**3GPP TSG-CT WG1 Meeting #133e-bisC1-22XXXX**

**E-meeting, 17-21 January 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **3765** | **rev** | **4** | **Current version:** | **17.5.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | UAS security information obtained during UUAA |
|  |  |
| ***Source to WG:*** | Lenovo, Motorola Mobility, InterDigital, Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | ID\_UAS |  | ***Date:*** | 2022-01-17 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)...Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Agreed SA3 document SA3 CR S3-214463 indicate that the UUAA authroization payload can include UAS security that is used to establish security between the UAV and the USS. The 3GPP entities which are responsible for the UUAA i.e. AMF and SMF are to pass along this information as part of UUAA authroization payload to the UAV. |
|  |  |
| ***Summary of change:*** | The CR add a note that if the UAS security information is provided by the USS as part of the UUAA, then it is passed along by AMF and SMF.Reference to security aspects of UAS is added.A reference to TS 33.256 has been added.The text has been expanded to add more parameter details to the current text. |
|  |  |
| ***Consequences if not approved:*** | Stage 3 for the feature is missing. |
|  |  |
| ***Clauses affected:*** | 2, 5.4.4.2, 6.4.1.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Next Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

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

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

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

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

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

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

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

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

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

[6AB] 3GPP TS 23.256: "Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2".

[6B] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[6C] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[6D] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[6E] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

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

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

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

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

[10A] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

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

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

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

[13A] 3GPP TS 24.080: "Mobile radio interface layer 3 Supplementary services specification; Formats and coding".

[13B] 3GPP TS 24.193: "Access Traffic Steering, Switching and Splitting; Stage 3".

[13C] 3GPP TS 24.173: "IMS Multimedia telephony communication service and supplementary services; Stage 3".

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

[14A] 3GPP TS 24.250: "Protocol for Reliable Data Service; Stage 3".

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

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

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

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

[19] 3GPP TS 24.526: "UE policies for 5G System (5GS); Stage 3".

[19BA] 3GPP TS 24.539: "5G System (5GS); Network to TSN translator (TT) protocol aspects; Stage 3".

[19A] 3GPP TS 24.535: "Device-Side Time-Sensitive Networking (TSN) Translator (DS-TT) to Network-Side TSN Translator (NW-TT) protocol aspects; Stage 3".

[19B] 3GPP TS 24.587: "Vehicle-to-Everything (V2X) services in 5G System (5GS); Protocol aspects; Stage 3"

[19C] 3GPP TS 24.588: "Vehicle-to-Everything (V2X) services in 5G System (5GS); User Equipment (UE) policies; Stage 3"

[19D] Void.

[19E] 3GPP TS 24.554: "Proximity-service (ProSe) in 5G System (5GS) protocol aspects; Stage 3".[19F] 3GPP TS 24.555: "Proximity-services (ProSe) in 5G System (5GS); User Equipment (UE) policies; Stage 3".

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

[20AA] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

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

[20AB] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

[20B] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

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

[21A] 3GPP TS 29.526: "5G System; Network Slice-Specific Authentication and Authorization (NSSAA) services; Stage 3".

[21B] 3GPP TS 29.256: "5G System; Uncrewed Aerial Systems Network Function (UAS-NF); Aerial Management Services; Stage 3.

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

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

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

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

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

[23B] 3GPP TS 33.256: "Security aspects of Uncrewed Aerial Systems (UAS)".

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

[24A] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

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

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

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

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

[25D] 3GPP TS 36.306: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio access capabilities".

[25E] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".

[26] 3GPP TS 37.355: "LTE Positioning Protocol (LPP)".

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

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

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

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

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

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

[31AA] 3GPP TS 38.509: "Special conformance testing functions for User Equipment (UE)".

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

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

[33A] IETF RFC 3095: "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP and uncompressed".

[33B] Void.

[33C] Void.

[33D] IETF RFC 8415: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

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

[34A] IETF RFC 3843: "RObust Header Compression (ROHC): A Compression Profile for IP".

[35] Void.

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

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

[37] IETF RFC 7542: "The Network Access Identifier".

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

[38A] IETF RFC 4815: "RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095".

[38B] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

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

[39A] IETF RFC 5225: "RObust Header Compression (ROHC) Version 2: Profiles for RTP, UDP, IP, ESP and UDP Lite".

[39B] IETF RFC 5795: "The RObust Header Compression (ROHC) Framework".

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

[40A] IETF RFC 6603: "Prefix Exclude Option for DHCPv6-based Prefix Delegation".

[40B] IETF RFC 6846: "RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)".

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

[42] ITU-T Recommendation E.212: "The international identification plan for public networks and subscriptions", 2016-09-23.

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

[43A] IEEE Std 802.1AS-2020: "IEEE Standard for Local and metropolitan area networks--Timing and Synchronization for Time-Sensitive Applications".

[43B] IEEE Std 1588™-2019: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[43C] Void.

[43D] Void.

[43E] Void.

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] IEEE "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)".

[49] BBF TR-069: "CPE WAN Management Protocol".

[50] BBF TR-369: "User Services Platform (USP)".

[51] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[52] IETF RFC 8106:"IPv6 Router Advertisement Options for DNS Configuration".

[53] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services; Stage 2".

[54] 3GPP TS 23.380: "IMS Restoration Procedures".

[55] IETF RFC 3948: "UDP Encapsulation of IPsec ESP Packets".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Next Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 5.4.4.2 Generic UE configuration update procedure initiated by the network

The AMF shall initiate the generic UE configuration update procedure by sending the CONFIGURATION UPDATE COMMAND message to the UE.

The AMF shall in the CONFIGURATION UPDATE COMMAND message either:

a) include one or more of the following parameters: 5G-GUTI, TAI list, allowed NSSAI that may include the mapped S-NSSAI(s), LADN information, service area list, MICO indication, NITZ information, configured NSSAI that may include the mapped S-NSSAI(s), rejected S-NSSAI(s) in the Rejected NSSAI IE or in the Extended rejected NSSAI IE, network slicing subscription change indication, operator-defined access category definitions, SMS indication, service gap time value, "CAG information list", UE radio capability ID, 5GS registration result, UE radio capability ID deletion indication, truncated 5G-S-TMSI configuration, T3447 value, "list of PLMN(s) to be used in disaster condition", disaster roaming wait range or disaster return wait range;

Editor's note (WI MINT, CR#3437): Whether the PLMN offering disaster roaming can provide an indication that the disaster condition has ended in the CONFIGURATION UPDATE COMMAND message to a UE registered for disaster roaming is FFS.

b) include the Configuration update indication IE with the Registration requested bit set to "registration requested"; or

c) include a combination of both a) and b).

If the UE is registering or registered for onboarding services in SNPN, the serving SNPN shall not provide the configured NSSAI, the allowed NSSAI or the rejected NSSAI to the UE.

If the UE supports extended rejected NSSAI in roaming scenarios, the rejected S-NSSAI(s) shall be included in the Extended rejected NSSAI IE. Otherwise the rejected S-NSSAI(s) shall be included in the Rejected NSSAI IE.

If an acknowledgement from the UE is requested, the AMF shall indicate "acknowledgement requested" in the Acknowledgement bit of the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message and shall start timer T3555. Acknowledgement shall be requested for all parameters except when only NITZ is included.

To initiate parameter re-negotiation between the UE and network, the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message.

