WB-N1/CE mode (see subclause 4.19).  NOTE 9: In WB-N1 mode, if the UE supports CE mode B, then the timer value shall be calculated by using an NAS timer value which value 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.

NOTE: Timer T3396 is defined in 3GPP TS 24.008 [12].

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  NOTE 4  NOTE 5 | 16s  In WB-N1/CE mode, 24s | PDU SESSION ACTIVE PENDING | Transmission of PDU SESSION ESTABLISHMENT REQUEST message | PDU SESSION ESTABLISHMENT ACCEPT message received or  PDU SESSION ESTABLISHMENT REJECT message received or  PDU SESSION ESTABLISHMENT REQUEST received in a DL NAS TRANSPORT message with 5GMM cause #22, #28, #65. #67, #69, #90 or #91 | Retransmission of PDU SESSION ESTABLISHMENT REQUEST message |
| T3581  NOTE 4  NOTE 5 | 16s  In WB-N1/CE mode, 24s | PDU SESSION MODIFICATION PENDING | 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 or  PDU SESSION MODIFICATION REQUEST received in a DL NAS TRANSPORT message with 5GMM cause #22, #28. #67, #69, or #90 | Retransmission of PDU SESSION MODIFICATION REQUEST message |
| T3582  NOTE 4  NOTE 5 | 16s  In WB-N1/CE mode, 24s | PDU SESSION INACTIVE PENDING | 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 |
| T3584 | NOTE 3 | PDU SESSION ACTIVE PENDING  PDU SESSION MODIFICATION PENDING  PDU SESSION ACTIVE or PDU SESSION INACTIVE PENDING | PDU SESSION ESTABLISHMENT REJECT, PDU SESSION MODIFICATION REJECT, or PDU SESSION RELEASE COMMAND received with 5GSM cause #67 and with a timer value for T3584  PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST received in a DL NAS TRANSPORT message with 5GMM cause #67 and with a timer value for T3584 (see subclause 5.4.5.3.3) | PDU SESSION RELEASE COMMAND or PDU SESSION MODIFICATION COMMAND or DEREGISTRATION REQUEST with the re-registration type "re-registration required" | None |
| T3585 | NOTE 3 | PDU SESSION ACTIVE PENDING  PDU SESSION MODIFICATION PENDING  PDU SESSION ACTIVE or PDU SESSION INACTIVE PENDING | PDU SESSION ESTABLISHMENT REJECT, PDU SESSION MODIFICATION REJECT, or PDU SESSION RELEASE COMMAND received with 5GSM cause #69 and with a timer value for T3585  PDU SESSION ESTABLISHMENT REQUEST, or PDU SESSION MODIFICATION REQUEST received in a DL NAS TRANSPORT message with 5GMM cause #69 and with a timer value for T3585(see subclause 5.4.5.3.3) | PDU SESSION RELEASE COMMAND or PDU SESSION MODIFICATION COMMAND or DEREGISTRATION REQUEST with the re-registration type "re-registration required" | None |
| Back-off timer |  |  | defined in 3GPP TS 24.008 [12] |  |  |
| 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.  NOTE 3: The value of this timer is provided by the network.  NOTE 4: In NB-N1 mode, then the timer value shall be calculated as described in subclause 4.18.  NOTE 5: In WB-N1 mode, if the UE supports CE mode B and operates in either CE mode A or CE mode B, then the timer value is as described in this table for the case of WB-N1/CE mode (see subclause 4.20). | | | | | |

NOTE 1: The back-off timer is used to describe a logical model of the required UE behaviour. This model does not imply any specific implementation, e.g. as a timer of timestamp.

NOTE 2: Reference to back-off timer in this section can either refer to use of timer T3396 or to use of a different packet system specific timer within the UE. Whether the UE uses T3396 as a back-off timer or it uses different packet system specific timers as back-off timers is left up to UE implementation.

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  NOTE 3  NOTE 4 | 15s  In WB-N1/CE mode, 23s | PROCEDURE TRANSACTION PENDING | Transmission of PDU SESSION AUTHENTICATION COMMAND message | PDU SESSION AUTHENTICATION COMPLETE message received | Retransmission of PDU SESSION AUTHENTICATION COMMAND message |
| T3591  NOTE 3  NOTE 4 | 16s  In WB-N1/CE mode, 24s | PDU SESSION MODIFICATION PENDING | 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  NOTE 3  NOTE 4 | 16s  In WB-N1/CE mode, 24s | PDU SESSION INACTIVE PENDING | 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  NOTE 3  NOTE 4 | Default  60s  (NOTE 2) | PDU SESSION MODIFICATION PENDING | 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.  NOTE 3: In NB-N1 mode, the timer value shall be calculated as described in subclause 4.18.  NOTE 4: In WB-N1 mode, if the UE supports CE mode B and operates in either CE mode A or CE mode B, then the timer value is as described in this table for the case of WB-N1/CE mode (see subclause 4.20). | | | | | |

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 or SNPN 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 or SNPN which by subscription offers roaming to that UE but not in that tracking area.

Cause #15 – No suitable cells in tracking area

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 UE, by subscription, is not allowed to operate, but when it should find another allowed tracking area in the same PLMN or an equivalent PLMN or the same SNPN.

NOTE 2: Cause #15 and cause #12 differ in the fact that cause #12 does not trigger the UE to search for another allowed tracking area on the same PLMN or SNPN.

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 or SNPN where the UE by subscription or operator policy, is not allowed to operate in N1 mode. This cause is also sent for the case when the UE does not support CAG feature and the UE is allowed to access the 5GS via CAG cells only.

Cause #31 – Redirection to EPC required

This 5GMM cause is sent to the UE if it requests service in a PLMN where the UE by operator policy, is not allowed in 5GCN and redirection to EPC is required.

Cause #72 – Non-3GPP access to 5GCN not allowed

This 5GMM cause is sent to the UE if it requests accessing 5GCN over non-3GPP access in a PLMN, where the UE by subscription, is not allowed to access 5GCN over non-3GPP access.

Cause #74 – Temporarily not authorized for this SNPN

This 5GMM cause is sent to the UE if it requests access, or if the network initiates a de-registration procedure, in a cell belonging to an SNPN with a non-globally-unique SNPN identity for which the UE has no subscription to operate.

Cause #75 – Permanently not authorized for this SNPN

This 5GMM cause is sent to the UE if it requests access, or if the network initiates a de-registration procedure, in a cell belonging to an SNPN with a globally-unique SNPN identity for which the UE either has no subscription to operate or the UE's subscription has expired.

Cause #76 – Not authorized for this CAG or authorized for CAG cells only

This 5GMM cause is sent to the UE if the UE requests access or de-registration:

i) in a CAG cell with a CAG-ID which is not included in the UE's "allowed CAG list" for the PLMN; or

ii) in a non-CAG cell, wherein the UE is only allowed to access 5GS via CAG cells

Cause #77 – Wireline access area not allowed

This 5GMM cause is sent to the 5G-RG or the W-AGF acting on behalf of the FN-CRG if the 5G-RG or the W-AGF acting on behalf of the FN-CRG request accessing 5GCN over a wireline access network belonging to a wireline access area, where the 5G-RG or the W-AGF acting on behalf of the FN-CRG are not allowed by subscription to access the 5GCN over the wireline access.

## A.3 Causes related to PLMN or SNPN 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 of the 3GPP access or in an area of the wireline access, which is a part of the UE's non-allowed area or is not a part of the UE's allowed area.

Cause #43 – LADN not available

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

Cause #62 – No network slices available

This 5GMM cause is sent by the network if none of the requested network slice(s) in the registration request are allowed and there are no default network slice(s) configured in the network.

Cause #65 – Maximum number of PDU sessions reached

This 5GMM cause is used by the network to indicate that the procedure requested by the UE was rejected as the network has reached the maximum number of simultaneously active PDU sessions for the UE.

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.

Cause #71 – 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 #73 – Serving network not authorized

This 5GMM cause is sent to the UE if the UE initiates registration towards a serving network and the serving network fails to be authorized by the UE's home network.

Cause #90 – Payload was not forwarded

This 5GMM cause is sent by the network to indicate that the requested service cannot be provided because payload could not be forwarded by AMF.

Cause #91 – DNN not supported or not subscribed in the slice

This 5GMM cause is sent by the network to indicate that the requested service cannot be provided because payload could not be forwarded by AMF because the DNN is not supported or not subscribed in the slice selected by the network if the UE did not indicate a slice, or the DNN is not supported or not subscribed in the slice indicated by the UE.

Cause #92 – Insufficient user-plane resources for the PDU session

This 5GMM cause is sent by the network to indicate that the requested service cannot be provided due to insufficient user-plane resources for the PDU session.

## 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 #8 – Operator Determined Barring

This 5GSM cause is used by the network to indicate that the requested service was rejected by the SMF due to Operator Determined Barring.

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, revoked by the external DN, or rejected by 5GCN due to a failed user authentication or authorization.

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 #32 – Service option not supported

This 5GSM cause is used by the network when the UE requests a service which is not supported by the PLMN.

Cause #33 – Requested service option not subscribed

This 5GSM cause is sent when the UE requests a service option for which it has no subscription.

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 #38 – Network failure

This 5GSM cause is used by the network to indicate that the requested service was rejected due to an error situation in the network.

Cause #39 – Reactivation requested

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

Cause #41 – Semantic error in the TFT operation

This 5GSM cause is used by the UE to indicate a semantic error in the TFT operation included in the request.

Cause #42 – Syntactical error in the TFT operation

This 5GSM cause is used by the UE to indicate a syntactical error in the TFT operation included in the request.

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 identified by the PDU session identity IE in the request or the command is not active.

Cause #44 – Semantic errors in packet filter(s)

This 5GSM cause is used by the network or the UE to indicate that the requested service was rejected due to one or more semantic errors in packet filter(s) of the QoS rule included in the request.

Cause #45 – Syntactical error in packet filter(s)

This 5GSM cause is used by the network or the UE to indicate that the requested service was rejected due to one or more syntactical errors in packet filter(s) of the QoS rule included in the request.

Cause #46 –Out of LADN service area

This 5GSM cause is used by the network to indicate the UE is out of the LADN service area.

Cause #47 –PTI mismatch

This 5GSM cause is used by the network or UE to indicate that the PTI provided to it does not match any PTI in use.

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 #57 – PDU session type IPv4v6 only allowed

This 5GSM cause is used by the network to indicate that only PDU session types IPv4, IPv6 or IPv4v6 are allowed for the requested IP connectivity.

Cause #58 – PDU session type Unstructured only allowed

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

Cause #61 – PDU session type Ethernet only allowed

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

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 invalid for the specific 5GSM message.

Cause #82 – Maximum data rate per UE for user-plane integrity protection is too low

This 5GSM cause is used by the network to indicate that the requested service cannot be provided because the maximum data rate per UE for user-plane integrity protection is too low.

Cause #83 – Semantic error in the QoS operation

This 5GSM cause is used by the network or the UE to indicate that the requested service was rejected due to a semantic error in the QoS operation included in the request.

Cause #84 – Syntactical error in the QoS operation

This 5GSM cause is used by the network or the UE to indicate that the requested service was rejected due to a syntactical error in the QoS operation included in the request.

Cause #85 – Invalid mapped EPS bearer identity

This 5GSM cause is used by the network or the UE to indicate that the mapped EPS bearer identity value provided to it is not a valid value or the mapped EPS bearer identified by the mapped EPS bearer identity does not exist.

## 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

## C.1 Storage of 5GMM information for UEs not operating in SNPN access mode

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;

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

e) SOR counter (see subclause 9.11.3.51); and

f) UE parameter update counter (see subclause 9.11.3.53A).

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);

- NSSAI inclusion mode(s);

- MPS indicator;

- MCS indicator;

- operator-defined access category definitions;

- network-assigned UE radio capability IDs; and

- "CAG information list", if the UE supports CAG.

Each configured NSSAI consists of S-NSSAI(s) stored together with a PLMN identity, if it is associated with a PLMN. The UE shall store the S-NSSAI(s) of the HPLMN. If the UE is in the VPLMN, the UE shall also store the configured NSSAI for the current PLMN and any necessary mapped S-NSSAI(s). 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).

Each NSSAI inclusion mode is associated with a PLMN identity and access type. The NSSAI inclusion mode(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 NSSAI inclusion mode(s).

The MPS indicator is stored together with a PLMN identity of the PLMN that provided it, and is valid in that RPLMN or equivalent PLMN. The MPS indicator 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 MPS indicator.

The MCS indicator is stored together with a PLMN identity of the PLMN that provided it, and is valid in that RPLMN or equivalent PLMN. The MCS indicator 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 MCS indicator.

Operator-defined access category definitions are stored together with a PLMN identity of the PLMN that provided them, and is valid in that PLMN or equivalent PLMN. The operator-defined access category definitions 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 operator-defined access category definitions. The maximum number of stored operator-defined access category definitions is UE implementation dependent.

Each network-assigned UE radio capability ID is stored together with a PLMN identity of the PLMN that provided it as well as a mapping to the corresponding UE radio configuration, and is valid in that PLMN. A network-assigned UE radio capability ID 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 network-assigned UE radio capability ID. The UE shall be able to store at least the last 16 received network-assigned UE radio capability IDs. There shall be only one network-assigned UE radio capability ID stored for a given combination of PLMN identity and UE radio configuration and any existing UE radio capability ID shall be deleted when a new UE radio capability ID is added for the same combination of PLMN identity and UE radio configuration. If the UE receives a network-assigned UE radio capability ID with a Version ID value different from the value included in the network-assigned UE radio capability ID(s) stored at the UE for the serving PLMN, the UE may delete these stored network-assigned UE radio capability ID(s).

The allowed NSSAI(s) can be stored in a non-volatile memory in the ME together with the SUPI from the USIM. Allowed NSSAI consists of S-NSSAI(s) stored together with a PLMN identity, if it is associated with a PLMN. If the allowed NSSAI is stored, then the UE shall store the S-NSSAI(s) of the HPLMN. If the UE is in the VPLMN, the UE shall also store the allowed NSSAI for the serving PLMN and any necessary mapping of the allowed NSSAI for the serving PLMN to the S-NSSAI(s) of the HPLMN. The allowed 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 allowed 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.

The "CAG information list" 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 "CAG information list".

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

The following 5GMM parameters shall be stored per SNPN in a non-volatile memory in the ME together with the subscriber identifier associated with the SNPN identity of the SNPN in the "list of subscriber data" configured in the ME (see 3GPP TS 23.122 [5]):

a) 5G-GUTI;

b) last visited registered TAI;

c) 5GS update status;

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

e) configured NSSAI(s);

f) NSSAI inclusion mode(s);

g) MPS indicator;

h) MCS indicator;

i) operator-defined access category definitions; and

j) network-assigned UE radio capability IDs.

Each configured NSSAI consists of S-NSSAI(s) stored together with an SNPN identity, if it is associated with an SNPN.

Each NSSAI inclusion mode is associated with an SNPN identity and access type.

The MPS indicator is stored together with an SNPN identity of the SNPN that provided it, and is valid in that registered SNPN.

The MCS indicator is stored together with an SNPN identity of the SNPN that provided it, and is valid in that registered SNPN.

Operator-defined access category definitions are stored together with an SNPN identity of the SNPN that provided them, and are valid in that SNPN. The maximum number of stored operator-defined access category definitions is UE implementation dependent.

Each network-assigned UE radio capability ID is stored together with an SNPN identity of the SNPN that provided it as well as a mapping to the corresponding UE radio configuration, and is valid in that SNPN. The UE shall be able to store at least the last 16 received network-assigned UE radio capability IDs. There shall be only one network-assigned UE radio capability ID stored for a given combination of SNPN identity and UE radio configuration and any existing UE radio capability ID shall be deleted when a new UE radio capability ID is added for the same combination of SNPN identity and UE radio configuration. If the UE receives a network-assigned UE radio capability ID with a Version ID value different from the value included in the network-assigned UE radio capability ID(s) stored at the UE for the serving SNPN, the UE may delete these stored network-assigned UE radio capability ID(s).

The allowed NSSAI(s) can be stored in a non-volatile memory in the ME. Allowed NSSAI consists of S-NSSAI(s) stored together with an SNPN identity, if it is associated with an SNPN.

Annex D (normative):  
UE policy delivery service

## D.1 General

### D.1.1 Overview

The PCF may provide the UE with one or more UE policies using the network-requested UE policy management procedure. The UE provides the PCF with a list of one or more stored UE policy section identifiers (UPSIs), and the PCF provides each UE policy using one or more UE policy sections, each identified by aUPSI. 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.

The UE provides the PCF with the UE policy related capabilities such as the UE's support for ANDSP and the UE's OS Id.

The UE can also request the PCF to provide V2XP as specified in 3GPP TS 24.587 [19B].

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

When the PCF or the UE initiates a procedure, it shall include a valid PTI value in the message header of the command message or the request message. When the UE initiates a procedure, the UE shall use a PTI value in range between 01H and 77H. When the PCF initiates a procedure, the PCF shall use a PTI value in range between 80H and FEH.

When the PCF initiates a transaction related procedure (i.e. a procedure consisting of more than one message and the messages are related), it shall include a valid PTI value in the message header of the command message.

If a response message is sent as result of a received command or request message, the UE or the PCF shall include in the response message the PTI value received within the received command or request message (see examples in figure D.1.2.1, figure D.1.2.2 and figure D.1.2.3).

If a command message is sent as result of a received request message, the PCF shall include in the command message the PTI value received with the request message (see examples in figure D.1.2.3).



Figure D.1.2.1: Network-requested transaction related procedure



Figure D.1.2.2: UE-requested transaction related procedure rejected by the network



Figure D.1.2.3: UE-requested transaction related procedure triggering a network-requested transaction related procedure

NOTE: In earlier versions of this protocol, the UE can include in the response message a PTI value which is not the same as the one received within the command message, and therefore the PCF could not associate the response message from the UE to the command message sent.

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

b) encode the information about the UE policy sections to be added, modified or deleted in a UE policy section management list IE as specified in subclause D.6.2 and include it in a MANAGE UE POLICY COMMAND message;

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

d) start timer T3501 (see example in figure D.2.1.2.1).

NOTE: The PCF starts a different timer T3501 for each allocated PTI value.



