# ETSI TS 129 514 V17.11.0 (2024-04)


**5G;**
**5G System;**
**Policy Authorization Service;**
**Stage 3**
**(3GPP TS 29.514 version 17.11.0 Release 17)**

Reference
RTS/TSGC-0329514vhb0

Keywords
5G

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

# Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

# Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present specification provides the stage 3 definition of the Policy Authorization Service of the 5G System.

The 5G System Architecture is defined in 3GPP TS 23.501 [2]. The stage 2 definition and related procedures for the Npcf Policy Authorization Service are specified in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

The 5G System stage 3 call flows are provided in 3GPP TS 29.513 [7].

The Technical Realization of the Service Based Architecture and the Principles and Guidelines for Services Definition are specified in 3GPP TS 29.500 [5] and 3GPP TS 29.501 [6].

The Policy Authorization Service is provided by the Policy Control Function (PCF). This service creates policies as requested by the authorised AF for the PDU Session to which the AF session is bound.

# 2 References

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

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

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

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

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

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

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

[6] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[7] 3GPP TS 29.513: "5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3".

[8] 3GPP TS 29.512: "5G System; Session Management Policy Control Service; Stage 3".

[9] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[10] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[11] OpenAPI: "OpenAPI Specification Version 3.0.0", https://spec.openapis.org/oas/v3.0.0..

[12] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[13] 3GPP TS 29.508: "5G System; Session Management Event Exposure Service; Stage 3".

[14] 3GPP TS 29.554: "5G System; Background Data Transfer Policy Control Service; Stage 3".

[15] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

[16] IEEE 802.3-2015: "IEEE Standard for Ethernet".

[17] IEEE 802.1Q-2014: "Bridges and Bridged Networks".

[18] IETF RFC 7042: "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters".

[19] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[20] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[21] IETF RFC 7396: "JSON Merge Patch".

[22] 3GPP TS 32.291: "5G System; Charging service; Stage 3".

[23] 3GPP TS 22.153: "5G System; "Multimedia Priority Service".

[24] IETF RFC 7807: "Problem Details for HTTP APIs".

[25] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[26] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[27] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

[28] 3GPP TR 21.900: "Technical Specification Group working methods".

[29] 3GPP TS 24.292: "IP Multimedia (IM) Core Network (CN) subsystem Centralized Services (ICS); Stage 3".

[30] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction".

[31] IETF RFC 5761: "Multiplexing RTP Data and Control Packets on a Single Port".

[32] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[33] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[34] IETF RFC 5031: "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services".

[35] IETF RFC 5009: "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".

[36] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[37] IETF RFC 3556: "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[38] IETF RFC 3959 (December 2004): "The Early Session Disposition Type for the Session Initiation Protocol (SIP)".

[39] 3GPP TS 23.380: "IMS Restoration Procedures".

[40] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[41] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Protocol specification".

[42] IETF RFC 8101: "IANA Registration of New Session Initiation Protocol (SIP), Resource-Priority Namespace for Mission Critical Push To Talk Service".

[43] 3GPP TS 24.281: "Mission Critical Video (MCVideo) signalling control; Protocol specification".

[44] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[45] 3GPP TS 22.179: "Mission Critical Push to Talk (MCPTT) over LTE; Stage 1".

[46] 3GPP TS 22.280: "Mission Critical (MC) services common requirements".

[47] 3GPP TS 22.281: "Mission Critical (MC) video over LTE".

[48] 3GPP TS 22.282: "Mission Critical (MC) data over LTE".

[49] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[50] IETF RFC 4574: "The Session Description Protocol (SDP) Label Attribute".

[51] 3GPP TS 26.238: "Uplink Streaming".

[52] IETF RFC 6733: "Diameter Base Protocol".

[53] 3GPP TS 29.519: "5G System; Usage of the Unified Data Repository service for Policy Control Data, Application Data and Structured Data for Exposure; Stage 3".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Application Function (AF)**: Element offering application(s) that use PDU session resources.

**AF Application identifier:** An identifier that refers to the particular service the NF service consumer session belongs to. In the context of application detection control, it refers to the application identifier used by the PCF in the PCC rule as specified in 3GPP TS 29.512 [8].

**AF application session context:** Application level session context established by an application level signalling protocol offered by the AF that requires a session context set-up with explicit session context description before the use of the service.

**MCS session:** A session for which priority treatment is applied for allocating and maintaining radio and network resources to support the Mission Critical Service (MCS). MCS is defined in 3GPP TS 22.179 [45], 3GPP TS 22.280 [46], 3GPP TS 22.281 [47], and 3GPP TS 22.282 [48].

**MPS session:** A session for which priority treatment is applied for allocating and maintaining radio and network resources to support the Multimedia Priority Service (MPS). MPS is defined in 3GPP TS 22.153 [23].

**PCC rule:** Set of information enabling the detection of a service data flow and providing parameters for policy control and/or charging control.

**Service information:** Set of information conveyed from the AF/NEF to the PCF by the Npcf_PolicyAuthorization service to be used as a basis for PCC decisions at the PCF, including information about the AF/NEF application session context (e.g. application identifier, type of media, bandwidth, IP address and port number).

**Service data flow:** An aggregate set of packet flows.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

| | |
|---|---|
| 5G-RG | 5G Residential Gateway |
| AF | Application Function |
| ARP | Allocation and Retention Priority |
| ATSSS | Access Traffic Steering, Switching and Splitting |
| BBF | Broadband Forum |
| BSSID | Basic Service Set IDentifier |
| CHEM | Coverage and Handoff Enhancements using Multimedia error robustness feature |
| CHF | Charging Function |

| | |
|---|---|
| DCCF | Data Collection Coordination Function |
| DEI | Drop Eligible Indicator |
| DNAI | DN Access Identifier |
| DNN | Data Network Name |
| DS-TT | Device-side TSN translator |
| DSL | Digital Subscriber Line |
| DTS | Data Transport Service |
| EAS | Edge Application Server |
| ePDG | evolved Packet Data Gateway |
| E-UTRA | Evolved Universal Terrestrial Radio Access |
| FLUS | Framework for Live Uplink Streaming |
| FN-RG | Fixed Network Residential Gateway |
| GEO | Geosynchronous Orbit |
| GPSI | Generic Public Subscription Identifier |
| HFC | Hybrid Fiber-Coaxial |
| H-PCF | PCF in the HPLMN |
| IMS | IP-Multimedia Subsystem |
| JSON | JavaScript Object Notation |
| LEO | Low Earth Orbit |
| MA | Multi-Access |
| MCPTT | Mission Critical Push to Talk Service |
| MCVideo | Mission Critical Video |
| MEO | Medium Earth Orbit |
| MPS | Multimedia Priority Service |
| NEF | Network Exposure Function |
| NID | Network Identifier |
| NR | New Radio |
| NRF | Network Repository Function |
| NWDAF | Network Data Analytics Function |
| NW-TT | Network-side TSN translator |
| PCC | Policy and Charging Control |
| PCF | Policy Control Function |
| PCP | Priority Code Point |
| P-CSCF | Proxy Call Session Control Function |
| PEI | Permanent Equipment Identifier |
| PMIC | Port Management Information Container |
| PON | Passive Optical Network |
| PRA | Presence Reporting Area |
| PSA | PDU Session Anchor |
| QoS | Quality of Service |
| RFSP | RAT Frequency Selection Priority |
| RTCP | Real Time Control Protocol |
| RTP | Real Time Protocol |
| SDF | Service Data Flow |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SMF | Session Management Function |
| S-NSSAI | Single Network Slice Selection Assistance Information |
| SNPN | Stand-alone Non-Public Network |
| SSID | Service Set IDentifier |
| SUPI | Subscription Permanent Identifier |
| TNAP | Trusted Non-3GPP Access Point |
| TSC | Time Sensitive Communication |
| TSCAI | Time Sensitive Communication Assistance Information |
| TSCTSF | Time Sensitive Communication and Time Synchronization Function |
| TSN | Time Sensitive Networking |
| UDR | Unified Data Repository |
| UMIC | User plane node Management Information Container |
| UPF | User Plane Function |
| URSP | UE Route Selection Policy |
| VID | VLAN Identifier |
| VLAN | Virtual Local Area Network |

| | |
|---|---|
| V-PCF | PCF in the VPLMN |
| W-5GAN | Wireline 5G Access Network |
| W-5GBAN | Wireline 5G BBF Access Network |
| W-5GCAN | Wireline 5G Cable Access Network |
| W-AGF | Wireline Access Gateway Function |

# 4 Npcf_PolicyAuthorization Service

## 4.1 Service Description

### 4.1.1 Overview

The Npcf_PolicyAuthorization Service, as defined in 3GPP TS 23.502 [3] and in 3GPP TS 23.503 [4], is provided by the Policy Control Function (PCF).

The Npcf_PolicyAuthorization service authorises a NF service consumer request and creates policies as requested by the authorised NF service consumer for the PDU session to which the AF session is bound to. This service also allows the NF service consumer to subscribe/unsubscribe to notifications on events (e.g. access type change, PLMN change, usage report, access network information report).

### 4.1.2 Service Architecture

The 5G System Architecture is defined in 3GPP TS 23.501 [2]. The Policy and Charging control related 5G architecture is also described in 3GPP TS 23.503 [4] and 3GPP TS 29.513 [7].

The only known NF service consumers of the Npcf_PolicyAuthorization service are the Application Function (AF), the Network Exposure Function (NEF), the Time Sensitive Communication and Time Synchronization Function (TSCTSF) and the Policy Control Function for the UE (PCF for the UE).

The Npcf_PolicyAuthorization service is provided by the PCF and consumed by the AF, the NEF, the TSCTSF and, when the PCF for the PDU session and the PCF for the UE are different, the PCF for the UE, as shown in figure 4.1.2-1 for the SBI representation model and in figure 4.1.2-2 for the reference point representation model.

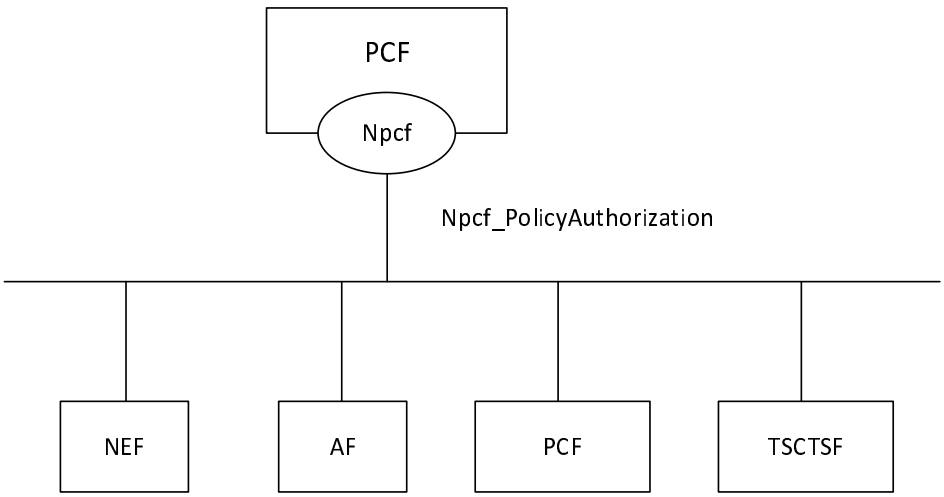


**Figure 4.1.2-1: Npcf_PolicyAuthorization service Architecture, SBI representation**

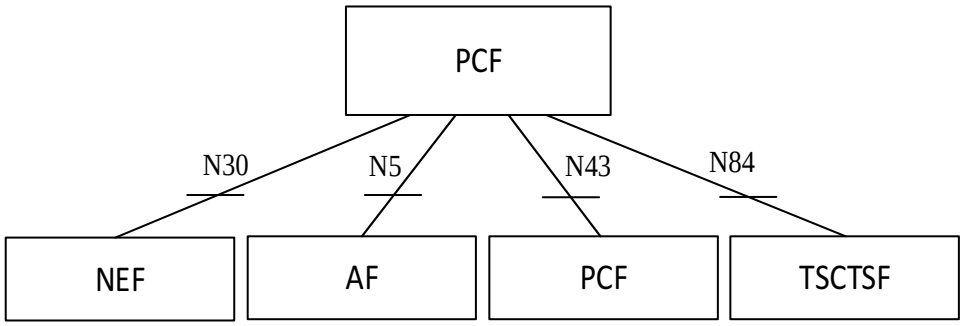


**Figure 4.1.2-2: Npcf_PolicyAuthorization service Architecture, reference point representation**

NOTE: When the N43 reference point exists, i.e. when the PCF is a NF service consumer of the Npcf_PolicyAuthorization service, the PCF for the UE interacts with the PCF for the PDU session.

## 4.1.3 Network Functions

### 4.1.3.1 Policy Control Function (PCF)

The PCF (Policy Control Function) is a functional element that encompasses:

- policy control decision and flow based charging control functionalities;
- access and mobility policy decisions for the control of e.g. the UE Service Area Restrictions and RAT/RFSP control; and
- UE Policy for the Access network discovery and selection policy and UE Route Selection Policy (URSP).

The policy control decision and flow based charging control functionalities enable the PCF to provide network control regarding the service data flow detection, gating, QoS and flow based charging (except credit management) towards the SMF/UPF.

The PCF receives session and media related information from the Npcf_PolicyAuthorization service consumers and notifies them of subscribed traffic plane events.

The PCF may receive from the NF service consumers the request to monitor the requested service and media information and notifies them of the UL/DL/round-trip delay of the requested flows.

The PCF may receive service routing requirements and the indication of receiving notifications about user plane path changes from the Npcf_PolicyAuthorization service consumers.

The PCF may receive from the NF service consumers the specific required QoS and a prioritized list of alternative QoS profiles and notifies them about the QoS target the access network guarantees.

The PCF checks that the service information provided by the NF service consumer is consistent with the operator defined policy rules before storing the service information.

The PCF uses the received service information and the subscription information when it applies as basis for the policy and charging control decisions.

The PCF derives PCC rules and provisions them to the SMF via the Npcf_SMPolicyControl service and subscribes to traffic plane events via policy control request triggers as described in 3GPP TS 29.512 [8].

In 5GS interworking with external time sensitive networks (e.g.TSN network), the PCF:

- notifies the NF service consumer (i.e. TSN AF or TSCTSF) about the TSC user plane node and DS-TT port information corresponding to a PDU session;
- enables the NF service consumer (i.e. TSN AF or TSCTSF) configures the TSC user plane node and ports by forwarding TSC user plane node management containers and port management containers to the SMF as described in 3GPP TS 29.512 [8];

- notifies the NF service consumer (i.e. TSN AF or TSCTSF) about updated TSC user plane node configuration and port configuration by forwarding TSN bridge management containers and port management containers received from the SMF; and

- uses the received QoS and TSC assistance information to derive the policy information delivered in the PCC rule to the SMF as described in 3GPP TS 29.512 [8].

#### 4.1.3.2 NF Service Consumers

The known NF service consumers are the AF, the NEF, the TSCTSF and the PCF (for a UE), as defined in 3GPP TS 23.502 [3].

The AF is an element offering control to applications that require the policy and charging control of traffic plane resources; specific user plane paths for the requested traffic, the monitoring of the required service QoS, and/or specific QoS and alternative QoS profiles. The AF uses the Npcf_PolicyAuthorization service to provide service information to the PCF.

In 5GS interworking with TSN networks, the TSN AF is an element offering to TSC control functions an interface to 5GS to forward TSC user plane node and port management configuration, and to set the QoS policy required to forward the TSC traffic making use of the 5GS traffic plane resources.

The AFs can be deployed by the same operator offering the access services or can be provided by external third-party service provider. If the AF is not allowed by the operator to access directly the PCF, the AF uses the external exposure framework via NEF to interact with the PCF, as described in clause 5.20 of 3GPP TS 23.501 [2].

The Network Exposure Function (NEF) supports external exposure of capabilities of network functions.

The AF trusted by the operator or the NEF can use the TSCTSF to interface with PCF to support time sensitive communication and time synchronization. The TSCTSF is an element offering, to internal and/or external time sensitive AF (via NEF), control to handle from/towards the PCF the required TSC user plane node and port management configuration, and to set in the PCF the QoS policy required to forward TSC traffic.

The PCF providing session management policy control for a UE (i.e. PCF for a PDU session) and the PCF providing UE policy control and/or access and mobility control for this same UE (i.e. PCF for a UE) may be different PCFs. When access and mobility policies depend on traffic plane events (as e.g. application detection control), the PCF for a UE may act as an NF service consumer of the PCF for the PDU session by subscribing to such events.

## 4.2 Service Operations

### 4.2.1 Introduction

Service operations defined for the Npcf_PolicyAuthorization Service are shown in table 4.2.1-1.

**Table 4.2.1-1: Npcf_PolicyAuthorization Service Operations**

| Service Operation Name | Description | Initiated by |
|---|---|---|
| Npcf_PolicyAuthorization_Create | Determines and installs the policy according to the service information provided by an authorized NF service consumer. | NF service consumer (e.g. AF, NEF) |
| Npcf_PolicyAuthorization_Update | Determines and updates the policy according to the modified service information provided by an authorized NF service consumer. | NF service consumer (e.g. AF, NEF) |
| Npcf_PolicyAuthorization_Delete | Provides means to delete the application session context of the NF service consumer. | NF service consumer (e.g. AF, NEF) |
| Npcf_PolicyAuthorization_Notify | Notifies NF service consumers of the subscribed events. | PCF |
| Npcf_PolicyAuthorization_Subscribe | Allows NF service consumers to subscribe to the notifications of events. | NF service consumer (e.g. AF, NEF, PCF for a UE) |
| Npcf_PolicyAuthorization_Unsubscribe | Allows NF service consumers to unsubscribe from the notifications of events. | NF service consumer (e.g. AF, NEF, PCF for a UE) |

NOTE 1: The NEF and the AF use the Npcf_PolicyAuthorization service in the same way.

NOTE 2: The PCF is the consumer when the PCF for the UE and the PCF for the PDU session are different in the Npcf_PolicyAuthorization_Notify/Subscribe/Unsubscribe operations.

NOTE 3: The NWDAF and the DCCF can be NF service consumers of the Npcf_PolicyAuthorization_Notify/Subscribe/Unsubscribe operations to perform data collection for UEs. However, there is no data collected from the PCF by the NWDAF or the DCCF defined in this Release of the specification.

## 4.2.2 Npcf_PolicyAuthorization_Create service operation

### 4.2.2.1 General

The Npcf_PolicyAuthorization_Create service operation authorizes the request from the NF service consumer, and optionally communicates with Npcf_SMPolicyControl service to determine and install the policy according to the information provided by the NF service consumer.

The Npcf_PolicyAuthorization_Create service operation creates an application session context in the PCF.

The following procedures using the Npcf_PolicyAuthorization_Create service operation are supported:

- Initial provisioning of service information.
- Gate control.
- Initial Background Data Transfer policy indication.
- Initial provisioning of sponsored connectivity information.
- Subscription to Service Data Flow QoS notification control.
- Subscription to Service Data Flow Deactivation.
- Initial provisioning of traffic routing information.
- Subscription to resources allocation outcome.
- Invocation of Multimedia Priority Services.
- Support of content versioning.
- Request of access network information.
- Initial provisioning of service information status.
- Provisioning of signalling flow information.
- Support of resource sharing.
- Indication of Emergency traffic.
- Invocation of MCPTT.
- Invocation of MCVideo.
- Priority sharing indication.
- Subscription to out of credit notification.
- Subscription to Service Data Flow QoS Monitoring information.
- Provisioning of TSCAI input information and TSC QoS related data.
- Provisioning of TSC user plane node management information and port management information.
- P-CSCF restoration enhancements.

- Support of CHEM feature.
- Support of FLUS feature.
- Subscription to EPS Fallback report.
- Subscription to TSC user plane node related events.
- Initial provisioning of required QoS information.
- Support of QoSHint feature.
- Subscription to reallocation of credit notification.
- Subscription to satellite backhaul category changes.

#### 4.2.2.2 Initial provisioning of service information

This procedure is used to set up an AF application session context for the service as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

Figure 4.2.2.2-1 illustrates the initial provisioning of service information.

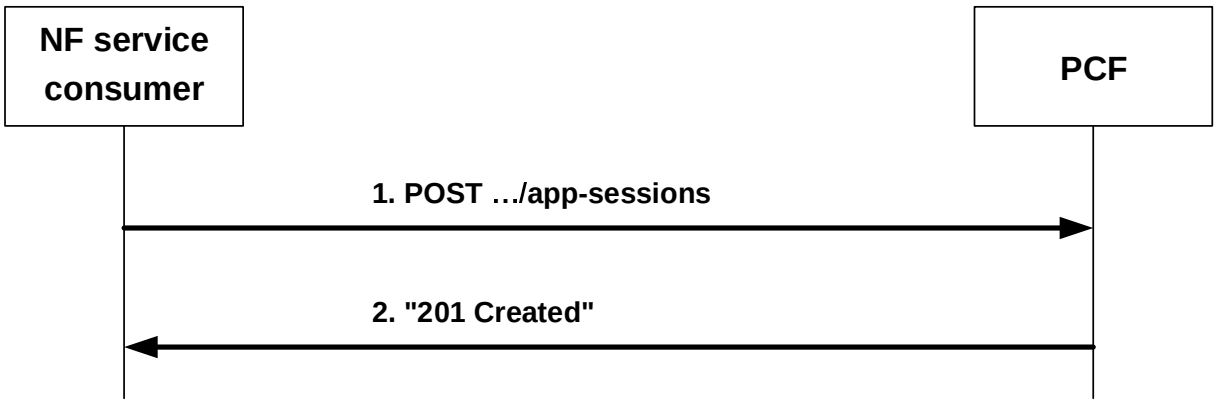


**Figure 4.2.2.2-1: Initial provisioning of service information**

When a new AF application session context is being established and media information for this application session context is available at the NF service consumer and the related media requires PCC control, the NF service consumer shall invoke the Npcf_PolicyAuthorization_Create service operation by sending the HTTP POST request to the resource URI representing the "Application Sessions" collection resource of the PCF, as shown in figure 4.2.2.2-1, step 1.

The NF service consumer shall include in the "AppSessionContext" data type in the payload body of the HTTP POST request a partial representation of the "Individual Application Session Context" resource by providing the "AppSessionContextReqData" data type. The "Individual Application Session Context" resource and the "Events Subscription" sub-resource are created as described below.

The NF service consumer shall provide in the body of the HTTP POST request:

- for IP type PDU sessions, the IP address (IPv4 or IPv6) of the UE in the "ueIpv4" or "ueIpv6" attribute; and
- for Ethernet type PDU sessions, the MAC address of the UE in the "ueMac" attribute.

For Ethernet type PDU sessions, if the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported, the "ueMac" attribute containing the MAC address of the DS-TT port as received from the PCF during the reporting of TSC user plane node information as defined in clause 4.2.5.16.

NOTE 1: The determination of the DS-TT port MAC address is specified in clause 5.28.2 of 3GPP TS 23.501 [2]. The DS-TT port MAC address is used as identifier of the PDU session related to the reported TSC user plane node information.

For IP type PDU sessions, if the "TimeSensitiveCommunication" feature is supported, the "ueIpv4" or "ueIpv6" attribute containing the IPv4 or IPv6 address of the UE as received from the PCF during the reporting of user plane node information as defined in clause 4.2.5.16.

NOTE 2: The IP address of the PDU session is used as identifier of the PDU session related to the reported TSC user plane node information.

The NF service consumer shall provide the corresponding service information in the "medComponents" attribute if available. The AF shall indicate to the PCF as part of the "medComponents" attribute whether the service data flow(s) (IP or Ethernet) should be enabled or disabled with the "fStatus" attribute.

If the "AuthorizationWithRequiredQoS" feature as defined in clause 5.8 is supported, the AF may provide within the MediaComponent data structure required QoS information as specified in clause 4.2.2.32.

The AF may include the AF application identifier in the "afAppId" attribute into the body of the HTTP POST request in order to indicate the particular service that the AF session belongs to.

The AF application identifier may be provided at both "AppSessionContextReqData" data type level, and "MediaComponent" data type level. When provided at both levels, the AF application identifier provided at "MediaComponent" data type level shall have precedence.

The AF application identifier at the "AppSessionContextReqData" data type level may be used to trigger the PCF to indicate to the SMF/UPF to perform the application detection based on the operator's policy as defined in 3GPP TS 29.512 [8].

If the "IMS_SBI" feature is supported, the NF service consumer may include the AF charging identifier in the "afChargId" attribute for charging correlation purposes.