NOTE 1: Generic UE configuration update procedure can be initiated by the AMF for updating the emergency number list, the extended emergency number list or both by indicating "registration requested" in the Registration requested bit of the Configuration update indication IE in the CONFIGURATION UPDATE COMMAND message to the UE.

If a new allowed NSSAI information or AMF re-configuration of supported S-NSSAIs requires an AMF relocation, the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE and include the Allowed NSSAI IE in the CONFIGURATION UPDATE COMMAND message.

If the AMF includes a new configured NSSAI in the CONFIGURATION UPDATE COMMAND message and the new configured NSSAI requires an AMF relocation as specified in 3GPP TS 23.501 [8], the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE in the message.

If the AMF includes a new configured NSSAI in the CONFIGURATION UPDATE COMMAND message, the subscription information includes the NSSRG information, and the UE has set the NSSRG bit in the 5GMM capability IE of the REGISTRATION REQUEST message to:

a) "NSSRG supported", then the AMF shall include the NSSRG information in the CONFIGURATION UPDATE COMMAND message; or

b) "NSSRG not supported", then the configured NSSAI shall include one or more S-NSSAIs each of which is associated with all the NSSRG value(s) of the subscribed S-NSSAI(s) marked as default.

If the CONFIGURATION UPDATE COMMAND message is initiated only due to changes to the allowed NSSAI and these changes require the UE to initiate a registration procedure, but the AMF is unable to determine an allowed NSSAI for the UE as specified in 3GPP TS 23.501 [8], then the CONFIGURATION UPDATE COMMAND message shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE, and shall not contain any other parameters.

If the AMF needs to enforce a change in the restriction on the use of enhanced coverage or use of CE mode B as described in subclause 5.3.18, the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE and "release of N1 NAS signalling connection not required" in the Signalling connection maintain request bit of the Additional configuration indication IE in the CONFIGURATION UPDATE COMMAND message.

If a network slice-specific authentication and authorization procedure for an S-NSSAI is completed as a:

a) success, the AMF shall include this S-NSSAI in the allowed NSSAI over the same access of the requested S-NSSAI; or

b) failure, the AMF shall include this S-NSSAI in the rejected NSSAI for the failed or revoked NSSAA with the rejection cause "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization" over either 3GPP access or non-3GPP access.

If authorization is revoked for an S-NSSAI that is in the current allowed NSSAI for an access type, the AMF shall:

a) provide a new allowed NSSAI to the UE, excluding the S-NSSAI for which authorization is revoked; and

b) provide a new rejected NSSAI for the failed or revoked NSSAA, including the S-NSSAI in the rejected NSSAI for which the authorization is revoked, with the rejection cause "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization".

The allowed NSSAI and the rejected NSSAI shall be included in the CONFIGURATION UPDATE COMMAND message to reflect the result of the procedures subject to network slice-specific authentication and authorization.

NOTE 2: If there are multiple S-NSSAIs subject to network slice-specific authentication and authorization, it is implementation specific if the AMF informs the UE about the outcome of the procedures in one or more CONFIGURATION UPDATE COMMAND messages.

If the AMF includes the Network slicing indication IE in the CONFIGURATION UPDATE COMMAND message with the Network slicing subscription change indication set to "Network slicing subscription changed", and changes to the allowed NSSAI require the UE to initiate a registration procedure, but the AMF is unable to determine an allowed NSSAI for the UE as specified in 3GPP TS 23.501 [8], then the CONFIGURATION UPDATE COMMAND message shall additionally indicate "registration requested" in the Registration requested bit of the Configuration update indication IE and shall not include an allowed NSSAI.

If EAC mode is activated, the AMF shall perform NSAC for S-NSSAI(s) subject to NSAC before such S-NSSAI(s) are included in the allowed NSSAI in the CONFIGURATION UPDATE COMMAND message. If EAC mode is deactivated, the AMF shall perform NSAC for S-NSSAI(s) subject to NSAC after such S-NSSAI(s) are included in the allowed NSSAI in the CONFIGURATION UPDATE COMMAND message.

If the UE supports extended rejected NSSAI and the AMF determines that maximum number of UEs reached for one or more S-NSSAI(s) in the allowed NSSAI as specified in subclause 4.6.2.5, the AMF shall include the rejected NSSAI containing one or more S-NSSAIs with the rejection cause "S-NSSAI not available due to maximum number of UEs reached" in the Extended rejected NSSAI IE in the CONFIGURATION UPDATE COMMAND message. In addition, the AMF may include a back-off timer value for each S-NSSAI with the rejection cause "S-NSSAI not available due to maximum number of UEs reached" included in the Extended rejected NSSAI IE of the CONFIGURATION UPDATE COMMAND message.

If the UE does not indicate support for extended rejected NSSAI and the maximum number of UEs has been reached, the AMF should include the rejected NSSAI containing one or more S-NSSAIs with the rejection cause "S-NSSAI not available in the current registration area" in the Rejected NSSAI IE and should not include these S-NSSAIs in the allowed NSSAI in the CONFIGURATION UPDATE COMMAND message. In addition, the AMF may based on the network policies start a local implementation specific timer for the UE per rejected S-NSSAI and upon expiration of the local implementation specific timer, the AMF may remove the rejected S-NSSAI from the rejected NSSAI and update to the UE by initiating the generic UE configuration update procedure.

NOTE 3: Based on network policies, the AMF can include the S-NSSAI(s) for which the maximum number of UEs has been reached in the rejected NSSAI with rejection causes other than "S-NSSAI not available in the current registration area".

If the AMF needs to update the LADN information, the AMF shall include the LADN information in the LADN information IE of the CONFIGURATION UPDATE COMMAND message.

If the AMF needs to update the "CAG information list", the AMF shall include the CAG information list IE in the CONFIGURATION UPDATE COMMAND message. If the AMF needs to update the "CAG information list" and the UE:

a) has an emergency PDU session; and

b) is in

1) a CAG cell and none of the CAG-ID(s) supported by the CAG cell is included in the "allowed CAG list" for the current PLMN in the updated "CAG information list"; or

2) a non-CAG cell and the entry for the current PLMN in the updated "CAG information list" includes an "indication that the UE is only allowed to access 5GS via CAG cells";

the AMF may indicate to the SMF to perform a local release of all non-emergency PDU sessions associated with 3GPP access. The AMF shall not indicate to the SMF to release the emergency PDU session. If the AMF indicated to the SMF to perform a local release of all non-emergency PDU sessions associated with 3GPP access, the network shall behave as if the UE is registered for emergency services and shall set the 5GS registration result IE value to "Registered for emergency services" in the CONFIGURATION UPDATE COMMAND message.

If the AMF:

- updated the "CAG information list" to remove one or more CAG-ID(s) in the Allowed CAG list for the serving PLMN or an equivalent PLMN; or

- updated the "CAG information list" to set the "indication that the UE is only allowed to access 5GS via CAG cells" for the serving PLMN or an equivalent PLMN which was not set before,

then upon completion of the configuration update procedure and if the UE does not have an emergency PDU session, the AMF shall initiate the release of the N1 NAS signalling connection according to subclause 5.3.1.3.

If the AMF needs to update the truncated 5G-S-TMSI configuration for a UE in NB-N1 mode using control plane CIoT 5GS optimization, the AMF shall include the Truncated 5G-S-TMSI configuration IE in the CONFIGURATION UPDATE COMMAND message.

If the AMF includes a UE radio capability ID deletion indication IE in the CONFIGURATION UPDATE COMMAND message, the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE.