Figure D.2.1.2.1: Network-requested UE policy management procedure

Upon receipt of the MANAGE UE POLICY COMMAND message with a PTI value currently not used, for each instruction included in the UE policy section management list IE, the UE shall:

a) store the received UE policy section of the instruction, if the UE has no stored UE policy section associated with the same UPSI as the UPSI associated with the instruction;

b) replace the stored UE policy section with the received UE policy section of the instruction, if the UE has a stored UE policy section associated with the same UPSI as the UPSI associated with the instruction; or

c) delete the stored UE policy section, if the UE has a stored UE policy section associated with the same UPSI as the UPSI associated with the instruction and the UE policy section contents of the instruction is empty.

The UE may continue storing a received UE policy section for a PLMN or SNPN when the UE registers in another PLMN or SNPN. If necessary, the UE may delete UE policy sections stored for a PLMN or SNPN other than the RPLMN and the HPLMN or the registered SNPN, before storing the new received UE policy sections.

When storing a UE policy sections received from an SNPN, the UE shall associate the NID of that SNPN with the UPSI of the stored UE policy section.

NOTE: The maximum number of UE policy sections for PLMNs or SNPNs other than the HPLMN and the RPLMN or the registered SNPN that the UE can store and how the UE selects the UE policy sections to be deleted are up to the UE implementation.

#### 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 including the PTI value received within the MANAGE UE POLICY COMMAND 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 T3501. The PCF should ensure that the PTI value assigned to this procedure is not released immediately.

NOTE: The way to achieve this is implementation dependent. For example, the PCF can ensure that the PTI value assigned to this procedure is not released during the time equal to or greater than the default value of timer T3501.

#### 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) set the PTI IE to the PTI value received within the MANAGE UE POLICY COMMAND message and encode the UPSI associated with the instructions which could not be executed successfully and the associated UE policy delivery service 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 T3501. Any instruction that was included in the UE policy section management list IE and whose associated UPSI is not included in a UE policy section management result IE of the received MANAGE UE POLICY COMMAND REJECT message is considered as successfully executed.

The PCF should ensure that the PTI value assigned to this procedure is not released immediately.

NOTE: The way to achieve this is implementation dependent. For example, the PCF can ensure that the PTI value assigned to this procedure is not released during the time equal to or greater than the default value of timer T3501.

Upon receipt of the notification from the AMF that the UE is not reachable, the PCF shall stop the T3501.

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

The following abnormal cases can be identified:

a) T3501 expired.

The PCF shall, on the first expiry of the timer T3501, retransmit the MANAGE UE POLICY COMMAND message and shall reset and start timer T3501. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3501, the PCF shall abort the procedure and release the allocated PTI.

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

The following abnormal cases can be identified:

a) Receipt of an instruction associated with a UPSI which has a PLMN ID part that is not equal to the PLMN ID of the UE's HPLMN and the instruction contains a UE policy part with a UE policy part type set to "URSP".

The UE shall set the UE policy delivery service cause to #111 (Protocol error, unspecified) for the instruction in the UE policy section management result IE of the MANAGE UE POLICY COMMAND REJECT message.

b) Receipt of an instruction associated with a UPSI which has a PLMN ID part that is not equal to the PLMN ID of the UE's HPLMN or the UE's RPLMN and the instruction contains a UE policy part with a UE policy part type set to "ANDSP".

The UE shall set the UE policy delivery service cause to #111 (Protocol error, unspecified) for the instruction in the UE policy section management result IE of the MANAGE UE POLICY COMMAND REJECT message.

c) Transmission failure of the MANAGE UE POLICY COMPLETE message indication from lower layers.

The UE shall not diagnose an error and consider the network-initiated UE policy delivery procedure complete.

NOTE 1: Considering the network-initiated UE policy delivery procedure complete as a result of this abnormal case does not cause the UE to revert the execution of the instructions included in the MANAGE UE POLICY COMMAND message.

d) Transmission failure of the MANAGE UE POLICY COMMAND REJECT message indication from lower layers.

The UE shall not diagnose an error and consider the network-initiated UE policy delivery procedure complete.

NOTE 2: Considering the network-initiated UE policy delivery procedure complete as a result of this abnormal case does not cause the UE to revert the execution of the instructions included in the MANAGE UE POLICY COMMAND message and successfully processed by the UE.

e) Receipt of a MANAGE UE POLICY COMMAND message with a PTI set to the same value as the PTI of a previously received MANAGE UE POLICY COMMAND message.

The UE shall discard the message and retransmit the MANAGE UE POLICY COMMAND COMPLETE or MANAGE UE POLICY COMMAND REJECT message transmitted in response to the previously received MANAGE UE POLICY COMMAND message.

NOTE 3: The way to achieve this is UE implementation dependent. For example, the UE can assume that on the fifth expiry of timer T3501, the PCF will abort the procedure and that the PTI value assigned to the procedure will be released.

### D.2.2 UE-initiated UE state indication procedure

#### D.2.2.1 General

The purpose of the UE-initiated UE state indication procedure is:

a) to deliver the UPSI(s) of the UE policy section(s) which are:

- identified by a UPSI with the PLMN ID part indicating the HPLMN or the selected PLMN; and

- stored in the UE;

to the PCF if the UE has one or more stored UE policy sections identified by a UPSI with the PLMN ID part indicating the HPLMN or the selected PLMN; and

b) to indicate whether UE supports ANDSP; and

c) to deliver the UE's one or more OS Ids.

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

In order to initiate the UE-initiated UE state indication procedure, the UE shall create a UE STATE INDICATION message. The UE:

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

b) if not operating in SNPN access mode, shall include the UPSI(s) of the UE policy section(s) which are identified by a UPSI with the PLMN ID part indicating the HPLMN or the selected PLMN available in the UE in the UPSI list IE;

c) if operating in SNPN access mode, shall include UPSI(s) of the UE policy section(s) which are identified by a UPSI:

- with the PLMN ID part indicating the MCC and MNC of the selected SNPN; and

- associated with the NID of the selected PLMN;

available in the UE in the UPSI list IE;

d) shall specify whether the UE supports ANDSP in the UE policy classmark IE; and

e) may include the UE's one or more OS Ids in the UE OS Id IE.

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



Figure D.2.2.2.1: UE-initiated UE state indication procedure

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

Upon receipt of the UE STATE INDICATION message, the PCF shall operate as described in 3GPP TS 23.502 [9] and 3GPP TS 29.525 [21].

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

Apart from the case described in subclause D.2.2.3, no abnormal cases have been identified.

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

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

When the UE needs to apply URSP as specified in 3GPP TS 24.526 [19], the UE shall consider all UE policy parts with URSP contents currently stored at the UE.

When the UE needs to apply V2XP as specified in 3GPP TS 24.588 [19C], the UE shall consider all UE policy parts with V2XP contents currently stored at the UE.

## D.4 Void

## 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 service message type  D.6.1 | M | V | 1 |
|  | UE policy section management list | UE policy section management list  D.6.2 | M | LV-E | 11-65533 |
| NOTE: The total length of the MANAGE UE POLICY COMMAND message content cannot exceed 65535 octets (see Payload container contents maximum length as specified in subclause 9.11.3.39.1). | | | | | |

### 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 service 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 service message type  D.6.1. | M | V | 1 |
|  | UE policy section management result | UE policy section management result  D.6.3 | M | LV-E | 11-65533 |
| NOTE: The total length of the MANAGE UE POLICY COMMAND REJECT message content cannot exceed 65535 octets (see Payload container contents maximum length as specified in subclause 9.11.3.39.1). | | | | | |

### D.5.4 UE state indication

#### D.5.4.1 Message definition

The UE STATE INDICATION message is sent by the UE to the PCF:

a) to deliver the UPSI(s) of the UE policy section(s) stored in the UE;

b) to indicate whether the UE supports ANDSP; and

c) to deliver the the UE's one or more OS Ids;

see table D.5.4.1.1.

Message type: UE STATE INDICATION

Significance: dual

Direction: UE to network

Table D.5.4.1.1: UE STATE INDICATION message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | PTI | Procedure transaction identity  9.6 | M | V | 1 |
|  | UE STATE INDICATION message identity | UE policy delivery service message type  D.6.1 | M | V | 1 |
|  | UPSI list | UPSI list  D.6.4 | M | LV-E | 9-65531 |
|  | UE policy classmark | UE policy classmark  D.6.5 | M | LV | 2-4 |
| 41 | UE OS Id | OS Id  D.6.6 | O | TLV | 18-242 |
| NOTE: The total length of the UE STATE INDICATION message content cannot exceed 65535 octets (see Payload container contents maximum length as specified in subclause 9.11.3.39.1). | | | | | |

## D.6 Information elements coding

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

Table D.6.1.1: UE policy delivery service 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 |  | | UE STATE INDICATION message | |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |  | | UE POLICY PROVISIONING REQUEST message (see NOTE) | |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |  | | UE POLICY PROVISIONING REJECT message (see NOTE) | |
|  | | | | | | | | | | | |
| All other values are reserved | | | | | | | | | | | |
| NOTE: Coding and usage of UE POLICY PROVISIONING REQUEST message and UE POLICY PROVISIONING REJECT message are specified in 3GPP TS 24.587 [19B]. | | | | | | | | | | | |

### 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 12 octets and a maximum length of 65534 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

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |
| 0 | 0 | 1 | 1 | V2XP |
| 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 24.526 [19] for the UE policy part type field set to "URSP" or "ANDSP" and encoded as specified in 3GPP TS 24.588 [19C] for the UE policy part type field set to "V2XP". | | | | |
|  | | | | |

### 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 12 octets and a maximum length of 65534 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 subresult

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
| Result 1 | | | | | | | | | octet d+4  octet d+8 |
| Result 2 | | | | | | | | | octet d+9  octet d+13 |
| … | | | | | | | | | octet d+14  …  octet e |
| Result N | | | | | | | | | octet e+1  octet e+5 |

Figure D.6.3.4: UE policy section management subresult 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+1, and bits 4 to 1 of octet d+2) | | | | | | | | | |
|  | | | | | | | | | |
| 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+2, and octet d+3) | | | | | | | | | |
|  | | | | | | | | | |
| 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. | | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | | | | | |
| Result (octet f to f+4) | | | | | | | | | |
|  | | | | | | | | | |
| 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 10 octets and a maximum length of 65532 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 e+2\* | |

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. |
|  |

### D.6.5 UE policy classmark

The purpose of the UE policy classmark information element is to provide the network with information about the policy aspects of the UE.

The UE policy classmark information element is coded as shown in figure D.6.5.1 and table D.6.5.1.

The UE policy classmark 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 |  |
| Policy information IEI | octet 1 | | | | | | | |
| Length of Policy information contents | octet 2 | | | | | | | |
| 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0  Spare | 0 Spare | 0 Spare | SupportANDSP | octet 3 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | octet 4\* -5\* |
| Spare |  | | | | | | | |

Figure D.6.5.1: UE policy classmark information element

Table D.6.5.1: UE policy classmark information element

|  |  |
| --- | --- |
| Support of ANDSP by the UE (SupportANDSP) (octet 3, bit 1) | |
| Bit | |
| 1 |  |
| 0 | ANDSP not supported by the UE |
| 1 | ANDSP supported by the UE |
|  | |
|  | |
| All other bits in octet 3 to 5 are spare and shall be coded as zero, if the respective octet is included in the information element. | |

### D.6.6 UE OS Id

The purpose of the UE OS Id information element is to provide the network with information about the OS of the UE.

The UE OS Id information element is coded as shown in figure D.6.6.1 and table D.6.6.1.

The UE OS Id is a type 4 information element with a minimum length of 18 octet and a maximum length of 242 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| OS Id IEI | octet 1 | | | | | | | |
| Length of OS Id information contents | octet 2 | | | | | | | |
| OS Id\_1 | octets 3 - 18 | | | | | | | |
| … | … | | | | | | | |
| OS Id\_15 | octets 227\* -242\* | | | | | | | |

Figure D.6.6.1: UE OS Id information element

Table D.6.6.1: UE OS Id information element

|  |
| --- |
| OS Id: |
| The OS Id is coded as a sequence of a sixteen octet OS Id value field. The OS Id value field is defined as Universally Unique IDentifier (UUID) as specified in IETF RFC 4122 [35A]. |

## D.7 Timers of UE policy delivery service

Timers of UE policy delivery service are shown in table D.7.1.

Table D.7.1: Timers of UE policy delivery service – PCF side

| TIMER NUM. | TIMER VALUE | CAUSE OF START | NORMAL STOP | ON  THE 1st, 2nd, 3rd, 4th EXPIRY |
| --- | --- | --- | --- | --- |
| T3501 | NOTE 1 | Transmission of MANAGE UE POLICY COMMAND | MANAGE UE POLICY COMMAND COMPLETE or MANAGE UE POLICY COMMAND REJECT message received | Retransmission of MANAGE UE POLICY COMMAND message |
| NOTE 1: The value of this timer is network dependent. | | | | |

## D.8 Handling of unknown, unforeseen, and erroneous UPDS data

### D.8.1 General

The procedures specified in the subclause apply to those messages which pass the checks described in this subclause.

This subclause also specifies procedures for the handling of unknown, unforeseen, and erroneous UPDS data by the receiving entity. These procedures are called "error handling procedures", but in addition to providing recovery mechanisms for error situations they define a compatibility mechanism for future extensions of the UPDS.

Subclauses D.8.1 to D.8.8 shall be applied in order of precedence.

Detailed error handling procedures in the network are implementation dependent and may vary from PLMN to PLMN. However, when extensions of UPDS are developed, networks are assumed to have the error handling which is indicated in this subclause as mandatory ("shall") and that is indicated as strongly recommended ("should").

Also, the error handling of the network is only considered as mandatory or strongly recommended when certain thresholds for errors are not reached during a dedicated connection.

For definition of semantical and syntactical errors see 3GPP TS 24.007 [11], subclause 11.4.2.

### D.8.2 Message too short or too long

#### D.8.2.1 Message too short

When a message is received that is too short to contain a complete message type information element, that message shall be ignored, c.f. 3GPP TS 24.007 [11].

#### D.8.2.2 Message too long

The maximum size of a UE policy delivery service message is 65535 octets.

### D.8.3 Unknown or unforeseen procedure transaction identity

#### D.8.3.1 Procedure transaction identity

The following network procedures shall apply for handling an unknown, erroneous, or unforeseen PTI received in a UPDS message:

a) In case the network receives a MANAGE UE POLICY COMPLETE message or MANAGE UE POLICY COMMAND REJECT message in which the PTI value is an assigned or unassigned value that does not match any PTI in use, the network shall ignore the UPDS message.

b) In case the network receives a UPDS message in which the PTI value is a reserved value, the network shall ignore the UPDS message.

The following UE procedures shall apply for handling an unknown, erroneous, or unforeseen PTI received in a UPDS message:

a) In case the UE receives a UPDS message in which the PTI value is a reserved value, the UE shall ignore the UPDS message.

### D.8.4 Unknown or unforeseen message type

If the UE or the network receives a UPDS message with message type not defined for the UPDS or not implemented by the receiver, it shall ignore the UPDS message.

NOTE: A message type not defined for the UPDS in the given direction is regarded by the receiver as a message type not defined for the UPDS, see 3GPP TS 24.007 [11].

If the UE receives a message not compatible with the UPDS state, the UE shall ignore the UPDS message.

If the network receives a message not compatible with the UPDS state, the network actions are implementation dependent.

### D.8.5 Non-semantical mandatory information element errors

#### D.8.5.1 Common procedures

When on receipt of a message,

a) an "imperative message part" error; or

b) a "missing mandatory IE" error

is diagnosed or when a message containing:

a) a syntactically incorrect mandatory IE;

b) an IE unknown in the message, but encoded as "comprehension required" (see 3GPP TS 24.007 [11]); or

c) an out of sequence IE encoded as "comprehension required" (see 3GPP TS 24.007 [11]) is received,

the UE shall ignore the UPDS message;

the network shall proceed as follows:

the network shall:

1) try to treat the message (the exact further actions are implementation dependent); or

2) ignore the message.

### D.8.6 Unknown and unforeseen IEs in the non-imperative message part

#### D.8.6.1 IEIs unknown in the message

The UE shall ignore all IEs unknown in a message which are not encoded as "comprehension required" (see 3GPP TS 24.007 [11]).

The network shall take the same approach.

#### D.8.6.2 Out of sequence IEs

The UE shall ignore all out of sequence IEs in a message which are not encoded as "comprehension required" (see 3GPP TS 24.007 [11]).

The network should take the same approach.

#### D.8.6.3 Repeated IEs

If an information element with format T, TV, TLV, or TLV-E is repeated in a message in which repetition of the information element is not specified in subclause D.5, the UE shall handle only the contents of the information element appearing first and shall ignore all subsequent repetitions of the information element. When repetition of information elements is specified, the UE shall handle only the contents of specified repeated information elements. If the limit on repetition of information elements is exceeded, the UE shall handle the contents of information elements appearing first up to the limit of repetitions and shall ignore all subsequent repetitions of the information element.

The network should follow the same procedures.

### D.8.7 Non-imperative message part errors

This category includes:

a) syntactically incorrect optional IEs; and

b) conditional IE errors.

#### D.8.7.1 Syntactically incorrect optional IEs

The UE shall treat all optional IEs that are syntactically incorrect in a message as not present in the message.

The network shall take the same approach.

#### D.8.7.2 Conditional IE errors

When upon receipt of a UPDS message the UE diagnoses a "missing conditional IE" error or an "unexpected conditional IE" error, or when it receives a UPDS message containing at least one syntactically incorrect conditional IE, the UE shall ignore the message.

When the network receives a message and diagnoses a "missing conditional IE" error or an "unexpected conditional IE" error or when it receives a message containing at least one syntactically incorrect conditional IE, the network shall either:

a) try to treat the message (the exact further actions are implementation dependent); or

b) ignore the message.

### D.8.8 Messages with semantically incorrect contents

When a message with semantically incorrect contents is received, the UE shall perform the foreseen reactions of the procedural part of subclauses D.2. If, however no such reactions are specified, the UE shall ignore the message.

The network should follow the same procedure.