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported the NF service consumer may provide TSC information as specified in clauses 4.2.2.24 and 4.2.2.25.

The NF service consumer may also include the "evSubsc" attribute of "EventsSubscReqData" data type to request the notification of certain user plane events. The NF service consumer shall include the events to subscribe to in the "events" attribute, and the notification URI where to address the Npcf_PolicyAuthorization_Notify service operation in the "notifUri" attribute. The events subscription is provisioned in the "Events Subscription" sub-resource.

The AF shall also include the "notifUri" attribute in the "AppSessionContextReqData" data type to indicate the URI where the PCF can request to the AF the deletion of the "Individual Application Session Context" resource.

If the PCF cannot successfully fulfil the received HTTP POST request due to the internal PCF error or due to the error in the HTTP POST request, the PCF shall send the HTTP error response as specified in clause 5.7.

Otherwise, when the PCF receives the HTTP POST request from the NF service consumer, the PCF shall apply session binding as described in 3GPP TS 29.513 [7]. To allow the PCF to identify the PDU session for which the HTTP POST request applies, the NF service consumer shall provide in the body of the HTTP POST request:

- for IP type PDU session, either the "ueIpv4" attribute or "ueIpv6" attribute containing the IPv4 or the IPv6 address applicable to an IP flow or IP flows towards the UE; and

- for Ethernet type PDU session, the "ueMac" attribute containing the UE MAC address applicable to an Ethernet flow or Ethernet flows towards the UE.

The NF service consumer may provide DNN in the "dnn" attribute, SUPI in the "supi" attribute, GPSI in the "gpsi" attribute, the S-NSSAI in the "sliceInfo" attribute if available for session binding. The NF service consumer may also provide the domain identity in the "ipDomain" attribute.

NOTE 3: The "ipDomain" attribute is helpful in the following scenario: Within a network slice, there are several separate IP address domains, with SMF/UPF(s) that allocate Ipv4 IP addresses out of the same private address range to UE PDU sessions. The same IP address can thus be allocated to UE PDU sessions served by SMF/UPF(s) in different address domains. If one PCF controls several SMF/UPF(s) in different IP address domains, the UE IP address is thus not sufficient for the session binding. A NF service consumer can serve UEs in different IP address domains, either by having direct IP interfaces to those domains, or by having interconnections via NATs in the user plane between the UPF and the NF service consumer. If a NAT is used, the NF service consumer obtains the IP address allocated to the UE PDU session via application level signalling and supplies it for the session binding to the PCF in the "ueIpv4" attribute. The NF service consumer supplies an "ipDomain" attribute denoting the IP address domain behind the NAT in addition. The NF service consumer can derive the appropriate value from the source address (allocated by the NAT) of incoming user plane packets. The value provided in the "ipDomain" attribute is operator configurable.

NOTE 4: The "sliceInfo" attribute is helpful in the scenario where multiple network slices are deployed in the same DNN, and the same IPv4 address may be allocated to UE PDU sessions in different network slices. If one PCF controls several network slices, the UE IP address is not sufficient for the session binding. The NF service consumer supplies "sliceInfo" attribute denoting the network slice that allocated the IPv4 address of the UE PDU session. How the NF service consumer derives S-NSSAI is out of the scope of this specification.

NOTE 5: When the scenario described in NOTE 3 applies and the NF service consumer is a P-CSCF it is assumed that the P-CSCF has direct IP interfaces to the different IP address domains and that no NAT is located between the UPF and P-CSCF. How a non-IMS NF service consumer obtains the UE private IP address to be provided to the PCF is out of scope of the present release; it is unspecified how to support applications that use a protocol that does not retain the original UE's private IP address.

If the PCF fails in executing session binding, the PCF shall reject the Npcf_PolicyAuthorization_Create service operation with an HTTP "500 Internal Server Error" response including the "cause" attribute set to "PDU_SESSION_NOT_AVAILABLE".

If the request contains the "medComponents" attribute the PCF shall store the received service information. The PCF shall process the received service information according to the operator policy and may decide whether the request is accepted or not. The PCF may take the priority information within the "resPrio" attribute into account when making this decision.

If the service information provided in the body of the HTTP POST request is rejected (e.g. the subscribed guaranteed bandwidth for a particular user is exceeded or the authorized data rate in that slice for a UE is exceeded), the PCF shall indicate in an HTTP "403 Forbidden" response message the cause for the rejection including the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED".

If the PCF detects that a temporary network failure has occurred (e.g. the SGW has failed as defined in clause B.3.3.3 or B.3.4.9 of 3GPP TS 29.512 [8]) and the AF initiates an Npcf_PolicyAuthorization_Create service operation, the PCF shall reject the request with an HTTP "403 Forbidden" response including the "cause" attribute set to "TEMPORARY_NETWORK_FAILURE".

If the service information provided in the HTTP POST request is rejected due to a temporary condition in the network (e.g. the NWDAF reported the network slice selected for the PDU session is congested), the PCF may include in the "403 Forbidden" response the "cause" attribute set to "REQUESTED_SERVICE_TEMPORARILY_NOT_AUTHORIZED". The PCF may also provide a retry interval within the "Retry-After" HTTP header field. When the NF service consumer receives the retry interval within the "Retry-After" HTTP header field, the NF service consumer shall not send the same service information to the PCF again (for the same application session context) until the retry interval has elapsed. The "Retry-After" HTTP header is described in 3GPP TS 29.500 [5] clause 5.2.2.2.

NOTE 6: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8] and the authorized data rate for any of those cases in a slice is exceeded due to the bandwidth demands of the new service information, it is also possible to accept the request based on operator policies. In this case the derived PCC rule(s) belonging to the authorized GBR service data flows can include a different MBR and/or have a different charging than the one applicable if the data rate is not exceeded as specified in 3GPP TS 29.512 [8].

The PCF may additionally provide the acceptable bandwidth within the attribute "acceptableServInfo" included in the "ExtendedProblemDetails" data structure returned in the rejection response message.

To allow the PCF and SMF/UPF to perform PCC rule authorization and QoS flow binding for the described service data flows, the NF service consumer shall supply:

- for IP type PDU session, both source and destination IP addresses and port numbers in the "fDescs" attribute within the "medSubComps" attribute, if such information is available; and

- for Ethernet type PDU session, the Ethernet Packet filters in the "ethfDescs" attribute within the "medSubComps" attribute, if such information is available.

The NF service consumer may specify the ToS traffic class (i.e. ToS (IPv4) or TC (IPv6) value) within the "tosTrCl" attribute for the described service data flows together with the "fDescs" attribute.

NOTE x1: A ToS/TC value can be useful when another packet filter attribute is needed to differentiate between packet flows. For example, packet flows encapsulated and encrypted by a tunnelling protocol can be differentiated by the ToS/TC value of the outer header if appropriately set by the application. To use ToS/TC for service data flow detection, network configuration needs to ensure there is no ToS/TC re-marking applied along the path from the application to the PSA UPF and the specific ToS/TC values are managed properly to avoid potential collision with other usage (e.g., paging policy differentiation).

The NF service consumer may include the "resPrio" attribute at the "AppSessionContextReqData" data type level to assign a priority to the AF Session as well as include the "resPrio" attribute at the "MediaComponent" data type level to assign a priority to the service data flow. The presence of the "resPrio" attribute in both levels does not constitute a conflict as they each represent different types of priority. The reservation priority at the "AppSessionContextReqData" data type level provides the relative priority for an AF session while the reservation priority at the "MediaComponent" data type level provides the relative priority for a service data flow within a session. If the "resPrio" attribute is not specified, the requested priority is PRIO_1.

The PCF shall check whether the received service information requires PCC rules to be created and provisioned as specified in 3GPP TS 29.513 [7]. Provisioning of PCC rules to the SMF shall be carried out as specified at 3GPP TS 29.512 [8].

Based on the received subscription information from the NF service consumer, the PCF may create a subscription to event notifications for a related PDU session from the SMF, as described in 3GPP TS 29.512 [8].

If the PCF created an "Individual Application Session Context" resource, the PCF shall send to the NF service consumer a "201 Created" response to the HTTP POST request, as shown in figure 4.2.2.2-1, step 2. The PCF shall include in the "201 Created" response:

- a Location header field; and

- an "AppSessionContext" data type in the payload body.

The Location header field shall contain the URI of the created individual application session context resource i.e. "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}".

When "Events Subscription" sub-resource is created in this procedure, the NF service consumer shall build the sub-resource URI by adding the path segment "/events-subscription" at the end of the URI path received in the Location header field.

The "AppSessionContext" data type payload body shall contain the representation of the created "Individual Application Session Context" resource and may include the "Events Subscription" sub-resource.

The PCF shall include in the "evsNotif" attribute:

- if the NF service consumer subscribed to the event "PLMN_CHG" in the HTTP POST request, the "event" attribute set to "PLMN_CHG" and the "plmnId" attribute including the PLMN Identifier or the SNPN Identifier if the PCF has previously requested to be updated with this information in the SMF;

NOTE 7: The SNPN Identifier consists of the PLMN Identifier and the NID.

- if the NF service consumer subscribed to the event "ACCESS_TYPE_CHANGE" in the HTTP POST request, the "event" attribute set to "ACCESS_TYPE_CHANGE" and:

  i. the "accessType" attribute including the access type, and the "ratType" attribute including the RAT type when applicable for the notified access type; and

ii. if the "ATSSS" feature is supported, the "addAccessInfo" attribute with the additional access type information if available, where the access type is encoded in the "accessType" attribute, and the RAT type is encoded in the "ratType" attribute when applicable for the notified access type; and

NOTE 8: For a MA PDU session, if the "ATSSS" feature is not supported by the NF service consumer the PCF includes the "accessType" attribute and the "ratType" attribute with a currently active combination of access type and RAT type (if applicable for the notifed access type). When both 3GPP and non-3GPP accesses are available, the PCF includes the information corresponding to the 3GPP access.

iii. the "anGwAddr" attribute including access network gateway address when available,

if the PCF has previously requested to be updated with this information in the SMF; and

- if the "IMS_SBI" feature is supported and if the NF service consumer subscribed to the "CHARGING_CORRELATION" event in the HTTP POST request, the "event" attribute set to "CHARGING_CORRELATION" and may include the "anChargIds" attribute containing the access network charging identifier(s) and the "anChargAddr" attribute containing the access network charging address.

The NF service consumer subscription to other specific events using the Npcf_PolicyAuthorization_Create request is described in the related clauses. Notification of events when the applicable information is not available in the PCF when receiving the Npcf_PolicyAuthorization_Create request is described in clause 4.2.5.

The acknowledgement towards the NF service consumer should take place before or in parallel with any required PCC rule provisioning towards the SMF.

NOTE 9: The behaviour when the NF service consumer does not receive the HTTP response message, or when it arrives after the internal timer waiting for it has expired, or when it arrives with an indication different than a success indication, are outside the scope of this specification and based on operator policy.

#### 4.2.2.3 Gate control

This procedure is used by an NF service consumer to instruct the PCF about when the service data flow(s) are to be enabled or disabled for a PDU session.

The AF shall include in the HTTP POST request message described in subclause 4.2.2.2 the "fStatus" attribute for the flows to be enabled or disabled within the "medComponents" or "medSubComps" attributes.

If a "medSubComps" attribute contains a "flowUsage" attribute with the value "RTCP", then the IP Flows described by that media subcomponent shall be enabled in both directions irrespective of the value of the "fStatus" attribute of the corresponding media component.

As result of this action, the PCF shall set the appropriate gate status for the corresponding active PCC rule(s).

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2.

#### 4.2.2.4 Initial Background Data Transfer policy indication

This procedure is used by a NF service consumer to indicate a transfer policy negotiated for background data transfer using the Npcf_BDTPolicyControl service as described in 3GPP TS 29.554 [14].

The NF service consumer may include in the HTTP POST request message described in clause 4.2.2.2 a reference identifier related to a transfer policy negotiated for background data transfer in the "bdtRefId" attribute.

NOTE 1: The PCF will retrieve the corresponding transfer policy from the UDR based on the reference identifier within the "bdtRefId" attribute. In case only one PCF is deployed in the network, transfer policies can be locally stored in the PCF and the interaction with the UDR is not required.

If the PCF cannot retrieve the transfer policy, the PCF shall set to TP_NOT_KNOWN the "servAuthInfo" attribute in the HTTP response message to the NF service consumer to indicate that the transfer policy is unknown.

If the time window of the received transfer policy has expired, the PCF shall set to TP_EXPIRED the "servAuthInfo" attribute in the HTTP response message to indicate to the NF service consumer that the transfer policy has expired. Otherwise, if the time window of the received transfer policy has not yet occurred, the PCF shall set to

TP_NOT_YET_OCCURRED the "servAuthInfo" attribute in the HTTP response message to the NF service consumer to indicate that the time window of the transfer policy has not yet occurred.

NOTE 2: In the case that the PCF cannot retrieve the transfer policy, the transfer policy time window has not yet occurred or the transfer policy expired, the PCF makes the decision without considering the transfer policy.

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2.

### 4.2.2.5 Initial provisioning of sponsored connectivity information

This procedure is used by a NF service consumer to indicate sponsored data connectivity when "SponsoredConnectivity" feature is supported.

The NF service consumer shall provide in the "AppSessionContext" data type of the HTTP POST request message described in clause 4.2.2.2 an application service provider identity and a sponsor identity within the "aspId" attribute and "sponId" attribute within the "ascReqData" attribute. Additionally, the NF service consumer may provide an indication to the PCF of sponsored data connectivity not enabled by including the "sponStatus" attribute set to "SPONSOR_DISABLED".

To support the usage monitoring of sponsored data connectivity, the NF service consumer may subscribe with the PCF to the notification of usage threshold reached. The NF service consumer shall include:

- an entry of the "AfEventSubscription" data type in the "events" attribute with the "event" attribute set to "USAGE_REPORT"; and
- the "usgThres" attribute of "UsageThreshold" data type in the "EventsSubscReqData" data type with:
  a) the total volume in the "totalVolume" attribute; or
  b) the uplink volume only in the "uplinkVolume" attribute; or
  c) the downlink volume only in the "downlinkVolume"; and/or
  d) the time in the "duration" attribute.

NOTE 1: If the NF service consumer is in the user plane, the AF can handle the usage monitoring and therefore it is not required to provide a usage threshold to the PCF as part of the sponsored connectivity functionality.

When the NF service consumer indicated to enable sponsored data connectivity, and the UE is roaming in a VPLMN, the following procedures apply:

- If the NF service consumer is located in the HPLMN, for home routed roaming case and when the operator policies do not allow accessing the sponsored data connectivity with this roaming case, the H-PCF shall reject the service request and shall include in the HTTP "403 Forbidden" response message the "cause" attribute set to "UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY".
- If the NF service consumer is located in the VPLMN, the V-PCF shall reject the service request and shall include in the HTTP "403 Forbidden" response message the "cause" attribute set to "UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY".

When the NF service consumer indicated to enable sponsored data connectivity, and the UE is non-roaming or roaming with the home routed case and the operator policies allow accessing the sponsored data connectivity with this roaming case, the following procedures apply:

- If the SMF does not support sponsored connectivity and the required reporting level for that service indicates a sponsored connectivity level according to 3GPP TS 29.512 [8], then the PCF shall reject the request and shall include in the HTTP "403 Forbidden" response message the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED".
- If the SMF supports sponsored data connectivity feature or the required reporting level is different from sponsored connectivity level as described in 3GPP TS 29.512 [8], then the PCF, based on operator policies, shall check whether it is required to validate the sponsored connectivity data. If it is required, it shall perform the authorizations based on sponsored data connectivity profiles. If the authorization fails, the PCF shall include in

the HTTP "403 Forbidden" response message the "cause" attribute set to "UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY".

NOTE 2: The PCF is not required to verify that a trust relationship exists between the operator and the sponsors.

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2.

### 4.2.2.6 Subscriptions to Service Data Flow QoS notification control

The subscription to Service Data Flow QoS notification control is used by a NF service consumer to subscribe to receive a notification when the GBR QoS targets for one or more service data flows can no longer (or can again) be guaranteed.

NOTE: It may happen that the GBR QoS targets for one or more PCC rules (i.e. Service Data Flows) cannot be guaranteed, either permanently or temporarily in the radio access network.

The NF service consumer shall use the "EventsSubscReqData" data type as described in clause 4.2.2.2 and shall include in the HTTP POST request message an event within the "events" attribute with the "event" attribute set to "QOS_NOTIF".

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2.

As result of this action, the PCF shall set the appropriate subscription to QoS notification control for the corresponding PCC rule(s) as described in in 3GPP TS 29.512 [8].

### 4.2.2.7 Subscription to Service Data Flow Deactivation

This procedure is used by NF service consumer to subscribe to the notification of deactivation of one or more Service Data Flows within the AF application session context.

NOTE: It may happen that one or more PCC rules (i.e. Service Data Flows) are deactivated at the SMF at certain time, either permanently or temporarily, due to e.g. release of resources or out of credit condition.

The NF service consumer shall use the "EventsSubscReqData" data type as described in clause 4.2.2.2 and shall include in the HTTP POST request message an event within the "events" attribute with the "event" attribute set to "FAILED_RESOURCES_ALLOCATION".

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2.

As result of this action, the PCF shall set the appropriate subscription to service data flow deactivation for the corresponding PCC rule(s) as described in in 3GPP TS 29.512 [8].

### 4.2.2.8 Initial provisioning of traffic routing information

This procedure is used by a NF service consumer to:

- influence SMF traffic routing decisions to a local access to a Data Network identified by a DNAI; and/or
- request subscriptions to notifications about UP path management events related to the PDU session,

when "InfluenceOnTrafficRouting" feature is supported.

NOTE 1: The NF service consumer uses the Npcf_PolicyAuthorization service for requests targeting specific on-going PDU sessions of individual UE(s). The NF service consumer requests that target existing or future PDU Sessions of multiple UE(s) or any UE are sent via the NEF and may target multiple PCF(s), as described in 3GPP TS 29.513 [7].

The NF service consumer shall include in the HTTP POST request message described in clause 4.2.2.2 the "afRoutReq" attribute of "AfRoutingRequirement" data type with specific routing requirements for the application traffic flows either within "AppSessionContextReqData" data type for the service indicated in the "afAppId" attribute, or within the "medComponents" attribute. When provided at both levels, the "afRoutReq" attribute value in the "medComponents" attribute shall have precedence over the "afRoutReq" attribute included in the "AppSessionContextReqData" data type.

The NF service consumer may include traffic routing requirements together with service information.

The NF service consumer may request to influence SMF traffic routing decisions to a DNAI. The NF service consumer shall include in the "afRoutReq" attribute:

a) A list of routes to locations of applications in the "routeToLocs" attribute. Each element of the list shall contain:

   - a DNAI in the "dnai" attribute to indicate the location of the application towards which the traffic routing is applied; and

   - a routing profile identifier in the "routeProfId" attribute, and/or the explicit routing information in the "routeInfo" attribute.

The NF service consumer may include in the "afRoutReq" attribute:

a) Indication of application relocation possibility in the "appReloc" attribute.

b) Temporal validity during which the NF service consumer request is valid shall be indicated with the "startTime" and "stopTime" attributes.

c) Spatial validity during which the NF service consumer request is valid shall be indicated in terms of validity areas encoded in the "spVal" attribute of "SpatialValidity" data type. The "SpatialValidity" data type consists of a list of presence areas included in the "presenceInfoList" attribute, where each element shall include the presence reporting area identifier in the "praId" attribute and may include the elements composing a presence area encoded in the attributes: "trackingAreaList", "ecgList", "ncgList", "globalRanNodeIdList".

d) Indication of UE IP address preservation in the "addrPreserInd" attribute if the URLLC feature is supported.

e) If the SimultConnectivity feature is supported:

   - indication of simultaneous connectivity temporarily maintained in the source and target PSA during the edge re-location procedure in the "simConnInd" attribute; and

   - if the "simConnInd" attribute is set to true, the minimum time interval to be considered for inactivity of the traffic routed via the source PSA in the "simConnTerm" attribute.

f) EAS IP replacement information in the "easIpReplaceInfos" attribute if the EASIPreplacement feature is supported.

g) Indication of EAS rediscovery in the "easRedisInd" attribute if the EASDiscovery feature is supported.

h) Maximum allowed user plane latency in the "maxAllowedUpLat" attribute if the AF_latency feature is supported.

NOTE 2: The EAS IP Replacement information and the information indicating the EAS rediscovery are not provided simultaneously.

The NF service consumer may also subscribe to notifications about UP path management events. The NF service consumer shall include in the "upPathChgSub" attribute:

- notifications of early and/or late DNAI change, using the attribute "dnaiChgType" indicating whether the subscription is for "EARLY", "LATE" or "EARLY_LATE";

- the notification URI where the NF service consumer is receiving the Nsmf_EventExposure_Notify service operation in the "notificationUri" attribute; and

- the notification correlation identifier assigned by the NF service consumer in the "notifCorreId" attribute.

If the URLLC feature is supported, the NF service consumer may include an indication of NF service consumer acknowledgement to be expected as an "afAckInd" attribute within the "upPathChgSub" attribute.

When the feature "RoutingReqOutcome" is supported:

- the PCF may set the "servAuthInfo" attribute in the HTTP response message to "ROUT_REQ_NOT_AUTHORIZED" when the PCF determines, e.g. based on subscription, the AF influence on traffic routing is not allowed for the PDU session;

- when the NF service consumer requests the steering of traffic to a DNAI and/or the subscription to notifications about UP path management events, the NF service consumer may subscribe to notifications of failures in the

enforcement of UP path changes including within the "evSubsc" attribute the "event" attribute value "UP_PATH_CHG_FAILURE" in an entry of the "events" array.

NOTE 3: In the case that the PCF determines that the requested AF routing requirements cannot be applied and returns the "servAuthInfo" attribute in the HTTP response, the PCF makes the decision without considering the requested AF routing requirements.

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2.

The PCF shall store the routing requirements included in the "afRoutReq" attribute.

The PCF shall check whether the received routing requirements requires PCC rules to be created or provisioned to include or modify traffic steering policies, the AF transaction identifier and the application relocation possibility as specified in 3GPP TS 29.513 [7]. Provisioning of PCC rules to the SMF shall be carried out as specified in 3GPP TS 29.512 [8].

NOTE 4: The NF service consumer receives the notification about UP path management events by the Nsmf_EventExposure_Notify service operation as defined in clause 4.2.2.2 of 3GPP TS 29.508 [13].

### 4.2.2.9 Void

### 4.2.2.10 Subscription to resources allocation outcome

This procedure is used by a NF service consumer to subscribe to notifications when the resources associated to the corresponding service information have been allocated and/or cannot be allocated.

The NF service consumer shall use the "EventsSubscReqData" data type as described in clause 4.2.2.2 and shall include in the HTTP POST request message:

- if the NF service consumer requests the PCF to provide a notification when the resources associated to the service information have been allocated, an event entry within the "events" attribute with the "event" attribute set to "SUCCESSFUL_RESOURCES_ALLOCATION"; and/or
- if the NF service consumer requests the PCF to provide a notification when the resources associated to the service information cannot be allocated, an event entry within the "events" attribute with the "event" attribute set to "FAILED_RESOURCES_ALLOCATION".

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2.

As a result of this action, the PCF shall set the appropriate subscription to notification of resources allocation outcome for the corresponding PCC Rule(s) as described in 3GPP TS 29.512 [8].

### 4.2.2.11 Void

### 4.2.2.12 Invocation of Multimedia Priority Services

#### 4.2.2.12.1 General

This procedure allows a NF service consumer, as per 3GPP TS 22.153 [23], to request prioritized access to system resources in situations such as during congestion.

The NF service consumer may include the "mpsId" attribute to indicate that the new AF session relates to an MPS session.

The "mpsId" attribute shall contain the national variant for the MPS service name indicating an MPS session. The "resPrio" attribute shall include the priority value of the related priority service.

If the NF service consumer supports the SBI Message Priority mechanism for an MPS session, it shall include the "3gpp-Sbi-Message-Priority" custom HTTP header towards the PCF as described in clause 6.8.2 of 3GPP TS 29.500 [5].

NOTE 1: If the NF service consumer supports the SBI Message Priority mechanism for an MPS session, the NF service consumer will include the "3gpp-Sbi-Message-Priority" custom HTTP header with a priority value equivalent to the value of the "resPrio" attribute. Highest user priority value is mapped in the corresponding lowest value of the "3gpp-Sbi-Message-Priority" custom HTTP header.