If the AMF needs to redirect the UE to EPC as described in subclause 4.8.4A.2, the AMF shall indicate "registration requested" in the Registration requested bit of the Configuration update indication IE and "release of N1 NAS signalling connection not required" in the Signalling connection maintain request bit of the Additional configuration indication IE in the CONFIGURATION UPDATE COMMAND message.

If the UE is not in NB-N1 mode and the UE supports RACS, the AMF may include either a UE radio capability ID IE or a UE radio capability ID deletion indication IE in the CONFIGURATION UPDATE COMMAND message.

During an established 5GMM context, the network may send none, one, or more CONFIGURATION UPDATE COMMAND messages to the UE. If more than one CONFIGURATION UPDATE COMMAND message is sent, the messages need not have the same content.

Upon receipt of the successful result of the UUAA-MM procedure from the UAS-NF, the AMF shall include:

a) the service-level-AA response with the value set to the UUAA-MM result, set to "Service level authentication and authorization was successful";

b) if a new CAA-Level UAV ID is provided by the UAS-NF, the service-level device ID with the value set to the new CAA-Level UAV ID;

c) if received the UUAA authorization payload from the UAS-NF:

1) the service-level-AA payload type, with the values set to "UUAA payload"; and

2) the service-level-AA payload, with the value set to the UUAA authorization payload;

in the Service-level-AA container IE of the CONFIGURATION UPDATE COMMAND message.

NOTE 4: UAS security information can be included in the UUAA authorization payload by the USS as specified in 3GPP TS 33.256 [23B].

If the AMF needs to deliver to the UE the UUAA revocation notification received from the UAS-NF, the AMF shall include the Service-level-AA response IE with SLAR set to "Service level authentication and authorization was not successful or service level authorization is revoked" in the Service-level-AA container IE of the CONFIGURATION UPDATE COMMAND message.

If the AMF detects that the UUAA-MM procedure has:

a) succeeded, the AMF shall set the service-level-AA response to "Service level authentication and authorization was successful"; or

b) failed, the AMF shall set the service-level-AA response to "Service level authentication and authorization was not successful".

NOTE 5: If the AMF receives the HTTP code set to "4xx" or "5xx" as specified in 3GPP TS 29.500 [20AA] or the AMF detects that the UUAA-MM failure as specified in 3GPP TS 29.256 [21B], then the AMF considers the UUAA-MM procedure has failed.

If the UE supports MINT, the AMF may include the List of PLMNs to be used in disaster condition IE in the CONFIGURATION UPDATE COMMAND message.

If the UE supports MINT, the AMF may include the Disaster roaming wait range IE in the CONFIGURATION UPDATE COMMAND message.

If the UE supports MINT, the AMF may include the Disaster return wait range IE in the CONFIGURATION UPDATE COMMAND message.

NOTE 6: The AMF can determine the content of the "list of PLMN(s) to be used in disaster condition", the value of the disaster roaming wait range and the value of the disaster return wait range based on the network local configuration.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Next Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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

If the connectivity with the requested DN is accepted by the network, the SMF shall create a PDU SESSION ESTABLISHMENT ACCEPT message.

If the UE requests establishing an emergency PDU session, the network shall not check for service area restrictions or subscription restrictions when processing the PDU SESSION ESTABLISHMENT REQUEST message.

The SMF shall set the Authorized QoS rules IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the authorized QoS rules of the PDU session and may include the authorized QoS flow descriptions IE of the PDU SESSION ESTABLISHMENT ACCEPT message set to the authorized QoS flow descriptions of the PDU session.

NOTE 1: This is applicable also if the PDU session establishment procedure was initiated to perform handover of an existing PDU session between 3GPP access and non-3GPP access, and even if the authorized QoS rules and authorized QoS flow descriptions for source and target access of the handover are the same.

The SMF shall ensure that the number of the packet filters used in the authorized QoS rules of the PDU Session does not exceed the maximum number of packet filters supported by the UE for the PDU session. If the received request type is "initial emergency request", the SMF shall set the Authorized QoS flow descriptions IE according to the initial QoS parameters used for establishing emergency services configured in the SMF emergency configuration data.

SMF shall set the Authorized QoS flow descriptions IE to the authorized QoS flow descriptions of the PDU session, if:

a) the Authorized QoS rules IE contains at least one GBR QoS flow;

b) the QFI is not the same as the 5QI of the QoS flow identified by the QFI; or

c) the QoS flow can be mapped to an EPS bearer as specified in subclause 4.11.1 of 3GPP TS 23.502 [9].

If interworking with EPS is supported for the PDU session, the SMF shall set in the PDU SESSION ESTABLISHMENT ACCEPT message:

a) the Mapped EPS bearer contexts IE to the EPS bearer contexts mapped from one or more QoS flows of the PDU session; and

b) the EPS bearer identity parameter in the Authorized QoS flow descriptions IE to the EPS bearer identity corresponding to the QoS flow, for each QoS flow which can be transferred to EPS.

If the "Create new EPS bearer" operation code in the Mapped EPS bearer contexts IE was received, and there is no corresponding Authorized QoS flow descriptions IE in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall send a PDU SESSION MODIFICATION REQUEST message including a Mapped EPS bearer contexts IE to delete the mapped EPS bearer context. If the EPS bearer identity parameter in the Authorized QoS flow descriptions IE was received, the operation code is "Create new QoS flow description" and there is no corresponding Mapped EPS bearer contexts IE in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall not diagnose an error, and shall keep storing the association between the QoS flow and the corresponding EPS bearer identity.

Furthermore, the SMF shall store the association between the QoS flow and the mapped EPS bearer context, for each QoS flow which can be transferred to EPS.

The SMF shall set the selected SSC mode IE of the PDU SESSION ESTABLISHMENT ACCEPT message to:

a) the received SSC mode in the SSC mode IE included in the PDU SESSION ESTABLISHMENT REQUEST message based on one or more of the PDU session type, the subscription and the SMF configuration;

b) either the default SSC mode for the data network listed in the subscription or the SSC mode associated with the SMF configuration, if the SSC mode IE is not included in the PDU SESSION ESTABLISHMENT REQUEST message.

If the PDU session is an emergency PDU session, the SMF shall set the Selected SSC mode IE of the PDU SESSION ESTABLISHMENT ACCEPT message to "SSC mode 1". If the PDU session is a non-emergency PDU session of "Ethernet" or "Unstructured" PDU session type, the SMF shall set the Selected SSC mode IE to "SSC mode 1" or "SSC mode 2". If the PDU session is a non-emergency PDU session of "IPv4", "IPv6" or "IPv4v6" PDU session type, the SMF shall set the selected SSC mode IE to "SSC mode 1", "SSC mode 2", or "SSC mode 3".

If the PDU session is a non-emergency PDU session and the UE is not registered for onboarding services in SNPN, the SMF shall set the S-NSSAI IE of the PDU SESSION ESTABLISHMENT ACCEPT message to:

a) the S-NSSAI of the PDU session; and

b) the mapped S-NSSAI (if available in roaming scenarios).

The SMF shall set the Selected PDU session type IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the selected PDU session type, i.e. the PDU session type of the PDU session.