Annex E (informative):  
Void

Annex F (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 |
| 2018-09 | CT#81 | CP-182139 | 0001 |  | F | Replace unknown "registration update accept" | 15.1.0 |
| 2018-09 | CT#81 | CP-182142 | 0003 | 2 | F | Pass (Extended) Emergency Number List to upper layers | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0004 |  | F | Correcting access selection for SMS over NAS | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0006 | 1 | F | Referring to the correct bits for SMS over NAS during the registration procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0007 | 1 | F | Setting and checking 5GS update status | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0008 | 1 | F | Clarifications on MICO indication | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0009 | 1 | F | Timer T3540 clarifications | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0010 | 3 | F | Network Slicing Subscription Change Indication | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0012 |  | F | Correction for PDU session context | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0013 | 1 | F | Correction for establishment of user-plane resources | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0014 | 1 | F | Correction for establishment cause | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0016 | 4 | F | Correction for maximum data rate per UE for integrity protection for DRBs | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0018 | 3 | F | Invalid DNN | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0020 | 1 | F | Correction for 5GMM cause #90 in subclause A.3 | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0021 |  | F | Editor's notes in UPDP | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0023 | 2 | F | Exchange of extended protocol configuration options | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0024 | 1 | F | 5G QoS - restructuring QoS rules IE | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0025 | 1 | F | Correction for editor's note on further 5GSM causes and further minor issues | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0026 |  | F | Correction and alignment of cause code values | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0027 | 2 | F | UAC information and establishment cause when uplink user data packet is to be sent for a PDU session with suspended user-plane resources | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0028 | 2 | F | Corrections for operator-defined access categories | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0030 | 1 | F | AMF Region ID (8 bits), AMF Set ID (10 bits), and AMF Pointer (6 bits) | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0031 | 1 | F | Correcting message definition of message including EENL | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0032 | 2 | F | SMF knowledge that a UE is configured for high priority access | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0035 | 2 | F | Authentication for normal services not accepted by network | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0036 | 4 | C | Addition of ABBA in 5G based primary authentication procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0037 | 2 | C | Alignment and correction of mapped security context creation at S1 to N1 mode HO | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0038 | 1 | C | Addition of NAS container IE for N1 mode HO | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0039 | 1 | F | Correction and update of S1 mode to N1 mode NAS transparent container | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0040 | 1 | C | Removal of MAC editor´s note | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0041 | 1 | F | Removal of transparent container at N1 mode to S1 mode HO | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0042 |  | F | Correction of 5GS TAC LSB | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0043 | 1 | B | Handling of Emergency PDU sessions and null algorithms | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0044 | 2 | B | Request for Kamf re-derivation | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0045 | 1 | F | Mobility Registration when T3346 running | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0046 |  | F | DL NAS Transport message | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0047 | 1 | F | Single-registration mode | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0048 |  | F | Authentication Response | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0049 | 2 | F | Parameters for PDU session establishment due to change of SSC mode 3 or 2 PSA | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0054 | 2 | F | Equivalent PLMNs | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0055 | 2 | F | Remove the remaining instance of SUPI paging | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0056 | 2 | F | PDU session status | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0058 | 1 | F | Clarification on NAS level MM congestion Control | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0060 | 3 | B | SM cause for out of LADN service area | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0064 | 1 | F | Removal of redundant MICO statement | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0065 | 4 | C | LADN indication from UE at registration | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0066 |  | F | Mapping to configured NSSAI for HPLM shall be included if available | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0069 | 2 | F | Abnormal Cases in the UE for mobilty and periodic Registration Update Procedures | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0070 | 1 | D | Correction to 5GMM Substate | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0071 | 1 | F | Definition of emergency and non-emergency PDU sessions | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0074 | 2 | F | PDU session establish criteria for emergency PDU sessions | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0075 | 3 | F | Service request allowed for PDU release outside LADN | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0076 | 2 | F | Handling of Transmission failure for Service request message. | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0077 | 4 | B | How to determine the maximum number of established PDU sessions | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0079 | 2 | F | UAC and setting of the Uplink data status IE | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0080 | 1 | C | Non-3GPP access to 5GCN not allowed | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0082 | 2 | B | Including S-NSSAI received in EPS in Requested NSSAI and in PDU session establishment request upon inter-system change from S1 mode to N1 mode | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0083 |  | B | UE configuration for AC 11-15 and MCS (access identity 2) | 15.1.0 |
| 2018-09 | CT#81 | CP-182142 | 0084 |  | B | UE configuration for NAS signalling low priority via OMA-DM or USIM not applicable in 5GS | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0085 | 2 | F | Miscellaneous corrections | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0086 | 2 | F | Clarifications on ATTEMPTING-REGISTRATION-UPDATE | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0087 | 2 | F | UE behaviour in substate ATTEMPTING-REGISTRATION-UPDATE | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0090 |  | F | Service area list IE | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0091 | 1 | F | Handling of forbidden tracking area list | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0092 | 2 | F | Corrections for authentication | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0094 | 4 | F | Trigger for mobility and periodic registration update | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0095 |  | F | Abnormal cases in the UE for network-initiated de-registration procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0096 | 4 | F | Add attempt counter to Service Request procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0097 | 1 | F | Authentication procedure during registration procedure for mobility and periodic registration update | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0098 | 4 | F | Registration procedure for mobility and periodic registration update | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0099 | 3 | F | Release of the N1 NAS signalling connection | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0100 | 2 | F | Resetting of registration attempt counter | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0101 | 4 | F | On #27 N1 mode not allowed | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0102 | 3 | F | Adding EPLMN list related descriptions | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0104 | 2 | F | Provision of IWK N26 indication in registration update procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0105 |  | F | Corrections for interworking with EPS | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0106 | 4 | F | Emergency Services Support indicator for non-3GPP access | 15.1.0 |
| 2018-09 | CT#81 | CP-182219 | 0107 | 7 | C | Network control for always-on PDU sessions | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0108 |  | F | Corrections on inconsistent descriptions for 5GSM and 5GMM | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0110 |  | F | Corrections on the timers of 5GMM | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0112 | 1 | F | No operation code for UE policy management | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0113 | 1 | F | Correction on UE behaviour for 5GSM congestion control | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0114 |  | F | Correction on UE security capability IE | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0115 | 5 | F | Including SD when Mapped configured SD is included in S-NSSAI | 15.1.0 |
| 2018-09 | CT#81 | CP-182142 | 0116 | 3 | F | Updates to deleting a derived QoS rule in the UE | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0117 |  | F | Provisioning of ANDSP for non-3GPP access | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0118 |  | D | Fix incorrect references | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0120 | 2 | F | Addition of ngKSI in DEREGISTRATION REQUEST | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0123 | 2 | F | Storing of MPS indicator in non-volatile memory of mobile | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0124 | 4 | C | NW slicing and delayed re-registration due to emergency services | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0125 | 1 | F | Addtion of cause values for service request reject | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0126 | 3 | F | UE actions when other causes received at SERVICE REJECT | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0128 |  | F | Missing general description on sub-clause 9.10 | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0130 |  | F | Correction to general message format | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0131 |  | F | Plain 5GS NAS message | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0134 | 1 | F | Correction to the 5GMM capability IE | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0135 |  | F | Correction to the 5GS identity type IE | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0136 | 1 | F | Correction to the 5GS network feature support IE | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0137 | 1 | F | Editorials and minor corrections | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0138 |  | F | Security procedures and handling after inter-system change | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0140 |  | F | 5GMM aspects of NAS over non-3GPP access | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0141 | 2 | F | Resolution of editor's note on equivalent PLMN list | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0142 |  | F | Resolution of editor's notes on 5GMM sub-layer design | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0143 |  | F | Resolution of editor's note on UE behaviour in substate 5GMM-DEREGISTERED.ATTEMPTING-REGISTRATION | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0144 |  | F | Resolution of editor's note on other sub-states of state 5GMM-DEREGISTERED | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0145 | 3 | F | Resolution of editor's note on sub-states of state 5GMM-REGISTERED | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0146 | 1 | F | Resolution of editor's note on the key derivation function field | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0147 |  | F | Resolution of editor's note on security context coordination | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0148 |  | F | Removal of unnecesary editor's notes FFS | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0151 |  | F | Resolution of editor's note on handling of unknown, unforeseen, and erroneous protocol data | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0153 | 2 | C | AMF taking both EMC and EMC BS availability into account in setting EMF | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0154 | 1 | F | Clarification on SM congestion control specific to PLMN | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0155 | 1 | F | Aligning T35cd handling upon NW initiated SM request with T3396 and T35ef | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0156 | 2 | F | Clarification on stopping back-off timers upon reception of NW initiated SM request | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0157 | 1 | F | Clarification for registration attempt counter handling and introduction of lower layer failure | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0158 | 2 | B | Introduction of 5GMM cause #15 | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0159 | 1 | F | Timer for re-enabling N1 mode capability | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0160 |  | F | Lists of 5GS forbidden tracking areas | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0162 | 1 | F | Local release of a persistent PDU session | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0163 | 1 | F | Correction on retry of PDU session establishment procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0164 |  | F | Correction to 5GSM/ESM coordination | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0165 |  | F | Correction on PDU address IE | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0166 | 1 | F | 5GSM congestion control over AMF on PDU session modification procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0167 | 3 | F | Exception handling in QoS operation | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0168 | 1 | F | Correction on PTI mismatch | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0169 | 1 | B | Establishment of N1 NAS signalling connection due to change in the network slicing information | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0170 | 2 | F | Release of N1 NAS signalling connection due to change in the network slicing information | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0171 | 3 | F | Multiple S-NSSAIs in PDU session establishment | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0173 | 3 | F | Clarifications on UE 5GSM capabilities and procedures during inter-working with EPS | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0174 | 1 | B | Interworking between ePDG/EPC and NG-RAN/5GCN | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0176 | 1 | B | Interworking between E-UTRAN/EPC and N3IWF/5GCN | 15.1.0 |
| 2018-09 | CT#81 | CP-182142 | 0178 | 2 | F | UE re-registration when the AMF cannot determine an Allowed NSSAI | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0180 | 2 | F | Local release of a PDU session due to 5GSM cause #43: Invalid PDU session identity | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0182 | 2 | C | Common NAS security transparent container IE for intra-5G HO and S1 to N1 inter-system HO | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0184 | 1 | F | Handling of PDU session type after intersystem change from N1 mode to S1 mode | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0185 | 2 | F | Allowed NSSAI of a single-registration mode UE within a network with N26 | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0187 | 1 | F | SMF selection based on DNN for transfer a PDN connection from EPS to 5GS | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0188 | 1 | F | UE behaviour for determination of the UE presence in LADN service area | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0189 | 3 | F | Correction on emergency PDU session handling | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0190 | 1 | F | No EMM parameters handling for DR mode UEs due to rejected service request | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0192 | 3 | F | Clarification on activation of UP resources of PDU session | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0194 | 1 | B | Access attempt barred for the UE-initiated NAS transport procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182142 | 0195 | 5 | F | UE configured for EAB and access category 1 | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0197 | 1 | F | No bearer for N1 NAS | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0198 | 4 | F | Correction of S-NSSAI based congestion control | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0199 | 1 | F | Clean-up in definitions | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0200 | 4 | F | Clarify abnormal cases in the UE for independency of 5GMM procedures between accesses | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0203 | 2 | B | Storing Configured NSSAI when the PLMN is changed | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0206 |  | F | Incorrect statement for handling of security context at IWK | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0207 | 2 | F | Correction to SSC mode selection | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0208 | 2 | F | Corrections to terms and references | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0209 | 1 | C | Revision on AMF transport behaviour of 5GSM message | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0210 | 2 | F | Differences between NAS over 3GPP access and NAS over non-3GPP access | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0212 | 6 | B | Preferred list terminating at ME or USIM | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0213 | 4 | F | Clarification on network-initiated de-registration procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0214 |  | F | Correction of detach terminology | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0215 |  | F | Clarification on S-NSSAI based congestion control for PDU session modification procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0216 | 4 | B | SOR acknowledge message coding | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0232 | 1 | F | SMS over NAS re-transmission upon delivery failure on one Access Type | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0233 | 2 | F | Corrections in EAP based primary authentication procedure (alternative 2) | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0234 |  | F | Correction for multi-homed IPv6 PDU session | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0235 | 1 | F | Correction for transfer of a PDN connection from untrusted non-3GPP access connected to EPC | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0237 | 1 | F | Correction for generation of QoS rules | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0239 |  | F | Interworking for multi-homed IPv6 PDU session | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0241 | 1 | F | Clarification of N1 NAS signalling connection release in AMF on generic UE configuration update completion | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0242 | 1 | F | Requests for emergency services fallback from upper layers | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0245 |  | F | Corrections to the Identification and Registration procedures | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0246 |  | F | Correct abnormal procedures reference when handling CC #22 (Congestion) | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0247 | 1 | F | Non-IP PDN connection type for S1 to N1 interworking | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0248 | 1 | F | Non-3GPP de-registration timer | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0250 | 3 | F | Substates for registration result | 15.1.0 |
| 2018-09 | CT#81 | CP-182142 | 0251 | 1 | F | Updating NS Configuration via registration procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0254 | 4 | B | SUCI encoding format and protection scheme | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0255 | 1 | C | Clarify the method of configuring the UE to use Access Identity 1 | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0256 | 1 | B | Handling of error case when UE gets URSP from VPLMN | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0258 | 2 | F | Correction for abnormal cases in the UE of service request procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0259 | 1 | F | Setting of RRC establishment cause for operator-defined access categories | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0262 |  | F | Alignment with terminology "emergency PDU session" throughout TS 24.501 | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0263 | 1 | F | TAI removed from list of Servie area lists after reject from network | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0264 | 1 | F | EAP message IE mandatory in PDU SESSION AUTHENTICATION messages | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0269 | 1 | F | Corrections related to the authentication procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0271 | 2 | F | Security parameter carrying DL NAS COUNT during N1 to S1 mode HO | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0272 | 2 | F | Adding procedures for updating local emergency numbers in other modes | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0275 |  | F | Authentication response parameter IE to be of fixed length (24.501) | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0276 |  | F | Correction to the PDU Session ID value in Allowed PDU session status IE | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0277 | 2 | F | Reactivation result indicating insufficient resources during service request procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0278 | 1 | C | Registration procedure triggered by a change of UE Radio Capability | 15.1.0 |
| 2018-09 | CT#81 | CP-182142 | 0280 | 2 | F | Updates to RRC fallback indication while in 5GMM-CONNECTED mode, or while in 5GMM-CONNECTED mode with RRC inactive indication | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0281 | 2 | C | PDU Session Release due to Semantic or Syntactical Errors | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0282 | 3 | F | Removal of 5GSM cause from ePCO for PDU Session Release Complete | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0283 |  | F | Correction on PTI definition | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0284 | 1 | F | Resolving EN on fatal causes in 5GMM/5GSM state machine | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0285 | 1 | F | Uplink data handling for MT notification | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0286 | 1 | F | Fallback handling for RRC inactive | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0287 | 1 | F | Correction on PDU session modification procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0289 | 1 | F | RRC establishment cause for EAB | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0290 | 2 | C | NW slicing and delayed registration due to emergency services, reject PDU session request | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0291 | 1 | F | Correction to the UE security capability IE encoding | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0292 | 3 | F | Additions to UE configuration update completion clause | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0293 | 2 | F | Removal of local PDU session relase statement in UCU procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0294 |  | F | Resolution of editor's notes in D.3 and D.6.2 | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0295 |  | F | Resolution of the editor's note on value of the non-3GPP de-registration timer value | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0296 |  | F | Resolution of editor's note on the format of the authentication parameters | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0297 | 2 | F | Resolution of editor's note on unknown or unforeseen PDU session identity | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0298 |  | F | Resolution of editor's note on other types of payload for the NAS transport procedure(s) | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0300 | 2 | F | Serving network name format for primary authentication | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0301 | 1 | B | Initial registration not accepted due to serving network not authorized | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0303 | 1 | F | 5GSM cause #xx –out of LADN service area | 15.1.0 |
| 2018-09 | CT#81 | CP-182142 | 0304 | 1 | F | UE policy delivery protocol in the scope | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0305 | 1 | F | AMF pointer pointing one or more AMFs | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0306 |  | F | Corrections in the conditions for SMS via non-3GPP access | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0308 |  | F | 5GMM STATUS message sent by the AMF when certain error conditions are detected upon receipt of 5GMM protocol data in the AMF | 15.1.0 |
| 2018-09 | CT#81 | CP-182137 | 0311 | 1 | F | Interworking with E-UTRAN connected to EPC of a UE registered to 5GC via non-3GPP access | 15.1.0 |