When the PCF receives the "mpsId" attribute indicating an MPS session, the PCF shall take specific actions on the corresponding PDU session to ensure that the MPS session is prioritized as specified in 3GPP TS 29.512 [8].

NOTE 2: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8], it is possible that, subject to operator policy and national/regional regulations, prioritised services are exempted from the limitation of data rate per network slice. In that case the PCF will handle the request from the NF service consumer even if the authorized data rate per network slice is exceeded.

#### 4.2.2.12.2 MPS for DTS

MPS for DTS is the means for an NF service consumer to invoke/revoke the Priority PDU connectivity service for the default QoS flow only, i.e. without designating a particular service data flow for priority service. MPS for DTS applies only to non-IMS DNNs.

When the "MPSforDTS" feature is supported, to invoke MPS for DTS, the NF service consumer includes the "mpsAction" attribute, set to "ENABLE_MPS_FOR_DTS" or "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS". These "mpsAction" attribute values signal a QoS change to the default QoS flow and service data flows mapped to the default QoS flow without the creation of a new QoS flow.

When the "ENABLE_MPS_FOR_DTS" value is received, and allowed by local policy, the PCF does not check the user's MPS subscription details. When the "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS" value is received, and allowed by local policy, the PCF shall check the user's MPS subscription to authorize the request. When the request is to authorize and enable, and the request is not authorized (e.g. not allowed by MPS subscription), the PCF shall indicate in an HTTP "403 Forbidden" response message the cause for the rejection including the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED".

NOTE: How the NF service consumer checks the MPS for DTS authorization is out of scope of the present document.

When creating an Individual Application Session Context resource, due to the invocation or revocation of MPS for DTS, the NF service consumer may subscribe to the outcome of the default QoS updates by setting within the "evSubsc" attribute an event in the "events" array with:

- the "event" attribute set to the value "SUCCESSFUL_QOS_UPDATE" to report that the invocation/revocation requested by the NF service consumer was successful; and/or
- the "event" attribute set to the value "FAILED_QOS_UPDATE" to report that the invocation/revocation requested by the NF service consumer has failed to be successful.

The NF service consumer may use the procedure specified in clause 4.2.2.12.3 to open a new priority PDU session related to the AF signalling IP flow between the UE and NF service consumer.

#### 4.2.2.12.3 Provisioning of MPS for DTS signalling flow information

This clause is applicable to provisioning of signalling flow information for MPS for DTS if the MPSforDTS feature is supported as described in clause 5.8.

This procedure allows NF service consumer to provision information about the AF signalling IP flows between the UE and the NF service consumer.

The NF service consumer shall provide:

- the IP address (IPv4 or IPv6) of the UE in the "ueIpv4" or "ueIpv6" attribute;

- the "mpsId" attribute; and
- a media component within the "medComponents" attribute including:
  - the "medCompN" attribute set to "0"; and
  - the media subcomponent within the "medSubComps" attribute representing the AF signalling IP flow, where the media subcomponent shall contain:
    - the "flowUsage" attribute set to the value "AF_SIGNALLING";
    - the "fDesc" attribute containing the IP flows of the AF signalling flow; and
    - the "fStatus" set to the value "ENABLED".

The PCF shall determine whether the request is accepted or not. If accepted, the PCF shall perform session binding and shall reply to the NF service consumer as described in clause 4.2.2.2. If rejected, the PCF shall indicate in an HTTP "403 Forbidden" response message the cause for the rejection including the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED".

The PCF shall set appropriate QoS values for the AF signalling IP flow and shall install the corresponding dynamic PCC rule for the AF signalling IP flows.

The NF service consumer may de-provision the information about the AF signalling IP flows at any time. To do that, if the "Individual Application Session Context" resource is only used to provide information about the AF Signalling IP flows, the NF service consumer shall remove the resource by sending an Npcf_PolicyAuthorization_Delete service operation towards the PCF as defined in clause 4.2.4.2. Otherwise, the NF service consumer shall remove the IP flow within the media component invoking the Npcf_PolicyAuthorization_Update service operation as defined in clause 4.2.3.17.

NOTE: Combining the request for the AF signalling flow with an MPS for DTS invocation/revocation request is not supported in this release.

### 4.2.2.13 Support of content versioning

The support of the media component versioning is optional. When the "MediaComponentVersioning" feature is supported, the NF service consumer and the PCF shall comply with the procedures specified in this clause.

If required by operator policies, the NF service consumer shall assign a content version to the media component related to certain service and shall provide assigned content version to the PCF in the "contVer" attribute included in the corresponding media component entry of the "medComponents" attribute.

If the PCF receives the "contVer" attribute for a certain media component, the PCF shall follow the procedures described in 3GPP TS 29.512 [8], clause 4.2.6.2.14.

### 4.2.2.14 Request of access network information

This procedure is used by a NF service consumer to request the PCF to report the access network information (i.e. user location and/or user timezone information) at the creation of the "Individual Application Session Context" resource, when the "NetLoc" feature is supported.

The NF service consumer shall include in the HTTP POST request message described in clause 4.2.2.2:

- an entry of the "AfEventSubscription" data type in the "events" attribute with:
  a) the "event" attribute set to the value "ANI_REPORT"; and
  b) the "notifMethod" attribute set to the value "ONE_TIME"; and
- the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

When the PCF determines that the access network does not support the access network information reporting because the SMF does not support the NetLoc feature, the PCF shall respond to the NF service consumer including in the

"EventsNotification" data type the "noNetLocSupp" attribute set to "ANR_NOT_SUPPORTED" value. Otherwise, the PCF shall immediately configure the SMF to provide such access information, as specified in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer with an HTTP response message as described in clause 4.2.2.2.

### 4.2.2.15 Initial provisioning of service information status

When the "IMS_SBI" feature is supported, the NF service consumer may provide the status of the service information.

If the NF service consumer provides service information that has been fully negotiated (e.g. based on the SDP answer), the NF service consumer may include the "servInfStatus" attribute set to "FINAL". In this case the PCF shall authorize the session and provision the corresponding PCC rules to the SMF.

The NF service consumer may additionally provide preliminary service information not fully negotiated yet (e.g. based on the SDP offer) at an earlier stage. To do so, the NF service consumer shall include the "servInfStatus" attribute set to "PRELIMINARY". Upon receipt of such preliminary service information, the PCF shall perform an early authorization check of the service information. If the NF service consumer requests the PCF to report the access network information together with preliminary service information, the PCF shall immediately configure the SMF to provide the access network information.

### 4.2.2.16 Provisioning of signalling flow information

This clause is applicable when IMS restoration is supported according to the supported feature "ProvAFsignalFlow" as described in clause 5.8.

This procedure allows NF service consumer to provision information about the AF signalling IP flows between the UE and the NF service consumer.

The NF service consumer shall provide:

- the IP address (IPv4 or IPv6) of the UE in the "ueIPv4" or "ueIPv6" attribute; and
- a media component within the "medComponents" attribute including:
  - the "medCompN" attribute set to "0"; and
  - one or more media subcomponents within the "medSubComps" attribute representing the AF signalling IP flows, where each media subcomponent shall contain:
    - the "flowUsage" attribute set to the value "AF_SIGNALLING";
    - the "fNum" attribute set according to the rules described in Annex C;
    - the "fDesc" attribute containing the IP flows of the AF signalling flow;
    - the "fStatus" set to the value "ENABLED"; and
    - the "afSigProtocol" set to the value corresponding to the signalling protocol used between the UE and the NF service consumer.

The PCF shall perform session binding and shall reply to the NF service consumer as described in clause 4.2.2.2.

PCC rules related to the AF signalling IP flows could have been provisioned to SMF using the corresponding procedures specified in 3GPP TS 29.512 [8] at an earlier stage (e.g. typically at the establishment of the QoS flow for AF Signalling IP Flows). The PCF shall install the corresponding dynamic PCC rule for the AF signalling IP flows.

The NF service consumer may de-provision the information about the AF signalling IP flows at any time. To do that, if the "Individual Application Session Context" resource is only used to provide information about the AF Signalling IP flows, the NF service consumer shall remove the resource by sending an Npcf_PolicyAuthorization_Delete service operation as service operation towards the PCF as defined in clause 4.2.4.2. Otherwise, the NF service consumer shall remove the IP flows within the media component invoking the Npcf_PolicyAuthorization_Update service operation as defined in clause 4.2.3.17.

### 4.2.2.17 Support of resource sharing

This procedure is used by a NF service consumer to indicate that a media component of an Individual Application Session Context resource may share resources with other media components in the related direction in other Individual Application Session Context resources when the "ResourceSharing" feature is supported.

The NF service consumer may include the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute within a media component of the "medComponents" attribute to indicate that the related media of the created new Individual Application Session Context resource may share resources with other media components in the related direction that include the same value for the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute.

The PCF shall reply to the NF service consumer with an HTTP response message as described in clause 4.2.2.2.

If the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute are provided within a media component of the "medComponents" attribute, the PCF may apply the mechanisms for resource sharing as described in 3GPP TS 29.512 [8], clause 4.2.6.2.8.

### 4.2.2.18 Indication of Emergency traffic

When the "IMS_SBI" feature is supported, this procedure allows a NF service consumer to indicate that the new AF session context relates to emergency traffic.

The NF service consumer may include the "servUrn" attribute to indicate that the new AF session context relates to emergency traffic. Additionally, the NF service consumer may include the "afReqData" attribute to indicate the additional information requested for the AF session context.

When the PCF receives the "servUrn" attribute indicating an emergency session, the PCF may apply special policies, for instance prioritising service flows relating to the new AF session context, allowing these service flows free of charge or exempting the service flows from the limitation of data rate per network slice when the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8]).

If the "servUrn" attribute indicates that the new NF service consumer session context relates to emergency traffic and the "afReqData" attribute is received, the PCF shall reply to the NF service consumer as described in clause 4.2.2.2 and shall provide the requested available user information in the "ueIds" attribute included within the "ascRespData" attribute in the HTTP "201 Created" response.

NOTE 1: The "supi" attribute within the "ueIds" attribute contains an IMSI, if available, when the UE accesses a PLMN and contains either an IMSI or a network-specific identifier that takes the form of an NAI, if available, when the UE accesses a SNPN. For both, PLMN access and SNPN access, the "gpsi" attribute within the "ueIds" attribute contains an MSISDN, if available, and the "pei" attribute contains an IMEI(SV).

If the NF service consumer supports the SBI Message Priority mechanism for an emergency session, it shall include the "3gpp-Sbi-Message-Priority" custom HTTP header towards the PCF as described in clause 6.8.2 of 3GPP TS 29.500 [5].

NOTE 2: If the NF service consumer supports the SBI Message Priority mechanism for an emergency session, the NF service consumer includes the "3gpp-Sbi-Message-Priority" custom HTTP header based on NF service consumer policies in relation to valid values of the "servUrn" attribute. The highest user priority value is mapped to the corresponding lowest value of the "3gpp-Sbi-Message-Priority" custom HTTP header.

When the new AF session context does not indicate emergency traffic and the session binding function detects that the binding is to a PDU session established to the Emergency DNN, the PCF shall reject the HTTP POST request and shall indicate in an HTTP "403 Forbidden" response message the cause for the rejection including the "cause" attribute set to "UNAUTHORIZED_NON_EMERGENCY_SESSION".

### 4.2.2.19 Invocation of MCPTT

When the feature "MCPTT" is supported by the NF service consumer and the PCF, this procedure allows a NF service consumer to request prioritized access to system resources in situations such as an MCPTT session with priority call.

The NF service consumer may include the "mcpttId" attribute to indicate that the new "Individual Application Session Context" resource relates to an MCPTT session with priority call.

When the PCF receives the "mcpttId" attribute indicating an MCPTT session and the "resPrio" attribute, the PCF shall take specific actions on the corresponding PDU session to ensure that the MCPTT session is prioritized as specified in 3GPP TS 29.512 [8].

NOTE: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8], it is possible that, subject to operator policy and national/regional regulations, prioritised services are exempted from the limitation of data rate per network slice. In that case the PCF will handle the request from the NF service consumer even if the authorized data rate per network slice is exceeded.

Additionally, when the "PrioritySharing" feature is supported, the PCF may receive the "prioSharingInd" attribute within the media component received in the "medComponents" attribute as described in clause 4.2.2.21. In this case, and if "MCPTT-Preemption" feature is supported, the PCF may receive pre-emption information as also described in clause 4.2.2.21.

For the handling of MCPTT session with priority call, see Annex B.13

### 4.2.2.20 Invocation of MCVideo

When the feature "MCVideo" is supported by the NF service consumer and the PCF, this procedure allows a NF service consumer to request prioritized access to system resources in situations such as an MCVideo session with priority call.

The NF service consumer may include the "mcVideoId" attribute to indicate that the new "Individual Application Session Context" resource relates to an MCVideo session with priority call.

When the PCF receives the "mcVideoId" attribute indicating an MCVideo session and the "resPrio" attribute, the PCF shall take specific actions on the corresponding PDU session to ensure that the MCVideo session is prioritized as specified in 3GPP TS 29.512 [8].

NOTE: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8], it is possible that, subject to operator policy and national/regional regulations, prioritised services are exempted from the limitation of data rate per network slice. In that case the PCF will handle the request from the NF service consumer even if the authorized data rate per network slice is exceeded.

For the handling of MCVideo session with priority call, see Annex B.15.

### 4.2.2.21 Priority sharing indication

When the "PrioritySharing" feature is supported, the NF service consumer may indicate to the PCF that the related media flow is allowed to use the same Allocation and Retention Priority (ARP) as media flows belonging to other "Individual Application Session Context" resources.

The NF service consumer may include the "prioSharingInd" attribute set to "ENABLED" within a media component of the "medComponents" attribute to indicate to the PCF that the related media flow is allowed to use the same Allocation and Retention Priority as media flows which:

- are assigned the same 5QI in the PCF; and
- belong to other "Individual Application Session Context" resources bound to the same PDU session that also contain the "prioSharingInd" attribute set to "ENABLED".

If the "MCPTT-Preemption" feature is supported, the NF service consumer may also include:

- within a media component of the "medComponents" attribute, the "preemptCap" attribute containing the suggested pre-emption capability value and the "preemptVuln" attribute containing the suggested pre-emption vulnerability value, for the PCF to determine ARP values;
- within the "ascReqData" attribute in the request body, the "preemptControlInfo" attribute containing the pre-emption control information for the PCF to perform pre-emption control as described in 3GPP TS 29.512 [8], clause 4.2.6.2.9; and

- within the "evSubsc" attribute, the "event" attribute set to "FAILED_RESOURCES_ALLOCATION" to request the notification for resource allocation failure.

Upon reception of this information, the PCF shall behave as described in 3GPP TS 29.512 [8], clause 4.2.6.2.9. For the handling of MCPTT sessions, see Annex B.10.

NOTE 1: Service data flow deactivation procedures will apply according to clauses 4.2.2.7, 4.2.3.7, 4.2.5.5.

NOTE 2: This enhancement avoids the risk that a QoS flow establishment request is rejected if the maximum number of active QoS flows is exceeded.

The PCF shall reply to the NF service consumer with an HTTP response message as described in clause 4.2.2.2.

### 4.2.2.22 Subscription to Out of Credit notification

This procedure is used by the NF service consumer if the "IMS_SBI" feature is supported to subscribe to notifications of credit not available for the Service Data Flows within the AF application session context.

NOTE: It can happen that there are one or more PCC rules (i.e. Service Data Flows) with credit not available, each one with their corresponding termination action (terminate, redirect, access restricted).

The NF service consumer shall use the "EventsSubscReqData" data type as described in clause 4.2.2.2 and shall include in the HTTP POST request message an event within the "evSubsc" attribute with the "event" attribute set to the value "OUT_OF_CREDIT".

As result of this action, the PCF shall set the appropriate subscription to out of credit notification for the corresponding PCC rule(s) as described in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer with an HTTP response message as described in clause 4.2.2.2.

### 4.2.2.23 Subscriptions to Service Data Flow QoS Monitoring Information

The subscription to Service Data Flow QoS monitoring information is used by a NF service consumer to receive a notification about the packet delay between UPF and UE, when the "QoSMonitoring" feature is supported.

The NF service consumer shall use the "EventsSubscReqData" data type as described in clause 4.2.2.2 and shall include:

- the requested QoS monitoring parameter(s) to be measured (i.e. DL, UL and/or round trip packet delay) within the "reqQosMonParams" attribute;
- an entry of the "AfEventSubscription" data type per requested notification method in the "events" attribute with:
  a) the "event" attribute set to the value "QOS_MONITORING"; and
  b) the "notifMethod" attribute set to the value "EVENT_DETECTION" or "PERIODIC"; and
  c) when the "notifMethod" attribute is set to the value "PERIODIC", the periodic time for reporting and, if the feature "PacketDelayFailureReport" is supported, the maximum period with no QoS measurement results reported within the "repPeriod" attribute; and
  d) when the "notifMethod" attribute is set to the value "EVENT_DETECTION", the minimum waiting time between subsequent reports within the "waitTime" attribute and, if the feature "PacketDelayFailureReport" is supported, the maximum period with no QoS measurement results reported within the "repPeriod" attribute;
- when the "notifMethod" attribute set to the value "EVENT_DETECTION", the "qosMon" attribute, with the required Qos Monitoring information, i.e.:
  a) the delay threshold for downlink with the "repThreshDl" attribute;
  b) the delay threshold for uplink with the "repThreshUl" attribute; and/or
  c) the delay threshold for round trip with the "repThreshRp" attribute.

The NF service consumer may include in "EventsSubscReqData" data type the notification correlation identifier assigned by the AF within the "notifCorreId" attribute and, if the feature "ExposureToEAS" is supported, the "directNotifInd" attribute set to true to indicate direct event notification of QoS Monitoring data from the UPF.

The NF service consumer shall include more than one "AfEventSubscription" data type within the "EventsSubscReqData" data type if more than one notification method is required.

The PCF shall reply to the AF as described in clause 4.2.2.2.

As result of this action, the PCF shall set the appropriate subscription to QoS Monitoring information for the corresponding PCC rule(s) as described in 3GPP TS 29.512 [8].

### 4.2.2.24 Provisioning of TSCAI input Information and QoS related data

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported the NF service consumer (i.e. TSN AF or TSCTSF) may provide TSCAI input information within the TSC assistance container and QoS related data to the PCF by the Npcf_PolicyAuthorization_Create service operation to describe the TSC traffic pattern and QoS characteristics for use in the 5G System.

The NF service consumer (i.e. TSN AF or TSCTSF) shall derive the TSCAI input information and the QoS related data for a given TSC stream or flow of aggregated TSC streams. The TSCTSF may determine the TSCAI input information and the related QoS data based on information provided by an AF/NEF, and may provide it for IP type and Ethernet type of PDU sessions as specified in clauses 4.15.6.6 and 4.15.6.6a of TS 23.502 [3]. In case of integration with IEEE TSN network, the TSN AF determines the TSCAI input information as defined in clause 5.27.2.2 of 3GPP TS 23.501 [2] and the QoS related data as defined in clause 5.28.4 of 3GPP TS 23.501 [2].

To indicate the TSCAI input information of a TSC stream or aggregated set of TSC streams, the NF service consumer (i.e. TSN AF or TSCTSF) may include for the uplink flow direction (ingress interface of the DS-TT/UE) in the "tscaiInputUl" attribute and/or for the downlink flow direction (ingress interface of the NW-TT) the "tscaiInputDl" attribute included in a media component entry of the "medComponents" attribute:

- the time period between the start of two bursts of a TSC stream or aggregated TSC streams in reference to the external GM encoded in the "periodicity" attribute;
- the arrival time of the first data burst of a TSC stream or aggregated TSC streams in reference to the external GM encoded in the "burstArrivalTime" attribute; and
- if the "TimeSensitiveCommunication" feature is supported, the time period an application can survive without any burst, i.e., the survival time, in terms of maximum number of messages encoded in the "surTimeInNumMsg" attribute or in time units encoded in the "surTimeInTime" attribute.

NOTE: A single burst (message is equivalent to burst) is expected within a single periodicity. The survival time in terms of maximum number of messages represents the time period result of multiplying the periodicy by the indicated number of messages.

The uplink and/or downlink flow of the TSC stream or aggregated set of TSC streams shall be encoded within the corresponding "MediaSubComponent" entries of the "medSubComps" attribute, for PDU sessions of Ethernet type in the "ethfDescs" attribute and for PDU sessions of IP type in the "fDescs" attribute.

When the feature "TimeSensitiveCommunication" is supported, to indicate the time domain the NF service consumer is located in (i.e. the (g)PTP domain), the NF service consumer may include the "tscaiTimeDom" attribute in the corresponding media component entry of the "medComponents" attribute.

To indicate the TSC QoS related data of a TSC stream or aggregated set of TSC streams, the NF service consumer (i.e. TSN AF or TSCTSF) may include in the "tsnQos" attribute included in a media component entry of the "medComponents" attribute;

- the maximum burst size encoded in the "maxTscBurstSize" attribute;
- the maximum time a packet may be delayed encoded in the "tscPackDelay" attribute;
- the TSC traffic priority in scheduling resources among other TSC streams encoded in the "tscPrioLevel" attribute.

The NF service consumer (i.e. TSN AF or TSCTSF) may also include the max bitrates in uplink and downlink within the "marBwUl" attribute and the "marBwDl" attribute of the "medComponents" attribute respectively. In case of integration with IEEE TSN network, the TSN AF determines the maximum flow bit rate as defined in Annex I of 3GPP TS 23.501 [2]. In case of integration with a TSC network other than IEEE TSN network, the TSCTSF may additionally include the "mirBwUl" attribute and the "mirBwDl" attribute of the "medComponents" attribute to indicate the requested guaranteed bit rates in uplink and downlink respectively.

When the feature "TimeSensitiveCommunication" is supported, and the feature "AuthorizationWithRequiredQoS" is supported as specified in clause 4.2.2.32, the NF service consumer (i.e. TSCTSF or TSN AF) may provide within an entry of the "medComponents" attribute a reference to pre-defined QoS information within the "qosReference" attribute instead of providing the attributes "tsnQos", "marBwUl", "marBwDl", "mirBwUl", and/or "mirBwDl". Additionally, if the NF service consumer supports adjustments to different QoS parameter combinations, the NF service consumer may provide a prioritized list of one or more QoS references within the "altSerReqs" attribute as specified in clause 4.2.2.32.

When the feature "TimeSensitiveCommunication" is supported, the feature "AltSerReqsWithIndQoS" is supported as specified in clause 4.2.2.32, and the NF service consumer (i.e. TSCTSF or TSN AF) provides within an entry of the "medComponents" attribute individual QoS information (e.g. within the "tsnQos", "marBwUl" and/or "marBwDl" attributes as described in this clause, then the NF service consumer may provide adjustments to different QoS parameter combinations within a prioritized list of one or more Requested Alternative QoS Parameter set(s) within the "altSerReqsData"attribute as specified in clause 4.2.2.32.

The PCF shall reply to the NF service consumer (i.e. TSN AF or TSCTSF) as described in clause 4.2.2.2.

The PCF shall check whether the received TSCAI input container and TSC QoS related data require to create PCC rules to provide the SMF with derived QoS characteristics and the received TSCAI input container. Provisioning of PCC rule(s) to the SMF shall be carried out as specified in 3GPP TS 29.512 [8].

### 4.2.2.25 Provisioning of TSC user plane node management information and port management information

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported, the NF service consumer (i.e., the TSN AF or the TSCTSF) may provide a UMIC for the TSC user plane node functionality of UPF/NW-TT and PMIC(s) for the DS-TT port and/or the NW-TT ports to configure the 5G system as a TSC user plane node bridge by invoking the Npcf_PolicyAuthorization_Create service operation to the PCF.

The NF service consumer may include in the "AppSessionContextReqData" data type:

- the DS-TT PMIC encoded in the attribute "tsnPortManContDstt" and/or the one or more NW-TT PMIC(s) encoded in the "tsnPortManContNwtts" attribute, if available, for the DS-TT port and NW-TT ports allocated for a PDU session. The PMIC(s) are encoded in the "PortManagementContainer" data type, which includes the port management information in the "portManCont" attribute and the related port number in the "portNum" attribute; and/or

- the UMIC encoded in the "tsnBridgeManCont", if available, for the TSC user plane node functionality of the UPF/NW-TT allocated for a PDU session. The UMIC is encoded in the "BridgeManagementContainer" data type.

As result of this action, the PCF shall provide the received DS-TT and/or NW-TT PMIC(s) and/or UMIC for the corresponding PDU session as described in 3GPP TS 29.512 [8].