If the PDU SESSION ESTABLISHMENT REQUEST message includes a PDU session type IE set to "IPv4v6", the SMF shall select "IPv4", "IPv6" or "IPv4v6" as the Selected PDU session type. If the subscription, the SMF configuration, or both, are limited to IPv4 only or IPv6 only for the DNN selected by the network, the SMF shall include the 5GSM cause value #50 "PDU session type IPv4 only allowed", or #51 "PDU session type IPv6 only allowed", respectively, in the 5GSM cause IE of the PDU SESSION ESTABLISHMENT ACCEPT message.

If the selected PDU session type is "IPv4", the SMF shall include the PDU address IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the PDU address IE to an IPv4 address is allocated to the UE in the PDU session.

If the selected PDU session type is "IPv6", the SMF shall include the PDU address IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the PDU address IE to an interface identifier for the IPv6 link local address allocated to the UE in the PDU session.

If the selected PDU session type is "IPv4v6", the SMF shall include the PDU address IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the PDU address IE to an IPv4 address and an interface identifier for the IPv6 link local address, allocated to the UE in the PDU session.

If the selected PDU session type of a PDU session established by the W-AGF acting on behalf of the FN-RG is "IPv4v6" or "IPv6", the SMF shall also indicate the SMF's IPv6 link local address in the PDU address IE of the PDU SESSION ESTABLISHMENT ACCEPT message.

If the PDU session is a non-emergency PDU session and the UE is not registered for onboarding services in SNPN, the SMF shall set the DNN IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the DNN determined by the AMF of the PDU session.

The SMF shall set the Session-AMBR IE of the PDU SESSION ESTABLISHMENT ACCEPT message to the Session-AMBR of the PDU session.

If the selected PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet" and if the PDU SESSION ESTABLISHMENT REQUEST message includes a 5GSM capability IE with the RQoS bit set to "Reflective QoS supported", the SMF shall consider that reflective QoS is supported for QoS flows belonging to this PDU session and may include the RQ timer IE set to an RQ timer value in the PDU SESSION ESTABLISHMENT ACCEPT message.

If the selected PDU session type is "IPv4", "IPv6", "IPv4v6" or "Ethernet" and if the PDU SESSION ESTABLISHMENT REQUEST message includes a Maximum number of supported packet filters IE, the SMF shall consider this number as the maximum number of packet filters that can be supported by the UE for this PDU session. Otherwise the SMF considers that the UE supports 16 packet filters for this PDU session.

The SMF shall consider that the maximum data rate per UE for user-plane integrity protection supported by the UE for uplink and the maximum data rate per UE for user-plane integrity protection supported by the UE for downlink are valid for the lifetime of the PDU session.

If the value of the RQ timer is set to "deactivated" or has a value of zero, the UE considers that RQoS is not applied for this PDU session.

NOTE 2: If the 5G core network determines that reflective QoS is to be used for a QoS flow, the SMF sends reflective QoS indication (RQI) to UPF to activate reflective QoS. If the QoS flow is established over 3GPP access, the SMF also includes reflective QoS Attribute (RQA) in QoS profile of the QoS flow during QoS flow establishment.

If the selected PDU session type is "IPv6" or "IPv4v6" and if the PDU SESSION ESTABLISHMENT REQUEST message includes a 5GSM capability IE with the MH6-PDU bit set to "Multi-homed IPv6 PDU session supported", the SMF shall consider that this PDU session is supported to use multiple IPv6 prefixes.

If the selected PDU session type is "Ethernet", the PDU SESSION ESTABLISHMENT REQUEST message includes a 5GSM capability IE with the EPT-S1 bit set to "Ethernet PDN type in S1 mode supported" and the network supports Ethernet PDN type in S1 mode, the SMF shall set the EPT-S1 bit of the 5GSM network feature support IE of the PDU SESSION ESTABLISHMENT ACCEPT message to "Ethernet PDN type in S1 mode supported".

If the DN authentication of the UE was performed and completed successfully, the SMF shall set the EAP message IE of the PDU SESSION ESTABLISHMENT ACCEPT message to an EAP-success message as specified in IETF RFC 3748 [34], provided by the DN.

Based on local policies or configurations in the SMF and the Always-on PDU session requested IE in the PDU SESSION ESTABLISHMENT REQUEST message (if available), if the SMF determines that either:

a) the requested PDU session needs to be established as an always-on PDU session (e.g. because the PDU session is for time synchronization or TSC, for URLLC, or for both), the SMF shall include the Always-on PDU session indication IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the value to "Always-on PDU session required"; or

b) the requested PDU session shall not be established as an always-on PDU session and:

i) if the UE included the Always-on PDU session requested IE, the SMF shall include the Always-on PDU session indication IE in the PDU SESSION ESTABLISHMENT ACCEPT message and shall set the value to "Always-on PDU session not allowed"; or

ii) if the UE did not include the Always-on PDU session requested IE, the SMF shall not include the Always-on PDU session indication IE in the PDU SESSION ESTABLISHMENT ACCEPT message.

If the PDU session is an MA PDU session, the SMF shall include the ATSSS container IE in the PDU SESSION ESTABLISHMENT ACCEPT message. The SMF shall set the content of the ATSSS container IE as specified in 3GPP TS 24.193 [13B]. If the UE requests to establish user plane resources over the second access of an MA PDU session which has already been established over the first access and the parameters associated with ATSSS previously provided to the UE are not to be updated, the "ATSSS container contents" shall not be included in the ATSSS container IE in the PDU SESSION ESTABLISHMENT ACCEPT message.

If the PDU session is a single access PDU session containing the MA PDU session information IE with the value set to "MA PDU session network upgrade is allowed" and:

a) if the SMF decides to establish a single access PDU session, the SMF shall not include the ATSSS container IE in the PDU SESSION ESTABLISHMENT ACCEPT message; or

b) if the SMF decides to establish an MA PDU session, the SMF shall include the ATSSS container IE in the PDU SESSION ESTABLISHMENT ACCEPT message, which indicates to the UE that the requested single access PDU session was established as an MA PDU Session.

If the network decides that the PDU session is only for control plane CIoT 5GS optimization, the SMF shall include the control plane only indication in the PDU SESSION ESTABLISHMENT ACCEPT message.

If:

a) the UE provided the IP header compression configuration IE in the PDU SESSION ESTABLISHMENT REQUEST message; and

b) the SMF supports IP header compression for control plane CIoT 5GS optimization;

the SMF shall include the IP header compression configuration IE in the PDU SESSION ESTABLISHMENT ACCEPT message.

If:

a) the UE provided the Ethernet header compression configuration IE in the PDU SESSION ESTABLISHMENT REQUEST message; and

b) the SMF supports Ethernet header compression for control plane CIoT 5GS optimization;

the SMF shall include the Ethernet header compression configuration IE in the PDU SESSION ESTABLISHMENT ACCEPT message.

If the PDU SESSION ESTABLISHMENT REQUEST included the Requested MBS container IE with the MBS operation set to "Join MBS session", the SMF:

a) shall include the TMGI for the MBS session IDs that the UE is allowed to join, if any, in the Received MBS container IE and shall set the MBS Decision to "MBS join is accepted" for each of those Received MBS information;

b) shall include the TMGI for MBS session IDs that the UE is not allowed to join, if any, in the Received MBS container IE, shall set the MBS Decision to "MBS join is rejected" for each of those Received MBS information and shall set the Rejection cause for each of those Received MBS information with the reason of rejection; and

c) may include in the Received MBS container IE the MBS service area for each MBS session and include in it the MBS TAI list, the NR CGI list or both, that identify the service area(s) for the local MBS service

in the PDU SESSION ESTABLISHMENT ACCEPT message. If the UE has set the Type of MBS session ID to "Source specific IP multicast address" in the Requested MBS container IE for certain MBS session(s) in the PDU SESSION MODIFICATION REQUEST message, the SMF may include the Source IP address information and Destination IP address information in the Received MBS information together with the TMGI for each of those MBS sessions.