| 2018-09 | CT#81 | CP-182142 | 0313 | 2 | F | Use of S-NSSAI and session-AMBR provided during the EPS bearer context modification procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0314 | 1 | F | Handling of inter-access handover of a PDU session whose S-NSSAI is not allowed for the target access | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0319 | 1 | F | 5GSM sublayer states for PDU session inactive | 15.1.0 |
| 2018-09 | CT#81 | CP-182139 | 0321 | 1 | F | Rename of T3584 and T3585 | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0322 |  | F | Correction on acknowledgement handling of UE configuration update | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0323 | 1 | F | Correction on NW initiated de-registration procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0326 | 1 | F | Service area restrictions | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0327 | 3 | F | Disabling and re-enabling N1 mode capability | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0328 | 1 | F | Clarification on packet filters | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0329 | 1 | F | Correction on 5G-GUTI type encoding | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0330 | 1 | F | Correction on EAP-AKA' based primary authentication | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0331 |  | F | Correction on 5GSM state mapping when interworking | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0333 | 1 | F | Removal of Default EPS Bearer (DEB) indication | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0334 | 1 | F | Correction on interaction with upper layers | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0337 | 2 | F | Security Context | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0339 | 3 | B | Emergency call in limited service state | 15.1.0 |
| 2018-09 | CT#81 | CP-182201 | 0340 | 3 | C | Emergency call error handling | 15.1.0 |
| 2018-09 | CT#81 | CP-182138 | 0341 | 2 | F | PDU session status in notification response message | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0342 | 1 | F | Clarifications on inclusion of S-NSSAI in 5GSM request | 15.1.0 |
| 2018-09 | CT#81 | CP-182133 | 0344 |  | F | Correction for LADN | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0345 | 1 | F | Definition of user-plane resources | 15.1.0 |
| 2018-09 | CT#81 | CP-182136 | 0346 | 1 | F | Handling of PDU session(s) not supporting interworking with EPS | 15.1.0 |
| 2018-09 | CT#81 | CP-182141 | 0350 |  | D | Terminology correction | 15.1.0 |
| 2018-09 | CT#81 | CP-182131 | 0351 | 3 | F | Clarification on MICO indication and LADN information via generic UE configuration update procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0352 | 1 | F | Clarification on the temporary identity in the service request procedure | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0353 |  | F | Abbreviation update for NITZ | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0355 |  | D | Duplicated subclause for registration request message | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0356 | 1 | D | Editorial corrections | 15.1.0 |
| 2018-09 | CT#81 | CP-182135 | 0357 | 2 | B | DL and UL NAS Transport procedure updates for SOR | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0358 | 1 | F | Conditions to send registration complete message. | 15.1.0 |
| 2018-09 | CT#81 | CP-182132 | 0359 | 1 | F | Condition for starting timer T3540 | 15.1.0 |
| 2018-09 | CT#81 | CP-182140 | 0361 | 2 | F | Security context mapping at 5GS to EPS HO | 15.1.0 |
| 2018-09 | CT#81 | CP-182134 | 0363 | 2 | F | Correction to reset registration attempt counter | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0365 | 3 | F | Adding the reference to T3346 | 15.1.0 |
| 2018-09 | CT#81 | CP-182130 | 0367 | 1 | F | Access attempt due to delivery of LPP message/transparent container/UE policy container | 15.1.0 |
| 2018-12 | CT#82 | CP-183032 | 0103 | 6 | F | Clarification on coordination between 5GMM and 5GSM | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0121 | 10 | F | Clarification to VoPS indicator | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0274 | 4 | F | Correct Extended Local Emergency Numbers List deletion upon PLMN change | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0315 | 4 | F | Operator-controlled inclusion of NSSAI in access stratum connection establishment | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0371 | 2 | F | Correction for maximum data rate per UE for integrity protection for DRBs for PDU sessions in non-3GPP access which are transferable to 3GPP access | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0372 | 1 | F | Correction for 3GPP PS data off and non-IP user data packets | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0373 | 2 | F | Corrections for determination of RRC establishment cause and establishment cause for non-3GPP access | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0374 |  | F | Corrections for MTU PCO parameters handling | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0376 | 2 | F | Correction for SM PDU DN request container coding | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0379 | 1 | F | UAC: Correction for SMSoIP sent over DNN other that "IMS" | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0380 | 2 | F | UAC: Correction for operator-defined access categories | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0381 | 1 | F | DRX parameters IE definition | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0383 | 1 | F | Removal of UE security capability from Intra N1 mode NAS container | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0385 |  | F | Correct procedure for determining registered PLMN | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0392 | 1 | F | Definition of emergency registration | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0393 | 1 | F | Correction for EAP based primary authentication and AUTHENTICATION REJECT | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0394 |  | F | Correction for LADN information encoding | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0395 | 3 | B | Dynamic Routing indicator update description | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0398 | 1 | F | ABBA handling for 5G-AKA based authentication procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0399 | 2 | F | ABBA handling when initiating EAP procedures | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0401 | 3 | F | Clarification on NAS message field format and mapping | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0402 | 1 | F | Correction to home country definition | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0403 | 1 | F | Signalling Default Configured NSSAI indication in the registration procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0404 | 1 | F | Rename "configured NSSAI not associated with a PLMN" to align to new stage 2 terminology | 15.2.0 |
| 2018-12 | CT#82 | CP-183032 | 0405 | 1 | F | "SMS subscribed indication" in CONFIGURATION UPDATE COMMAND | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0406 | 1 | F | S-NSSAI not allowed by AMF | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0407 |  | F | Continued need to align with terminology "emergency PDU session" throughout TS 24.501 | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0408 | 1 | F | Ambiguity in the use of the terms "no other parameter" and "no parameters" | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0409 |  | F | Change EMCW to EMCN3 | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0410 | 2 | F | Miscellaneous wording, terminology and reference corrections | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0411 |  | F | Rejected NSSAI clarifications | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0413 | 1 | F | Rejected NSSAI sent in CONFIGURATION UPDATE COMMAND – Alt 2 | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0415 |  | F | UAC – meaning of "the broadcast of categories a, b or c" | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0416 | 2 | F | Clarification of "registration requested" in CONFIGURATION UPDATE COMMAND | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0417 | 5 | F | Updates on steering of roaming handling and information coding | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0419 | 3 | F | Security context usage during NAS security mode control procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0420 | 1 | F | Corrections on GFBR parameter for QoS flow | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0421 | 1 | F | Correction to UE behavior when disabling N1 mode for non-3GPP access | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0423 | 1 | F | Mapped QoS information validation (Solution 1) | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0424 | 4 | B | Protection of initial NAS messages – overall description | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0425 | 4 | B | Support for protection of initial NAS messages | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0426 | 2 | B | Update to 5GS registration type IE and introduction of a new 5GS update type IE | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0427 | 1 | F | S-NSSAI received in Notify payload during PDN connection establishment over ePDG/EPC | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0428 |  | F | No interworking to ePDG/EPC for Ethernet and unstructured PDU sessions | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0429 |  | F | Addition of UE capability for LPP in 5GMM capability IE | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0430 | 1 | F | Correct superfluous test for N1 mode and S1 mode capability | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0431 | 1 | F | Change UE policy classmark as mandatory IE | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0432 | 2 | F | Forward compatibility for UE security capability IE and a few other IEs | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0433 | 1 | F | Introduction of Replayed S1 UE security capabilities | 15.2.0 |
| 2018-12 | CT#82 | CP-183033 | 0434 | 1 | F | Applicability of UAC for other cases of NAS message transport | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0435 | 5 | F | Emergency registered | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0436 | 3 | F | Correction to domain selection rules for EPS/RAT Fallback | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0438 |  | F | UL data status upon fallback indication from lower layers | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0440 | 1 | F | Misc. corrections to 24.501 | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0441 | 2 | F | Clarification on handling of PDU session for LADN | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0442 | 2 | F | Correction to determination method of LADN DNN | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0443 | 1 | F | Correction to trigger of the mobility and periodic registration update procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0444 | 1 | F | Abnormal cases in the network side for Configuration update prcedure. | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0445 | 1 | F | Correction in emergency reg cause name | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0446 |  | F | UE behavior on NW initiated deregistration procedure with #22 | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0447 | 1 | F | Miscellaneous corrections | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0448 | 3 | F | Resetting service request attempt counter upon receipt of the REGISTRATION ACCEPT message | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0450 |  | F | Correction in determining sytactic errors for PDU session establishment accept | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0451 |  | F | T3540 started by the UEon getting 5GMM cause #27 – N1 mode not allowed | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0452 | 2 | F | Clarification on UE identities used for registration | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0454 | 1 | F | Transition from 5GMM-CONNECTED mode with RRC inactive indication to 5GMM-IDLE mode triggered by radio capability update | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0455 | 1 | F | Finalizing 5GSM timers on the UE and SMF side | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0458 | 1 | F | Local PDU session release upon receipt of PDU Session Release Reject with 5GSM cause #34 (service option temporarily out of order) or #35 (PTI already in use) | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0460 | 3 | F | Clarifications on the EAP based AKA procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0461 | 1 | F | Applicability of the Service area list IE indicating all TAIs to equivalent PLMNs | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0464 | 1 | F | Clarification on PDU session transfer from non-3GPP to 3GPP access when 3GPP PS data off UE status is activated | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0465 | 1 | F | EAP-Identification in EAP-AKA' primary authentication and key agreement procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0467 | 1 | F | Excluding mobility procedures from ODAC access control checks | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0470 | 3 | F | Alignment of 5G-GUTI assignment with SA3 | 15.2.0 |
| 2018-12 | CT#82 | CP-183034 | 0471 | 1 | F | Network initiated de-registration in case of emergency PDU session | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0472 |  | F | Resolution of editor's note on always-on PDU session | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0473 |  | F | Addition of 5GSM cause values | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0474 |  | F | Resolution of editor's note on operator-defined access category | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0476 | 6 | C | Support for Traffic Segregation | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0479 |  | F | Correct reference to Mapped EPS bearer contexts | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0480 |  | F | Aborted UE-initiated NAS transport procedure for delivery of SMS/LPP message/UE policy container | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0484 | 3 | F | Clarification on back-off timer upon PLMN change | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0485 | 2 | F | Emergency call in limited service state | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0490 | 2 | F | Correction on Network slicing indication | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0491 |  | F | Correction on De-registration procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0492 | 1 | F | Correction on dual-registration mode | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0494 | 1 | F | Correction to Configured NSSAI for the HPLMN | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0499 |  | F | Updates to 5GS mobility management aspects subclause | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0500 | 5 | F | Editorials and minor corrections | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0501 | 3 | F | Adding necessary term defintions | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0502 | 1 | F | Resolution of editor's notes on abnormal case handling when rejection with "Extended wait time" received from lower layers | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0503 | 1 | F | Resolution of editor's note on maximum length of the 5GS mobile identity IE | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0505 | 1 | F | Resolution of editor's note in sub-clause 4.8.3 | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0506 | 1 | F | Correct unified access control applicability in 5GMM-REGISTERED.UPDATE-NEEDED | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0507 | 3 | F | Correct non-3GPP registration accept procedure when local emergency numbers are received from a different country | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0509 | 1 | F | Remove editor's note for MT LCS | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0510 | 1 | F | Reusing T3519 for Initial Registration procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0511 | 2 | F | Abnormal cases for Registration procedure for mobility and periodic registration update | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0516 | 1 | F | Correction on handling of mandatory IE errors | 15.2.0 |
| 2018-12 | CT#82 | CP-183035 | 0517 | 1 | F | Correction on handling of invalid PSI | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0518 | 2 | F | Clarification on PLMN's maximum number of PDU sessions | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0519 | 1 | F | Handling on collision of PDU session establishment and release procedures | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0521 |  | F | Correction on QoS rules IE | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0522 | 2 | F | Correction on QoS flow description IE | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0523 | 1 | F | Correction of storage of operator-defined access categories | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0525 | 2 | F | Clarification on coordination between 5GMM and EMM for a UE in DRM | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0526 |  | F | The UE behavior in non-3GPP access and in state ATTEMPTING-REGISTRATION | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0528 | 1 | F | Enabling use of and disabling use of MICO mode | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0529 | 2 | F | Apply service area restrictions in NAS procedures | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0530 | 1 | F | Abnormal cases in 5GSM procedures | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0532 |  | F | Clarifications on UE behaviour upon receiving RRC fallback indication | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0533 | 2 | F | Corrections for interworking with EPS | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0534 | 1 | F | Release of the N1 NAS signalling connection upon Service Accept message | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0535 | 1 | F | QoS rules verification during PDU session establishment procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0536 | 1 | F | Clarifications on UE and network state | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0537 | 1 | F | T3517 handling and emergency services fallback | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0540 | 2 | F | Revisions on N1 NAS signaling connection establishment and release | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0541 | 1 | F | Disabling N1 mode capability for 3GPP access and impacts to PLMN selection | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0543 | 1 | F | UE's homogeneous support of emergency services fallback per RAT | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0544 |  | F | Context management for 3GPP access and non-3GPP access due to SR rejection | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0545 | 2 | F | Clarification on setting a service type of a SERVICE REQUEST message | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0546 | 1 | F | UL NAS TRNAPORT message pending due to network slicing information update | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0547 |  | F | Distinction in AMF-side abnormal cases for generic UE configuration update procedure with respect to 5G-GUTI update | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0548 | 1 | F | Handling of security contexts by a UE operating in dual-registration mode | 15.2.0 |
| 2018-12 | CT#82 | CP-183036 | 0549 | 2 | F | Establishment of secure exchange of NAS messages during inter-system change between N1 mode and S1 mode | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0550 | 2 | D | Terminology alignment regarding support for interworking without N26 | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0551 | 3 | F | Correction on reporting change of 3GPP PS data off UE status | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0553 | 1 | F | Correction on Uplink data status handling | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0557 | 2 | F | Correction of LADN information for generic UE configuration update procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0559 |  | F | Management of the registration attempt counter and the attach attempt counter during inter-system change | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0560 | 1 | F | No direct security protection to 5GSM | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0562 | 1 | F | No S-NSSAI for emergency PDU sessions | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0563 | 1 | F | S-NSSAI selection for S-NSSAI based congestion control | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0565 | 2 | F | UE in registered state without registration complete | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0569 | 1 | F | Abnormal Cases in the UE for initial registration | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0571 | 2 | F | Addition of 24.501 overview | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0572 | 2 | F | Service area restrictions applicable for PLMNs in registration area | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0573 | 1 | F | Periodically erase of service area restriction list | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0574 | 1 | F | Completion of mobile identity IE definition in messages | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0575 |  | F | Correction of erroneously encoded IE | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0576 | 2 | F | Correction for local release | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0577 | 3 | F | UAC - providing access identities for barring checks of AS triggered access attempts | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0578 | 2 | F | Correction for indicating 3GPP PS data off status | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0580 | 1 | F | UPSIs in UE STATE INDICATION | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0582 | 1 | F | Initial registration for emergency PDU session | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0583 | 2 | F | Multiple 5G-GUTIs | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0584 |  | F | Correction on Maximum number of supported packet filters | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0585 |  | F | T3584 and T3585 update in Timer table | 15.2.0 |
| 2018-12 | CT#82 | CP-183037 | 0586 | 1 | F | Abnormal case for T3550 | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0590 | 1 | F | No UPF Resources at PDU Session Establishment | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0591 | 2 | F | Clarifications on NAS level mobility management congestion control | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0592 | 1 | F | SOR over control plane in non-3GPP access | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0593 | 1 | F | Handling of target CN type by NAS upon redirection to E-UTRA cell | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0594 | 3 | C | Procedure for UDM-triggered UE parameters update | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0595 | 1 | F | Sending of 5GSM capability IE and Maximum number of supported packet filters IE in in PDU SESSION ESTABLISHMENT REQUEST with request type "existing PDU session" | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0597 | 3 | F | Correction of reference | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0598 | 2 | C | Clarification on 5GSM cause\_#46 out of LADN service area | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0604 | 2 | C | Clarification on congestion control upon intersystem change | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0605 |  | F | Editorial correction related to LADN | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0606 | 1 | F | Correcting the structure of LADN related description | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0607 | 2 | F | N3GPP de-registration timers handling at long MM back-off time | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0608 | 1 | F | Abnormal cases in the network side for Configuration update prcedure. | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0609 | 1 | F | Abnormal cases in the UE side for Configuration update prcedure. | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0610 | 1 | F | Handling of 5GSM reject causes #50 and #51 for PDU types IPv4v6. | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0611 | 1 | F | Correction to QoS rules verification during PDU session establishment. | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0612 | 1 | F | QoS rules verification during PDU session modification. | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0613 | 1 | F | QoS flow descriptions IE to be set by SMF mandatory in PDU establishment accept for initial request. | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0614 | 1 | B | MCS Indicator and Access Identity 2 | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0615 | 3 | F | SUCI encoding and support of NAI format | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0617 | 1 | F | UAC for simultaneous access attempt triggers | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0618 | 1 | F | Reset of registration attempt counter | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0619 |  | F | Reset of service request attempt counter | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0622 |  | F | CN paging handling in RRC inactive | 15.2.0 |