### 4.2.2.26 Invocation of Mission Critical Services

This procedure allows a NF service consumer, as per 3GPP TS 22.179 [45], to request prioritized access to system resources in situations such as during congestion.

The NF service consumer may include the "mcsId" attribute to indicate that the new AF session relates to an MCS session.

The "mcsId" attribute shall contain the national variant for the MCS service name indicating an MCS session. The "resPrio" attribute shall include the priority value of the related priority service.

If the NF service consumer supports the SBI Message Priority mechanism for an MCS session, it shall include the "3gpp-Sbi-Message-Priority" custom HTTP header towards the PCF as described in clause 6.8.2 of 3GPP TS 29.500 [5].

NOTE: If the NF service consumer supports the SBI Message Priority mechanism for an MCS session, the NF service consumer will include the "3gpp-Sbi-Message-Priority" custom HTTP header with a priority value equivalent to the value of the "resPrio" attribute. Highest user priority value is mapped in the corresponding lowest value of the "3gpp-Sbi-Message-Priority" custom HTTP header.

When the PCF receives the "mcsId" attribute indicating an MCS session, the PCF shall take specific actions on the corresponding PDU session to ensure that the MCS session is prioritised as specified in 3GPP TS 29.512 [8].

### 4.2.2.27 P-CSCF restoration enhancements

The P-CSCF restoration custom operation is applicable when the PCF based Restoration Enhancement, as defined in 3GPP TS 23.380 [39], represented by the supported feature "PCSCF-Restoration-Enhancement" is supported by both P-CSCF and PCF.

Figure 4.2.2.27-1 illustrates the P-CSCF restoration enhancements.

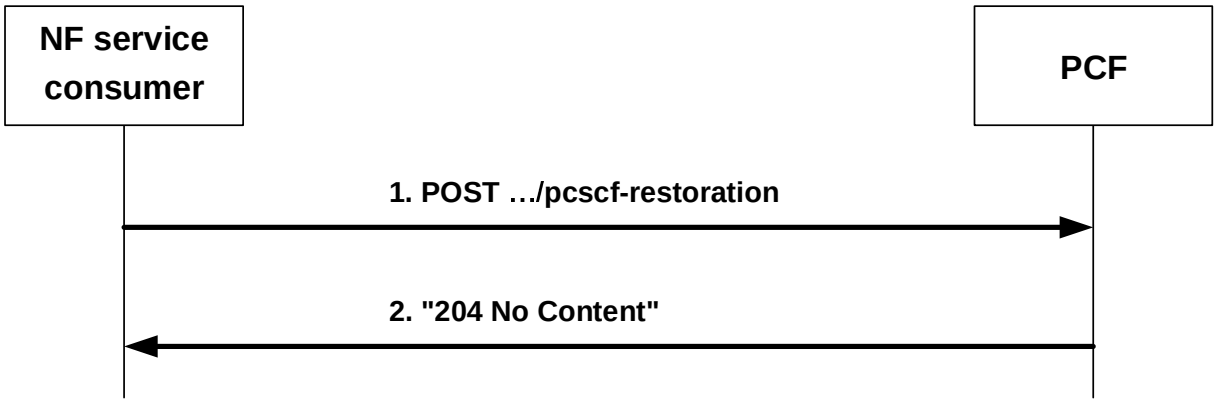


**Figure 4.2.2.27-1: P-CSCF restoration enhancements**

The P-CSCF acting as a NF service consumer shall invoke the "P-CSCF restoration" custom operation sending an HTTP POST request to the resource URI representing the custom operation (POST …/pcscf-restoration) as shown in figure 4.2.2.27-1, step 1, in case P-CSCF restoration needs to be performed.

The P-CSCF shall include in the "PcscfRestorationRequestData" data type in the payload body of the HTTP POST request:

- the IP address (IPv4 or IPv6) of the UE in the "ueIpv4" or "ueIpv6" attribute, and if the IP address is not unique (e.g. private IPv4 case), the "ipDomain" attribute or the "sliceInfo" attribute if available; or
- if the IP address is not available or if the IP address is not unique and the "ipDomain" attribute and the "sliceInfo" attribute are not available, the SUPI in the "supi" attribute and the DNN in the "dnn" attribute.

The PCF shall identify the PDU session for which the HTTP POST request applies. If the PCF fails in identifying the PDU session, the PCF shall reject the "P-CSCF restoration" custom operation with an HTTP "500 Internal Server Error" response including the "cause" attribute set to "PDU_SESSION_NOT_AVAILABLE".

Otherwise, the PCF shall acknowledge the request and shall send to the NF service consumer a "204 No content" response to the HTTP POST request, as shown in figure 4.2.2.27-1, step 2.

The PCF shall send a request for P-CSCF restoration to the SMF for the corresponding PDU session as described in 3GPP TS 29.512 [8], clause 4.2.3.18.

#### 4.2.2.28 Support of CHEM feature

When CHEM feature is supported, the NF service consumer may include the value of Maximum Packet Loss Rate for UL within the "maxPacketLossRateUl" attribute and/or the value of Maximum Packet Loss Rate for DL within the "maxPacketLossRateDl" attribute in "medComponents" attribute. For CHEM feature, see Annex B.14.

#### 4.2.2.29 Support of FLUS feature

When "FLUS" feature is supported by the NF service consumer, the NF service consumer may include the "flusId" attribute within a media component of the "medComponents" attribute to indicate that the related media of the created new Individual Application Session Context resource corresponds to a FLUS media stream. Additional QoS information for the treatment of FLUS media may be provided within "desMaxLatency" attribute and/or "desMaxLoss" attribute.

#### 4.2.2.30 Subscription to EPS Fallback report

When the "EPSFallbackReport" feature is supported, the NF service consumer subscribes to EPS Fallback report to be notified of the rejection in 5GS of the requested resources associated to service information for voice media type and the subsequent fallback to EPS of the resources associated to the voice media and other medias requested by this NF service consumer.

The NF service consumer shall use the "EventsSubscReqData" data type as described in clause 4.2.2.2 and shall include in the HTTP POST request message an event within the "events" attribute with the "event" attribute set to "EPS_FALLBACK". The NF service consumer shall request to the PCF to report EPS Fallback in conjuction with providing the PCF with NF service consumer service information for voice media type as described in clause 4.2.2.2.

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2.

As result of this action, the PCF shall set the appropriate subscription to EPS Fallback report for the corresponding PCC rule(s) as described in in 3GPP TS 29.512 [8].

#### 4.2.2.31 Subscription to TSC user plane node related events

This procedure is used by the NF service consumer (i.e. TSN AF or TSCTSF) if the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported to subscribe to notifications of updated TSC user plane node information, e.g., DS-TT PMIC and/or NW-TT PMIC(s) and/or UMIC availability within the Individual Application Session Context resource created to handle the TSC user plane node in the context of a PDU session.

The NF service consumer shall use the "EventsSubscReqData" data type as described in clause 4.2.2.2 and shall include in the HTTP POST request message within the "evSubsc" attribute an event within "events" attribute with the "event" attribute set to the value "TSN_BRIDGE_INFO" to subscribe to the reception of TSC user plane node information.

The PCF shall reply to the NF service consumer with an HTTP response message as described in clause 4.2.2.2.

As result of this action, the PCF shall set the corresponding subscription to TSC user plane node related events for the corresponding PDU session as described in as described in 3GPP TS 29.512 [8].

#### 4.2.2.32 Initial provisioning of required QoS information

This procedure is used by a NF service consumer to request that a data session to a UE is set up with a specific QoS (e.g. low latency or jitter) and priority handling when the "AuthorizationWithRequiredQoS" feature is supported.

The NF service consumer may provide within one or more entries of the "medComponents" attribute included in the "ascReqData" attribute of the HTTP POST request message described in clause 4.2.2.2 a reference to pre-defined QoS information within the "qosReference" attribute.

Additionally, if the NF service consumer supports adjustment to different QoS parameter combinations, the NF service consumer may provide a prioritized list of one or more QoS references within the "altSerReqs" attribute, where the lower the index of the array for a given entry, the higher the priority.

If the "AltSerReqsWithIndQoS" feature is supported, and the NF service consumer requests that the data session to a UE is set up with individual QoS parameters (i.e., with QoS information within "medComponents" attribute, e.g. the

"tsnQos", "marBwUl" and/or "marBwDl" attributes, instead of a QoS reference within the "qosReference" attribute), the NF service consumer may instead of the "altSerReqs" attribute provide a prioritized list of alternative service requirements that include Requested Alternative QoS Parameter set(s) within the "altSerReqsData" attribute, where the lower the index of the array for a given entry, the higher the priority.

If the "DisableUENotification" feature is supported, the AF may also indicate to the PCF that the UE does not need to be informed about changes related to Alternative QoS Profiles by including the "disUeNotif" attribute set to true.

When the NF service consumer provides the "altSerReqs" attribute or the "altSerReqsData" attribute, the NF service consumer shall also subscribe to receive notifications from the PCF when the resources associated to the corresponding service information have been allocated as described in clause 4.2.2.10 and when the GBR QoS targets for one or more service data flows can no longer (or can again) be guaranteed, as described in clause 4.2.2.6.

Due to the received QoS information, the PCF may need to provision or modify the related PCC rules as specified in 3GPP TS 29.513 [7] and provide the related information towards the SMF following the corresponding procedures specified in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2.

### 4.2.2.33 Support of QoSHint feature

If the QoSHint feature is supported by the NF service consumer, the NF service consumer may include the "desMaxLatency" attribute and/or "desMaxLoss" attribute within a media component of the "medComponents" attribute to indicate that the related media of the created Individual Application Session Context resource has specific latency and/or loss demands.

### 4.2.2.34 Subscription to Reallocation of Credit notification

This procedure is used by the NF service consumer if the "IMS_SBI" and the "ReallocationOfCredit" features are supported to subscribe to notifications of reallocation of credit for the Service Data Flows within the AF application session context.

The NF service consumer shall use the "EventsSubscReqData" data type as described in clause 4.2.2.2 and shall include in the HTTP POST request message an event within the "evSubsc" attribute with the "event" attribute set to the value "REALLOCATION_OF_CREDIT".

As result of this action, the PCF shall set the appropriate subscription to reallocation of credit notification for the corresponding PCC rule(s) as described in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer with an HTTP response message as described in clause 4.2.2.2.

### 4.2.2.35 Subscription to satellite backhaul category changes

When the feature "SatelliteBackhaul" is supported, the subscription to satellite backhaul category changes is used by a NF service consumer to subscribe to receive a notification when the satellite backhaul category changes and when the backhaul category changes between satellite backhaul and non-satellite backhaul.

The NF service consumer shall use the "evSubsc" attribute as described in clause 4.2.2.2 and shall include in the HTTP POST request message an event within the "events" attribute with the "event" attribute set to "SAT_CATEGORY_CHG".

The PCF shall reply to the NF service consumer as described in clause 4.2.2.2. The PCF shall include the "evsNotif" attribute with an entry in the "evNotifs" array with the "event" attribute set to "SAT_CATEGORY_CHG" and the "satBackhaulCategory" attribute including the satellite backhaul category or the indication of non-satellite backhaul if the PCF has previously requested to the SMF to be updated with this information.

As result of this action, the PCF shall set the appropriate subscription to satellite backhaul changes for the PDU session, if not previously subscribed, as described in in 3GPP TS 29.512 [8].

## 4.2.3 Npcf_PolicyAuthorization_Update service operation

### 4.2.3.1 General

The Npcf_PolicyAuthorization_Update service operation provides updated application level information from the NF service consumer and optionally communicates with the Npcf_SMPolicyControl service to determine and install the policy according to the information provided by the NF service consumer.

The Npcf_PolicyAuthorization_Update service operation updates an application session context in the PCF.

The following procedures using the Npcf_PolicyAuthorization_Update service operation are supported:

- Modification of service information.
- Gate control.
- Background Data Transfer policy indication at policy authorization update.
- Modification of sponsored connectivity information.
- Modification of Subscription to Service Data Flow QoS notification control.
- Modification of Subscription to Service Data Flow Deactivation.
- Update of traffic routing information.
- Modification of subscription to resources allocation outcome.
- Modification of Multimedia Priority Services.
- Support of content versioning.
- Request of access network information.
- Modification of service information status.
- Support of SIP forking.
- Provisioning of signalling flow information.
- Support of resource sharing.
- Modification of MCPTT.
- Modification of MCVideo.
- Priority sharing indication.
- Modification of subscription to out of credit notification.
- Modification of Subscription to Service Data Flow QoS Monitoring Information.
- Update of TSCAI Input Information and TSC QoS related data.
- Provisioning of TSC user plane node management information and port management information.
- Support of CHEM feature.
- Support of FLUS feature.
- Subscription to EPS Fallback report.
- Modification of required QoS information.
- Support of QoSHint feature.
- Modification of subscription to reallocation of credit notification.

- Modification of subscription to satellite backhaul category changes.

### 4.2.3.2 Modification of service information

This procedure is used to modify an existing application session context as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4] when the feature "PatchCorrection" is supported.

Figure 4.2.3.2-1 illustrates the modification of service information using HTTP PATCH method.

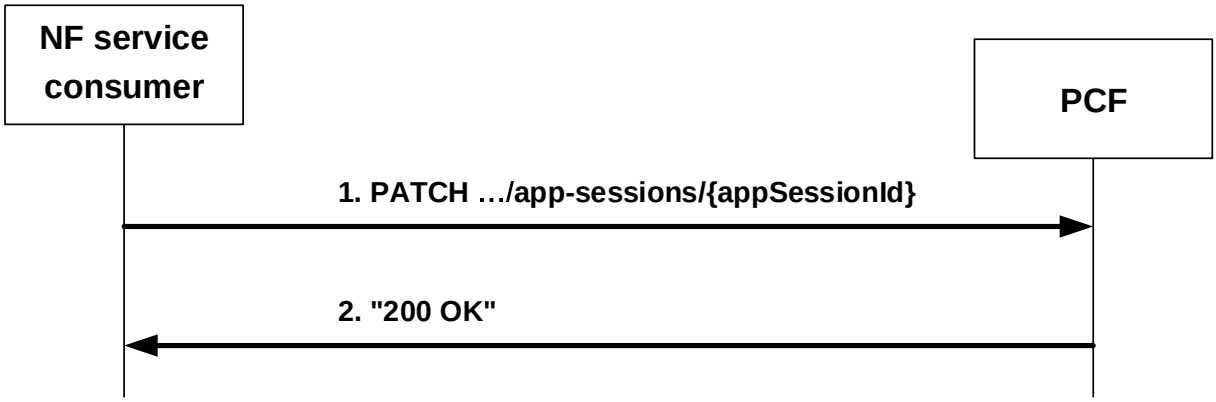


**Figure 4.2.3.2-1: Modification of service information using HTTP PATCH**

The NF service consumer may modify the application session context information at any time (e.g. due to an AF session modification or internal NF service consumer trigger) and invoke the Npcf_PolicyAuthorization_Update service operation by sending the HTTP PATCH request message to the resource URI representing the "Individual Application Session Context" resource, as shown in figure 4.2.3.2-1, step 1, with the modifications to apply.

The JSON body within the PATCH request shall include the "AppSessionContextUpdateDataPatch" data type and shall be encoded according to "JSON Merge Patch", as defined in IETF RFC 7396 [21]. The modifications to apply are encoded within the attributes of the "ascReqData" attribute, as described below and in subsequent clauses.

The NF service consumer may include the updated service information in the "medComponents" attribute of the "ascReqData" attribute.

If the "AuthorizationWithRequiredQoS" feature as defined in clause 5.8 is supported, the NF service consumer may provide within the MediaComponentRm data structure an update of the required QoS information as specified in clause 4.2.3.30.

The NF service consumer may include in the "ascReqData" attribute an AF application identifier in the "afAppId" attribute to trigger the PCF to indicate to the SMF/UPF to perform the application detection based on the operator's policy as defined in 3GPP TS 29.512 [8].

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported, the NF service consumer may provide TSC user plane node related information as specified in clauses 4.2.3.24 and 4.2.3.25.

The NF service consumer may also create, modify or remove events subscription information by sending the HTTP PATCH request message to the resource URI representing the "Individual Application Session Context" resource.

The NF service consumer shall create event subscription information by including in the "ascReqData" attribute the "evSubsc" attribute of "EventsSubscReqDataRm" data type with the corresponding list of events to subscribe to; and the "notifUri" attribute with the notification URI where the PCF shall send the notifications.

The NF service consumer shall update existing event subscription information by including in the "ascReqData" attribute an updated value of the "evSubsc" attribute of the "EventsSubscReqDataRm" data type as follows:

- The "events" attribute shall include the new complete list of subscribed events.
- When the NF service consumer requests to update the additional information related to an event (e.g. the NF service consumer needs to provide new thresholds to the PCF in the "usgThres" attribute related to the

"USAGE_REPORT" event) the NF service consumer shall include the additional information, which shall completely replace the previously provided one.

NOTE 1: Note that when the NF service consumer requests to remove an event, this event is not included in the "events" attribute.

NOTE 2: When an event is included in the "events" attribute and its related additional information is set to null, the PCF considers the subscription to this event is active, but the related procedures stop applying.

NOTE 3: When an event is removed from the "events" attribute but its related information is not set to null, the PCF considers the subscription to this event is terminated, the related additional information is removed, and the related procedures stop applying.

The NF service consumer shall remove existing event subscription information by setting to null the "evSubsc" attribute included in the "ascReqData" attribute.

Events with "notifMethod" set to "ONE_TIME" shall only apply at the time the NF service consumer requests their subscription. Once the event report is performed, the subscription to this event is automatically terminated in the PCF and the related information is removed. The presence of a one-time event, together with its related additional information when applicable, during an update procedure shall represent the recreation of the subscription to this event in the PCF.

NOTE 4: The "notifUri" attribute within the EventsSubscReqData data structure can be modified to request that subsequent notifications are sent to a new NF service consumer.

If the PCF cannot successfully fulfil the received HTTP PATCH request due to the internal PCF error or due to the error in the HTTP PATCH request, the PCF shall send the HTTP error response as specified in clause 5.7.

If the feature "ES3XX" is supported, and the PCF determines the received HTTP PATCH request needs to be redirected, the PCF shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [5].

Otherwise, the PCF shall process the received service information according the operator policy and may decide whether the HTTP request message is accepted or not.

If the updated service information is not acceptable (e.g. the subscribed guaranteed bandwidth for a particular user is exceeded or the authorized data rate in that slice for the UE is exceeded), the PCF shall include in an HTTP "403 Forbidden" response message the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED".

If the PCF detects that a temporary network failure has occurred (e.g. the SGW has failed as defined in clause B.3.3.3 or B.3.4.9 of 3GPP TS 29.512 [8]) and the AF initiates an Npcf_PolicyAuthorization_Update service operation, the PCF shall reject the request with an HTTP "403 Forbidden" response including the "cause" attribute set to "TEMPORARY_NETWORK_FAILURE".

If the service information provided in the HTTP PATCH request is rejected due to a temporary condition in the network (e.g. the NWDAF reported the network slice selected for the PDU session is congested), the PCF may include in the "403 Forbidden" response the "cause" attribute set to "REQUESTED_SERVICE_TEMPORARILY_NOT_AUTHORIZED". The PCF may also provide a retry interval within the "Retry-After" HTTP header field. When the NF service consumer receives the retry interval within the "Retry-After" HTTP header field, the NF service consumer shall not send the same service information to the PCF again (for the same application session context) until the retry interval has elapsed. The "Retry-After" HTTP header is described in 3GPP TS 29.500 [5] clause 5.2.2.2.

NOTE 5: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8] and the authorized data rate in a slice is exceeded due to the bandwidth demands of the modified service information, it is also possible to accept the request based on operator policies. In this case the derived PCC rule(s) belonging to the authorized GBR service data flows can include a different MBR and/or have a different charging than the one applicable if the data rate is not exceeded as specified in 3GPP TS 29.512 [8].

The PCF may additionally provide the acceptable bandwidth within the attribute "acceptableServInfo" included in the "ExtendedProblemDetails" data structure returned in the rejection response message.

If the request is accepted, the PCF shall update the service information with the new information received. Due to the updated service information, the PCF may need to create, modify or delete the related PCC rules as specified in

3GPP TS 29.513 [7] and provide the updated information towards the SMF following the corresponding procedures specified in 3GPP TS 29.512 [8].

Based on the received subscription information from the NF service consumer, the PCF may create a subscription to event notifications or may modify the existing subscription to event notifications, for a related PDU session from the SMF, as described in 3GPP TS 29.512 [8].

The PCF shall reply with the HTTP response message to the NF service consumer and may include the "AppSessionContext" data type payload body with the representation of the modified "Individual Application Session Context" resource and may include the "Events Subscription" sub-resource.

The PCF shall include in the "evsNotif" attribute:

- if the NF service consumer subscribed to the "PLMN_CHG" event in the HTTP PATCH request, the "event" attribute set to "PLMN_CHG" and the "plmnId" attribute including the PLMN Identifier or the SNPN Identifier if the PCF has previously requested to be updated with this information in the SMF;

NOTE 6: The SNPN Identifier consists of the PLMN Identifier and the NID.

- if the NF service consumer subscribed to the event "ACCESS_TYPE_CHANGE" event in the HTTP PATCH request, the "event" attribute set to "ACCESS_TYPE_CHANGE" and:

  i. the "accessType" attribute including the access type, and the "ratType" attribute including the RAT type when applicable for the notified access type; and

  ii. if the "ATSSS" feature is supported, the "addAccessInfo" attribute with the additional access type information if available, where the access type is encoded in the "accessType" attribute, and the RAT type is encoded in the "ratType" attribute when applicable for the notified access type; and

NOTE 7: For a MA PDU session, if the "ATSSS" feature is not supported by the NF service consumer, the PCF includes the "accessType" attribute and the "ratType" attribute with a currently active combination of access type and RAT type (if applicable for the notifed access type). When both 3GPP and non-3GPP accesses are available, the PCF includes the information corresponding to the 3GPP access.

  iii. the "anGwAddr" attribute including access network gateway address when available,

  if the PCF has previously requested to be updated with this information in the SMF; and

- if the "IMS_SBI" feature is supported and if the NF service consumer subscribed to the "CHARGING_CORRELATION" event in the HTTP PATCH request, the "event" attribute set to "CHARGING_CORRELATION" and may include the "anChargIds" attribute containing the access network charging identifier(s) and the "anChargAddr" attribute containing the access network charging address.

The NF service consumer subscription to other specific events using the Npcf_PolicyAuthorization_Update request is described in the related clauses. Notification of events when the applicable information is not available in the PCF when receiving the Npcf_PolicyAuthorization_Update request is described in clause 4.2.5.

The HTTP response message towards the NF service consumer should take place before or in parallel with any required PCC rule provisioning towards the SMF.

If the PCF does not have an existing application session context for the application session context being modified (such as after a PCF failure), the PCF shall reject the HTTP request message with the HTTP response message with the applicable rejection cause.

#### 4.2.3.3 Gate control

This procedure is used by a NF service consumer to modify in the PCF the service data flow(s) that are to be enabled or disabled to pass through the PDU session.

The NF service consumer shall use the HTTP PATCH method to modify the gate control information.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, in the media component(s) included in the "medComponents" attribute at media and/or media subcomponent level, the "fStatus" attribute for the flows to be enabled or disabled with the appropriate value.

If a "medSubComps" attribute contains a "flowUsage" attribute with the value "RTCP", then the IP Flows described by that media subcomponent shall be enabled in both directions irrespective of the value of the "fStatus" attribute of the corresponding media component.

As result of this action, the PCF shall set the appropriate gate status for the corresponding active PCC rule(s).

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

#### 4.2.3.4 Background Data Transfer policy indication at policy authorization update

This procedure is used by a NF service consumer to indicate at policy authorization update a transfer policy negotiated for background data transfer using the Npcf_BDTPolicyControl service as described in 3GPP TS 29.554 [14].

The NF service consumer may include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, a new reference id in the "bdtRefId" attribute.

NOTE 1: The PCF will retrieve the corresponding transfer policy from the UDR based on the reference identifier within the "bdtRefId" attribute. In case only one PCF is deployed in the network, transfer policies can be locally stored in the PCF and the interaction with the UDR is not required.

If the PCF cannot retrieve the transfer policy, the PCF shall set to TP_NOT_KNOWN the "servAuthInfo" attribute in the HTTP response message to the NF service consumer to indicate that the transfer policy is unknown.