NOTE 3: Including the Source IP address information and Destination IP address information in the Received MBS information in that case is to allow the UE to perform the mapping between the requested MBS session ID and the provided TMGI.

NOTE 4: In SNPN, TMGI is used together with NID to identify an MBS Session.

If the request type is "existing PDU session", the SMF shall not perform network slice admission control for the PDU session, except for when EPS counting is not required for the S-NSSAI of the PDU session for network slice admission control and the PDU session is established due to transfer the PDN connection from S1 mode to N1 mode in case of inter-system change.

The SMF shall send the PDU SESSION ESTABLISHMENT ACCEPT message.

Upon receipt of a PDU SESSION ESTABLISHMENT ACCEPT message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, the UE shall stop timer T3580, shall release the allocated PTI value and shall consider that the PDU session was established.

If the PDU session establishment procedure was initiated to perform handover of an existing PDU session between 3GPP access and non-3GPP access, then upon receipt of the PDU SESSION ESTABLISHMENT ACCEPT message the UE shall locally delete any authorized QoS rules, authorized QoS flow descriptions and the parameters provided in the Protocol configuration options IE when in S1 mode or the Extended protocol configuration options IE stored for the PDU session before processing the new received authorized QoS rules, authorized QoS flow descriptions and the parameters provided in the Extended protocol configuration options IE, if any.

NOTE 5: For the case of handover from 3GPP access to non-3GPP access, deletion of the QoS flow descriptions implies deletion of the associated EPS bearer identities, if any, and according to subclause 6.1.4.1 also deletion of the associated EPS bearer contexts. Regarding the reverse direction, for PDU sessions via non-3GPP access the network does not allocate associated EPS bearer identities (see 3GPP TS 23.502 [9], subclause 4.11.1.4.1).

For an MA PDU session already established on a single access, upon receipt of PDU SESSION ESTABLISHMENT ACCEPT message over the other access:

a) the UE shall delete the stored authorized QoS rules;

b) if the authorized QoS flow descriptions IE is included in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall delete the stored authorized QoS flow descriptions; and

c) if the mapped EPS bearer contexts IE is included in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall delete the stored mapped EPS bearer contexts.

The UE shall store the authorized QoS rules, and the session-AMBR received in the PDU SESSION ESTABLISHMENT ACCEPT message for the PDU session. The UE shall also store the authorized QoS flow descriptions if it is included in the Authorized QoS flow descriptions IE of the PDU SESSION ESTABLISHMENT ACCEPT message for the PDU session.

If the number of the authorized QoS rules, the number of the packet filters, or the number of the authorized QoS flow descriptions associated with the PDU session have reached the maximum number supported by the UE upon receipt of a PDU SESSION ESTABLISHMENT ACCEPT message, then the UE may initiate the PDU session release procedure by sending a PDU SESSION RELEASE REQUEST message with 5GSM cause #26 "insufficient resources".

For a PDU session that is being established with the request type set to "initial request", "initial emergency request" or "MA PDU request", or a PDU session that is being transferred from EPS to 5GS and established with the request type set to "existing PDU session" or "existing emergency PDU session" or a PDU session that is being handed over between non-3GPP access and 3GPP access and established with the request type set to "existing PDU session" or "existing emergency PDU session ", the UE shall verify the authorized QoS rules and the authorized QoS flow descriptions provided in the PDU SESSION ESTABLISHMENT ACCEPT message for different types of errors as follows:

a) Semantic errors in QoS operations:

1) When the rule operation is "Create new QoS rule", and the DQR bit is set to "the QoS rule is the default QoS rule" when there's already a default QoS rule.

2) When the rule operation is "Create new QoS rule", and there is no rule with the DQR bit set to "the QoS rule is the default QoS rule".

3) When the rule operation is "Create new QoS rule" and two or more QoS rules associated with this PDU session would have identical precedence values.

4) When the rule operation is an operation other than "Create new QoS rule".

5) When the rule operation is "Create new QoS rule", the DQR bit is set to "the QoS rule is not the default QoS rule", and the UE is in NB-N1 mode.

6) When the rule operation is "Create new QoS rule" and two or more QoS rules associated with this PDU session would have identical QoS rule identifier values.

7) When the rule operation is "Create new QoS rule", the DQR bit is set to "the QoS rule is not the default QoS rule", and the PDU session type of the PDU session is "Unstructured".

8) When the flow description operation is an operation other than "Create new QoS flow description".

9) When the flow description operation is "Create new QoS flow description", the QFI associated with the QoS flow description is not the same as the QFI of the default QoS rule and the UE is NB-N1 mode.

10) When the flow description operation is "Create new QoS flow description", the QFI associated with the QoS flow description is not the same as the QFI of the default QoS rule, and the PDU session type of the PDU session is "Unstructured".

 In case 4, case 5, or case 7 if the rule operation is for a non-default QoS rule, the UE shall send a PDU SESSION MODIFICATION REQUEST message to delete the QoS rule with 5GSM cause #83 "semantic error in the QoS operation".

 In case 8, case 9, or case 10, the UE shall send a PDU SESSION MODIFICATION REQUEST message to delete the QoS flow description with 5GSM cause #83 "semantic error in the QoS operation".

 Otherwise for all the cases above, the UE shall initiate a PDU session release procedure by sending a PDU SESSION RELEASE REQUEST message with 5GSM cause #83 "semantic error in the QoS operation".

b) Syntactical errors in QoS operations:

1) When the rule operation is "Create new QoS rule", the QoS rule is a QoS rule of a PDU session of IPv4, IPv6, IPv4v6 or Ethernet PDU session type, and the packet filter list in the QoS rule is empty.

2) When the rule operation is "Create new QoS rule", the DQR bit is set to "the QoS rule is the default QoS rule", the PDU session type of the PDU session is "Unstructured", and the packet filter list in the QoS rule is not empty.

3) When there are other types of syntactical errors in the coding of the Authorized QoS rules IE or the Authorized QoS flow descriptions IE, such as: a mismatch between the number of packet filters subfield and the number of packet filters in the packet filter list when the rule operation is "delete existing QoS rule" or "create new QoS rule", or the number of packet filters subfield is larger than the maximum possible number of packet filters in the packet filter list (i.e., there is no QoS rule precedence subfield included in the QoS rule IE), the QoS Rule Identifier is set to "no QoS rule identifier assigned", or the QoS flow identifier is set to "no QoS flow identifier assigned".

4) When, the rule operation is "Create new QoS rule", there is no QoS flow description with a QFI corresponding to the QFI of the resulting QoS rule and the UE determines, by using the QoS rule’s QFI as the 5QI, that there is a resulting QoS rule for a GBR QoS flow (as described in 3GPP TS 23.501 [8] table 5.7.4-1).

5) When the flow description operation is "Create new QoS flow description", and the UE determines that there is a QoS flow description of a GBR QoS flow (as described in 3GPP TS 23.501 [8] table 5.7.4-1) which lacks at least one of the mandatory parameters (i.e., GFBR uplink, GFBR downlink, MFBR uplink and MFBR downlink). If the QoS flow description does not include a 5QI, the UE determines this by using the QFI as the 5QI.