| 2018-12 | CT#82 | CP-183038 | 0623 | 2 | F | Procedure collision handling in paging and notification procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0624 |  | F | Resolution of editor's note on different TAI for 4G and for 5G | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0625 |  | F | Correction on 'E' bit for deleting QoS flow description | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0626 |  | F | EMM parameters handling for EPC interworking | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0627 | 1 | F | Registration rejected because of non-3GPP access to 5GCN is not allowed | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0628 | 2 | F | Correction to SUPI definition due to NAI format | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0629 |  | F | Correct secured packet procedures | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0630 | 2 | F | Abnormal cases for EAP-based AKA | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0631 | 1 | F | CONFIGURATION UPDATE COMMAND with no parameters other than registraion requested. | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0633 | 1 | F | Correction of the UE-initiated de-registration procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183039t | 0634 | 1 | F | Definition of a 5GMM cause for DNN subscription check failure | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0635 | 1 | F | Stopping T3511 after transitioning to 5GMM-CONNECTED mode | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0636 | 2 | F | Clarification on storage of UE policy sections of multiple PLMNs | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0637 | 1 | F | Corrections to UE handling of reject with cause #13 | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0639 | 1 | F | Clarification on the Selected EPS NAS security algorithms | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0641 | 3 | F | Handling errors due to missing QoS flow descriptions parameters for GBR QoS flows | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0642 | 2 | F | Clarification on inclusion of Requested NSSAI during periodic registration updating | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0643 | 1 | F | The release of the existing N1 NAS signalling connection after UCU | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0646 | 1 | F | Always-on PDU sessions and associated access | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0647 | 1 | F | Clarification on the applicability of NSSAI to the EPLMNs | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0648 | 1 | F | Clarification on the applicability of service area restrictions to the EPLMNs | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0649 | 1 | F | QFI and QRI values in 5GSM messages | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0650 | 2 | F | Corrections on operation mode selection | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0651 | 1 | F | Clarification on handling of PDU sessions associated with 3GPP access and non-3GPP access for interworking | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0652 |  | F | Clarifications on Configuration Update procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183039 | 0653 |  | F | Correction on timer T3511 | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0654 | 2 | F | Clarification on Notification procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0655 | 1 | F | Clarification on handling of invalid LADN DNN in registration procedure – Alt 1 | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0657 | 1 | F | Correction for LADN information IE | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0659 |  | F | Editorial correction for the generic UE configuration update procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0660 | 1 | F | UE behavior in ATTEMPTING-REGISTRATION state | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0661 | 1 | F | UE-AMF selected PLMN ID mismatch in INACTIVE state | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0662 |  | F | UL NAS Transport behavior due to transmission failure | 15.2.0 |
| 2018-12 | CT#82 | CP-183029 | 0663 | 1 | F | UAC: Correction for operator-defined access categories of acknowledgement | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0664 | 2 | F | Lower layer indication on the establishment/release of user plane resources | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0665 | 3 | F | Setting the Uplink data status and Service type IEs after receiving a fallback indication from the lower layers | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0666 | 2 | F | Indication of a reason for failure in reactivating a PDU session | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0667 | 1 | F | Adding the case that UE initiates the registration procedure for mobility and periodic registration | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0668 | 1 | F | Handling of network rejection with 5GSM cause values #50, #51, and #54 | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0669 | 2 | F | Mobility and periodic registration update triggered by indications from lower layers | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0673 | 1 | F | UE STATE INDICATION message delivered in a REGISTRATION REQUEST message | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0674 | 1 | F | Correction to operator-defined access category criteria type values | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0677 | 1 | F | Exceptions for UEs configured for high priority access in handling T3396, T3584, and T3585 | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0678 |  | D | Removal of non-seamless non-3GPP offload from definitions | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0679 | 4 | F | UE identifier provided during an initial registration procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0680 | 1 | F | Revisons on PDU Session Eestablishment procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0682 | 1 | F | UE registered for emergency services upon authentication failure | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0683 |  | F | Update the trigger of mobility registration update initiation | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0684 | 2 | F | Clarification on T3346 for registration procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0686 | 2 | F | Support sending multiple payloads via Payload container | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0687 | 1 | F | Correction on LADN information handling | 15.2.0 |
| 2018-12 | CT#82 | CP-183040 | 0688 | 2 | F | Mapping of a NOTIFICATION message to an access category | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0690 | 2 | F | Transmission of SUCI in DEREGISTRATION REQUEST | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0691 |  | F | Clarification on missing subclause | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0692 |  | F | Stop T3516 when authentication reject received | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0693 | 1 | F | Limited service and no SUPI states in 5GMM instance for non-3GPP accesst | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0695 | 1 | F | QoS flow and mapped EPS bearer context | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0696 | 1 | F | Corrections on 5GSM IEs | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0697 | 1 | F | Correction on 5GSM congestion control | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0698 |  | F | Correction on PTI value release | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0699 | 1 | F | Corrections on QoS rules IE | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0700 | 1 | F | UE handling for semantic error in the QoS operation | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0701 |  | F | Resolution of editor's note on abnormal case handling for the UE-initiated UE state indication procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0702 | 1 | F | Resolution of editor's note on abnormal case handling for the network-requested UE policy management procedure | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0703 |  | F | Resolution of editor's note on the information the N3IWF maintains for a registered UE | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0709 | 2 | F | Congestion control | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0711 | 1 | F | Correction to authentication abnormal cases | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0712 | 1 | F | Corrections for non-3GPP access idle mode | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0715 | 1 | F | Integrity protection maximum data rate for UL and DL | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0717 | 1 | F | General section for limited service state over non-3GPP access | 15.2.0 |
| 2018-12 | CT#82 | CP-183041 | 0718 |  | F | T35xx in Annex D | 15.2.0 |
| 2019-01 | CT#82 |  |  |  |  | Change of IEI values from 7E to 74 and from 7F to 75 | 15.2.1 |
| 2019-03 | CT#83 | CP-190084 | 0382 | 9 | F | Correct Extended Local Emergency Numbers List use involving WLAN | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0638 | 3 | F | Clarification for abnormal case handling of registration procedure after inter-system change from S1 mode to N1 mode | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0706 | 6 | F | Resolution on the editor's note on abnormal cases in the UE for the PDU EAP message reliable transport procedure | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0721 | 2 | F | Clarification on inclusion of the Uplink data status IE in the SERVICE REQUEST message after an RRC fallback indication | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0724 | 4 | F | Corrections to Annex D | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0725 | 2 | F | Update reference for UE policy control service | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0728 | 1 | F | Completion of correction for local release | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0729 | 2 | F | UAC - access attempt matching criteria of operator-defined access categoryt | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0731 | 2 | F | Correcting the name of ITU-T Recommendation E.212 | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0732 | 2 | F | 5GSM - request type not included in PDU SESSION ESTABLISHMENT REQUEST | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0734 | 2 | F | AMF rejecting PDU session establishment when the DNN is not subscribed | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0735 | 1 | F | Correction for acknowledgement of extended emergency number list | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0741 | 3 | F | Mobility between 5GS over non-3GPP access and EPS over 3GPP access | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0743 | 1 | F | PDU session status for IWK without N26 | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0744 | 2 | F | EPS GUTI provided to lower layer | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0745 | 1 | F | Length of 5G-S-TMSI | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0746 | 3 | F | S1 UE security capability | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0747 | 2 | F | Clarification on creating new QoS flowst | 15.3.0 |
| 2019-03 | CT#83 | CP-190084 | 0750 | 1 | F | Correction to handling of #50 and #51t | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0752 | 1 | F | PDU session modification for emergency PDU sessions. | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0753 | 1 | F | Removal of unncessary text. | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0754 | 1 | F | QoS flow description to be added in PDU session modification command | 15.3.0 |
| 2019-03 | CT#83 | CP-190100 | 0758 |  | F | Correction of the erroneous length of EAP messageIE | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0759 | 2 | F | Update of SUCI encoding | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0762 |  | F | Minor corrections to TS 24.501 | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0763 | 2 | F | Cleanup on support of multiple payloads for NAS transport | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0765 | 1 | F | Correction on initial NAS message protection | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0766 | 2 | F | Correction on 5GS mobile identity IE name | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0767 | 1 | F | Addition of the 5GSM cause IE in the PDU SESSION MODIFICATION COMPLETE message | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0768 | 2 | D | Minor corrections for interworking | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0769 | 1 | F | Change of "a wildcard DNN" to "the wildcard DNN" | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0771 | 2 | F | Adding missing abnormal cases for initial registration (UE side) | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0772 | 2 | F | Clarification for the use of the default value for T3512 | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0773 | 3 | F | Removal of UE security capabilities from the S1 mode to N1 mode NAS transparent container | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0774 | 2 | F | Clarification on NSSAI inclusion mode after an inter-system change from S1 mode to N1 mode | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0780 | 1 | F | Corrections to UE policy section management result | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0785 | 1 | F | Removal of abnormal case handling for collision between initial registration and paging or notification | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0788 |  | D | DNN as a common IE | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0791 | 2 | F | Generic UE configuration update procedure during registration procedure | 15.3.0 |
| 2019-03 | CT#83 | CP-190085 | 0792 |  | D | References for NAS signalling connection recovery and a fallback indication from the lower layers | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0796 | 1 | F | Corrections on fallback indication from lower layers | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0798 | 2 | F | Correction to the notification procedure | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0801 | 1 | D | Correction on sub-clause numbering | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0802 | 3 | F | Handling of QoS flow description without valid EPS bearer contextt | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0803 |  | F | Correction on the lengths of 5GSM procedures | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0804 | 2 | F | Corrections on Mapped EPS bearer context IE | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0805 | 2 | F | Handling of missing QoS flow description and QoS rule | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0806 | 3 | F | UE re-registration following UE parameters update | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0807 | 1 | F | Clarification on providing NSSAI to the lower layer | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0808 | 1 | F | Adjustment of relevent timers when T3346 is included in the 5GMM message | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0809 | 1 | F | Clarification on PDU Session Modification procedure | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0810 | 1 | F | Clarification on the behaviors of UE and SMF during the inter-system change | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0812 | 2 | F | Several corrections to messages and IEs | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0814 | 2 | F | Correction to IEI values | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0815 | 2 | F | Resolution on editor's notes on whether explicit start and stop indications for SMS over NAS is needed | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0817 |  | F | Correction to the definition of UE STATE INDICATION message content | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0819 | 1 | F | Reference corrections on UE’s state change due to congestion control | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0820 | 3 | F | Correction to behaviour upon receipt of 5GMM reject cause for a UE in single-registration mode | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0821 | 1 | F | Informing the UE about the integrity protection failure at S1 to N1 mode change | 15.3.0 |
| 2019-03 | CT#83 | CP-190086 | 0823 | 1 | F | Handling of abnormal case when UE gets UE policies with incorrect PLMN ID | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0824 |  | F | Abnormal case handling for cause#72 | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0829 | 3 | F | Correction on handling of invalid PSI | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0831 |  | F | Correction for missing 5QIs | 15.3.0 |
| 2019-03 | CT#83 | CP-190174 | 0833 | 4 | F | Possible criterion for the selection of the requested NSSAI | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0834 | 2 | F | Skip barring checks during fallback handling | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0835 | 1 | F | Correct missing Non-3GPP NW policies IE | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0836 | 1 | F | 5G-GUTI provided to lower layer | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0838 | 1 | F | Handling of abnormal authentication errors | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0839 | 1 | F | Update the conditions on the AMF to provide the configured NSSAI to the UE | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0844 | 1 | F | Rejected NSSAI for current registration area | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0845 | 1 | F | Removal of Editor’s note on home network public key and home network public key identifier update and removal of protection scheme identifier | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0846 | 1 | F | Update of PDU session authentication and authorization messages | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0847 | 2 | F | Update of error handling for Mapped EPS bearer contexts IE | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0849 | 1 | F | Correction for Cause code #7 | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0854 | 1 | F | 3GPP PS Data Off UE status change and congestion control in AMF - alternative 2 | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0855 | 1 | F | Retransmission of PDU SESSION ESTABLISHMENT REQUEST | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0856 | 1 | F | Retransmission of PDU SESSION MODIFICATION REQUEST | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0857 | 1 | F | Retransmission of PDU SESSION RELEASE REQUEST | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0859 | 1 | F | Correction in EAP handling | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0860 |  | F | Issue in SNN | 15.3.0 |
| 2019-03 | CT#83 | CP-190087 | 0862 | 2 | F | Temporary identity allocation | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0863 |  | F | Initial maximum number of packet filters for associated PDU session | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0864 | 1 | F | SUCI to be used for the registration for emergency services | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0867 |  | F | Correction to the inclusion of requested QoS rule and requested QoS flow descripstion in PDU session modification request. | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0868 | 1 | F | Wrong message name | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0870 | 2 | F | SUCI applicability | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0873 | 1 | F | Transmission failure at UE side for UE policy delivery procedure | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0875 | 2 | F | Upper layer request while T3540 is running | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0876 | 1 | F | Encoding of Routing indicator set to default value 0 | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0877 | 2 | F | OS Id information element | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0878 | 1 | F | Clarification on deregistration procedure. | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0880 | 1 | D | Correction of the use of word "wants" | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0883 | 1 | F | Handling on errors of QoS flow description operations | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0885 | 1 | F | Addressing missing scenarios and providing other clarifications related to fallback indication | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0888 | 2 | F | Handling when the UE indicated security capabilities are invalid or unacceptable | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0889 | 1 | F | Correction in UE-initiated de-registration procedure initiation | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0891 | 1 | F | Reporting QoS error when a delete or modify operation is received for a non-existent QoS rule | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0892 | 1 | F | Presence of the precedence and QFI fields in QoS rules | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0894 | 2 | F | Mandating UE sending registration complete for SOR | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0895 | 1 | F | Improvement on 5G-GUTI allocation after network triggered service request | 15.3.0 |
| 2019-03 | CT#83 | CP-190088 | 0899 | 2 | F | Clarification on the authorized QoS rule modification | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0901 | 1 | F | Clarification on congestion control upon intersystem change | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0902 | 4 | F | Default EPS bearer associates with the default QoS rule | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0907 | 2 | F | NSSAI inclusion mode, EPLMNs, and registration area | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0910 | 2 | F | 5GSM messages for a PDU session associated with non-3GPP access exchanged via 3GPP access | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0911 | 1 | F | Mobility and periodic registration update initiation by a UE in inactive mode reselecting an EPLMN cell | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0912 | 1 | F | Change of N1 mode capability on UE mode change or on IMS availability change | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0914 | 1 | F | Inclusion of a 5G-GUTI mapped from the valid 4G-GUTI in the REGISTRATION REQUEST message during an initial registration is not available in Rel-15 | 15.3.0 |
| 2019-03 | CT#83 | CP-190209 | 0915 | 3 | F | Correction to the REGISTRATION REQUEST msg when the Payload container IE is included | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0917 | 1 | F | Correction to the length of the IMEISV | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0918 | 1 | F | Correcton on handing of downlink signalling and data for non-3GPP PDU session | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0919 |  | F | Correction to the Payload container IE | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0920 |  | F | Correction to several 5GMM IEs | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0921 | 1 | F | Mapped configured S-NSSAI from the S-NSSAI(s) of the HPLMN | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0922 |  | F | Use of stored NSSAI inclusion mode during initial registrationt | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0923 |  | F | Correction to the Operator-defined access category definitions IE t | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0925 | 1 | F | Non-delivery of PDU SESSION ESTABLISHMENT ACCEPT | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0926 | 1 | F | Correction to Service area list IE Type of list "11" | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0927 | 1 | F | Setting of 5GSM cause value #36 regular deactivation | 15.3.0 |
| 2019-03 | CT#83 | CP-190092 | 0929 | 3 | F | Local release | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0930 | 1 | F | Adding the UE local configuration option in 24.501 | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0933 |  | F | Handling of Replayed S1 UE security capabilities IE in Security Mode Command message | 15.3.0 |
| 2019-03 | CT#83 | CP-190089 | 0934 | 2 | F | Clarifications on use of PCF-provided PTI for UE policies delivery | 15.3.0 |
| 2019-03 | CT#83 | CP-190101 | 0720 | 1 | F | Initiation of Service Request after reception of Notification over non-3GPP while the UE is in 5GMM-CONNECTED mode with RRC inactive indication in the 3GPP access | 16.0.0 |
| 2019-03 | CT#83 | CP-190106 | 0730 | 4 | B | SINE\_5G: Back-off control and retry restriction mechanisms in 5GS | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0733 | 1 | F | Transfer of a PDU session among 5G-ANs and DNN | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0739 | 5 | F | Handling for QoS Flow status synchronization failure | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0775 | 5 | F | Clarification on rejected NSSAI for the PLMN | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0782 | 1 | F | 5G-GUTI as additional guti in initial registration and UE holds 4G-GUTI | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0786 | 1 | D | Consistent description on release of N1 NAS signalling connection | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0787 | 1 | F | Correction to TFT check | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0789 | 4 | F | Handling of indication to the 5GSM sublayer in case of 5GSM message not forwarded to SMF due to service area restrictions | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0797 | 3 | F | Alignment for the notification procedure | 16.0.0 |