If the time window of the received transfer policy has expired, the PCF shall set to TP_EXPIRED the "servAuthInfo" attribute in the HTTP response message to indicate to the NF service consumer that the transfer policy has expired. Otherwise, if the time window of the received transfer policy has not yet occurred, the PCF shall set to TP_NOT_YET_OCCURRED the "servAuthInfo" attribute in the HTTP response message to the NF service consumer to indicate that the time window of the transfer policy has not yet occurred.

NOTE 2: In the case that the PCF cannot retrieve the transfer policy, the transfer policy time window has not yet occurred or the transfer policy expired, the PCF makes the decision without considering the transfer policy.

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

#### 4.2.3.5 Modification of sponsored connectivity information

This procedure is used by a NF service consumer to modify sponsored data connectivity when "SponsoredConnectivity" feature is supported.

The NF service consumer shall use the HTTP PATCH method to modify the sponsored connectivity information.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, an application service provider identity and a sponsor identity within the "aspId" attribute and "sponId" attribute, and optionally an indication of whether to enable or disable sponsored data connectivity within the "sponStatus" attribute set to the applicable value to provide sponsored connectivity information or to update existing sponsored connectivity information.

If the NF service consumer requests to enable sponsored data connectivity the NF service consumer shall change the "sponStatus" attribute value to "SPONSOR_ENABLED".

If the NF service consumer requests to disable sponsored data connectivity the NF service consumer shall provide an indication to disable sponsored data connectivity to the PCF by setting the "sponStatus" attribute to "SPONSOR_DISABLED".

To support the usage monitoring of sponsored data connectivity, the NF service consumer may also include in the HTTP PATCH a new or modified "evSubsc" attribute of "EventsSubscReqDataRm" data type with:

- the usage thresholds to apply in the "usgThres" attribute; and
- the subscription to usage monitoring for sponsored data connectivity in an entry of the "events" attribute of the "AfEventSubscription" data type with the "event" attribute set to "USAGE_REPORT".

NOTE 1: If the NF service consumer is in the user plane, the NF service consumer can handle the usage monitoring and therefore it is not required to provide a usage threshold to the PCF as part of the sponsored data connectivity information.

When the NF service consumer indicated to enable sponsored data connectivity, and the UE is roaming with the visited access case, the following procedures apply:

- If the NF service consumer is located in the HPLMN, for home routed roaming case and when operator policies do not allow accessing the sponsored data connectivity with this roaming case, the H-PCF shall reject the service request and shall include in the HTTP "403 Forbidden" response message the "cause" attribute set to "UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY".

- If the NF service consumer is located in the VPLMN, the V-PCF shall reject the service request and shall include in the HTTP "403 Forbidden" response message the "cause" attribute set to "UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY".

When the NF service consumer indicated to enable sponsored data connectivity, and the UE is in the non-roaming case or roaming with the home routed case and the operator policies allow accessing the sponsored data connectivity with this roaming case, the following procedures apply:

- If the SMF does not support sponsored connectivity and the required reporting level for that service indicates a sponsored connectivity level according to 3GPP TS 29.512 [8], then the PCF shall reject the request and shall include in the HTTP "403 Forbidden" response message the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED".

- If the SMF supports sponsored data connectivity feature or the required reporting level is different from sponsored connectivity level as described in 3GPP TS 29.512 [8], then the PCF, based on operator policies, shall check whether it is required to validate the sponsored connectivity data. If it is required, it shall perform the authorizations based on sponsored data connectivity profiles. If the authorization fails, the PCF shall include in the HTTP "403 Forbidden" response message the "cause" attribute set to "UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY".

NOTE 2: The PCF is not required to verify that a trust relationship exists between the operator and the sponsors.

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

### 4.2.3.6 Modification of Subscription to Service Data Flow QoS notification control

This procedure is used in the NF service consumer to modify in the PCF the subscription to notification about whether the GBR QoS targets can no longer (or can again) be guaranteed.

The NF service consumer shall use the HTTP PATCH method to update the "Events Subscription" sub-resource together with the modifications to the "Individual Application Session Context" resource.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the updated values of the "EventsSubscReqDataRm" data type, which either shall include in the "events" attribute a new element with the "event" attribute set to "QOS_NOTIF" to indicate the subscription to QoS notification control, or shall not include in the "events" attribute an existing element with the "event" attribute set to "QOS_NOTIF" to indicate the termination of the subscription to QoS notification control.

As result of this action, the PCF shall set the appropriate subscription to QoS notification control for the corresponding active PCC rule(s) as described in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

### 4.2.3.7 Modification of Subscription to Service Data Flow Deactivation

This procedure is used by a NF service consumer to modify in the PCF the subscription to the notification of deactivation of one or more Service Data Flows within the AF application session context.

The NF service consumer shall use the HTTP PATCH method to update the "Events Subscription" sub-resource together with the modifications to the "Individual Application Session Context" resource.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the updated values of the "EventsSubscReqDataRm" data type, which either shall include in the "events" attribute a new element with the "event" attribute set to "FAILED_RESOURCES_ALLOCATION" to indicate the subscription to service data flow deactivation, or shall not include in the "events" attribute an existing element with the "event" attribute set to "FAILED_RESOURCES_ALLOCATION".

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

As result of this action, the PCF shall set the appropriate subscription to service data flow deactivation for the corresponding PCC rule(s) as described in in 3GPP TS 29.512 [8].

### 4.2.3.8 Update of traffic routing information

This procedure is used by NF service consumer to modify in the PCF the traffic routing information to a local access to a DNN, and/or to modify the subscription to notifications about UP path management when "InfluenceOnTrafficRouting" feature is supported.

When the "SimultConnectivity" feature is supported, this procedure may be used to modify (create, delete, update) the indication of simultaneous connectivity temporarily maintained for the source and target PSA and/or the indication of the minimum time interval to be considered for inactivity for the traffic routed via the source PSA.

When the "URLLC" feature is supported, this procedure may be used to modify (create, delete, update) the indication of UE IP address preservation.

When the "EASIPreplacement" feature is supported, this procedure may be used to modify (initially provide, delete, update) the EAS IP replacement information to the PCF.

The NF service consumer shall use the HTTP PATCH method.

To modify traffic routing information, the NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, an updated "afRoutReq" attribute(s) with the modified traffic routing information. To modify the indication of simultaneous connectivity and/or the termination of the simultaneous connectivity, the NF service consumer shall include an updated "simConnInd" attribute and/or an updated "simConnTem" attribute, if applicable. To modify the indication of UE IP address preservation, the NF service consumer shall include the updated indication of UE IP address preservation in the "addrPreserInd" attribute, if applicable. To modify the EAS IP replacement information, the NF service consumer shall include the updated/new "easIpReplaceInfos" attribute, if applicable. To modify the maximum allowed user plane latency, the NF service consumer shall include the updated/new "maxAllowedUpLat" attribute, if applicable.

To modify the subscription to notifications about UP path management events (create, delete or modify), the NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the updated values of the "upPathChgSub" attribute with the modified subscription to UP path management events.

When the feature "RoutingReqOutcome" is supported:

- and the NF service consumer is creating or modifying AF routing information, the PCF may set the "servAuthInfo" attribute in the HTTP response message to "ROUT_REQ_NOT_AUTHORIZED" when the PCF determines, e.g. based on subscription, the AF influence on traffic routing is not allowed for the PDU session;

- when the NF service consumer requests the update of the steering of traffic to a DNAI and/or the subscription to notifications about UP path management events, the NF service consumer may subscribe to notifications of failures in the enforcement of UP path changes including within the "evSubsc" attribute the "event" attribute value "UP_PATH_CHG_FAILURE" in an entry of the "events" array, or may remove the subscription to notification of failures in the enforcement of UP path changes by not including the the "event" attribute value "UP_PATH_CHG_FAILURE" in an entry of the "events" array of the "evSubsc" attribute.

NOTE: In the case that the PCF determines that the requested AF routing requirements cannot be applied and returns the "servAuthInfo" attribute in the HTTP response, the PCF makes the decision without considering the requested AF routing requirements.

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

The PCF shall store the application routing requirements included in the "afRoutReq" attribute.

The PCF shall check whether the updated application routing requirements require PCC rules to be created or modified to include updated traffic steering policies, or the AF transaction identifier, or to update the application relocation possibility as specified in 3GPP TS 29.513 [7]. Provisioning of PCC rules to the SMF shall be carried out as specified at 3GPP TS 29.512 [8].

#### 4.2.3.9 Void

#### 4.2.3.10 Modification of subscription to resources allocation outcome

This procedure is used in the NF service consumer to modify in the PCF the subscription to notification about resources allocation outcome.

The NF service consumer shall use the HTTP PATCH method to update the "Events Subscription" sub-resource together with the modifications to the "Individual Application Session Context" resource.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the updated values of the "EventsSubscReqDataRm" data type, which either include in the "events" attribute a new element with the "event" attribute set to "SUCCESSFUL_RESOURCES_ALLOCATION" and/or "FAILED_RESOURCES_ALLOCATION" or remove in the "events" attribute an existing element with the "event" attribute set to "SUCCESSFUL_RESOURCES_ALLOCATION" and/or "FAILED_RESOURCES_ALLOCATION".

As a result of this action, the PCF shall set the appropriate subscription to notification of resources allocation outcome in the corresponding PCC Rule(s) as described in 3GPP TS 29.512 [8].

#### 4.2.3.11 Void

#### 4.2.3.12 Modification of Multimedia Priority Services

The NF service consumer may include, in the "ascReqData" attribute, the "mpsId" attribute if it was not previously provided in order to indicate that the modified AF session relates to an MPS session.

If the NF service consumer supports the SBI Message Priority mechanism for an MPS session, the NF service consumer shall include the "3gpp-Sbi-Message-Priority" custom HTTP header towards the PCF as described in clause 4.2.2.12.1.

If the PCF receives the "mpsId" attribute, the PCF shall take specific actions on the corresponding PDU session to ensure that the MPS session is prioritized as defined in 3GPP TS 29.512 [8].

NOTE: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8], it is possible that, subject to operator policy and national/regional regulations, prioritised services are exempted from the limitation of data rate per network slice. In that case the PCF will handle the request from the NF service consumer even if the authorized data rate per network slice is exceeded.

When the feature "MPSforDTS" is supported, the NF service consumer includes the "mpsAction" attribute to invoke or revoke MPS for DTS, as specified in clause 4.2.2.12.2. When invoking MPS for DTS, the NF service consumer shall include the "mpsAction" attribute set to "ENABLE_MPS_FOR_DTS" or "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS". When the "ENABLE_MPS_FOR_DTS" value is received in the "mpsAction" attribute, and allowed by local policy, the PCF does not check the authorization of the request. When the "AUTHORIZE_AND_ENABLE_MPS_FOR_DTS" value is received in the "mpsAction" attribute, and allowed by local policy, the PCF shall check the user's MPS subscription to authorize the request. When the request is to authorize and enable, and the request is not authorized (e.g. not allowed by MPS subscription), the PCF shall indicate in an HTTP "403 Forbidden" response message the cause for the rejection including the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED".

To revoke MPS for DTS, the NF service consumer shall include the "mpsAction" attribute set to "DISABLE_MPS_FOR_DTS". When the "DISABLE_MPS_FOR_DTS" value is received in the "mpsAction" attribute, and allowed by local policy, the PCF does not check the authorization of the request.

When modifying an Individual Application Session Context resource due to the invocation or revocation of the MPS for DTS service, the NF service consumer may subscribe to the outcome of the QoS updates by setting within the "evSubsc" attribute an event within the "events" array with:

- the "event" attribute set to the value "SUCCESSFUL_QOS_UPDATE" to report that the invocation/revocation requested by the NF service consumer was successful; and/or
- the "event" attribute set to the value "FAILED_QOS_UPDATE" to report that the invocation/revocation requested by the NF service consumer has failed.

#### 4.2.3.13 Support of content versioning

The support of the media component versioning is optional. When the "MediaComponentVersioning" feature is supported, the NF service consumer and the PCF shall comply with the procedures specified in this clause.

Upon each media component modification encoded in the "medComponents" attribute included in the "ascReqData" attribute, if the content version was previously assigned to a media component, the NF service consumer shall assign a new content version. All the content related to that media component shall be included and the content version shall be unique for the lifetime of the media component.

NOTE: The NF service consumer will include all the content of the media component in each media component modification in order to ensure that the media component is installed with the proper information regardless of the outcome of the QoS flow procedure related to previous interactions that are not reported to the PCF yet.

If the PCF receives the "contVer" attribute for a certain media component, the PCF shall follow the procedures described in 3GPP TS 29.512 [8], clause 4.2.6.2.14.

#### 4.2.3.14 Request of access network information

This procedure is used by a NF service consumer to request access network information for an existing "Individual Application Session Context" resource at service information modification when the "NetLoc" feature is supported.

NOTE 1: Clause 4.2.6.6 describes the NF service consumer request of access network information without providing service information.

The NF service consumer shall create event subscription information by including in the "AppSessionContextUpdateData" data type the "evSubsc" attribute of "EventsSubscReqData" data type with the corresponding list of events to subscribe to.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute:

- an entry of the "AfEventSubscription" data type in the "events" attribute with:
  a) the "event" attribute set to the value "ANI_REPORT"; and
  b) the "notifMethod" attribute set to the value "ONE_TIME"; and
- the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

When the PCF determines that the access network does not support the access network information reporting because the SMF does not support the NetLoc feature, the PCF shall respond to the NF service consumer including in the "EventsNotification" data type the "noNetLocSupp" attribute set to "ANR_NOT_SUPPORTED" value. Otherwise, the PCF shall immediately configure the SMF to provide such access information, as specified in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer with an HTTP response message as described in clause 4.2.3.2.

NOTE 2: The NF service consumer does not invoke the Npcf_PolicyAuthorization_Update service operation to remove subscription to access network information report since the "Access Network Information Notification" is the one-time reported event. Once the access network information is reported to the NF service consumer the subscription to the access network information report is automatically terminated in the PCF and the related information is removed.

#### 4.2.3.15 Modification of service information status

When the "IMS_SBI" feature is supported, the NF service consumer may update the status of the service information. If the NF service consumer provides service information that has been fully negotiated (e.g. based on the SDP answer), the NF service consumer may include in the "ascReqData" attribute the "servInfStatus" attribute set to "FINAL". In this case the PCF shall authorize the session and provision the corresponding PCC rules to the SMF.

The NF service consumer may additionally provide preliminary service information not fully negotiated yet (e.g. based on the SDP offer) at an earlier stage. To do so, the NF service consumer shall include the "servInfStatus" attribute set to "PRELIMINARY". Upon receipt of such preliminary service information, the PCF shall perform an early authorization check of the service information. If the NF service consumer requests the PCF to report the access network information together with preliminary service information, the PCF shall immediately configure the SMF to provide the access network information.

#### 4.2.3.16 Support of SIP forking

When the "IMS_SBI" feature is supported, this procedure is used by a NF service consumer to indicate that an existing "Individual Application Session Context" resource comprises service information about several SIP dialogues.

The NF service consumer shall use the HTTP PATCH method to modify the service information.

The NF service consumer may include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the "sipForkInd" attribute and include the updated service information.

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

When the "sipForkInd" attribute gets the value:

- "SEVERAL_DIALOGUES", the PCF shall send additional PCC rules or individual data flow filters to already provided PCC rules as described in Annex B.3.1.
- "SINGLE_DIALOGUE", the PCF shall update installed PCC rules and Authorized-QoS information as described in Annex B.3.2.

#### 4.2.3.17 Provisioning of signalling flow information

This procedure is used by a NF service consumer to provision or de-provision information about the AF signalling IP flows between the UE and the NF service consumer.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute:

- when the procedure is used to provision information about the AF signalling IP flows, a media component within the "medComponents" attribute including the attributes described in clause 4.2.2.16 in the case of IMS restoration or clause 4.2.2.12.3 otherwise;
- when the procedure is used to de-provision information about the AF signalling IP flows, for the media subcomponents containing the AF signalling IP flows, the "fStatus" attribute set to the value "REMOVED".

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

#### 4.2.3.18 Support of resource sharing

When the "ResourceSharing" is supported by the NF service consumer and the PCF, the NF service consumer may include, in the "ascReqData" attribute, the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute within a media component of the "medComponents" attribute to indicate to the PCF that the related media of the modified Individual Application Session Context resource may share resources with other media components in the related direction that include the same value in the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute.

The NF service consumer may modify the conditions for resource sharing by including the media component within the "medComponents" attribute with a new value for the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute. The NF service consumer may indicate that the related media of the modified Individual Application Session resource is not

sharing resources with other media components in the related direction setting the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute to "null".

The NF service consumer shall use the HTTP PATCH method to update the "Individual Application Session Context resource" as described in clause 4.2.3.2.

If the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute are provided within a media component of the "medComponents" attribute, the PCF may apply the mechanisms for resource sharing as described in 3GPP TS 29.512 [8], clause 4.2.6.2.8.

### 4.2.3.19 Modification of MCPTT

The NF service consumer may include, in the "ascReqData" attribute, the "mcpttId" attribute in order to indicate that the modified "Individual Application Session Context" resource relates to the priority adjustment of an MCPTT session. When the PCF receives the "mcpttId" attribute related to that MCPTT session, the PCF may take specific actions on the corresponding PDU session to ensure that the MCPTT session is prioritized. For the handling of MCPTT session with priority call, see Annex B.13.

NOTE: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8], it is possible that, subject to operator policy and national/regional regulations, prioritised services are exempted from the limitation of data rate per network slice. In that case the PCF will handle the request from the NF service consumer even if the authorized data rate per network slice is exceeded.

Additionally, when the "PrioritySharing" feature is supported, the PCF may receive the "prioSharingInd" attribute within the media component received in the "medComponents" attribute as described in clause 4.2.2.21. In this case, and if "MCPTT-Preemption" feature is supported, the PCF may receive pre-emption information as also described in clause 4.2.3.21.

### 4.2.3.20 Modification of MCVideo

The NF service consumer may include, in the "ascReqData" attribute, the "mcVideoId" attribute in order to indicate that the modified "Individual Application Session Context" resource relates to the priority adjustment of an MCVideo session. When the PCF receives the "mcVideoId" attribute related to that MCVideo session, the PCF may take specific actions on the corresponding PDU session to ensure that the MCVideo session is prioritized. For the handling of MCVideo session with priority call, see Annex B.15.

NOTE: When the PCF supports data rate control per network slice and/or data rate control per network slice for a UE as specified in 3GPP TS 29.512 [8], it is possible that, subject to operator policy and national/regional regulations, prioritised services are exempted from the limitation of data rate per network slice. In that case the PCF will handle the request from the NF service consumer even if the authorized data rate per network slice is exceeded.

### 4.2.3.21 Priority sharing indication

When the "PrioritySharing" feature is supported, the NF service consumer may include the "prioSharingInd" attribute set to "ENABLED" within a media component of the "medComponents" attribute included in the "ascReqData" attribute to indicate to the PCF that the related media flow is allowed to use the same Allocation and Retention Priority (ARP) as media flows belonging to other "Individual Application Session Context" resources as described in clause 4.2.2.21. In this case, if the "MCPTT-Preemption" feature is supported, the NF service consumer may also include the "preemptCap", "preemptVuln" and "preemptControlInfo" attributes as described in clause 4.2.2.21.

When the "preemptControlInfo" attribute is modified, the latest provided value shall be applied to all potential media flow candidates.

If the NF service consumer earlier has indicated a media flow priority sharing to the PCF by setting the "prioSharingInd" attribute to "ENABLED", the NF service consumer may include the Priority-Sharing-Indicator AVP set to "DISABLED" within a media component of the "medComponents" attribute to indicate to the PCF that the related media flow shall not be part of the mechanism for sharing the Allocation and Retention Priority with other media flows any longer.

If this media flow was in priority sharing with other media flows the PCF should readjust the Allocation and Retention Priority for the remaining services sharing priority as described in 3GPP TS 29.512 [8], clause 4.2.6.2.9 and handle the

media flow excluded from priority sharing according to normal PCC/QoS rule provisioning procedures described in 3GPP TS 29.512 [8], clause 4.2.6.2.

If the NF service consumer earlier has indicated a media flow priority sharing to the PCF by setting the "prioSharingInd" attribute to "ENABLED" for media flows and the NF service consumer indicates to remove one or more of the media flows in priority sharing with other media flows, the PCF should readjust the Allocation and Retention Priority for the remaining services sharing priority as described in 3GPP TS 29.512 [8], clause 4.2.6.2.9 and handle the media flow removed according to normal PCC/QoS rule provisioning procedures described in 3GPP TS 29.212 [8], clause 4.2.6.2.

### 4.2.3.22 Modification of Subscription to Out of Credit notification

This procedure is used by the NF service consumer if the "IMS_SBI" feature is supported to modify in the PCF the subscription to notification about credit unavailability for the Service Data Flows within the AF application session context.

The NF service consumer shall use the HTTP PATCH method to update the "Events Subscription" sub-resource together with the modifications to the "Individual Application Session Context" resource.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the updated values of the "EventsSubscReqDataRm" data type, which either include in the "events" attribute a new element with the "event" attribute set to the value "OUT_OF_CREDIT" or remove from the "events" attribute the existing element with the "event" attribute set to the value "OUT_OF_CREDIT".

As a result of this action, the PCF shall set the appropriate subscription to out of credit notification for the corresponding PCC Rule(s) as described in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer with an HTTP response message as described in clause 4.2.3.2.

### 4.2.3.23 Modification of Subscription to Service Data Flow QoS Monitoring Information

This procedure is used by NF service consumer to modify the PCF subscription for notification about packet delay between UPF and UE, when the "QoSMonitoring" feature is supported.

The NF service consumer shall use the HTTP PATCH method to update the "Events Subscription" sub-resource together with the modifications to the "Individual Application Session Context" resource.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the updated values of the "evSubsc" attribute of "EventsSubscReqDataRm" data type, as follows:

- to create a subscription to notifications of QoS monitoring report:

  a) shall include the "events" array with an array that contains a new entry per requested notification method with the "event" attribute set to "QOS_MONITORING", and notification related information as described in clause 4.2.2.23;

  b) when the "notifMethod" of the new entry is "EVENT_DETECTION", shall include a "qosMon" attribute with the QoS monitoring information as described in clause 4.2.2.23.

  c) shall include the new requested QoS monitoring parameter(s) to be measured (i.e. DL, UL and/or round trip packet delay) within the "reqQosMonParams" attribute;

  d) may include the notification correlation identifier assigned by the AF within the "notifCorreId" attribute;

  e) if the feature " ExposureToEAS" is supported, may include the "directNotifInd" attribute set to true to indicate the direct event notification of QoS Monitoring data from the UPF; and

- to remove a subscription to QoS monitoring information:

  a) shall include the "events" array containing an array that shall omit the corresponding entry with the "event" attribute value "QOS_MONITORING";

  b) when the "notifMethod" attribute of the removed entry is "EVENT_DETECTION", it shall contain the "qosMon" attribute set to null;

c) if the "directNotifInd" attribute was previously provided, it shall contain the "directNotifInd" attribute set to null.

As result of this action, the PCF shall set the appropriate subscription to QoS monitoring information for the corresponding active PCC rule(s) as described in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

### 4.2.3.24 Update of TSCAI Input Information and TSC QoS related data

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported, the NF service consumer may update the TSCAI Input container and the TSC QoS related data held in an "Individual Application Session Context" resource using the Npcf_PolicyAuthorization_Update service operation to modify the TSCAI input information and QoS characteristics delivered to the SMF for use in the 5G System.

The NF service consumer shall use the HTTP PATCH method as described in clause 4.2.3.2 to modify TSCAI input container and the TSC QoS related information.

The NF service consumer may indicate TSCAI input information and/or TSC QoS related information for new TSC streams by adding, in the "ascReqData" attribute, one or more media component entries within the "medComponents" attribute including the "tsnQos" attribute and including the "tscaiInputUl" attribute and/or the "tscaiInputDl" attribute and, when the feature "TimeSensitiveCommunication" is supported, the "tscaiTimeDom" attribute, if available as described in clause 4.2.2.24.

The NF service consumer may update the TSCAI input information and/or the TSC QoS related information for existing TSC traffic by including the updated values in the "tscaiInputUl" attribute and/or "tscaiInputDl"attribute and/orupdated values in the "tsnQos" attribute included in a media component entry of the "medComponents" attribute included in the "ascReqData" attribute.

The NF service consumer may delete the TSCAI input information and TSC QoS related information of removed TSC traffic by removing the corresponding media component entries within the "medComponents" attribute included in the "ascReqData" attribute.