 In case 1, case 3 or case 4, if the QoS rule is not the default QoS rule, the UE shall send a PDU SESSION MODIFICATION REQUEST message including a requested QoS rule IE to delete the QoS rule with 5GSM cause #84 "syntactical error in the QoS operation". Otherwise, if the QoS rule is the default QoS rule, the UE shall initiate a PDU session release procedure by sending a PDU SESSION RELEASE REQUEST message with 5GSM cause #84 "syntactical error in the QoS operation".

 In case 2, if the QoS rule is the default QoS rule, the UE shall send a PDU SESSION MODIFICATION REQUEST message including a requested QoS rule IE to delete all the packet filters of the default QoS rule. The UE shall include the 5GSM cause #84 "syntactical error in the QoS operation".

 In case 5, if the default QoS rule is associated with the QoS flow description which lacks at least one of the mandatory parameters, the UE shall initiate a PDU session release procedure by sending a PDU SESSION RELEASE REQUEST message with 5GSM cause #84 "syntactical error in the QoS operation". Otherwise, the UE shall send a PDU SESSION MODIFICATION REQUEST message to delete the QoS flow description which lacks at least one of the mandatory parameters and the associated QoS rule(s), if any, with 5GSM cause #84 "syntactical error in the QoS operation".

NOTE 6: It is not considered an error if the UE determines that after processing all QoS operations on QoS rules and QoS flow descriptions there is a QoS flow description that is not associated with any QoS rule and the UE is not in NB-N1 mode.

c) Semantic errors in packet filters:

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

 If the QoS rule is the default QoS rule, the UE shall initiate a PDU session release procedure by sending a PDU SESSION RELEASE REQUEST message with 5GSM cause #44 "semantic error in packet filter(s)". Otherwise, the UE shall send a PDU SESSION MODIFICATION REQUEST message to delete the QoS rule with 5GSM cause #44 "semantic error in packet filter(s)".

d) Syntactical errors in packet filters:

1) When the rule operation is "Create new QoS rule" and two or more packet filters in the resultant QoS rule would have identical packet filter identifiers.

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

 If the QoS rule is the default QoS rule, the UE shall initiate a PDU session release procedure by sending a PDU SESSION RELEASE REQUEST message with 5GSM cause #45 "syntactical errors in packet filter(s)". Otherwise, the UE shall send a PDU SESSION MODIFICATION REQUEST message to delete the QoS rule with 5GSM cause #45 "syntactical errors in packet filter(s)".

If the Always-on PDU session indication IE is included in the PDU SESSION ESTABLISHMENT ACCEPT message and:

a) the value of the IE is set to "Always-on PDU session required", the UE shall consider the established PDU session as an always-on PDU session; or

b) the value of the IE is set to "Always-on PDU session not allowed", the UE shall not consider the established PDU session as an always-on PDU session.

The UE shall not consider the established PDU session as an always-on PDU session if the UE does not receive the Always-on PDU session indication IE in the PDU SESSION ESTABLISHMENT ACCEPT message.

The UE shall store the mapped EPS bearer contexts, if received in the PDU SESSION ESTABLISHMENT ACCEPT message. Furthermore, the UE shall also store the association between the QoS flow and the mapped EPS bearer context, for each QoS flow which can be transferred to EPS, based on the received EPS bearer identity parameter in Authorized QoS flow descriptions IE and the mapped EPS bearer contexts. The UE shall check each mapped EPS bearer context for different types of errors as follows:

NOTE 7: An error detected in a mapped EPS bearer context does not cause the UE to discard the Authorized QoS rules IE and Authorized QoS flow descriptions IE included in the PDU SESSION ESTABLISHMENT ACCEPT, if any.

a) Semantic error in the mapped EPS bearer operation:

1) When the operation code is an operation code other than "Create new EPS bearer".

2) When the operation code is "Create new EPS bearer" and there is already an existing mapped EPS bearer context with the same EPS bearer identity associated with any PDU session.

3) When the operation code is "Create new EPS bearer" and the resulting mapped EPS bearer context has invalid or missing mandatory parameters (e.g., mapped EPS QoS parameters or traffic flow template for a dedicated EPS bearer context).

 In case 2, if the existing mapped EPS bearer context is associated with the PDU session that is being established, the UE shall not diagnose an error, further process the create request and, if it was process successfully, delete the old EPS bearer context.

 Otherwise, the UE shall initiate a PDU session modification procedure by sending a PDU SESSION MODIFICATION REQUEST message to delete the mapped EPS bearer context with 5GSM cause #85 "Invalid mapped EPS bearer identity".

b) if the mapped EPS bearer context includes a traffic flow template, the UE shall check the traffic flow template for different types of TFT IE errors as follows:

1) Semantic errors in TFT operations:

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

 The UE shall initiate a PDU session modification procedure by sending a PDU SESSION MODIFICATION REQUEST message to delete the mapped EPS bearer context with 5GSM cause #41 "semantic error in the TFT operation".

2) Syntactical errors in TFT operations:

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

ii) When there are other types of syntactical errors in the coding of the TFT IE, such as a mismatch between the number of packet filters subfield, and the number of packet filters in the packet filter list when the rule operation is "delete existing QoS rule" or "create new QoS rule", or the number of packet filters subfield is larger than the maximum possible number of packet filters in the packet filter list (i.e., there is no QoS rule precedence subfield included in the QoS rule IE).

 The UE shall initiate a PDU session modification procedure by sending a PDU SESSION MODIFICATION REQUEST message with to delete the mapped EPS bearer context 5GSM cause #42 "syntactical error in the TFT operation".

3) Semantic errors in packet filters:

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

ii) When the resulting TFT does not contain any packet filter which applicable for the uplink direction.

 The UE shall initiate a PDU session modification procedure by sending a PDU SESSION MODIFICATION REQUEST message to delete the mapped EPS bearer context with 5GSM cause #44 "semantic errors in packet filter(s)".

4) Syntactical errors in packet filters:

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

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

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

 In case ii, if the old packet filters do not belong to the default EPS bearer context, the UE shall not diagnose an error and shall delete the old packet filters which have identical filter precedence values.

 In case ii, if one or more old packet filters belong to the default EPS bearer context, the UE shall initiate a PDU session modification procedure by sending a PDU SESSION MODIFICATION REQUEST message to delete the mapped EPS bearer context with 5GSM cause #45 "syntactical errors in packet filter(s)".

 In cases i and iii the UE shall initiate a PDU session modification procedure by sending a PDU SESSION MODIFICATION REQUEST message to delete the mapped EPS bearer context with 5GSM cause #45 "syntactical error in packet filter(s)".

If the UE detects different errors in the mapped EPS bearer contexts, QoS rules or QoS flow descriptions, the UE may send a single PDU SESSION MODIFICATION REQUEST message to delete the erroneous mapped EPS bearer contexts, QoS rules or QoS flow descriptions. In that case, the UE shall include a single 5GSM cause in the PDU SESSION MODIFICATION REQUEST message.

NOTE 8: The 5GSM cause to use cannot be different from: #41 "semantic error in the TFT operation", #42 "syntactical error in the TFT operation", #44 "semantic error in packet filter(s)", #45 "syntactical errors in packet filter(s)", #83 "semantic error in the QoS operation", #84 "syntactical error in the QoS operation", and #85 "Invalid mapped EPS bearer identity". The selection of a 5GSM cause is up to the UE implementation.