| 2019-03 | CT#83 | CP-190108 | 0830 |  | B | New 5QIs for Enhanced Framework for Uplink Streaming | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0840 |  | F | Update the conditions on the AMF to provide an allowed NSSAI based upon the default S-NSSAI(s) | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0841 | 1 | F | Alignment of terms of configured NSSAI and allowed NSSAI | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0842 | 1 | F | Provision of NSSAI information to the lower layers | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0843 | 1 | F | Correction for the UE configuration update procedure | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0848 | 1 | F | Clarification to definition of “ongoing service” | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0851 | 1 | F | Update of validity conditions for access identities 1 and 2 | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0852 |  | F | SR procedure for emergency services fallback when T3525 timer running | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0865 | 2 | F | Clarfication on allowed NSSAI storage in Non Volatile Memory | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0866 | 1 | F | UE state at lower layer failure on the NW side at initial registration | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0869 |  | F | Content of SMS payload container | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0872 | 1 | F | Correct mistake in case (i) in service request procedure | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0881 |  | D | Correction of wrong reference | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0886 | 2 | F | Clarifications related to fallback indication | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0896 |  | F | Correction on deriving mapped EPS security context for EPC interworking in connected mode | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0897 | 1 | F | Correction on abnormal case handlng at AMF for registration | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0904 | 2 | F | Clarification on MICO mode | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0905 |  | F | Correction on 5GMM cause #65 | 16.0.0 |
| 2019-03 | CT#83 | CP-190101 | 0924 |  | F | Correction to N1 NAS signalling connection establishment | 16.0.0 |
| 2019-03 | CT#83 |  |  |  |  | De-implementation of CR468 | 16.0.1 |
| 2019-03 | CT#83 |  |  |  |  | Completion of de-implementation of CR468 | 16.0.2 |
| 2019-06 | CT#84 | CP-191147 | 0936 |  | B | Interworking of Ethernet PDU session to Ethernet PDN connection | 16.1.0 |
| 2019-06 | CT#84 | CP-191137 | 0937 | 2 | B | PEI for 5G-CRG and FN-CRG | 16.1.0 |
| 2019-06 | CT#84 | CP-191137 | 0938 |  | B | Usage of ACS information PCO parameter | 16.1.0 |
| 2019-06 | CT#84 | CP-191137 | 0939 |  | B | Session-TMBR for PDU session in W-5GAN | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0944 | 5 | F | Handling of 5G NAS security contexts | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0946 | 1 | F | Handling of PDU session type | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 0948 | 2 | A | Precedence between access identities for derivation of RRC establishment cause and for derivation of establishment cause for non-3GPP access | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0949 |  | F | Clarifications on the validity of access identities | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0950 |  | F | Corrections to the length of the SOR transparent container and UE parameters update transparent container | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 0953 | 1 | A | Correction on T3396 | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0955 | 1 | F | Correction on the descriptions of 5GSM parameters and capabilities | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 0957 | 2 | A | Handling of PS Data Off status update | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 0959 | 1 | A | SR procedure for emergency services fallback when T3346 timer running | 16.1.0 |
| 2019-06 | CT#84 | CP-191148 | 0963 | 3 | B | Adding support for SNPNs (Stand-alone Non-Public Networks) | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0964 |  | F | Clarification on LADN information for the registered and equivalent PLMNs | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0965 | 3 | F | Clarification on the stop of T3540 | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0966 | 1 | F | Clarification on the creation of a single QoS flow during a PDU session modification procedure | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0968 | 2 | F | Correction to the checks on QoS rule operations - R16 | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0969 | 1 | B | Introduction of extended DRX for 5G CIoT | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0970 | 1 | B | Small data rate control, general description | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0971 | 1 | B | Small data rate control, activation | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0972 | 4 | B | Serving PLMN rate control, general description | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0973 | 4 | B | Serving PLMN rate control, activation | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0974 | 1 | B | Service Gap control in 5GS, general description | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0975 | 3 | B | Service Gap control in 5GS, activation with IE and indication flag | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0977 | 3 | B | Service Gap control in 5GS, enforcement in UE | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0978 | 3 | B | Service Gap control in 5GS, enforcement in AMF | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0979 | 1 | B | Service Gap control in 5GS, new time value via UCU procedure | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0980 | 1 | B | General Description for Restriction on use of enhanced coverage | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0981 | 1 | B | Updates to Registration procedure for Restriction on use of enhanced coverage | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0982 | 2 | B | Support for Reliable Data Service in 5GS | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0983 | 1 | F | Handling 5GMM cause #5 "PEI not accepted" | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0984 |  | F | Correcting UE state when disabling and re-enabling N1 mode | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0985 | 2 | F | Terminology definition for 5G\_CIoT | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0986 | 3 | B | General introduction on CIoT 5GS optimizations | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0987 | 5 | B | CIoT capability negotiation between UE and network | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0988 | 3 | B | CIoT optimisations redirection betwee EPC and 5GC | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0989 | 2 | B | Inter-RAT mobility to and from NB-IoT in 5GS | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 0990 | 3 | B | Congestion control for CP data transport in 5GS | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 0992 | 2 | A | Correction on the 5GSM S-NSSAI congestion control | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0993 | 2 | F | Network slicing indication | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 0995 | 1 | A | Correction on the SMS over NAS | 16.1.0 |
| 2019-06 | CT#84 | CP-191148 | 0997 | 2 | B | Providing CAG ID to the lower layer | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 0998 | 5 | B | UE behaviour upon receiving non-integrity protected NAS reject messages in 5GS | 16.1.0 |
| 2019-06 | CT#84 | CP-191217 | 1000 | 5 | A | Multiple NAS connections and 5G NAS security context change handling | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1002 | 1 | A | EPS bearer synchronization when moving from EPC to 5GC | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 1018 | 6 | F | UE-requested PDU session modification procedure and exemption indication | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 1019 | 1 | B | Active Time for MICO mode | 16.1.0 |
| 2019-06 | CT#84 | CP-191138 | 1020 | 5 | B | MA PDU request in UL NAS TRANSPORT message | 16.1.0 |
| 2019-06 | CT#84 | CP-191138 | 1021 | 4 | B | Update PDU session establishment procedure to support MA PDU session | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 1022 |  | F | Correction to Mico mode activation in the UE | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 1023 | 4 | F | Correction to rejected NSSAI deletion. | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 1025 |  | A | Correction of timer table | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 1027 | 2 | F | Coordination between GMM and 5GMM | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 1029 | 2 | F | Correction of requirements for the handling of access barring | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 1030 | 2 | B | Strictly periodic registration timer indication for MICO mode | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1037 | 2 | A | Network initiated deregistration update for cause #3 and #6 | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 1038 |  | F | Correction of typos in octet numbering for AMF Set ID | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 1039 |  | F | Stopping T3519 and deleting SUCI when receiving authentication reject | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 1041 | 1 | A | Correct UE parameters update data type | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 1043 | 2 | F | Clarifications to the Routing indicator encoding | 16.1.0 |
| 2019-06 | CT#84 | CP-191132 | 1045 | 1 | F | Correction on Payload container type information element | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 1046 | 2 | B | Introduction to UE selection of CN for 5G CIoT (for 24.501) | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1047 |  | F | Exception in suspension of 5GSM procedures in case of ongoing 5GMM procedures: Service request procedure initiated during connected mode | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1050 | 1 | A | PDU SESSION ESTABLISHMENT message sent via target access in case of handover of an existing PDU session between 3GPP access and non-3GPP access | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1052 | 2 | F | Retreival of an SMF ID during transfer of a PDN connection in EPS to 5GS | 16.1.0 |
| 2019-06 | CT#84 | CP-191146 | 1053 | 3 | F | Clarification of 5GSM cause values for which network may include a back-off timer or a re-attempt indicator | 16.1.0 |
| 2019-06 | CT#84 | CP-191148 | 1054 | 4 | B | Introduction of non-public network | 16.1.0 |
| 2019-06 | CT#84 | CP-191148 | 1055 | 1 | B | PLMN ID and NID provided to the lower layers | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1058 |  | F | Extensible Authentication Protocol specified in IETF RFC 3748 | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1059 |  | F | Corrections on security context terminologies | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1060 | 2 | F | Correction on UE handling for network initiated de-registration with #22 | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1061 | 1 | F | T3540 handling for re-registration triggered by UCU | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1062 | 2 | F | Correction on coding of "all other values are spare" | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1064 | 2 | A | Indication of resume failure from the lower layer | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1066 | 1 | F | Integrity protection failure | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1067 | 1 | F | Clarification related to dual registration mode | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1070 |  | F | Including the other cases in [S-NSSAI, DNN] combination back-off timer | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1071 | 4 | A | Correction to the Payload container IE | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 1073 | 3 | A | Correction because of wrong implementation of CR0763 and CR0919 | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1075 | 2 | A | Resolution of editor's notes on handling at emergency registration and emergency PDU sessions | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1077 | 2 | A | Resolution of editor's notes on handling at non-existing 5G NAS security context indicated by the UE when an emergency PDU session exists | 16.1.0 |
| 2019-06 | CT#84 | CP-191137 | 1078 | 3 | B | Introduction of general aspects of wireline access | 16.1.0 |
| 2019-06 | CT#84 | CP-191137 | 1082 | 1 | B | Introduction of references, definitions and abbreviations for 5WWC | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1088 | 1 | F | Correction on PTI error handling of the UE | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1090 | 1 | F | Correction on PTI error handling of the network | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1092 | 1 | F | Correction on QoS rule operation | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 1094 | 1 | A | Correction on handling of mapped EPS bearer contexts IE | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1096 | 2 | F | Correction on associating default EPS bearer with the default QoS rule | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1098 | 1 | F | Feature support after inter-system change from 5GS to EPS | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1100 | 3 | F | Correction on 5GSM IE handling when an error is detected | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1105 | 1 | F | Security Mode Command procedure when S1 mode supported | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1107 | 1 | F | Correction of term “user preference” to “UE local configuration” for inter-system change without N26 | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 1109 | 1 | A | Addition of missing codepoints for 5GSM causes | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1114 | 2 | F | Modification of the maximum number of supported packet filters | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1115 | 1 | F | 5GS-EPS interworking for Multi-homed IPv6 PDU Session not supported without N26 | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1118 | 3 | F | UE-requested PDU session modification for emergency PDU session | 16.1.0 |
| 2019-06 | CT#84 | CP-191133 | 1119 |  | F | Clarification of emergency support indications | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 1121 | 3 | A | Access control and indication that access barring is applicable for all access categories except categories '0' and '2' | 16.1.0 |
| 2019-06 | CT#84 | CP-191138 | 1122 | 2 | B | Multiple Access PDU Session | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 1124 | 1 | A | 5GSM cause value #29 semantic extension | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1128 | 4 | A | NSSAI inclusion mode in ePLMN | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 1129 | 1 | F | Interaction between active time for MICO mode and eDRX | 16.1.0 |
| 2019-06 | CT#84 | CP-191224 | 1130 | 4 | B | User plane CIoT 5GS optimization | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 1131 | 3 | B | CP only indication | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1133 | 1 | A | Handling of PDU session modification while a back-off timer is running | 16.1.0 |
| 2019-06 | CT#84 | CP-191148 | 1134 | 1 | B | Adding support for unified access control in SNPNs (Stand-alone Non-Public Networks) | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1135 | 1 | D | The phrase “outside the scope of the present document” is not used consistently | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1137 | 3 | F | Clarification regarding replayed UE security capabilities | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1140 | 1 | A | UE policy length mismatch | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1142 | 2 | F | Conditions for congestion control in AMF | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1146 | 3 | F | Correction of inconsistent requirements for the use of SUCI | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1147 | 1 | F | Disabling of N1 mode capability after emergency services fallback | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1149 | 1 | F | Clarification on disabling N1 mode capability when there is persistent PDU session | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1151 | 1 | A | Indicating PS data off status report for the UE in the Non-allowed Area | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1156 | 1 | F | Clarification of "registration requested" with no other parameters | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1157 |  | F | Updates to Network slicing indication | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1160 |  | F | Clarification on the length of the key stream for initial NAS message protection | 16.1.0 |
| 2019-06 | CT#84 | CP-191207 | 1162 | 4 | F | Applicability of the allowed NSSAI in an equivalent PLMN outside the UE’s registration area | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1164 | 3 | A | Handling of the ABBA parameter with a non-zero value and a length of more than 2 octets | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1165 | 1 | F | Clarifications to service area restrictions | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1168 | 1 | A | IEI for the Non-3GPP NW provided policies IE | 16.1.0 |
| 2019-06 | CT#84 | CP-191136 | 1169 |  | F | Reference to IEEE 802.3 | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1171 | 2 | A | Correction to serving network name (SNN) reference | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1173 | 1 | A | IEI for the UE OS Id IE | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1174 | 2 | F | Correction for PDU session modification with QFI change. | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1175 | 2 | F | Correction to PDU session release reject handling | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1176 | 1 | F | Correction to PDU session authentication result transport procedure. | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1177 | 1 | F | Clarification for transfter of PDU session for LADN to EPS. | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1178 | 1 | F | Correction to De-registration and registration procedure collision | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1179 |  | F | Clarification for 5GMM cause #3 and #6 in the SERVICE REJECT message | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1180 | 2 | F | Added detailed description for substates INITIAL-REGISTRATION-NEEDED and UPDATE-NEEDED | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1182 |  | D | Minor editorial corrections | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 1185 | 1 | A | Always-on PDU session | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1186 | 1 | F | S-NSSAI association for PDU session established in S1 mode | 16.1.0 |
| 2019-06 | CT#84 | CP-191130 | 1187 | 1 | B | 5GMM capability for SRVCC from NG-RAN to UTRAN | 16.1.0 |
| 2019-06 | CT#84 | CP-191130 | 1188 | 1 | B | MS classmark 2 and supported codec | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1191 | 2 | F | Handling of 5GSM parameters | 16.1.0 |
| 2019-06 | CT#84 | CP-191134 | 1193 | 2 | F | Handling of SM back-off timer | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1195 | 1 | A | DNN based congestion control for PDU session for LADN | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1197 |  | F | Terminology correction about PDU session type | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1199 | 1 | F | Definition of EMM-IDLE mode in TS 24.501 | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 1200 |  | F | No CIoT 5GS optimizations for non-3GPP access | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1203 | 2 | A | Network initiated EPS bearer synchronization when moving from EPC to 5GC | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1204 | 1 | F | Correction on follow-on request indicator | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1205 |  | F | Correction on UE behaviour in 5GMM-REGISTERED.PLMN-SEARCH | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1206 | 1 | A | Deletion of the 5GSM cause IE in the PDU SESSION MODIFICATION COMPLETE message | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1207 | 1 | F | Correction on the abnormal cases for registration procedure | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 1210 |  | F | Alignment of the Abnormal cases for eDRX between 5GS and EPS | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1211 | 1 | F | Collision handling | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1212 | 2 | F | Authenticate before deleting UE context | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 1213 | 3 | B | Uplink NAS message transmission and CIoT data transfer | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1214 | 1 | F | Correction on T3346 and EPLMN handling | 16.1.0 |
| 2019-06 | CT#84 | CP-191122 | 1219 | 2 | A | Alignment of the 5G ciphering and integrity algorithm identifiers | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1220 | 2 | F | Conditions to apply the "null-scheme" to generate the SUCI | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1221 |  | F | Correction on the description of code point for 128-5G-EA3 | 16.1.0 |
| 2019-06 | CT#84 | CP-191129 | 1222 | 1 | B | Service Gap control in 5GS, reject of UL NAS Transport message | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1227 | 2 | F | Transmission failure of Registration Request during Initial Reg proc | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1228 | 3 | F | Handling of Radio Link failure during service Req proc | 16.1.0 |
| 2019-06 | CT#84 | CP-191148 | 1229 | 1 | B | Abnormal case handling for receipt of 5GMM cause value #11 from a PLMN | 16.1.0 |
| 2019-06 | CT#84 | CP-191148 | 1231 | 2 | B | Packet filters based on N3IWF IP address and SPI for IPsec SA | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1238 | 1 | A | QoS flow for SIP signalling after inter-system change | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1239 | 1 | F | Handling of multiple QoS rule/flow parameters included in one PCO/ePCO | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1240 | 1 | F | Error handling of optional IEs in a payload container entry of the Payload container IE | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1241 |  | F | Add codings of 5GSM causes #41 and #42 | 16.1.0 |
| 2019-06 | CT#84 | CP-191124 | 1245 | 1 | A | Indication of syntactical or semantic errors related to SM policy association to UE | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1246 | 3 | F | Clean-up of general section for 5GMM aspects of network slicing | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1247 |  | F | Request from the upper layers to perform emergency service fallback | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1248 |  | F | Non-overlapping tracking areas | 16.1.0 |
| 2019-06 | CT#84 | CP-191146 | 1249 | 1 | C | 5GSM cause values #27, #50, #51 and #70 for SINE\_5G | 16.1.0 |
| 2019-06 | CT#84 | CP-191123 | 1251 | 1 | A | Correction to handling of cause #72 | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1254 | 2 | F | Originating MMTEL voice due to upper layers request while T3346 is running | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1257 |  | F | Shared or valid 5G NAS security context | 16.1.0 |
| 2019-06 | CT#84 | CP-191135 | 1264 | 1 | F | EAP-success of EAP-TLS received in SECURITY MODE COMMAND | 16.1.0 |
| 2019-09 | CT#85 | CP-192073 | 1056 | 5 | B | Provisioning of an allowed CAG list and a CAG access only indication | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1057 | 8 | B | 5GMM cause value for CAG | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1189 | 3 | F | PDU session modication command not forwarded to 5G AN | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1236 | 3 | B | Storage for CAG information | 16.2.0 |
| 2019-09 | CT#85 | CP-192060 | 1269 | 2 | B | Procedure for Multiple Access upgrade of PDU Session | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1270 | 1 | F | Handling the non-current 5G NAS security context after inter-system change from N1 mode to S1 mode | 16.2.0 |
| 2019-09 | CT#85 | CP-192060 | 1271 | 2 | B | NSSAI not allowed for MA PDU session establishment | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1273 |  | F | Updates to new stage-2 requirements of CAG information structure | 16.2.0 |
| 2019-09 | CT#85 | CP-192059 | 1274 | 2 | F | Wireline access is a type of non-3GPP access | 16.2.0 |
| 2019-09 | CT#85 | CP-192059 | 1276 | 2 | F | Management of service area restrictions in wireline access | 16.2.0 |
| 2019-09 | CT#85 | CP-192059 | 1277 | 2 | F | IP address allocation for 5G-RG | 16.2.0 |
| 2019-09 | CT#85 | CP-192059 | 1278 | 2 | B | Security for W-AGF acting on behalf of an FN-RGt | 16.2.0 |
| 2019-09 | CT#85 | CP-192059 | 1279 | 1 | C | Alignment with stage-2 on PEI for 5G-RG and FN-RG | 16.2.0 |
| 2019-09 | CT#85 | CP-192063 | 1280 | 2 | B | V2X capability and V2X PC5 capability | 16.2.0 |
| 2019-09 | CT#85 | CP-192063 | 1281 | 1 | B | USPS extension for V2X policy | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1282 |  | F | Incorrect security algorithm | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1283 |  | F | Registration attempt counter correction | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1286 | 2 | C | 5GMM cause values applicable in an SNPN | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1287 | 1 | F | Clarification for UE selecting a suitable cell that supports CIoT optimisation | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1288 | 1 | F | Core network type restriction determined by operator policy | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1290 | 1 | F | Disabling the N1 mode capability for 3GPP access in Idle mode | 16.2.0 |
| 2019-09 | CT#85 | CP-192060 | 1293 | 1 | C | PDU Session release for MA PDU Session | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1295 | 1 | F | Clarification on error check for QoS rules | 16.2.0 |
| 2019-09 | CT#85 | CP-192060 | 1297 | 1 | B | MA PDU session establishment reject due to unstructured PDU Session type | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1298 |  | F | Clarification for T3580 Stop condition | 16.2.0 |
| 2019-09 | CT#85 | CP-192060 | 1300 | 1 | B | MA PDU session modification for ATSSS parameters | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1302 | 3 | F | Staying in inactive upon resume failure with RRC staying in RRC\_INACTIVE | 16.2.0 |