Alternatively, when the "TimeSensitiveCommunication" and "AuthorizationWithRequiredQoS" features are supported, the NF service consumer (i.e., the TSCTSF or TSN AF) may update TSC QoS related information updating the "qosReference" attribute, and/or may indicate the update of the alternative service requirements updating the "altSerReqs" attribute as specified in clause 4.2.3.30.

When the "TimeSensitiveCommunication" and "AltSerReqsWithIndQoS" features are supported, the NF service consumer (i.e., the TSCTSF or TSN AF) may update TSC QoS related information updating the individual QoS requirement within the "tsnQos" attribute, and/or may indicate the update of the alternative service requirements updating the "altSerReqsData" attribute as specified in clause 4.2.3.30.

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

The PCF shall check whether the received TSCAI input information and TSC QoS related information require to modify or to remove PCC rules in the SMF. Provisioning of PCC rule(s) to the SMF shall be carried out as specified in 3GPP TS 29.512 [8].

### 4.2.3.25 Provisioning of TSC user plane node management information and port management information

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported the NF service consumer (i.e., the TSN AF or the TSCTSF) may provide a UMIC for the TSC user plane node functionality of the UPF/NW-TT and/or a PMIC for the DS-TT port and/or PMIC(s) for the NW-TT ports to update the configuration of the 5G system as a TSC user plane node by invoking the Npcf_PolicyAuthorization_Update service operation to the PCF.

The NF service consumer shall use the HTTP PATCH method as described in clause 4.2.3.2 to modify the "Individual Application Session Context" resource holding the UMIC and/or the DS-TT PMIC and/or NW-TT PMIC(s).

The NF service consumer may include in the "ascReqData" attribute:

- the DS-TT PMIC encoded in the "tsnPortManContDstt" and/or the one or more NW-TT PMIC(s)encoded in the "tsnPortManContNwtts", if available; and/or

- the UMIC encoded in the "tsnBridgeManCont", if available.

#### 4.2.3.26 Modification of Mission Critical Services

The NF service consumer may include, in the "ascReqData" attribute, the "mcsId" attribute if it was not previously provided in order to indicate that the modified AF session relates to an MCS session.

If the NF service consumer supports the SBI message priority mechanism for an MCS session, the NF service consumer shall include the "3gpp-Sbi-Message-Priority" custom HTTP header towards the PCF as described in clause 4.2.2.12.

If the PCF receives the "mcsId" attribute, the PCF shall take specific actions on the corresponding PDU session to ensure that the MCS session is prioritised as defined in 3GPP TS 29.512 [8].

#### 4.2.3.27 Support of CHEM feature

When CHEM feature is supported, the NF service consumer may include the value of Maximum Packet Loss Rate for UL within the "maxPacketLossRateUl" attribute and/or the value of Maximum Packet Loss Rate for DL within the "maxPacketLossRateDl" attribute in "medComponents" attribute. For CHEM feature, see Annex B.14.

#### 4.2.3.28 Support of FLUS feature

If the "FLUS" feature is supported by the NF service consumer, the NF service consumer may include the "flusId" attribute within a media component of the "medComponents" attribute to indicate that the related media of the modified Individual Application Session Context resource corresponds to a FLUS media stream. Additional QoS information for the treatment of FLUS media may be provided within "desMaxLatency" attribute and/or "desMaxLoss" attribute.

#### 4.2.3.29 Subscription to EPS Fallback report

When the "EPSFallbackReport" feature is supported, this procedure is used in the NF service consumer to subscribe to the notification of EPS Fallback events, if this event was not previously provisioned.

The NF service consumer shall use the HTTP PATCH method to update the "Events Subscription" sub-resource together with the modifications to the "Individual Application Session Context" resource.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the updated values of the "evSubsc" attribute of the "EventsSubscReqDataRm" data type, which shall include in the "events" attribute a new element with the "event" attribute set to "EPS_FALLBACK". The NF service consumer shall request to the PCF to report EPS Fallback in conjunction with providing the PCF with NF service consumer service information for voice media type as described in clause 4.2.3.2.

As result of this action, the PCF shall set the appropriate subscription to EPS Fallback for the corresponding active PCC rule(s) as described in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

#### 4.2.3.30 Modification of required QoS information

When the "AuthorizationWithRequiredQoS" feature is supported, this procedure is used by a NF service consumer to modify the required QoS by providing a different QoS reference(s) parameter while the AF session is ongoing. When the "AltSerReqsWithIndQoS" feature is supported, this procedure is used by a NF service consumer to modify the Requested Alternative QoS Parameter set(s).

The NF service consumer shall use the HTTP PATCH method to modify the required QoS information.

When the "AuthorizationWithRequiredQoS" feature is supported, the NF service consumer may include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, within one or more entries of the "medComponents" attribute included in the AppSessionContextUpdateData data type:

- a "qosReference" attribute, which may contain:

  i. a QoS reference, that replaces an existing QoS reference value if the "qosReference" attribute was previously provisioned, or creates a new one if no "qosReference" attribute was previously provisioned;

ii. a "null" value, which removes a previously provisioned "qosReference" attribute value.

- an "altSerReqs" attribute, which may contain:

  i. a prioritized list of alternative QoS references, which replaces an existing alternative QoS references list if the "altSerReqs" attribute was previously provisioned, or creates a new one if no "altSerReqs" attribute was previously provisioned;

  ii. a "null" value, which removes a previously provisioned alternative QoS references list.

When the "AltSerReqsWithIndQoS" feature is supported, and the service QoS is provided, or was previously provided using individual QoS parameters (e.g. "marBwUl" and/or "marBwDl", attributes) instead of a QoS reference, the NF service consumer may include within one or more entries of the "medComponents" attribute:

- an "altSerReqsData" attribute, which may contain:

  i. a prioritized list of alternative service requirements that include Requested Alternative QoS Parameter set(s), which replaces an existing list of alternative service requirements that include Requested Alternative QoS Parameter set(s) if the "altSerReqsData" attribute was previously provisioned, or creates a new one if no "altSerReqsData" attribute was previously provisioned;

  ii. a "null" value, which removes a previously provisioned list of alternative service requirements that include individual QoS parameter sets.

  NOTE: The modification of the individual QoS parameters is performed by provisioning within the "medComponents" attribute an update of the existing values or deleting the previously provided values, as described in clause 4.2.3.2.

When the "DisableUENotification" feature is supported, the NF service consumer may include a "disUeNotif" attribute, which may contain:

i. a "true" value if it was not provided or it was provided and set to "false";

ii. a "false" value if it was provided and set to "true".

When the NF service consumer provides the "altSerReqs" attribute containing a prioritized list of alternative QoS references or "altSerReqsData" attribute containing a prioritized list of alternative service requirements that include individual QoS parameter sets, the NF service consumer shall subscribe to receive notifications from the PCF when the resources associated to the corresponding service information have been allocated as described in clause 4.2.3.10 and when the GBR QoS targets for one or more service data flows can no longer (or can again) be guaranteed, as described in clause 4.2.3.6, if not previously subscribed.

Due to the updated required QoS information, the PCF may need to modify the related PCC rules as specified in 3GPP TS 29.513 [7] and provide the updated information towards the SMF following the corresponding procedures specified in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2.

### 4.2.3.31 Support of QoSHint feature

If the QoSHint feature is supported by the NF service consumer, the NF service consumer may include the "desMaxLatency" attribute and/or "desMaxLoss" attribute within a media component of the "medComponents" attribute to indicate that the related media of the modified Individual Application Session Context resource has specific latency and/or loss demands.

### 4.2.3.32 Modification of Subscription to Reallocation of Credit notification

This procedure is used by the NF service consumer if the "IMS_SBI" and the "ReallocationOfCredit" features are supported to modify in the PCF the subscription to notification about reallocation of credit for the Service Data Flows within the AF application session context.

The NF service consumer shall use the HTTP PATCH method to update the "Events Subscription" sub-resource together with the modifications to the "Individual Application Session Context" resource.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the updated values of the "EventsSubscReqDataRm" data type, which either include in the "events" attribute a new element with the "event" attribute set to the value "REALLOCATION_OF_CREDIT" or remove from the "events" attribute the existing element with the "event" attribute set to the value "REALLOCATION_OF_CREDIT".

As a result of this action, the PCF shall set the appropriate subscription to reallocation of credit notification for the corresponding PCC Rule(s) as described in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer with an HTTP response message as described in clause 4.2.3.2.

#### 4.2.3.33 Modification of Subscription to satellite backhaul category changes

When the feature "SatelliteBackhaul" is supported, this procedure is used in the NF service consumer to modify in the PCF the subscription to notification about satellite backhaul category changes.

The NF service consumer shall use the HTTP PATCH method to update the "Events Subscription" sub-resource together with the modifications to the "Individual Application Session Context" resource.

The NF service consumer shall include in the HTTP PATCH request message described in clause 4.2.3.2, in the "ascReqData" attribute, the updated values of the "EventsSubscReqDataRm" data type, which shall include in the "events" attribute a new element with the "event" attribute set to "SAT_CATEGORY_CHG" to indicate the subscription to changes of satellite backhaul category or changes between satellite backhaul and non-satellite backhaul.

As result of this action, the PCF shall set the appropriate subscription to satellite backhaul changes for the PDU session as described in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer as described in clause 4.2.3.2. The PCF shall include the "evsNotif" attribute with an entry in the "evNotifs" array with the "event" attribute set to "SAT_CATEGORY_CHG" and the "satBackhaulCategory" attribute including the satellite backhaul category or the indication of non-satellite backhaul if the PCF has previously subscribed with the SMF to changes in this information.

### 4.2.4 Npcf_PolicyAuthorization_Delete service operation

#### 4.2.4.1 General

The Npcf_PolicyAuthorization_Delete service operation provides means for the NF service consumer to delete the context of application session information.

The following procedures using the Npcf_PolicyAuthorization_Delete service operation are supported:

- AF application session context termination.
- Reporting usage for sponsored data connectivity.
- Termination of Multimedia Priority Services.
- Request and report of access network information.
- Termination of MCPTT.
- Termination of MCVideo.
- Priority sharing indication.
- Report of RAN-NAS release cause.
- Termination of Mission Critical Services.

#### 4.2.4.2 AF application session context termination

This procedure is used to terminate an AF application session context for the service as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

Figure 4.2.4.2-1 illustrates the application session context termination.

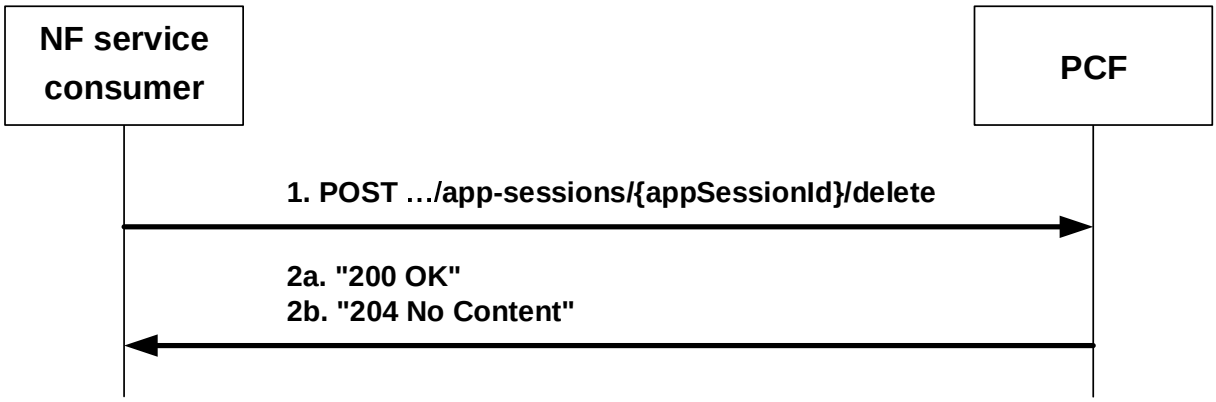


**Figure 4.2.4.2-1: Application session context termination**

When an AF session is terminated, and if the AF application session context was created as described in clause 4.2.2 or in clause 4.2.6.3, the NF service consumer shall invoke the Npcf_PolicyAuthorization_Delete service operation to the PCF using an HTTP POST request, as shown in figure 4.2.4.2-1, step 1.

The NF service consumer shall set the request URI to "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/delete".

The NF service consumer may include in the body of the HTTP POST the "EventsSubscReqData" data type with the "evSubsc" attribute indicating the corresponding list of events to subscribe to.

When the PCF receives the HTTP POST request from the NF service consumer, indicating the termination of the AF application session context information, the PCF shall acknowledge that request by sending an HTTP response message with the corresponding status code.

If the HTTP POST request from the NF service consumer is accepted, the PCF shall send to the NF service consumer:

a) if event information is reported, a "200 OK" response to HTTP POST request, as shown in figure 4.2.4.2-1, step 2a, including in the "AppSessionContext" data type the "evsNotif" attribute, which encodes within "evNotifs" attribute the event to report to the NF service consumer, if available, as described in clause 4.2.5.2. If the event information is not available at the PCF the PCF shall defer sending the response to the NF service consumer and shall immediately configure the SMF to provide such information, as specified in 3GPP TS 29.512 [8];

b) otherwise, the PCF shall send to the NF service consumer a "204 No Content".

Afterwards, the PCF shall free the network resources allocated for the Service Data Flow(s) corresponding to the deleted AF application session context information. In order to do that, the PCF shall initiate the request for the removal of any related PCC rules from the SMF, if not previously done, following the corresponding procedures specified in 3GPP TS 29.512 [8].

If the HTTP POST request from the NF service consumer is rejected, the PCF shall indicate in the response to HTTP POST request the cause for the rejection as specified in clause 5.7.

### 4.2.4.3 Reporting usage for sponsored data connectivity

When "SponsoredConnectivity" is supported, and the NF service consumer indicated to enable sponsored data connectivity and the NF service consumer provided usage thresholds for such sponsor to the PCF, the PCF shall report accumulated usage to the NF service consumer using the response of the Npcf_PolicyAuthorization_Delete service operation.

This procedure is initiated when:

- the "Individual Application Session Context" is deleted by the NF service consumer; or

- the PCF requests the deletion of the "Individual Application Session Context" to the NF service consumer, as described in clause 4.2.5.3, due to PDU session termination, the termination of all the service data flows of the AF session or the home operator policy disallowing the UE accessing the sponsored data connectivity in the roaming case.

To report the accumulated usage, the PCF shall immediately configure the SMF to retrieve the accumulated usage as specified in 3GPP TS 29.512 [8]. When the PCF receives the usage information from the SMF, the PCF shall notify the NF service consumer by including the "EventsNotification" data type in the response of the HTTP POST request as described in clause 4.2.4.2.

The PCF shall include:

- an event of the "AfEventNotification" data type in the "evNotifs" attribute with the matched event "USAGE_REPORT" in the "event" attribute; and

- the usage encoded in the "usgRep" attribute.

### 4.2.4.4 Void

### 4.2.4.5 Termination of Multimedia Priority Services

If the AF session being terminated corresponds to an MPS session, the PCF shall delete the PCC rules corresponding to the MPS session and the PCF shall revoke the actions related to the prioritization of the MPS session in the corresponding PDU Session as defined in 3GPP TS 29.512 [8].

If the AF session being terminated corresponds to an MPS for DTS session, the PCF shall revoke MPS for DTS session in the corresponding PDU Session as defined in 3GPP TS 29.512 [8].

### 4.2.4.6 Request and report of access network information

This procedure is used by a NF service consumer to request the PCF to report the access network information (i.e. user location and/or user timezone information) at the deletion of the "Individual Application Session Context" resource when the "NetLoc" feature is supported.

This procedure is initiated when:

- the "Individual Application Session Context" is deleted by the NF service consumer; or

- the PCF requests the deletion of the "Individual Application Session Context" from the NF service consumer, as described in clause 4.2.5.3, due to PDU session termination or the termination of all the service data flows of the AF session.

The NF service consumer shall include in the HTTP POST request message described in clause 4.2.4.2:

- an entry of the "AfEventSubscription" data type in the "events" attribute with:

  a) the "event" attribute set to the value "ANI_REPORT"; and

  b) the "notifMethod" attribute set to the value "ONE_TIME"; and

- the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

When the PCF determines that the access network does not support the access network information reporting because the SMF does not support the NetLoc feature, the PCF shall respond to the NF service consumer including in the "EventsNotification" data type the "noNetLocSupp" attribute set to "ANR_NOT_SUPPORTED" value. Otherwise, the PCF shall immediately configure the SMF to provide such access information, as specified in 3GPP TS 29.512 [8].

When the PCF receives the access network information from the SMF, the PCF shall provide the corresponding access network information to the NF service consumer by including the "EventsNotification" data type in the "200 OK" response to the HTTP POST request. The PCF shall include:

- in case of 3GPP access, the user location information in the "eutraLocation" or in the "nrLocation" attribute in the "ueLoc" attribute, if available and required;

- in case of untrusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if required, as follows:

  a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute, if available;

  b) the UDP source port or the TCP source port in the "portNumber" and "protocol" attributes, if available; and

  c) if the "WLAN_Location" feature is supported, the WLAN location information encoded in the "twapId" attribute, if available, that shall consist of:

     i. the SSID in the "ssId" attribute;

     ii. the BSSID the "bssId" attribute if available; and

     iii. the civic address in the "civicAddress" attribute if available;

NOTE 1: When the UE reaches the ePDG via a NAT, the combination of UE local IP address and the UE source port is needed for lawful interception purposes. The UE source port may be either a UDP or a TCP port, and it is indicated in the "protocol" attribute.

- in case of trusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if required, as follows:

  a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute, if available; and

  b) the UDP source port in the "portNumber" attribute if available; and

NOTE 2: The UDP protocol can be used between the UE and the TNGF to enable NAT traversal.

  c) either the TNAP identifier encoded in the "tnapId" attribute or the TWAP identifier encoded in the "twapId" attribute. The TNAP identifier and the TWAP identifier shall consist of:

     i. the SSID in the "ssId" attribute;

     ii. the BSSID the "bssId" attribute if available; and

     iii. the civic address in the "civicAddress" attribute if available;

- if user location was required, the time when it was last known in the "ueLocTime" attribute if available;

NOTE 3: The PCF derives the value of the "ueLocTime" attribute from the "userLocationInfoTime" attribute received from the SMF as specified in 3GPP TS 29.512 [8].

- the serving network identity i.e. the PLMN Identifier (the PLMN network code and the country code) or the SNPN Identifier (the PLMN Identifier and the NID) in the "plmnId" attribute, if user location information is required but not available in any access; and/or

- the UE timezone in the "ueTimeZone" attribute if required and available.

NOTE 4: The PCF forwards both 3GPP and non-3GPP access UE locations in the "ueLoc" attribute when both UE locations are provided by the SMF as defined in 3GPP TS 29.512 [8].

When the PCF receives from the SMF that the access network does not support access network information report, the PCF shall include the "noNetLocSupp" attribute set to "ANR_NOT_SUPPORTED", "TZR_NOT_SUPPORTED" or "LOC_NOT_SUPPORTED" value received from the SMF in the "EventsNotification" data type in the "200 OK" response to the HTTP POST request.

The PCF shall also include an event of the "AfEventNotification" data type in the "evNotifs" attribute with the "event" attribute set to the value "ANI_REPORT".

#### 4.2.4.7 Termination of MCPTT

If the "Individual Application Session Context" resource being removed corresponds to an MCPTT session, the PCF shall delete the PCC rules corresponding to the MCPTT session and the PCF shall revoke the actions related to the prioritization of the MCPTT session in the corresponding PDU Session as defined in 3GPP TS 29.512 [8].

#### 4.2.4.8 Termination of MCVideo

If the "Individual Application Session Context" resource being removed corresponds to an MCVideo session, the PCF shall delete the PCC rules corresponding to the MCVideo session and the PCF shall revoke the actions related to the prioritization of the MCVideo session in the corresponding PDU Session as defined in 3GPP TS 29.512 [8].

#### 4.2.4.9 Priority sharing indication

If the "Individual Application Session Context" resource being removed included the "prioSharingInd" attribute set to "ENABLED" within a media component of the "medComponents" attribute, if the related media flow(s) was in priority sharing with other media flows the PCF should readjust the Allocation and Retention Priority for the remaining services sharing Allocation and Retention Priority as described in 3GPP TS 29.512 [8], clause 4.2.6.2.9 and handle the media flow removed according to normal PCC/QoS rule provisioning procedures described in 3GPP TS 29.512 [8], clause 4.2.6.2.

#### 4.2.4.10 Report of RAN-NAS release cause

This procedure is used by a PCF to report about the RAN-NAS release cause together with access network information (i.e. user location and/or user timezone information) at the deletion of the "Individual Application Session Context" resource when the "RAN-NAS-Cause" feature is supported.

This procedure is initiated when:

- the "Individual Application Session Context" is deleted by the NF service consumer; or
- the PCF requests the deletion of the "Individual Application Session Context" from the NF service consumer, as described in clause 4.2.5.3, due to PDU session termination or the termination of all the service data flows of the AF session.

The PCF shall immediately configure the SMF to provide such RAN-NAS release cause together with access information, as specified in 3GPP TS 29.512 [8].

When the PCF receives the RAN-NAS release cause and access network information from the SMF, the PCF shall provide the corresponding access network information and RAN-NAS release cause to the NF service consumer by including the "EventsNotification" data type in the "200 OK" response to the HTTP POST request. The PCF shall include:

- in case of 3GPP access, the user location information in the "eutraLocation" or in the "nrLocation" attribute in the "ueLoc" attribute, if available;
- in case of untrusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if available, as follows:

  a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute;

  b) the UDP source port or the TCP source port in the "portNumber" and "protocol" attributes if available; and

  c) if the "WLAN_Location" feature is supported, the WLAN location information encoded in the "twapId" attribute, if available, that shall consist of:

     i. the SSID in the "ssId" attribute;

     ii. the BSSID the "bssId" attribute if available; and

     iii. the civic address in the "civicAddress" attribute if available;

NOTE 1: When the UE reaches the ePDG via a NAT, the combination of UE local IP address and the UE source port is needed for lawful interception purposes. The UE source port may be either a UDP or a TCP port, and it is indicated in the "protocol" attribute.

- in case of trusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if available, as follows:

  a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute, if available; and

  b) the UDP source port in the "portNumber" attribute if available; and

NOTE 2: The UDP protocol can be used between the UE and the TNGF to enable NAT traversal.

  c) either the TNAP identifier encoded in the "tnapId" attribute or the TWAP identifier encoded in the "twapId" attribute. The TNAP identifier and the TWAP identifier shall consist of:

     i. the SSID in the "ssId" attribute;

     ii. the BSSID the "bssId" attribute if available; and

     iii. the civic address in the "civicAddress" attribute if available;

- the serving network identity i.e. the PLMN Identifier (the PLMN network code and the country code) or the SNPN Identifier (the PLMN Identifier and the NID) in the "plmnId" attribute, if user location information is not available in any access;

- the UE timezone in the "ueTimeZone" attribute if available; and

- the RAN and/or NAS release cause in the "ranNasRelCauses" attribute, if available.

The PCF shall also include an event of the "AfEventNotification" data type in the "evNotifs" attribute with the "event" attribute set to the value "RAN_NAS_CAUSE".

#### 4.2.4.11 Termination of Mission Critical Services

If the AF session being terminated corresponds to an MCS session, the PCF shall delete the PCC rules corresponding to the MCS session and the PCF shall revoke the actions related to the prioritisation of the MCS session in the corresponding PDU Session as defined in 3GPP TS 29.512 [8].

#### 4.2.4.12 Void

### 4.2.5 Npcf_PolicyAuthorization_Notify service operation

#### 4.2.5.1 General

The Npcf_PolicyAuthorization_Notify service operation enables notification to NF service consumers that the previously subscribed event for the existing application session context occurred or that the application session context is no longer valid.

The following procedures using the Npcf_PolicyAuthorization_Notify service operation are supported:

- Notification about application session context event.
- Notification about application session context termination.
- Notification about Service Data Flow QoS notification control.
- Notification about service data flow deactivation.
- Reporting usage for sponsored data connectivity.
- Notification of resources allocation outcome.
- Reporting access network information.

- Notification of signalling path status.
- Notification about out of credit.
- Notification about TSC user plane node management information and/or port management information, Individual Application Session Context exists.
- Notification about Service Data Flow QoS Monitoring control.
- Report of EPS Fallback.
- Notification about TSC user plane node Information, no Individual Application Session Context exists.
- Notification about reallocation of credit.
- Notification of MPS for DTS outcome.
- Notification about application detection information.
- Notification about satellite backhaul category changes.
- Notification about UP path change enforcement failure.
- Notification about PDU session established/terminated events.