If there are mapped EPS bearer context(s) associated with a PDU session, but none of them is associated with the default QoS rule, the UE shall locally delete the mapped EPS bearer context(s) and shall locally delete the stored EPS bearer identity (EBI) in all the QoS flow descriptions of the PDU session, if any.

The UE shall only use the Control plane CIoT 5GS optimization for this PDU session if the Control plane only indication is included in the PDU SESSION ESTABLISHMENT ACCEPT message.

If the UE requests the PDU session type "IPv4v6" and:

a) the UE receives the selected PDU session type set to "IPv4" and does not receive the 5GSM cause value #50 "PDU session type IPv4 only allowed"; or

b) the UE receives the selected PDU session type set to "IPv6" and does not receive the 5GSM cause value #51 "PDU session type IPv6 only allowed";

the UE may subsequently request another PDU session for the other IP version using the UE-requested PDU session establishment procedure to the same DNN (or no DNN, if no DNN was indicated by the UE) and the same S-NSSAI associated with (if available in roaming scenarios) a mapped S-NSSAI (or no S-NSSAI, if no S-NSSAI was indicated by the UE) with a single address PDN type (IPv4 or IPv6) other than the one already activated.

If the UE requests the PDU session type "IPv4v6", receives the selected PDU session type set to "IPv4" and the 5GSM cause value #50 "PDU session type IPv4 only allowed", the UE shall not subsequently request another PDU session using the UE-requested PDU session establishment procedure to the same DNN (or no DNN, if no DNN was indicated by the UE) and the same S-NSSAI associated with (if available in roaming scenarios) a mapped S-NSSAI (or no S-NSSAI, if no S-NSSAI was indicated by the UE) to obtain a PDU session type different from the one allowed by the network until any of the following conditions is fulfilled:

a) the UE is registered to a new PLMN;

b) the UE is switched off; or

c) the USIM is removed or the entry in the "list of subscriber data" for the current SNPN is updated.

If the UE requests the PDU session type "IPv4v6", receives the selected PDU session type set to "IPv6" and the 5GSM cause value #51 "PDU session type IPv6 only allowed", the UE shall not subsequently request another PDU session using the UE-requested PDU session establishment procedure to the same DNN (or no DNN, if no DNN was indicated by the UE) and the same S-NSSAI associated with (if available in roaming scenarios) a mapped S-NSSAI (or no S-NSSAI, if no S-NSSAI was indicated by the UE) to obtain a PDU session type different from the one allowed by the network until any of the following conditions is fulfilled:

a) the UE is registered to a new PLMN;

b) the UE is switched off; or

c) the USIM is removed or the entry in the "list of subscriber data" for the current SNPN is updated.

NOTE 9: For the 5GSM cause values #50 "PDU session type IPv4 only allowed", and #51 "PDU session type IPv6 only allowed", re-attempt in S1 mode for the same DNN (or no DNN, if no DNN was indicated by the UE) is only allowed using the PDU session type(s) indicated by the network.

If the selected PDU session type of the PDU session is "Unstructured" or "Ethernet", the UE supports inter-system change from N1 mode to S1 mode, the UE does not support establishment of a PDN connection for the PDN type set to "non-IP" in S1 mode, and the parameters list field of one or more authorized QoS flow descriptions received in the Authorized QoS flow descriptions IE of the PDU SESSION ESTABLISHMENT ACCEPT message contains an EPS bearer identity (EBI), then the UE shall locally remove the EPS bearer identity (EBI) from the parameters list field of such one or more authorized QoS flow descriptions. Additionally the UE shall also initiate a PDU session modification procedure by sending a PDU SESSION MODIFICATION REQUEST message to delete the mapped EPS bearer context with 5GSM cause #85 "Invalid mapped EPS bearer identity".

If the selected PDU session type of the PDU session is "Ethernet", the UE supports inter-system change from N1 mode to S1 mode, the UE does not support establishment of a PDN connection for the PDN type set to "non-IP" in S1 mode, the UE, the network or both of them do not support Ethernet PDN type in S1 mode, and the parameters list field of one or more authorized QoS flow descriptions received in the Authorized QoS flow descriptions IE of the PDU SESSION ESTABLISHMENT ACCEPT message contains an EPS bearer identity (EBI), then the UE shall locally remove the EPS bearer identity (EBI) from the parameters list field of such one or more authorized QoS flow descriptions. Additionally, the UE shall also initiate a PDU session modification procedure by sending a PDU SESSION MODIFICATION REQUEST message to delete the mapped EPS bearer context with 5GSM cause #85 "Invalid mapped EPS bearer identity".

If the UE receives an IPv4 Link MTU parameter, an Ethernet Frame Payload MTU parameter, an Unstructured Link MTU parameter, or a Non-IP Link MTU parameter in the Extended protocol configuration options IE of the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall pass to the upper layer the received IPv4 link MTU size, the received Ethernet frame payload MTU size, the unstructured link MTU size, or the non-IP link MTU size.

NOTE 10: The IPv4 link MTU size corresponds to the maximum length of user data packet that can be sent either via the control plane or via N3 interface for a PDU session of the "IPv4" PDU session type.

NOTE 11: The Ethernet frame payload MTU size corresponds to the maximum length of a payload of an Ethernet frame that can be sent either via the control plane or via N3 interface for a PDU session of the "Ethernet" PDU session type.

NOTE 12: The unstructured link MTU size correspond to the maximum length of user data packet that can be sent either via the control plane or via N3 interface for a PDU session of the "Unstructured" PDU session type.

NOTE 13: A PDU session of "Ethernet" or "Unstructured" PDU session type can be transferred to a PDN connection of "non-IP" PDN type, thus the UE can request the non-IP link MTU parameter in the PDU session establishment procedure. The non-IP link MTU size corresponds to the maximum length of user data that can be sent either in the user data container in the ESM DATA TRANSPORT message or via S1-U interface as specified in 3GPP TS 24.301 [15].

If the 5G-RG receives an ACS information parameter in the Extended protocol configuration options IE of the PDU SESSION ESTABLISHMENT ACCEPT message, the 5G-RG shall pass the ACS URL in the received ACS information parameter to the upper layer.

If the UE has indicated support for CIoT 5GS optimizations and receives a small data rate control parameters container in the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall store the small data rate control parameters value and use the stored small data rate control parameters value as the maximum allowed limit of uplink user data for the PDU session in accordance with 3GPP TS 23.501 [8].

If the UE has indicated support for CIoT 5GS optimizations and receives an additional small data rate control parameters for exception data container in the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall store the additional small data rate control parameters for exception data value and use the stored additional small data rate control parameters for exception data value as the maximum allowed limit of uplink exception data for the PDU session in accordance with 3GPP TS 23.501 [8].

If the UE has indicated support for CIoT 5GS optimizations and receives an initial small data rate control parameters container or an initial additional small data rate control parameters for exception data container in the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall use these parameters for the newly established PDU Session. When the validity period of the initial parameters expire, the parameters received in a small data rate control parameters container or an additional small data rate control parameters for exception data container shall be used.

If the UE receives a Serving PLMN rate control IE in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall store the Serving PLMN rate control IE value and use the stored serving PLMN rate control value as the maximum allowed limit of uplink control plane user data for the corresponding PDU session in accordance with 3GPP TS 23.501 [8].