| 2019-09 | CT#85 | CP-192045 | 1306 | 1 | A | Maintaining the UL and DL NAS COUNTs after a handover from 5GS to EPS | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1308 | 2 | BV | PDU sessions and QoS flows for NB-IoT UEs | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1311 | 3 | B | Idle mode optimizations for 5G Control plane CIoT small data transfer t | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1315 | 1 | F | Performing registration update upon resume failure for reasons other than barring | 16.2.0 |
| 2019-09 | CT#85 | CP-192062 | 1316 | 2 | B | 5GMM capability update for eNS | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1318 | 1 | B | Header compression for control plane user datat | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1322 | 1 | B | UE behavior when RRC connection resume failst | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1323 | 1 | F | Correction on service gap timer | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1324 | 1 | F | Correction on T3448 value IE | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1325 | 1 | F | Alleviation of SM congestion | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1326 |  | F | Correction wrt EPS attempt counter to be used for Single Registration Failure use cases | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1328 |  | F | Correction on terminology regarding EPS bearer contextst | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1330 | 1 | F | Correction to SM procedures for back off timer not forwarded from 5GMM case. | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1332 |  | F | Deletion of RAND and RES on receiving Service Accept message | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1333 |  | F | Clarification for emergency call when T3396 or T3585 is running | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1334 | 1 | F | Removal of Editors Note for active timers in the NW | 16.2.0 |
| 2019-09 | CT#85 | CP-192083 | 1335 | 1 | B | Addition of LCS indication in 5GMM capability and 5GS NW capability | 16.2.0 |
| 2019-09 | CT#85 | CP-192083 | 1336 | 1 | B | Addition of location service message condition to Additional informaton IE | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1337 |  | F | Minor miscellaneous corrections | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1340 |  | F | Clarify encoding of EPS bearer identity | 16.2.0 |
| 2019-09 | CT#85 | CP-192071 | 1341 |  | F | Keep equivalent PLMNs list for Deregistration Request message with 5GMM cause #7 | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1344 |  | F | Correction to handling of operator-defined access category missing a standardized access category | 16.2.0 |
| 2019-09 | CT#85 | CP-192056 | 1345 | 1 | F | ODAC IEI correction | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1346 |  | F | Removal of eDRX support with RRC\_INACTIVE for NB-IoT | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1348 | 1 | F | IMEI not required for non-3GPP only UEs | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1351 | 1 | F | Emergency services fallback from non-3GPP access or ePDG/EPC | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1353 | 1 | F | Re-ordering of text on the applicability of access identities | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1354 | 1 | F | Trigger for NAS procedure retry in case NAS is put back in RRC inactivet | 16.2.0 |
| 2019-09 | CT#85 | CP-192069 | 1355 |  | B | Adding general description of RACS | 16.2.0 |
| 2019-09 | CT#85 | CP-192069 | 1356 | 1 | B | Signalling of UE support for RACS and of UE radio capability ID | 16.2.0 |
| 2019-09 | CT#85 | CP-192069 | 1357 | 2 | B | UE radio capability ID assignment by the network | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1358 | 1 | B | Signalling of UE support for transfer of port management information containers, MAC address and DS-TT residence time | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1359 | 2 | B | Adding support for transfer of Ethernet port management information containers | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1360 | 1 | F | Removal of Editor’s note on adding unified access control configuration to "list of subscriber data" for access to SNPNs | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1361 | 2 | F | Resolution of Editor’s notes on abnormal case handling for UE-initiated de-registration procedure in an SNPN | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1363 | 1 | F | Resolution of Editor’s notes on the applicability of MPS, MCS and delay tolerant in SNPNs | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1364 | 1 | F | Update of requirements on UE to construct packet filters based on the N3IWF destination IP address and the SPI for the IPsec SA | 16.2.0 |
| 2019-09 | CT#85 | CP-192083 | 1365 | 2 | B | NAS transport of supplementary services messages for a deferred 5GC-MT-LR | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1366 |  | F | Resolve Editor’s note on support indication for Small Data Rate Control | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1367 | 1 | B | Small data rate control parameters received in EPS | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1369 | 1 | F | Including EPS Preferred Network Behaviour to 5GCN | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1370 | 1 | F | General description on redirection of the UE by the core network | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1371 |  | F | No RRC inactive for NB-IoT | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1372 |  | F | Removal of Editor’s Note for the T3348 | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1380 |  | F | T3540 for 5GMM cause #31 or #73 | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1384 | 1 | F | Service gap control timer and MICO mode | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1385 | 2 | F | Service gap control, stop of timer via configuration update command | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1386 |  | F | Service gap control, MO service request when connected and timer running | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1387 | 2 | C | Service gap control, follow-on request indicator at mobility update registration | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1388 | 2 | 2 | Service gap control, follow-on request indicator at initial registration | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1391 |  | F | MICO mode and stop of active timer in AMF when UE enters 5GMM-CONNECTED | 16.2.0 |
| 2019-09 | CT#85 | CP-192062 | 1395 | 3 | C | Registration reject due to no available allowed S-NSSAI(s) | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1396 | 1 | F | Service gap control, MO SMS or LPP payload not allowed when connected | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1398 | 1 | F | Consistent use of PLMN ID for AKA | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1399 |  | F | Service reject without integrity protection | 16.2.0 |
| 2019-09 | CT#85 | CP-192052 | 1405 |  | F | Strictly periodic handling due to emergency service. | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1406 | 2 | F | Emergency call handling for a CAG only UE | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1408 |  | F | Collision of deregistration and other NAS procedure | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1410 |  | D | Missing inactive term. | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1411 | 1 | F | Handling of an emergency call in SNPN access mode. | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1412 | 1 | F | Initial NAS message protection | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1413 | 1 | F | Stopping conditions for Timer T3565. | 16.2.0 |
| 2019-09 | CT#85 | CP-192062 | 1421 | 4 | BV | Update of existing subclause for network slice specific authentication and authorizationt | 16.2.0 |
| 2019-09 | CT#85 | CP-192060 | 1425 | 1 | F | Updates to UE-requested PDU session procedures for converting to MA PDU session | 16.2.0 |
| 2019-09 | CT#85 | CP-192059 | 1427 | 2 | F | Applicability of unified access control for wireline 5G access network | 16.2.0 |
| 2019-09 | CT#85 | CP-192070 | 1434 | 2 | F | Correction of handling of 5GSM causes #27 and #70 for SINE\_5G | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1435 | 1 | F | Corrections to the disabling and re-enabling of N1 mode | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1436 | 1 | F | FPLMN list for 3GPP and non-3GPP access types | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1438 | 1 | F | Resolve ENs in clause 5.3.20 | 16.2.0 |
| 2019-09 | CT#85 | CP-192083 | 1440 | 1 | B | Access control on MO-LR | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1442 |  | F | Barred MO SMSoNAS | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1448 |  | F | Correction of the QoS rule operation name | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1453 | 2 | B | Handling of non-integrity protected messages in an SNPN | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1454 | 1 | C | Support of network slicing in an SNPN | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1456 | 1 | F | Lists of forbidden networks in an SNPN | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1457 | 1 | F | Lists of forbidden TAIs in an SNPN | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1458 | 1 | F | 5G-GUTI not globally unique in an SNPN | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1460 | 2 | C | Shared network broadcasting PLMN identity(ies) or SNPN identity(ies) | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1461 | 2 | F | Alignment on the implication description of type of list = “11” in service area list IE | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1466 | 1 | B | Support of time sensitive communication | 16.2.0 |
| 2019-09 | CT#85 | CP-192073 | 1470 | 2 | B | Port management information container: Delivery via the NAS protocol and coding | 16.2.0 |
| 2019-09 | CT#85 | CP-192054 | 1474 | 2 | F | Update the UE-requested PDU session establishment procedure regarding always-on PDU session for URLLC service | 16.2.0 |
| 2019-09 | CT#85 | CP-192054 | 1476 | 2 | F | Update the network-requested PDU session modification procedure regarding always-on PDU session for URLLC service | 16.2.0 |
| 2019-09 | CT#85 | CP-192057 | 1482 | 1 | F | Periodic update is allowed also in non-allowed area | 16.2.0 |
| 2019-12 | CT#86 | CP-193094 | 1233 | 4 | F | QoS operation upon activation of dedicated EPS bearer | 16.3.0 |
| 2019-12 | CT#86 | CP-193100 | 1275 | 3 | F | Management of forbidden area in wireline access | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1284 | 2 | F | Handling of unknown, unforeseen, and erroneous UPDS data in UE policy delivery service | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1327 | 4 | F | Handing of 5GMM parameters during certain mobility registration failurest | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1339 | 2 | F | Consistent back off timer handling for EPC interworking | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1342 | 2 | F | Local release when receiving REFRESH command for routing indicator in RRC inactive | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1349 | 3 | F | UAC check for services started in WLAN and being transferred to 3GPP access | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1352 | 2 | F | Addition of abnormal case handling for T3346 running in NAS transport procedure | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1373 | 4 | F | Maintenance of forbidden TA lists for non-integrity protected NAS reject | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1374 | 2 | F | EMM parameters handling for 5G ony causes | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1375 | 5 | F | Covering 5GMM cuase #31 for DoS attack | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1376 | 3 | F | UE checking the active EPS bearer ID for mapped QoS flows | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1378 | 3 | F | 5G NAS security context for interworking | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1397 | 2 | F | Clarification on handling of MP-REG | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1400 | 3 | F | Correction on handling and coding of Mapped EPS bearer contexts | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1401 | 4 | F | QoS rule and QoS flow error handling | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1402 | 2 | F | QoS error operation during interworking | 16.3.0 |
| 2019-12 | CT#86 | CP-193115 | 1403 | 1 | F | Correction on the condition for handling reattempt for PDU session type related rejection | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1404 | 1 | F | Additional 5GS PDU session rejection cause values | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1409 | 4 | F | Emergency registered state handling. | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1416 | 2 | F | Correction for N1 signalling connection release | 16.3.0 |
| 2019-12 | CT#86 | CP-193094 | 1418 | 3 | F | Emergency PDU session establishment upon expiry of timer T3580 | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1426 | 1 | F | Correction to the storage of 5GMM information; SOR counter and a UE parameter update counter | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1431 | 8 | B | Transmission of the UE CAG capability to the network | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1432 | 3 | F | Correction of 5GMM state for cause #27 "N1 mode not allowed" | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1433 | 3 | F | Correction and clarification of interworking with ePDG connected to EPC | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1449 | 1 | F | No requirement for network to store a back-off timer per UE and other criteria | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1450 | 5 | B | Slice-specific authentication and authorization procedure | 16.3.0 |
| 2019-12 | CT#86 | CP-193115 | 1452 | 3 | B | Back-off control in case of routing failure | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1469 | 3 | C | PDU session used for TSC established as an always-on PDU session | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1480 | 7 | F | Correction to delivery of mapped S-NSSAI(s) | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1489 |  | F | Correction of statement related to K'AMF derivation during S1 to N1 handover | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1490 | 1 | C | Condition to avoid redundant registration procedures during inter system change from S1 to N1 mode | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1493 | 1 | F | Removal of update status dependency for sub-state selection | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1494 | 2 | F | Handling of pending NAS messages during resume of the N1 NAS signalling connection | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1495 | 1 | F | Apply UAC during resume of the N1 NAS signalling connection | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1496 | 2 | F | Receiving deregistration with cause #72 when registered for both 3GPP and Non-3GPP accesst | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1497 | 2 | F | Correcting DDX description | 16.3.0 |
| 2019-12 | CT#86 | CP-193113 | 1499 |  | F | Correct UE radio capability ID reference | 16.3.0 |
| 2019-12 | CT#86 | CP-193101 | 1500 | 2 | B | MA PDU session release | 16.3.0 |
| 2019-12 | CT#86 | CP-193101 | 1501 |  | F | Add the missing MA PDU request | 16.3.0 |
| 2019-12 | CT#86 | CP-193101 | 1504 | 2 | F | MA PDU session rejection due to operator policy and subscription policy | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1505 | 6 | C | Introduction of pending NSSAI for network slice-specific authentication and authorization | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1506 | 1 | F | Resolving Editor’s Note for need of new EPD in CPSR message | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1507 | 1 | F | Resolving Editor’s Note on whether CIoT small data container IE can be TV format in CPSR message | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1509 | 2 | F | Corrections of service gap controlt | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1510 | 3 | B | Primary authentication using EAP methods other than EAP-AKA' and EAP-TLS | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1511 | 1 | B | Serving network name in SNPN | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1512 | 2 | B | Extensions of EAP-TLS usage in primary authentication | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1513 |  | B | Extensions of EAP-AKA' usage in primary authentication | 16.3.0 |
| 2019-12 | CT#86 | CP-193100 | 1514 | 1 | F | Further alignment with stage-2 on PEI for 5G-RG and FN-RG | 16.3.0 |
| 2019-12 | CT#86 | CP-193100 | 1515 | 1 | F | Corrections for wireline access service area restrictions | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1516 | 2 | F | Corrections related to Service Gap timer | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1517 | 1 | F | 5GS Control plane CIoT data transfer for UE in connected mode | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1518 | 2 | F | NAS message container for Control plane service request | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1519 | 4 | F | Abnormal case handling for uplink NAS transport for non-supporting UEs | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1520 | 2 | F | Applicability of existing emergency PDU session request type | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1523 |  | F | Corrections on the Port management information container IE | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1526 | 6 | F | Deregistration due to the failed network Slice-Specific Authentication and Authorization | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1527 | 1 | F | Correction of the misuse of T3525 | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1529 |  | F | Inclusion of the T3324 IE in REGISTRATION ACCEPT | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1532 | 1 | C | Control plane service request message and abnornal cases on the network side | 16.3.0 |
| 2019-12 | CT#86 | CP-193113 | 1535 | 1 | B | RACS support at EPS to 5GS IWK | 16.3.0 |
| 2019-12 | CT#86 | CP-193113 | 1539 | 1 | F | UE storage of RACS parameters in non-volatile memory | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1541 | 1 | B | Initial Small Data rate control parameters | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1542 |  | F | Reset of registration attempt counter at registration reject with cause #62 | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1543 |  | F | Incorrect reference in Authentication subclause | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1544 |  | F | IE inclusion criteria style alignment | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1545 | 1 | C | CP CIoT header compression, UE initiated re-configuration | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1546 | 1 | F | Corrrection to the notification procedure and collision with UE initiated de-registration | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1547 | 1 | F | Request of IMEISV via the security mode control procedure | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1548 | 1 | F | Service gap control, simultaneous registration over N3GPP access in same PLMN | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1549 | 3 | F | Registration reject due to no allowed slices and NW slice specific authentication and authorization | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1551 | 2 | F | Clarification to forbidden TAI lists for SNPN | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1552 | 1 | F | Clarification to PLMN-SEARCH substate. | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1553 | 1 | F | Correction to SNPN enabled terminology. | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1555 | 2 | F | 5GMM cause value #74 and requirements for non-integrity protected reject messages | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1556 | 1 | F | Discarding the REGISTRATION REJECT message with 5GMM cause #76 received without integrity protection | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1558 |  | F | Handling of the DEREGISTRATION REQUEST message with 5GMM cause value #74 or #75 in a PLMN | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1559 |  | F | Reset of the registration attempt counter upon receipt of NPN-based cause values | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1560 |  | F | Handling of T3510, T3517, and the service request attempt counter in an SNPN | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1561 | 4 | F | Missing requirement on UE policies for SNPN | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1562 | 1 | F | Corrections of RRC requirements specified in NAS specs | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1563 | 5 | F | Handling of maximum number of allowed active DRBs | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1565 |  | F | Correction to name of IE carrying residence time for TSN | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1569 |  | F | Stop conditions for timers T3580 and T3581 | 16.3.0 |
| 2019-12 | CT#86 | CP-193115 | 1570 | 1 | F | Correction to re-attempt indicator IE description | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1571 | 2 | F | 5GMM Cause #62 | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1574 |  | F | SMC message trigger | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1575 | 1 | F | Congestion control for UL NAS TRANSPORT message | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1577 | 1 | F | Applying small data rate control at inter-system change | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1578 | 1 | F | Counter events handling for SNPN | 16.3.0 |
| 2019-12 | CT#86 | CP-193118 | 1579 | 1 | F | 5GMM cause handling for SNPN | 16.3.0 |
| 2019-12 | CT#86 | CP-193101 | 1580 | 1 | F | Provision of MA PDU session information during the UE-initiated NAS transport procedure initiation | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1583 |  | F | Octet alignment for 5G-GUTI in 5GS mobile identity IE | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1584 | 1 | F | Clarification on handling of 5G NAS security context | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1585 | 1 | C | Resolving Editor’s notes on the Data Type field for the Control Plane Service Request message | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1586 | 1 | F | Registration upon change of UE radio capability during 5GMM-CONNECTED mode | 16.3.0 |
| 2019-12 | CT#86 | CP-193095 | 1589 |  | F | Handling of 5GSM cause #54 PDU session does not exist | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1590 | 1 | F | Correction to the indication upon receipt of 5GMM cause #91 | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1592 | 2 | F | Handling of errors in mapped EPS bearer contexts | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1593 | 1 | F | Cleanups and editorials | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1598 | 4 | B | "S-NSSAI not available in the current PLMN" when non NSSAA supported UE requesting the S-NSSAI subjects to NSSAA | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1602 | 6 | B | NSSAI storage impact with NSSAA | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1603 |  | F | EHPLMN and Dual registration | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1604 | 7 | F | CAG only UE and emergency procedure. | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1605 | 3 | F | SGC timer and handling during intersystem change | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1608 |  | F | Abbreviation of AUSF and UDM | 16.3.0 |
| 2019-12 | CT#86 | CP-193106 | 1619 | 1 | B | Release of NAS signalling connection for the UE authorized for V2X communication over PC5 | 16.3.0 |
| 2019-12 | CT#86 | CP-193113 | 1622 | 3 | F | Identification procedure for RACS | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1623 | 2 | F | Control plane service request, correction regarding service accept message applicability | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1625 | 2 | F | Precedence for segregation flow | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1628 | 4 | F | Unified Access Control for IMS registration related signalling | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1633 | 1 | B | Handling of non-integrity protected rejects when registered | 16.3.0 |
| 2019-12 | CT#86 | CP-193101 | 1636 |  | D | Editorial on PDU session establisment request upgraded to MA PDU session | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1640 | 1 | C | Handling of MT paging for CP-CIoT | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1647 | 2 | B | 5GS NAS extended timers for NB-N1 mode and WB-N1/CE mode devices | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1648 | 1 | C | Serving PLMN rate control at PDU session modification | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1649 | 1 | F | Clarification on the Mapped EPS bearer context | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1650 |  | D | Editorial corrections to text related to the status of PDU sessions during SR procedure | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1651 | 1 | F | Short MAC and ngKSI in Control plane service request NAS message | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1657 | 2 | B | Introduction of NSSAI efficient signalling for IoT devices | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1658 | 1 | C | Removal of Editor’s note on conditions of accepting registration | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1660 | 2 | F | UE behaviour when T3448 timer running | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1661 |  | F | AMF behaviour for mobility registration when SGC timer running | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1662 |  | F | Clarification on the UE policy container | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1663 | 1 | F | DNN Replacement | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1664 | 1 | F | Faulty and missing reference | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1665 | 1 | F | Correction of handling of de-registration procedure in ATTEMPTING-REGISTRATION-UPDATE | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1666 | 1 | F | Corrections and enhancements for T3540 | 16.3.0 |