### 4.2.5.2 Notification about application session context event

This procedure is invoked by the PCF to notify the NF service consumer when a certain, previously subscribed, application session context event occurs, as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

Figure 4.2.5.2-1 illustrates the notification about application session context event.

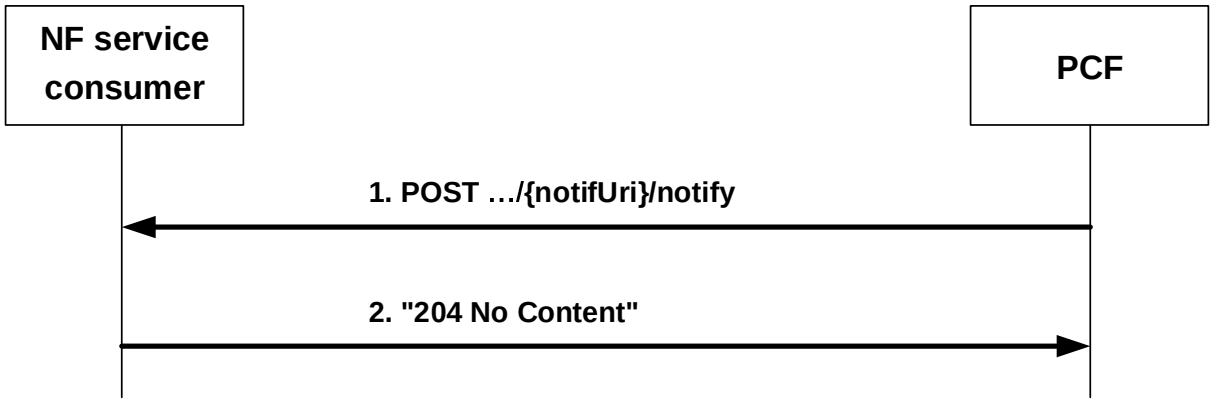


**Figure 4.2.5.2-1: Notification about application session context event**

When the PCF determines that the event for the existing AF application session context, to which the NF service consumer has subscribed to, occurred e.g. upon reception of an event notification for a PDU session from the SMF as described in 3GPP TS 29.512 [8], the PCF shall invoke the Npcf_PolicyAuthorization_Notify service operation by sending the HTTP POST request (as shown in figure 4.2.5.2-1, step 1) to the NF service consumer using the notification URI received in the subscription creation (or modification), as specified in clause 4.2.6, and appending the "notify" segment path at the end of the URI. The PCF shall provide in the body of the HTTP POST request the "EventsNotification" data type including:

- the Events Subscription resource identifier related with the notification in the "evSubsUri" attribute; and
- the list of the reported events in the "evNotifs" attribute. For each reported event, the "AfEventNotification" data type shall include the event identifier and may include additional event information.

The PCF shall include:

- if the NF service consumer subscribed to the "PLMN_CHG" event, the "event" attribute set to "PLMN_CHG" and the "plmnId" attribute including the PLMN Identifier or the SNPN Identifier if the PCF has requested to be updated with this information in the SMF;

NOTE 1: The SNPN Identifier consists of the PLMN Identifier and the NID.

- if the NF service consumer subscribed to the event "ACCESS_TYPE_CHANGE", the "event" attribute set to "ACCESS_TYPE_CHANGE" and:

  i. the "accessType" attribute including the access type, and the "ratType" attribute including the RAT type when applicable for the notified access type; and/or

  ii. if the "ATSSS" feature is supported and the PDU session is a MA PDU session:

    a. if it is the first access type report, and both, 3GPP and non-3GPP access information is available, the "addAccessInfo" attribute. The "addAccessInfo" attribute contains the additional access type information, where the access type is encoded in the "accessType" attribute, and the RAT type is encoded in the "ratType" attribute when applicable for the notified access type;

    b. if it is a subsequent access type change report:

      - if a new access type is added to the MA PDU session, the"addAccessInfo" attribute with the added access type encoded in the "accessType" attribute, and the RAT type encoded in the "ratType" attribute when applicable for the notified access type;

      - if an access type is released to the MA PDU session, the "relAccessInfo" attribute with the released access type encoded in the "accessType" attribute, and the RAT type encoded in the "ratType" attribute when applicable for the notified access type; and

NOTE 2: For a MA PDU session, if the "ATSSS" feature is not supported by the NF service consumer the PCF shall include the "accessType" attribute and the "ratType" attribute with a currently active combination of access type and RAT type. When both 3GPP and non-3GPP accesses are available, the PCF includes the information corresponding to the 3GPP access and only changes on activation and deactivation of 3GPP access are reported.

  iii. the "anGwAddr" attribute including access network gateway address when available; and

- if the "IMS_SBI" feature is supported and if the NF service consumer subscribed to the "CHARGING_CORRELATION" event, the "event" attribute set to "CHARGING_CORRELATION" and may include the "anChargIds" attribute containing the access network charging identifier(s) and the "anChargAddr" attribute containing the access network charging address.

The NF service consumer notification of other specific events using the Npcf_PolicyAuthorization_Notify request is described in the related clauses.

Upon the reception of the HTTP POST request from the PCF indicating that the PDU session and/or service related event occurred, the NF service consumer shall acknowledge that request by sending an HTTP response message with the corresponding status code.

If the HTTP POST request from the PCF is accepted, the NF service consumer shall acknowledge the receipt of the event notification with a "204 No Content" response to HTTP POST request, as shown in figure 4.2.5.2-1, step 2.

If the HTTP POST request from the PCF is not accepted, the NF service consumer shall indicate in the response to HTTP POST request the cause for the rejection as specified in clause 5.7.

If the feature "ES3XX" is supported, and the NF service consumer determines the received HTTP POST request needs to be redirected, the NF service consumer shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [5].

### 4.2.5.3 Notification about application session context termination

This procedure is invoked by the PCF to notify the NF service consumer that the application session context is no longer valid, as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

Figure 4.2.5.3-1 illustrates the notification about application session context termination.

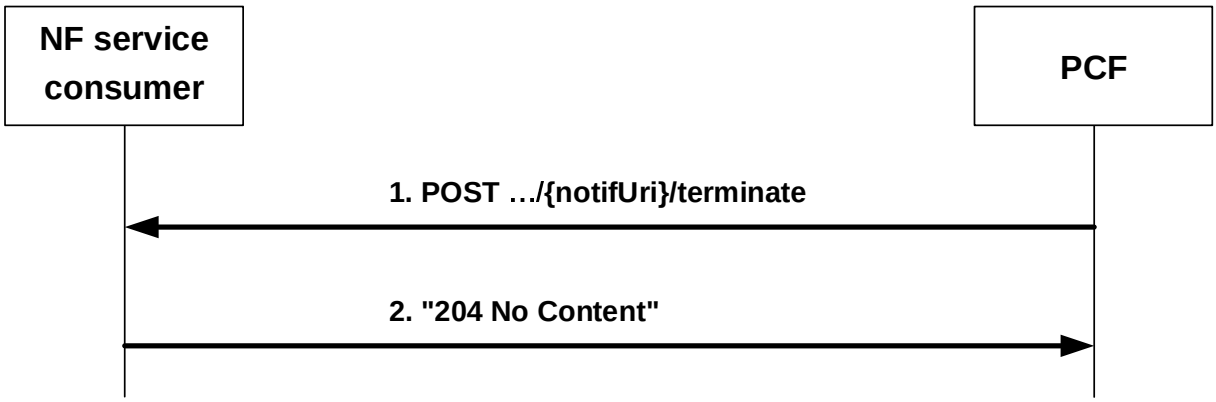


**Figure 4.2.5.3-1: Notification about application session context termination**

When the PCF determines that the AF application session context is no longer valid, the PCF shall invoke the Npcf_PolicyAuthorization_Notify service operation by sending the HTTP POST request (as shown in figure 4.2.5.3-1, step 1) using the notification URI received in the "Individual Application Session Context" context creation, as specified in clause 4.2.2 and clause 4.2.6.3, and appending the "terminate" segment path at the end of the URI, to trigger the NF service consumer to request the application session context termination (see clause 4.2.4.2). The PCF shall provide in the body of the HTTP POST request the "TerminationInfo" data type including:

- the Individual Application Session Context resource identifier related to the termination notification in the "resUri" attribute; and
- the application session context termination cause in the "termCause" attribute of the "TerminationCause" data type, indicating:
  - i) "PDU_SESSION_TERMINATION" when the PCF received from the SMF the indication of SM Policy Context termination without a specific PDU session release cause value;
  - ii) "ALL_SDF_DEACTIVATION" when the PCF received from the SMF the indication that all the SDFs of the Individual Application Session Context resource are deactivated or all resource allocation of an Individual Application Session Context fails because other reasons than "PS_TO_CS_HAN";
  - iii) "PS_TO_CS_HO" if the "IMS_SBI" feature is supported and the PCF received from the SMF:
    - a) the PDU session release cause value "PS_TO_CS_HO"; or
    - b) the failure code value "PS_TO_CS_HAN" for all the SDFs of the Individual Application Session Context resource;
  - iv) "INSUFICIENT_SERVER_RESOURCES" when the PCF is overloaded;
  - v) "INSUFFICIENT_QOS_FLOW_RESOURCES" when the PCF received that the maximum number of QoS flows for the PDU session is reached or there was a QoS flow resource limitation error; or
  - vi) "SPONSORED_DATA_CONNECTIVITY_DISALLOWED" when the PCF detects that due to operator policy the UE accessing the sponsored data connectivity is disallowed.

Upon the reception of the HTTP POST request from the PCF requesting the application session context termination, the NF service consumer shall acknowledge that request by sending an HTTP response message with the corresponding status code.

If the HTTP POST request from the PCF is accepted, the NF service consumer shall acknowledge the receipt of the application session context termination request with a "204 No Content" response to HTTP POST request (as shown in figure 4.2.5.3-1, step 2) and shall invoke the Npcf_PolicyAuthorization_Delete service operation to the PCF as described in clause 4.2.4.

If the HTTP POST request from the PCF is not accepted, the NF service consumer shall indicate in the response to HTTP POST request the cause for the rejection as specified in clause 5.7.

If the feature "ES3XX" is supported, and the NF service consumer determines the received HTTP POST request needs to be redirected, the NF service consumer shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [5].

### 4.2.5.4 Notification about Service Data Flow QoS notification control

When the PCF gets the knowledge that one or more SDFs:

- cannot guarantee the GBR QoS targets; or
- can guarantee again the GBR QoS targets;

the PCF shall inform the NF service consumer accordingly if the AF has previously subscribed as described in clauses 4.2.2.6 and 4.2.3.6.

The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include:

- within the "evNotifs" attribute an event entry of the "AfEventNotification" data type with the matched event "QOS_NOTIF" in the "event" attribute; and
- the "qncReports" array with:
  a) the "notifType" attribute to indicate whether the GBR targets for the indicated SDFs are "NOT_GUARANTEED" or "GUARANTEED" again;
  b) the identification of the affected service flows (if not all the flows are affected) encoded in the "flows" attribute if applicable; and
  c) if the "AuthorizationWithRequiredQoS" feature or the "AltSerReqsWithIndQoS" feature as defined in clause 5.8 is supported, the reference to the Alternative Service Requirement corresponding alternative QoS parameter set if received from the SMF within the "altSerReq" attribute. When the "altSerReq" attribute is omitted and the "notifType" attribute is NOT_GUARANTEED, it indicates that the lowest priority alternative QoS profile could not be fulfilled.

If "MediaComponentVersioning" feature is supported, and if the content version was included when the corresponding media component was provisioned, the "flows" attribute shall also contain the "contVers" attribute including the content version(s) of the media components. The PCF shall include more than one entry in the "contVers" attribute for the same media component if the PCF has received multiple content versions as described in clause 4.2.6.2.14 in 3GPP TS 29.512 [8].

When the NF service consumer receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF. The NF service consumer may also update the AF application session context information by sending an HTTP PATCH request to the PCF.

Signalling flows for Service Data Flow QoS notification control are presented in 3GPP TS 29.513 [7].

### 4.2.5.5 Notification about Service Data Flow Deactivation

When the PCF gets the knowledge that one or more SDFs have been deactivated, the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed as described in clauses 4.2.2.7 and 4.2.3.7.

When not all the service data flows within the AF application session context are affected, the PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include within the "evNotifs" attribute an event of "AfEventNotification" data type indicating the matched event "FAILED_RESOURCES_ALLOCATION" in the "event" attribute and the deactivated service data flows (if not all the flows are affected) encoded in the "flows" attribute.

NOTE 1: If the PCF detects that the PCC rules related to an AF application session context cannot be installed or modified because there is a temporary network failure (e.g. SGW failed according to clause B.3.3.3 or B.3.4.9 of 3GPP TS 29.512 [8]) and if requested by the AF, the PCF can notify the AF of the event "FAILED_RESOURCES_ALLOCATION".

If the "MediaComponentVersioning" feature is supported, and if the content version was included when the corresponding media component was provisioned as described in clause 4.2.5.8, the PCF shall also include in the "flows" attribute the "contVers" attribute with the content version(s) of the media components.

If the "RAN-NAS-Cause" feature is supported and the PCF received the RAN-NAS release cause and access network information from the SMF, the PCF shall provide in the "EventsNotification" data type of the HTTP POST request:

- in case of 3GPP access, the user location information in the "eutraLocation" or in the "nrLocation" attribute in the "ueLoc" attribute, if available;
- in case of untrusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if available, as follows:

  a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute;

  b) the UDP source port or the TCP source port in the "portNumber" and "protocol" attributes, if available; and

  c) if the "WLAN_Location" feature is supported, the WLAN location information encoded in the "twapId" attribute, if available, that shall consist of:

     i. the SSID in the "ssId" attribute;

     ii. the BSSID the "bssId" attribute if available; and

     iii. the civic address in the "civicAddress" attribute if available;

NOTE 2: When the UE reaches the ePDG via a NAT, the combination of UE local IP address and the UE source port is needed for lawful interception purposes. The UE source port may be either a UDP or a TCP port, and it is indicated in the "protocol" attribute.

- in case of trusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if available, as follows:

  a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute, if available; and

  b) the UDP source port in the "portNumber" attribute if available; and

NOTE 3: The UDP protocol can be used between the UE and the TNGF to enable NAT traversal.

  c) either the TNAP identifier encoded in the "tnapId" attribute or the TWAP identifier encoded in the "twapId" attribute. The TNAP identifier and the TWAP identifier shall consist of:

     i. the SSID in the "ssId" attribute;

     ii. the BSSID the "bssId" attribute if available; and

     iii. the civic address in the "civicAddress" attribute if available;

- the serving network identity i.e. the PLMN Identifier (the PLMN network code and the country code) or the SNPN Identifier (the PLMN Identifier and the NID) in the "plmnId" attribute, if user location information is not available in any access;
- the UE timezone in the "ueTimeZone" attribute if available; and
- the RAN and/or NAS release cause in the "ranNasRelCauses" attribute, if available.

NOTE 4: The PCF forwards both 3GPP and non-3GPP access UE locations in the "ueLoc" attribute when both UE locations are provided by the SMF as defined in 3GPP TS 29.512 [8].

The PCF shall include in the "evNotifs" attribute, together with the event "FAILED_RESOURCES_ALLOCATION", an event of the "AfEventNotification" data type with the "event" attribute set to the value "RAN_NAS_CAUSE".

The PCF shall include more than one entry in the "contVers" attribute for the same media component if the PCF has received multiple content versions as described in clause 4.2.6.2.14 in 3GPP TS 29.512 [8].

When the NF service consumer receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF. The NF service consumer may also update the AF application session context information by sending an HTTP PATCH request to the PCF.

When all the service data flows within the AF session are affected, the PCF shall inform the NF service consumer by sending a notification about application session context termination as defined in clause 4.2.5.3.

Signalling flows for Service Data Flow Deactivation cases are presented in 3GPP TS 29.513 [7].

### 4.2.5.6 Reporting usage for sponsored data connectivity

When "SponsoredConnectivity" is supported, the NF service consumer enabled sponsored data connectivity and the NF service consumer provided usage thresholds for such sponsor to the PCF, the PCF shall report accumulated usage to the NF service consumer using the Npcf_PolicyAuthorization_Notify service operation when:

- the PCF detects that the usage threshold provided by the NF service consumer has been reached; or
- the NF service consumer disables the sponsored data connectivity.

The PCF shall notify the NF service consumer of the accumulated usage by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include:

- an event of the "AfEventNotification" data type in the "evNotifs" attribute with the matched event "USAGE_REPORT" in the "event" attribute; and
- the accumulated usage, corresponding to the usage since the last report to the AF, encoded in the "usgRep" attribute.

When the NF service consumer receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF. The NF service consumer may terminate the AF session sending an HTTP POST as described in clause 4.2.4.2 or update the AF application session context information by providing a new usage threshold sending an HTTP PATCH request to the PCF as described in clause 4.2.3.5 or an HTTP PUT request to the PCF as described in clause 4.2.6.4.

NOTE: Once the accumulated usage is reported by the PCF to the AF, the monitoring will not start until the PCF receives the new threshold from the NF service consumer and provides it to the SMF.

### 4.2.5.7 Void

### 4.2.5.8 Notification about resources allocation outcome

When the PCF becomes aware that the resources associated to service information for one or more SDFs have been allocated, the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed to the "SUCCESSFUL_RESOURCES_ALLOCATION" event as described in clauses 4.2.2.10 and 4.2.3.10. The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2. The PCF shall include in the "evNotifs" attribute an entry with the "event" attribute set to "SUCCESSFUL_RESOURCES_ALLOCATION" and (if not all the flows are affected) the identification of the related media components in the "flows" attribute. If the "MediaComponentVersioning" feature is supported, the PCF shall also include in the "flows" attribute the "contVers" attribute with the content version(s) of the media components if the content version was included when the corresponding media component was provisioned.

If the "AuthorizationWithRequiredQoS" feature or the "AltSerReqsWithIndQoS" feature as defined in clause 5.8 is supported, when the PCF becomes aware that the resources associated to service information for one or more SDFs have been allocated and additionally receives the alternative QoS parameter set(s), the PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2. The PCF shall include:

- an entry in the "evNotifs" attribute with the "event" attribute set to "SUCCESSFUL_RESOURCES_ALLOCATION"; and

- the "succResourcAllocReports" attribute with the reference to the Alternative Service Requirement corresponding alternative QoS parameter set within the "altSerReq" attribute and the identification of the related media components in the "flows" attribute. If the "MediaComponentVersioning" feature is supported, the PCF shall also include in the "flows" attribute the "contVers" attribute with the content version(s) of the media components if the content version was included when the corresponding media component was provisioned.

When the PCF becomes aware that the resources associated to service information for one or more SDFs cannot be allocated, the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed to the "FAILED_RESOURCES_ALLOCATION" event as described in clauses 4.2.2.10 and 4.2.3.10. The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2. The PCF shall include:

- an entry in the "evNotifs" attribute with the "event" attribute set to "FAILED_RESOURCES_ALLOCATION"; and

- the "failedResourcAllocReports" attribute with the active/inactive status of the PCC rules related to certain media components encoded in the "mcResourcStatus" attribute, and (if not all the flows are affected) the identification of the related media components in the "flows" attribute. If the "MediaComponentVersioning" feature is supported, the PCF shall also include in the "flows" attribute the "contVers" attribute with the content version(s) of the media components if the content version was included when the corresponding media component was provisioned.

The PCF shall include more than one entry in the "contVers" attribute for the same media component if the PCF has received multiple content versions as described in clause 4.2.6.2.14 in 3GPP TS 29.512 [8].

NOTE: The NF service consumer will use the content version to identify the media component version that failed or succeeded when multiple provisions of the same media component occur in a short period of time. How the NF service consumer handles such situations is out of scope of this specification.

When the NF service consumer receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF.

Signalling flows for resource allocation outcome are presented in 3GPP TS 29.513 [7].

### 4.2.5.9 Void

### 4.2.5.10 Notification of signalling path status

When the PCF is notified of the loss or release of resources associated to the PCC rules corresponding with AF signalling IP flows, the PCF shall inform the NF service consumer about the loss of the signalling transmission path if the NF service consumer has previously subscribed as described in clause 4.2.6.7.

The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include within the "evNotifs" attribute an event of "AfEventNotification" data type indicating the matched event "FAILED_RESOURCES_ALLOCATION" in the "event" attribute and the deactivated IP flow encoded in the "flows" attribute.

If the "RAN-NAS-Cause" feature is supported and the PCF received the RAN-NAS release cause and/or access network information from the SMF, the PCF shall provide in the "EventsNotification" data type in the "200 OK" response to the HTTP POST request:

- in case of 3GPP access, the user location information in the "eutraLocation" or in the "nrLocation" attribute in the "ueLoc" attribute, if available;

- in case of untrusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if available, as follows:

a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute; and

b) the UDP source port or the TCP source port in the "portNumber" and "protocol" attributes, if available; and

c) if the "WLAN_Location" feature is supported, the WLAN location information encoded in the "twapId" attribute, if available, that shall consist of:

i. the SSID in the "ssId" attribute;

ii. the BSSID the "bssId" attribute if available; and

iii. the civic address in the "civicAddress" attribute if available;

NOTE 1: When the UE reaches the ePDG via a NAT, the combination of UE local IP address and the UE source port is needed for lawful interception purposes. The UE source port may be either a UDP or a TCP port, and it is indicated in the "protocol" attribute.

- in case of trusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if available, as follows:

a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute, if available; and

b) the UDP source port in the "portNumber" attribute if available; and

NOTE 2: The UDP protocol can be used between the UE and the TNGF to enable NAT traversal.

c) either the TNAP identifier encoded in the "tnapId" attribute or the TWAP identifier encoded in the "twapId" attribute. The TNAP identifier and the TWAP identifier shall consist of:

i. the SSID in the "ssId" attribute;

ii. the BSSID the "bssId" attribute if available; and

iii. the civic address in the "civicAddress" attribute if available;

- the serving network identity i.e. the PLMN Identifier (the PLMN network code and the country code) or the SNPN Identifier (the PLMN Identifier and the NID) in the "plmnId" attribute, if user location information is not available in any access;

- the UE timezone in the "ueTimeZone" attribute if available; and

- the RAN and/or NAS release cause in the "ranNasRelCauses" attribute, if available.

NOTE 3: The PCF forwards both 3GPP and non-3GPP access UE locations in the "ueLoc" attribute when both UE locations are provided by the SMF as defined in 3GPP TS 29.512 [8].

The PCF shall include in the "evNotifs" attribute, together with the event "FAILED_RESOURCES_ALLOCATION", an event of the "AfEventNotification" data type with the "event" attribute set to the value "RAN_NAS_CAUSE".

When the NF service consumer receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF.

#### 4.2.5.11 Reporting access network information

This procedure is used by the PCF to report the access network information (i.e. user location and/or user timezone information) to the NF service consumer when the "NetLoc" feature is supported.

When the PCF receives the access network information from the SMF, the PCF shall include the "EventsNotification" data type in the body of the HTTP POST request message sent to the NF service consumer as described in clause 4.2.5.2. The PCF shall include in the "EventsNotification" data type:

- in case of 3GPP access, the user location information in the "eutraLocation" or in the "nrLocation" attribute in the "ueLoc" attribute, if available and required;

- in case of untrusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if required, as follows:

a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute, if available;

b) the UDP source port or the TCP source port in the "portNumber" and "protocol" attributes, if available; and

c) if the "WLAN_Location" feature is supported, the WLAN location information encoded in the "twapId" attribute, if available, that shall consist of:

i. the SSID in the "ssId" attribute;

ii. the BSSID the "bssId" attribute if available; and

iii. the civic address in the "civicAddress" attribute if available;

NOTE 1: When the UE reaches the ePDG via a NAT, the combination of UE local IP address and the UE source port is needed for lawful interception purposes. The UE source port may be either a UDP or a TCP port, and it is indicated in the "protocol" attribute.