If the UE receives an APN rate control parameters container or an additional APN rate control for exception data parameters container in the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall store these parameters and use them to limit the rate at which it generates uplink user data messages for the PDN connection corresponding to the PDU session if the PDU session is transferred to EPS upon inter-system change from N1 mode to S1 mode in accordance with 3GPP TS 24.301 [15]. The received APN rate control parameters and additional APN rate control for exception data parameters shall replace any previously stored APN rate control parameters and additional APN rate control for exception data parameters, respectively, for this PDN connection.

If the UE receives an initial APN rate control parameters container or an initial additional APN rate control for exception data parameters container in the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message, the UE shall store these parameters in the APN rate control status and use them to limit the rate at which it generates exception data messages for the PDN connection corresponding to the PDU session if the PDU session is transferred to EPS upon inter-system change from N1 mode to S1 mode in accordance with 3GPP TS 24.301 [15]. The received APN rate control status shall replace any previously stored APN rate control status for this PDN connection.

NOTE 14: In the PDU SESSION ESTABLISHMENT ACCEPT message, the SMF provides either APN rate control parameters container, or initial APN rate control parameters container, in the Extended protocol configuration options IE, but not both.

NOTE 15: In the PDU SESSION ESTABLISHMENT ACCEPT message, the SMF provides either additional APN rate control for exception data parameters container, or initial additional APN rate control for exception data parameters container, in the Extended protocol configuration options IE, but not both.

If the network accepts the use of Reliable Data Service to transfer data for the PDU session, the network shall include the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message and include the Reliable Data Service accepted indicator. The UE behaves as described in subclause 6.2.15.

If the UE indicates support of DNS over (D)TLS by providing DNS server security information indicator to the network and optionally, if the UE wishes to indicate which security protocol type(s) are supported by the UE, providing the DNS server security protocol support and the network wants to enforce the use of DNS over (D)TLS, the network may include the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message and include the DNS server security information with length of two octets. Upon receiving the DNS server security information, the UE shall pass it to the upper layer. The UE shall use this information to send the DNS over (D)TLS (See 3GPP TS 33.501 [24]).

NOTE 16: Support of DNS over (D)TLS is based on the informative requirements as specified in 3GPP TS 33.501 [24] and it is implemented based on the operator requirement.

If the PDU SESSION ESTABLISHMENT REQUEST message includes the Service-level-AA container IE with the service-level device ID set to the CAA-level UAV ID, and the SMF is provided by the UAS-NF the successful UUAA-SM resultand the authorized CAA-level UAV ID, the SMF shall store the successful result together with the authorized CAA-level UAV ID and transmit the PDU SESSION ESTABLISHMENT ACCEPT message to the UE, where the PDU SESSION ESTABLISHMENT ACCEPT message shall include the Service-level-AA container IE containing:

a) the service-level-AA response, with the value to the service-level-AA result, set to "Service level authentication and authorization was successful";

b) if a new CAA-Level UAV ID is provided by the UAS-NF, the service-level device ID with the value set to the new CAA-level UAV ID; and

c) if received the UUAA authorization payload from the UAS-NF:

1) the service-level-AA payload type, with the values set to "UUAA payload"; and

2) the service-level-AA payload, with the value set to the UUAA authorization payload.

NOTE 17: UAS security information can be included in the UUAA authorization payload by the USS as specified in 3GPP TS 33.256 [23B].

If the network accepts establishment of the PDU session for C2 communication, the network shall include the Service-level-AA container IE in the PDU SESSION ESTABLISHMENT ACCEPT message. The Service-level-AA container IE:

a) includes C2 authorization result;

b) can include C2 session security information; and

c) can include service-level device ID with the value set to a new CAA-level UAV ID.

Upon receipt of the PDU SESSION ESTABLISHMENT ACCEPT message of the PDU session for C2 communication, if the Service-level-AA container IE is included and it contains a CAA-level UAV ID and the C2 authorization result, the UE shall replace its currently stored CAA-level UAV ID with the new CAA-level UAV ID.

The SMF may be configured with one or more PVS IP addresses or PVS names associated with the DNN and S-NSSAI used for onboarding services in SNPN, for configuration of SNPN subscription parameters in PLMN via the user plane, or for configuration of a UE in PLMN via the user plane with credentials for NSSAA or PDU session authentication and authorization procedure. If the PDU session was established for onboarding services in SNPN, or for configuration of SNPN subscription parameters in PLMN via the user plane, the network may include the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message and include the PVS IP address(es) or the PVS name(s) or both associated with the DNN and S-NSSAI of the established PDU session, if available. If the PDU session was established for configuration of a UE in PLMN via the user plane with credentials for NSSAA or PDU session authentication and authorization procedure, based on the subscribed DNN(s) and S-NSSAI(s) of the UE and the DNN and S-NSSAI of the established PDU session, the network should include the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message and include the PVS IP address(es) or the PVS name(s) or both, which are associated with the established PDU session and per subscribed DNN(s) and S-NSSAI(s) of the UE, if available.

NOTE 18: If the PDU session is established for configuration of SNPN subscription parameters in PLMN via the user plane, the DNN and S-NSSAI of the PDU session can only be used for configuration of SNPN subscription parameters in PLMN via the user plane.

If the UE indicates support for ECS configuration information provisioning by providing the ECS configuration information provisioning support indicator in the Extended protocol configuration options IE of the PDU SESSION ESTABLISHMENT REQUEST message, then the SMF may include the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message with at least one of ECS IPv4 Address, ECS IPv6 Address, and ECS FQDN included and may include an ECS provider identifier. The SMF may include spatial validity condition along with the ECS IPv4 Address, ECS IPv6 Address, or ECS FQDN respectively in the Extended protocol configuration options IE, if available. The UE upon receiving one or more ECS IPv4 address(es), if any, ECS IPv6 address(es), if any, or ECS FQDN(s), if any, an ECS provider identifier, if any, and the spatial validity condition associated with the ECS IPv4 Address, ECS IPv6 Address, or ECS FQDN respectively, if any, shall pass them to the upper layers.

NOTE 19: If an ECS provider identifier is included, then the IP address(es) and/or FQDN(s) are associated with the ECS provider identifier.

If the SMF needs to provide DNS server address(es) to the UE and the UE has provided the DNS server IPv4 address request, the DNS server IPv6 address request or both of them, in the PDU SESSION ESTABLISHMENT REQUEST message, then the SMF shall include the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message with one or more DNS server IPv4 address(es), one or more DNS server IPv6 address(es) or both of them. If the UE supports receiving DNS server addresses in protocol configuration options and receives one or more DNS server IPv4 address(es), one or more DNS server IPv6 address(es) or both of them, in the Extended protocol configuration options IE of the PDU SESSION ESTABLISHMENT ACCEPT message, then the UE shall pass the received DNS server IPv4 address(es), if any, and the received DNS server IPv6 address(es), if any, to upper layers.

NOTE 20: The received DNS server address(es) replace previously provided DNS server address(es), if any.

If the PDU session is established for IMS signalling and the UE has requested P-CSCF IPv6 address or P-CSCF IPv4 address, the SMF shall include P-CSCF IP address(es) in the Extended protocol configuration options IE in the PDU SESSION ESTABLISHMENT ACCEPT message.

NOTE 21: The P-CSCF selection functionality is specified in subclause 5.16.3.11 of 3GPP TS 23.501 [8].

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of Changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*