| 2019-12 | CT#86 | CP-193084 | 1668 | 2 | A | Handling of UE NAS Count during handover from N1 mode to S1 mode | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1669 | 2 | F | Handling multiple QoS errors during a PDU session modification procedure – Option 1 | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1674 | 1 | F | No info on S-NSSAI subject to NSSAA in UE | 16.3.0 |
| 2019-12 | CT#86 | CP-193169 | 1676 | 2 | F | Equivalent SNPNs not supported for stand-alone non-public networks | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1680 |  | F | 5GMM state in non-3GPP access not impacting EMM state of single-registered UE | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1681 | 1 | F | Registration attempt counter reset by single-registered UE | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1682 |  | F | Correction for 5GMM and inter-system change | 16.3.0 |
| 2019-12 | CT#86 | CP-193096 | 1683 |  | F | Correction for 5GSM and inter-system change with N26 | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1684 | 1 | F | Clarification to forbidden PLMN list | 16.3.0 |
| 2019-12 | CT#86 | CP-193100 | 1685 |  | C | Access stratum connection and user-plane resources for trusted non-3GPP access and wireline access | 16.3.0 |
| 2019-12 | CT#86 | CP-193100 | 1686 | 1 | B | Usage of PDU session identity for the PDU sessions requested by the TWIF | 16.3.0 |
| 2019-12 | CT#86 | CP-193100 | 1687 |  | C | Removal of Session-TMBRt | 16.3.0 |
| 2019-12 | CT#86 | CP-193100 | 1688 |  | C | 5G-RG and W-AGF acting on behalf of FN-RG performing UE requirements | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1690 |  | F | Correction for 5GS network feature support IE | 16.3.0 |
| 2019-12 | CT#86 | CP-193106 | 1692 | 1 | B | UPDS updates enabling UE-requested V2X policy provisioning procedure | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1693 | 1 | B | Exchange of port management capabilities during PDU session establishment | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1694 | 1 | C | Additional abnormal cases in SNPN | 16.3.0 |
| 2019-12 | CT#86 | CP-193106 | 1697 | 1 | B | 5QI 86 introduction | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1698 | 1 | F | Deletion of UE radio capability in the network | 16.3.0 |
| 2019-12 | CT#86 | CP-193115 | 1699 | 1 | C | Retry restriction on non-3GPP access | 16.3.0 |
| 2019-12 | CT#86 | CP-193115 | 1700 | 1 | F | No retry restriction for 5GSM cause value #39 | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1702 | 3 | C | Support of UE specific DRX for NB-IoT | 16.3.0 |
| 2019-12 | CT#86 | CP-193090 | 1705 | 1 | B | Transfer of Ciphering Key Information for Broadcast Location Assistance Data | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1707 |  | F | Timer T3448 | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1709 | 1 | F | Rejected NSSAI | 16.3.0 |
| 2019-12 | CT#86 | CP-193090 | 1710 | 1 | F | Sending location services data from 5GMM-IDLE mode using the Control Plane Service Request message | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1711 | 1 | F | Correction of the format of CIoT small data container | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1712 | 3 | F | Removal of a Code-Point in Control Plane Service Type | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1715 | 1 | F | Correction to EPLMN list deletion for 5GMM cause #7 | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1716 |  | F | Correction to UE OS ID encoding | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1717 | 3 | F | Removal of CAG suscription while emergency PDU session is established. | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1718 | 1 | F | Defenition of CAG cell, CAG ID and CAG selection | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1719 | 2 | F | Handling of Service request message in a non-subscribed CAG cell | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1720 | 1 | F | Updation of LIMITED SERVICE state for CAG | 16.3.0 |
| 2019-12 | CT#86 | CP-193116 | 1722 | 2 | F | Handling of parameters stored in the ME memory | 16.3.0 |
| 2019-12 | CT#86 | CP-193104 | 1723 | 2 | F | Network slice authentication and emergency procedure | 16.3.0 |
| 2019-12 | CT#86 | CP-193115 | 1728 |  | F | Excluding 5GSM causes for congestion control from SINE | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1730 | 1 | F | ngKSI for CONTROL PLANE SERVICE REQUEST message | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1731 |  | F | Inclusion of PDU session reactivation result error cause IE | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1732 | 1 | F | IMEI and IMEISV formats support | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1733 | 1 | F | PEI format for non-3GPP access only UE | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1737 | 1 | F | Correction to the coding of EPS bearer identity | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1740 | 1 | F | UE handling upon receipt of 5GSM #46 out of LADN service area | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1742 | 1 | C | CIoT user data container in UL NAS transport message not routable | 16.3.0 |
| 2019-12 | CT#86 | CP-193089 | 1744 | 1 | C | Service gap control, supporting UE sends MO user data when connected when timer running | 16.3.0 |
| 2019-12 | CT#86 | CP-193088 | 1749 | 2 | F | Correction on the condition for including CP only indication | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1752 |  | F | T3540 in Service Accept Case | 16.3.0 |
| 2019-12 | CT#86 | CP-193106 | 1753 | 1 | C | Access control for UE triggered V2X policy provisioning procedure | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1754 | 2 | F | Abnormal cases for 5GMM cause values #74 and #75 | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1755 | 1 | C | Rejected NSSAI in SNPNs | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1756 | 2 | C | Introduction of SNPN-specific attempt counter for non-3GPP access and counter for "the entry for the current SNPN considered invalid for non-3GPP access" events | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1758 | 1 | F | Maintenance of forbidden TA lists for non-integrity protected NAS reject in an SNPN | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1759 | 1 | F | Handling of UAC for an MO IMS registration related signalling | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1760 |  | D | Correction of the definition of Network slicing information | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1766 | 2 | F | Moving Annex E to TS 24.5xy | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1767 | 1 | F | Follow on request codepoint value | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1770 | 1 | F | No CAG access control for emergency services | 16.3.0 |
| 2019-12 | CT#86 | CP-193119 | 1772 | 2 | F | Coding of the CAG-ID | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1773 | 1 | D | Timer order in timer tables | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1774 | 1 | F | Mobility registration accept with NSSAIs | 16.3.0 |
| 2019-12 | CT#86 | CP-193097 | 1775 | 2 | F | Correction to PLMN change with 5G-EA0 | 16.3.0 |
| 2019-12 | CT#86 | CP-193101 | 1778 | 1 | D | Editorial on PDU session establisment request upgraded to MA PDU session | 16.3.0 |
| 2020-03 | CT#87e | CP-200117 | 1533 | 6 | C | NW slice specific authentication and authorization failure and revocation | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1567 | 2 | B | CAG information towards the lower layers for paging | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1641 | 5 | B | PDU session handling for N5CW device | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1672 | 4 | C | Handling of user-plane resources for NB-IoT UEs having at least two PDU sessions | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1689 | 2 | C | Secondary authentication and W-AGF acting on behalf of FN-RG | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1781 | 3 | F | Correcting unimplementable condition regarding N26 interworking support detection | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1784 | 2 | F | Maintain Selected EPS NAS security algorithms during N1 mode to N1 mode handover | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1785 |  | F | Correction for AUTHENTICATION REJECT handling | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1786 | 1 | D | Editorial correction of an input parameter for 5G NAS message integrity protection | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1789 | 1 | F | Correction to sending of EPS NAS message container in Registration Request message | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1793 |  | D | Correct “ANSDP” | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1794 | 2 | F | Handling of unsupported SSC mode | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1797 | 1 | F | Abnormal case for service request procedure | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1798 | 2 | F | Mapped EPS bearer contexts deletion | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1799 | 1 | F | Service Request for PS Data Off | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1800 | 1 | F | Abnormal case for UL NAS TRANSPORT | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1804 |  | F | Declare syntactical error when both MFBR uplink and MFBR downlink equal zero | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1805 | 1 | D | Editorial correction to T3447 timer behavior | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1807 | 1 | F | Handling multiple QoS errors during a PDU session establishment procedure | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1810 | 1 | F | Inclusion of PDU session reactivation result error cause IE | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1811 |  | F | Correction on NAS transparent container for 5G-4G interworking | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1812 | 2 | F | Deletion of the rejected NSSAI for the current registration area | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1813 |  | F | Trigger for stopping timer T3511 | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1814 |  | F | Correction on T3502 for deactivated value | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1815 | 1 | F | 5GMM cause #22 for resetting registration attempt counter | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1816 |  | F | Consistent use of additional 5G security information IE | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1817 |  | F | Correction on N26 interface indicator | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1818 |  | F | Correction on reference of TS 36.304 | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1819 | 1 | F | Inclusion of 5GSM cause in PDU session modification request | 16.4.0 |
| 2020-03 | CT#87e | CP-200111 | 1820 |  | F | Inclusion of 5GSM cause in PDU session release request | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1821 |  | F | PDU session establishment reject with 5GSM #29 | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1822 | 1 | F | Correction on QoS rule/QoS flow synchronization | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1824 | 1 | F | Correction on NAS COUNT handling for intra-N1 handover | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1825 | 1 | F | Correction on Uplink data status IE coding | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1826 |  | F | Acknowledgement of UCU procedure | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1827 | 1 | F | Update bullet index to include all NAS transport cases | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1828 | 1 | D | Editorial correction on payload container | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1829 | 2 | F | Corrections on UE-initiated NAS transport procedure initiation | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1834 | 2 | D | Corrections in specifying reasons for errors | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1835 | 1 | F | UE handling of invalid QoS flow description | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1836 | 2 | F | S-NSSAI as a mandatory parameter to support interworking with 5GS | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1837 | 1 | F | Optional IE description for release assistance indication IE | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1838 | 1 | F | UE handling of multiple QoS errors in EPS | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1839 | 1 | F | S-NSSAI value associated with the BO timer applied for all PLMNs | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1840 | 1 | F | Abnormal case handling for 5GMM cause value #90 along with a PDU SESSION MODIFICATION REQUEST message | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1842 |  | F | Correction in handling of persistent PDU session during the mobility registration update | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1843 |  | D | NAS signalling spelling correction | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1845 | 2 | F | Reject non-emergency PDU session request attempt while UE registered for emergency services in the network | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1846 |  | F | Correction to IEI values | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1847 | 1 | F | Correction to 5GMM cause IE | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1848 |  | F | Correction to UCU procedure abnormal cases on NW side for a new TAI list | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1853 | 3 | F | Service area restrictions, case missing for when UE is out of allowed tracking area list and RA | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1854 |  | F | Correction to the Mapped NSSAI IE | 16.4.0 |
| 2020-03 | CT#87e | CP-200112 | 1858 |  | D | Correcting reference to 5GSM procedures | 16.4.0 |
| 2020-03 | CT#87e | CP-200114 | 1860 | 2 | F | 5GSM capabilities for MA PDU session | 16.4.0 |
| 2020-03 | CT#87e | CP-200114 | 1862 | 4 | B | MA PDU session is not supported | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1869 | 2 | F | Cleanups on introduction of pending NSSAI | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1870 |  | F | SUCI used by W-AGF acting on behalf of FN-RG | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1871 |  | F | Resolving editor's note on W-AGF acting on behalf of FN-RG not using the "null integrity protection algorithm" 5G-IA0 | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1872 |  | F | Resolving editor's note on service area restrictions in case of FN-BRG | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1873 |  | F | Resolving editor's note in forbidden wireline access area | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1874 |  | F | Wireline 5G access network and wireline 5G access clean up | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1875 | 1 | F | PEI clean up | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1876 |  | F | Alignment for stop of enforcement of mobility restrictions in 5G-RG and W-AGF acting on behalf of FN-CRG | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1877 | 1 | F | Introduction of GCI and GLI | 16.4.0 |
| 2020-03 | CT#87e | CP-200109 | 1878 | 1 | F | Always-On PDU session and URLLC | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1879 | 1 | F | CAG information list storage | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1881 | 2 | F | Abnormal case for cause #31 | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1882 |  | F | Removal of Editor’s note on the use of the NOTIFICATION message in SNPNs | 16.4.0 |
| 2020-03 | CT#87e | CP-200135 | 1884 | 3 | B | Including CAG information list in REGISTRATION ACCEPT message | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1885 |  | F | Update of text on time synchronization | 16.4.0 |
| 2020-03 | CT#87e | CP-200125 | 1886 |  | F | Removal of Editor’s note on applicability of RACS to SNPNs | 16.4.0 |
| 2020-03 | CT#87e | CP-200125 | 1887 |  | C | Finalizing the encoding of the UE radio capability ID | 16.4.0 |
| 2020-03 | CT#87e | CP-200125 | 1888 | 1 | B | UE radio capability ID deletion upon Version ID change | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1889 | 2 | B | Handling of S-NSSAIs in the pending NSSAI | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1891 |  | F | Resolve Editor´s Notes on NB-N1 mode extended NAS timers for CE | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1892 |  | F | Resolve Editor´s Notes on WB-N1 mode extended NAS timers for CE | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1893 | 1 | F | Clarification on HPLMN S-NSSAI | 16.4.0 |
| 2020-03 | CT#87e | CP-200114 | 1896 | 1 | F | MA PDU session and one set of QoS parameters | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1899 | 1 | F | Update to registration procedure due to eNS | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1900 | 1 | F | Stop T3565 upon connection resumption | 16.4.0 |
| 2020-03 | CT#87e | CP-200125 | 1902 | 1 | F | RACS not apply for non-3GPP access | 16.4.0 |
| 2020-03 | CT#87e | CP-200114 | 1903 |  | F | Minor Correction to ATSSS container IE desciption | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1907 | 3 | B | Support for the signalling of the capability for receiving WUS assistance information | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1910 | 3 | F | Enabling mobility with (emergency) sessions/connections between the (trusted) non-3GPP access network connected to the 5GCN and the E-UTRANt | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1913 | 1 | F | UE behaviour for other causes in the rejected NSSAI during deregistration procedure | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1914 | 1 | F | Pending NSSAI update for the configured NSSAI in the CUC message | 16.4.0 |
| 2020-03 | CT#87e | CP-200139 | 1915 | 2 | F | Cleanup for NSSAA message and coding | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1916 | 1 | F | Rejected NSSAI during the initial registration procedure | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1917 | 1 | F | UE behaviour when T3447 running | 16.4.0 |
| 2020-03 | CT#87e | CP-200108 | 1918 | 1 | C | PDU session release | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 1919 |  | B | ACS information via DHCP | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1921 | 1 | D | Name of the rejected NSSAI cause values | 16.4.0 |
| 2020-03 | CT#87e | CP-200125 | 1922 |  | F | Clarification of the cause of start of T3550 | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1923 | 1 | F | Clarification of forbidden TAI lists for SNPN | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1924 |  | F | Deletion of all CAG-IDs of a CAG cell 5GMM cause for #76 | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1926 |  | F | Clarification of the rejected NSSAI cause value | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1927 |  | F | Removal of term CAG access control | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1928 |  | F | Definition alignment for UE-DS-TT residence time | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1930 |  | F | Ciphering and deciphering handling of CPSR message | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1932 | 1 | C | Truncated 5G-S-TMSI over NAS | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1933 |  | F | AMF behavior on stop T3448 | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1934 | 1 | F | Correction on SMS in payload container IE in CPSR message | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1935 | 1 | F | Correction on 5GMM cause #74/#75 for no touching non-3GPP access | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1937 |  | F | Correction on term "non-3GPP access" used in SNPN | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1938 |  | F | Reset the registration attempt counter for #76 in service reject | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1941 | 1 | F | ENs resolution for revoked or failed NSSAA | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1942 |  | D | Consistent name for NSSAA | 16.4.0 |
| 2020-03 | CT#87e | CP-200127 | 1943 |  | F | No retry in 4G for PDU session type related 5GSM causes | 16.4.0 |
| 2020-03 | CT#87e | CP-200127 | 1944 |  | F | Correction on UE retry restriction on EPLMN | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1945 | 1 | F | Clarification on Public Network Integrated NPN in TS 24.501 | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1946 | 1 | F | UE receives CAG information in SNPN access mode | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1947 | 2 | F | Establish PDU session to transfer port management information containers | 16.4.0 |
| 2020-03 | CT#87e | CP-200114 | 1948 | 2 | F | ATSSS Non-MPTCP traffic support | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1949 | 1 | F | Correction for the wrongly implemented CR1693r1 | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1953 |  | F | NSSAA revocation function | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1956 | 1 | F | Stopping of T3513 after connection resume for user plane CIoT 5GS optimization | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1958 |  | F | Correction UE behaviour when the UE recives the pending NSSAI | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1961 | 1 | F | Adding an editor’s note for suspend indication due to user plane CIoT 5GS optimization | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1966 | 1 | C | Recovery from fallback for UEs using CP CIoT optimization | 16.4.0 |
| 2020-03 | CT#87e | CP-200119 | 1968 |  | B | Triggering service request procedure for V2X communication over PC5 interface | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1971 | 1 | C | Removal of the use of Service area list IE during NSSAAt | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1973 |  | F | Additional triggers for deletion of pending S-NSSAI | 16.4.0 |
| 2020-03 | CT#87e | CP-200114 | 1976 | 1 | B | Considering allowed NSSAI when establishing MA PDU session | 16.4.0 |
| 2020-03 | CT#87e | CP-200114 | 1977 | 1 | B | UE Handling upon receipt of PDU session release command | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1978 | 1 | F | Correction to UL CIoT user data container not routable or not allowed to be routed | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1979 | 1 | F | Single downlink data only indication and release of N1 NAS signalling connection | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1980 | 2 | F | PDU session status with control plane service request message | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1981 | 1 | F | Service gap control, correction when to start service gap control timer in UE and NW | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1982 | 1 | F | Clarification of control plane service request message options | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1983 | 1 | C | UAC updates for NB-IoT to include "MO exception data" | 16.4.0 |
| 2020-03 | CT#87e | CP-200107 | 1984 | 1 | B | Clarification on the use of exception data reporting | 16.4.0 |
| 2020-03 | CT#87e | CP-200286 | 1985 | 5 | F | Update SNPN key differences | 16.4.0 |
| 2020-03 | CT#87e | CP-200109 | 1987 | 1 | F | Setting the Always-on PDU session indication IE in the PDU SESSION ESTABLISHMENT ACCEPT message | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1991 |  | F | AMF updates the UE NSSAI storage after network slice-specific authentication and authorization is completed | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1995 |  | F | Clarification on the S-NSSAI not subject to NSSAA included in allowed NSSAI | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1996 | 2 | F | Subscribed S-NSSAI marked as default and NSSAA | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 1997 |  | F | Additional conditions to the presence in the subscribed S-NSSAIs | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 1998 | 1 | F | Triggering mobility registration update due to manual CAG selection | 16.4.0 |
| 2020-03 | CT#87e | CP-200117 | 2000 | 1 | F | Emergency PDU session handling after NSSAA failure | 16.4.0 |
| 2020-03 | CT#87e | CP-200125 | 2002 |  | F | UE behaviour upon receipt of a UE radio capability ID deletion indication | 16.4.0 |
| 2020-03 | CT#87e | CP-200125 | 2005 | 1 | F | Additional condition to change UE radio capability ID during mobility registration update | 16.4.0 |
| 2020-03 | CT#87e | CP-200125 | 2006 | 1 | F | UE radio capability information storage not needed for RACS | 16.4.0 |
| 2020-03 | CT#87e | CP-200097 | 2008 | 3 | F | Handling of a UE with an emergency PDU session in terms of CAG | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 2012 | 2 | F | N1 mode capability disabling and re-enabling for SNPN | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 2013 | 1 | F | #31 not applicable in an SNPN | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 2015 | 1 | F | Validity of the USIM for an SNPN and for a specific access type | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 2016 |  | F | Handling of 5GMM cause values #62 in an SNPN | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 2017 | 1 | F | No mandate to support default configured NSSAI or network slicing indication | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 2018 | 2 | F | SNN coding | 16.4.0 |
| 2020-03 | CT#87e | CP-200130 | 2019 | 1 | F | 5GMM cause value #74 in an SNPN with a globally-unique SNPN identity | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 2020 | 1 | B | Registration of N5GC devices via wireline access | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 2021 | 1 | F | Correction on EUI-64 as PEI | 16.4.0 |
| 2020-03 | CT#87e | CP-200113 | 2022 |  | F | Corrections on N5CW support | 16.4.0 |
| 2020-03 | CT#87e |  |  |  |  | Addition of IEI values, editorial corrections, implementation of missing CR1985 | 16.4.1 |