- in case of trusted non-3GPP access, the user location information in the "n3gaLocation" attribute in the "ueLoc" attribute, if required, as follows:

a) the user local IP address in the "ueIpv4Addr" or "ueIpv6Addr" attribute, if available; and

b) the UDP source port in the "portNumber" attribute if available; and

NOTE 2: The UDP protocol can be used between the UE and the TNGF to enable NAT traversal.

c) either the TNAP identifier encoded in the "tnapId" attribute or the TWAP identifier encoded in the "twapId" attribute. The TNAP identifier and the TWAP identifier shall consist of:

i. the SSID in the "ssId" attribute;

ii. the BSSID the "bssId" attribute if available; and

iii. the civic address in the "civicAddress" attribute if available;

- if user location was required, the time when it was last known in the "ueLocTime" attribute if available;

NOTE 3: The PCF derives the value of the "ueLocTime" attribute from the "userLocationInfoTime" attribute received from the SMF as specified in 3GPP TS 29.512 [8].

- the serving network identity i.e. the PLMN Identifier (the PLMN network code and the country code) or the SNPN Identifier (the PLMN Identifier and the NID) in the "plmnId" attribute, if user location information is required but not available in any access; and/or

- the UE timezone in the "ueTimeZone" attribute if required and available.

NOTE 4: The PCF forwards both 3GPP and non-3GPP access UE locations in the "ueLoc" attribute when both UE locations are provided by the SMF as defined in 3GPP TS 29.512 [8].

When the PCF receives from the SMF that the access network does not support access network information report, the PCF shall include the "noNetLocSupp" attribute set to "ANR_NOT_SUPPORTED", "TZR_NOT_SUPPORTED" or "LOC_NOT_SUPPORTED" value received from the SMF in the "EventsNotification" data type in the "200 OK" response to the HTTP POST request.

The PCF shall also include an event of the "AfEventNotification" data type in the "evNotifs" attribute with the "event" attribute set to the value "ANI_REPORT".

NOTE 5: The PCF receives the access network information from the SMF if it is previously requested by the NF service consumer or at PDU session termination or at the termination of all the service data flows of the AF session.

The PCF shall not invoke the Npcf_PolicyAuthorization_Notify service operation with the "event" attribute set to the value "ANI_REPORT" to report to the NF service consumer any subsequently received access network information, unless the NF service consumer sends a new request for access network information.

#### 4.2.5.12 Notification about Out of Credit

If the "IMS_SBI" feature is supported and if the PCF becomes aware that there is no credit available in the CHF for one or more SDFs, the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed to the "OUT_OF_CREDIT" event as described in clauses 4.2.2.22 and 4.2.3.22.

The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include:

- in the "evNotifs" attribute an entry with the "event" attribute set to the value "OUT_OF_CREDIT"; and
- the "outOfCredReports" attribute containing in each entry of the "OutOfCreditInformation" data type the credit information for one or more service data flows. The "OutOfCreditInformation" data type shall contain the termination action in the "finUnitAct" attribute, and the identification of the affected service data flows (if not all the flows are affected) encoded in the "flows" attribute.

Upon the reception of the HTTP POST request from the PCF, the NF service consumer shall acknowledge that request by sending an HTTP response message as described in clause 4.2.5.2.

#### 4.2.5.13 Notification about TSC user plane node management information and/or port management information detection, Individual Application Session Context exists

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication"feature is supported and if the PCF becomes aware that, for an existing Individual Application Session Context resource, updated TSC user plane node information is available, e.g., a UMIC and/or a DS-TT PMIC and/or one or more NW-TT PMIC(s) are available, the PCF shall inform the NF service consumer (i.e., the TSN AF or the TSCTSF) accordingly, if the NF service consumer has previously subscribed as described in clause 4.2.2.31.

The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include in the "evNotifs" attribute an entry with the "event" attribute set to the value "TSN_BRIDGE_INFO", and the "tsnBridgeManCont" attribute and/or the "tsnPortManContDstt" attribute and/or the "tsnPortManContNwtts" attribute as received from the SMF if the PCF is aware that a UMIC and/or a DS-TT PMIC and/or one or more NW-TT PMIC(s) are available or updated.

Upon the reception of the HTTP POST request from the PCF, the NF service consumer shall acknowledge that request as specified in clause 4.2.5.2.

The NF service consumer may use the received UMIC and/or the received DS-TT PMIC and/or NW-TT PMIC(s) and the local configuration to construct the DS-TT port and or NW-TT port management information required to interwork with the external network (e.g. TSN).

If port management information shall be sent as a response of the received notification, the NF service consumer triggers the Npcf_PolicyAuthorization_Update service operation to send the port management information to the PCF as specified in clause 4.2.3. The NF service consumer delivers to the PCF the derived port management information containers as described in clause 4.2.3.25.

And/or if TSC user plane node management information shall be sent as a response of the received notification, the NF service consumer includes the UMIC in the Npcf_PolicyAuthorization_Update service operation as described in clause 4.2.3.25.

#### 4.2.5.14 Notification about Service Data Flow QoS Monitoring control

When the PCF gets the information about any one of the following items for one or more SDFs from the SMF:

- uplink packet delay(s);
- downlink packet delay(s); and/or
- round trip delay(s); or

- if the feature "PacketDelayFailureReport" is supported, indicator of packet delay measurement failure;

the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed as described in clauses 4.2.2.23 and 4.2.3.23 and 4.2.6.8.

The PCF shall notify the NF service consumer of the QoS monitoring events by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include:

- within the "evNotifs" attribute an event entry of the "AfEventNotification" data type with the matched event "QOS_MONITORING" in the "event" attribute; and
- the "qosMonReports" array with:
  a) the identification of the affected service flows (if not all the flows are affected) encoded in the "flows" attribute if applicable; and
  b) the uplink packet delays within the "ulDelays" attribute;
  c) the downlink packet delays within the "dlDelays" attribute; and/or
  d) the round trip packet delays within the "rtDelays" attribute; or
  e) if the feature "PacketDelayFailureReport" is supported, the packet delay measurement failure indicator within the"pdmf" attribute.

NOTE: The SMF reports one UL, DL and/or round-trip packet delay measurement for each periodic and/or event-triggered report as described in 3GPP TS 29.512 [8]. I.e, the PCF can include only one element within the "ulDelays", "dlDelays", and/or "rtDelays" array(s) respectively, each one with the received report from the SMF for the UL, DL and/or round trip delay(s).

### 4.2.5.15 Report of EPS Fallback

When "EPSFallbackReport" feature is supported and the PCF becomes aware of the EPS Fallback for the resources requested for a particular service information (voice media type), the PCF shall inform the NF service consumer if the NF service consumer has previously subscribed as described in clauses 4.2.2.30 and 4.2.3.29.

The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include within the "evNotifs" attribute an event entry of the "AfEventNotification" data type with the matched event "EPS_FALLBACK" in the "event" attribute.

When the NF service consumer receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF.

### 4.2.5.16 Notification about TSC user plane node Information, no Individual Application Session Context exists

If the "TimeSensitiveNetworking" or "TimeSensitiveCommunication" feature is supported and if the PCF becomes aware that TSC user plane node information for an external network (e.g. TSN) is available, but there is no "Individual Application Session Context" resource bound to the SM Policy Association updated with TSC user plane node related information, the PCF shall inform the NF service consumer (i.e. TSN AF or TSCTSF) about the detection of a TSC user plane node information in the context of a PDU session by sending a notification request:

- to the request URI locally configured in the PCF for the NF service consumer; or
- if the request URI for the TSCTSF is not locally configured in the PCF, to the notification URI registered by the TSCTSF in the NRF as default notification subscription for time sensitive communication and time synchronization notifications, and retrieved from NRF by the PCF using the discovery service, as specified in 3GPP TS 29.510[27] for the PDU session DNN/S-NSSAI.

NOTE 1: PCF configuration of TSN AF needs to ensure that the notification is addressed to a TSN AF that connects to the same external network the UPF/NW-TT connects to. How it is achieved is implementation specific. It can be based e.g. on dedicated DNN/S-NSSAI combinations or on the received TSC user plane node information.

NOTE 2: It is assumed that there is only one TSCTSF for a given DNN/S-NSSAI in this release of the specification.

Figure 4.2.5.16-1 illustrates the notification about TSC user plane node information when there is no Individual Application Session Context bound to the SM Policy Association.

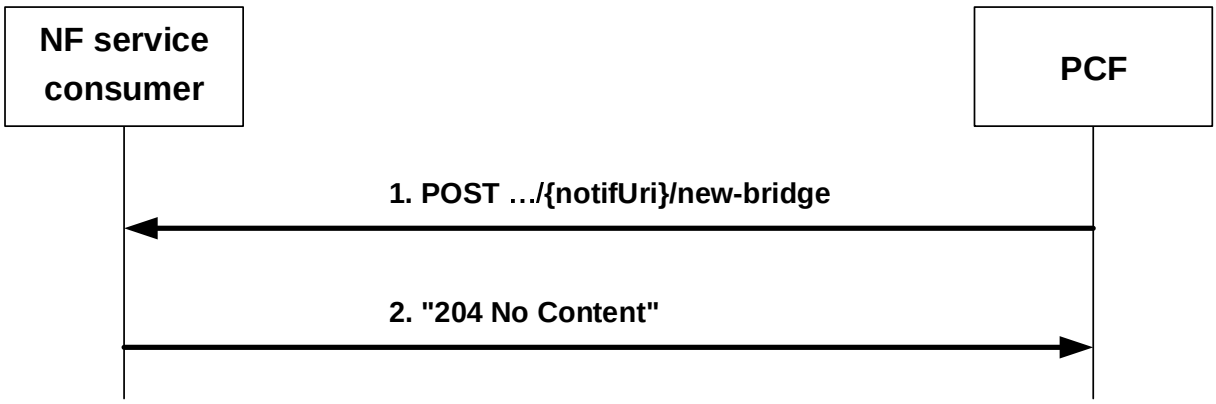


**Figure 4.2.5.16-1: Notification about TSC user plane node Information, no AF session context exists**

When the PCF determines that the AF application session context does not exist for the SM Policy Association that detected new port information and a notification URI for the NF service consumer can be determined, the PCF shall invoke the Npcf_PolicyAuthorization_Notify service operation by sending the HTTP POST request (as shown in figure 4.2.5.16-1, step 1) using the notification URI locally configured in the PCF or, retrieved from NRF, and appending the "new-bridge" segment path at the end of the URI, to trigger the NF service consumer (i.e. TSN AF or TSCTSF) to request the creation of an Invidual Application Session Context resource to handle the TSC user plane node detected in the context of a PDU session, configuring ports and TSC user plane node management information, and providing the corresponding TSCAI input containers and TSC traffic QoS related data (see clauses 4.2.2.2, 4.2.2.24, 4.2.2.25 and 4.2.2.31).

The PCF shall provide in the body of the HTTP POST request the "PduSessionTsnBridge" data type including TSC user plane node information as follows:

- the "tsnBridgeInfo" attribute as received from the SMF;
- the "tsnBridgeManCont" attribute as received from the SMF, if available;
- the "tsnPortManContDstt" attribute and/or "tsnPortManContNwtts" attribute as received from the SMF, if available; and
- when the "TimeSensitiveCommunication" feature is supported and for a PDU session of IP type, the UE IPv4 address within the "ueIpv4Addr" attribute or the UE IPv6 prefix within the "ueIpv6AddrPrefix", the DNN within the "dnn" attribute, the S-NSSAI within the "snssai" attribute and, if available, the domain identity within the "ipDomain" attribute if UE IPv4 address is provided.

NOTE 3: In the case of IP overlapping, the DNN, S-NSSAI and domain identity, if available, are required for session binding in the PCF. Domain identity applies as defined in clause 4.2.2.2.

Upon the reception of the HTTP POST request from the PCF, the NF service consumer shall acknowledge that request.

With the received information, the NF service consumer (i.e. TSN AF or TSCTSF) shall immediately trigger the creation of an Individual Application Session Context resource to handle in this association the configuration of the new TSC user plane node in the context of this PDU session, as described in clauses 4.2.2.2, 4.2.2.24, 4.2.2.25 and 4.2.2.31.

NOTE 4: For the time synchronization service, the subscription to UE availability for time-synchronization service can occur after the PDU Session establishment has been completed in 5GS. Similarly, for the AF session with required QoS, the indication of the required QoS and TSC Assistance Container information can occur after the completion of the PDU session establishment. In such cases, the PCF sends the notification to the TSCTSF about the detection of a TSC user plane node information during PDU session establishment, and the TSCTSF could defer the creation of the related "Individual Application Session Context" till the reception of the subscription to UE availability for time synchronization or the AF session with required QoS occurs, as specified in 3GPP TS 29.513[7].

The NF service consumer (i.e. TSN AF or TSCTSF) may use the received TSC user plane node information and/or the received DS-TT port management information container and/or NW-TT port management information containers and the local configuration to construct the DS-TT port and or NW-TT port management information required to interwork with the external network.

### 4.2.5.17 Notification about Reallocation of Credit

If the "IMS_SBI" and the "ReallocationOfCredit" features are supported and if the PCF becomes aware that there is credit reallocated for one or more SDFs after a former out of credit indication, the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed to the "REALLOCATION_OF_CREDIT" event as described in clauses 4.2.2.34 and 4.2.3.32.

The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include in the "evNotifs" attribute an entry with:

- the "event" attribute set to the value "REALLOCATION_OF_CREDIT"; and
- the SDFs that are impacted as consequence of the reallocation of credit condition encoded in the "flows" attribute.

Upon the reception of the HTTP POST request from the PCF, the NF service consumer shall acknowledge that request by sending an HTTP response message as described in clause 4.2.5.2.

### 4.2.5.18 Notification of MPS for DTS Outcome

When the MPSforDTS feature is supported and the PCF is informed about the successful default QoS update, the PCF shall notify the NF service consumer as described in clause 4.2.5.2, if the NF service consumer has previously subscribed to the "SUCCESSFUL_QOS_UPDATE" event as described in clauses 4.2.2.12.2 and 4.2.3.12. The PCF shall notify the NF service consumer by including within the "evNotifs" attribute, an entry with the "event" attribute set to "SUCCESSFUL_QOS_UPDATE".

When the MPSforDTS feature is supported and the PCF is informed about the failure of a default QoS update, the PCF shall notify the NF service consumer as described in clause 4.2.5.2, if the NF service consumer has previously subscribed to the "FAILED_QOS_UPDATE" event as described in clauses 4.2.2.12.2 and 4.2.3.12. The PCF shall notify the NF service consumer by including within the "evNotifs" attribute, an entry with the "event" attribute set to "FAILED_QOS_UPDATE".

### 4.2.5.19 Notification about Application Detection Information

When the "ApplicationDetectionEvents" feature is supported, when the PCF gets the knowledge that the traffic of the indicated application started or stopped, the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed as described in clauses 4.2.6.9.

The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include, for the detected application(s)'s traffic:

- within the "evNotifs" attribute an event entry of the "AfEventNotification" data type with the matched event "APP_DETECTION" in the "event" attribute; and
- the "adReports" array, which for each detected application's traffic shall include:

a) the "adNotifType" attribute to indicate whether the detection is about the start of the application's traffic encoded as the "APP_START" value, or about the stop of the application's traffic encoded as the "APP_STOP" value; and

b) the application identifier within the "afAppId" attribute.

When the NF service consumer receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF.

Signalling flows for the notification of application detection information are presented in 3GPP TS 29.513 [7].

NOTE: When the NF service consumer receives the notifications for multiple applications, the NF service consumer (e.g. the PCF for the UE) can determine which logic to apply (e.g. which AM policy to apply) based on local configuration and operator policy.

In this release of the specification application detection applies only to the application(s) with IP traffic.

### 4.2.5.20 Notification about satellite backhaul category changes

When the PCF gets the knowledge that there is a change of the backhaul used for the PDU session between satellite backhaul categories (i.e., GEO, MEO, LEO, or other satellite) or between a satellite and a non-satellite backhaul category, the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed as described in clauses 4.2.2.35 and 4.2.3.33 and 4.2.6.10.

The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include within the "evNotifs" attribute an event entry of the "AfEventNotification" data type with the matched event "SAT_CATEGORY_CHG" in the "event" attribute, and within the "satBackhaulCategory" attribute the received satellite backhaul category (i.e., GEO, MEO, LEO, or other satellite) or the indication of non-satellite backhaul.

When the NF service consumer receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF. The NF service consumer may also update the AF application session context information by sending an HTTP PATCH request to the PCF.

### 4.2.5.21 Notification about UP change enforcement failure

If the "RoutingReqOutcome" feature is supported and if the PCF becomes aware that the enforcement of the UP path change fails (as specified in clause 4.2.6.2.6.2 of 3GPP TS 29.512 [8]), the PCF shall inform the NF service consumer accordingly if the NF service consumer has previously subscribed to the "UP_PATH_CHG_FAILURE" event as described in clauses 4.2.2.8 and 4.2.3.8.

The PCF shall notify the NF service consumer by including the "EventsNotification" data type in the body of the HTTP POST request as described in clause 4.2.5.2.

The PCF shall include in the "evNotifs" attribute an entry with the "event" attribute set to the value "UP_PATH_CHG_FAILURE".

Upon the reception of the HTTP POST request from the PCF, the NF service consumer shall acknowledge that request by sending an HTTP response message as described in clause 4.2.5.2.

### 4.2.5.22 Notification about PDU session established/terminated events

If the PCF becomes aware that the SM Policy Association contains the callback URI of the PCF for a UE then, the PCF shall inform the NF service consumer (i.e. the PCF for a UE) about:

- the PDU session establishment, when the PCF receives the callback URI of the PCF for a UE from the SMF; and
- the PDU session termination, when the PCF receives the SM Policy Association termination from the SMF;

by sending a notification request to the received callback URI of the PCF for a UE.

Figure 4.2.5.22-1 illustrates the notification about PDU session established/terminated events.

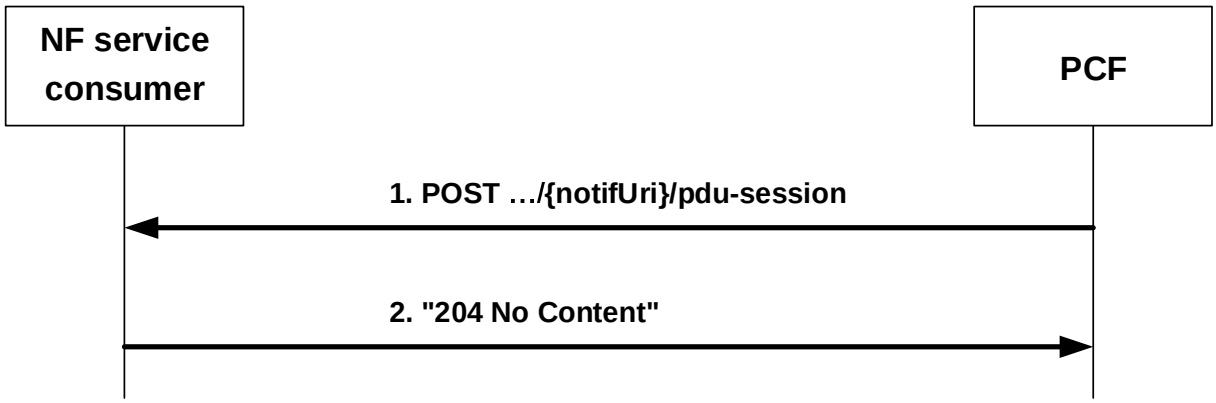


**Figure 4.2.5.22-1: Notification about PDU session established/terminated events**

When the PCF becomes aware that a SM Policy Association is receiving the callback URI of the PCF for a UE, or becomes aware that the SM Policy Association that is terminating contains the callback URI of the PCF for a UE, the PCF shall invoke the Npcf_PolicyAuthorization_Notify service operation by sending an HTTP POST request (as shown in figure 4.2.5.22-1, step 1) using the callback URI contained in the SM Policy Association and appending the "pdu-session" path segment at the end of the URI.

NOTE: The PCF includes in the notification request a Routing Binding Indication as specified in 3GPP TS 29.500 [5], clause 6.12 if an SBA binding indication relative to the PCF for a UE is available in the SM Policy Association together with the callback URI of the PCF for a UE.

The PCF shall provide in the body of the HTTP POST request the PduSessionEventNotification data type, which shall include an indication of PDU session establishment/termination as follows:

- the "evNotif" attribute, of "AfEventNotification" data type, which shall include the "PDU_SESSION_STATUS" event within the "event" attribute;
- the SUPI of the PDU session within the "supi" attribute;
- the served UE address as the identification of the reported PDU session:
  i. for IP type PDU sessions, the IP address (IPv4 or IPv6) of the UE in the "ueIpv4" or "ueIpv6" attribute; and
  ii. for Ethernet type PDU sessions, the MAC address of the UE in the "ueMac" attribute;
- whether the PDU session is established or terminated within the "status" attribute; and
- when the "status" attribute indicates "ESTABLISHED":
  i. the PCF addressing information where the NF service consumer (i.e. PCF for a UE) may send the subscription request to notification about the detected application traffic in the "pcfInfo" attribute; and
  ii. the context information of the related PDU session, i.e., the DNN withing the "dnn" attribute, the S-NSSAI within the "snssai" attribute and the GPSI within the "gpsi" attribute, if available.

Upon the reception of the HTTP POST request from the PCF, and if the request is accepted, the NF service consumer (i.e. PCF for a UE) shall acknowledge that request by sending an HTTP response message with a "204 No Content" status code as described in figure 4.2.5.22-1, step 2.

The NF service consumer (i.e. PCF for a UE) may use the notified PCF address(es) and SBA binding indication, if available, to subscribe with the PCF for a PDU session to the detection of application(s) traffic, as described in clause 4.2.6.9.

## 4.2.6 Npcf_PolicyAuthorization_Subscribe service operation

### 4.2.6.1 General

The Npcf_PolicyAuthorization_Subscribe service operation enables NF service consumers handling of subscription to events for the existing application session context. Subscription to events shall be created:

- within the application session context establishment procedure by invoking the Npcf_PolicyAuthorization_Create service operation, as described in clause 4.2.2; or
- within the application session context modification procedure by invoking the Npcf_PolicyAuthorization_Update service operation, as described in clause 4.2.3; or
- by invoking the Npcf_PolicyAuthorization_Subscribe service operation for the existing application session context, as described in clause 4.2.6.2.

The following procedures using the Npcf_PolicyAuthorization_Subscribe service operation is supported:

- Handling of subscription to events for the existing application session context.
- Initial subscription to events without provisioning of service information.
- Subscription to usage monitoring of sponsored data connectivity.
- Request of access network information.
- Subscription to notification of signalling path status.
- Subscription to Service Data Flow QoS Monitoring Information.
- Subscription to application detection notifications.
- Subscription to satellite backhaul category changes

### 4.2.6.2 Handling of subscription to events for the existing application session context

This procedure is used to create a subscription to events for the existing AF application session context bound to the corresponding PDU session or to modify an existing subscription, as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

Figure 4.2.6.2-1 illustrates the creation of events subscription information using HTTP PUT method.

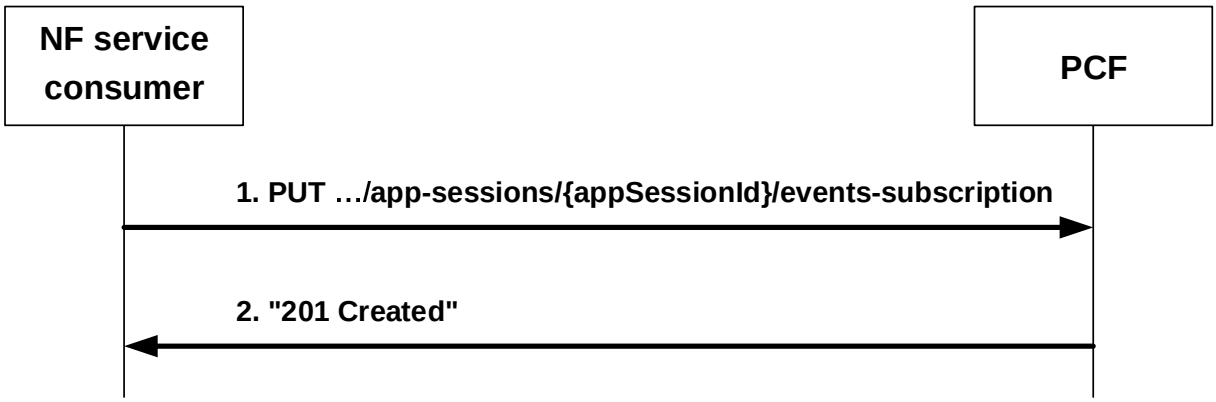


**Figure 4.2.6.2-1: Creation of events subscription information using HTTP PUT**

Figure 4.2.6.2-2 illustrates the modification of events subscription information using HTTP PUT method.

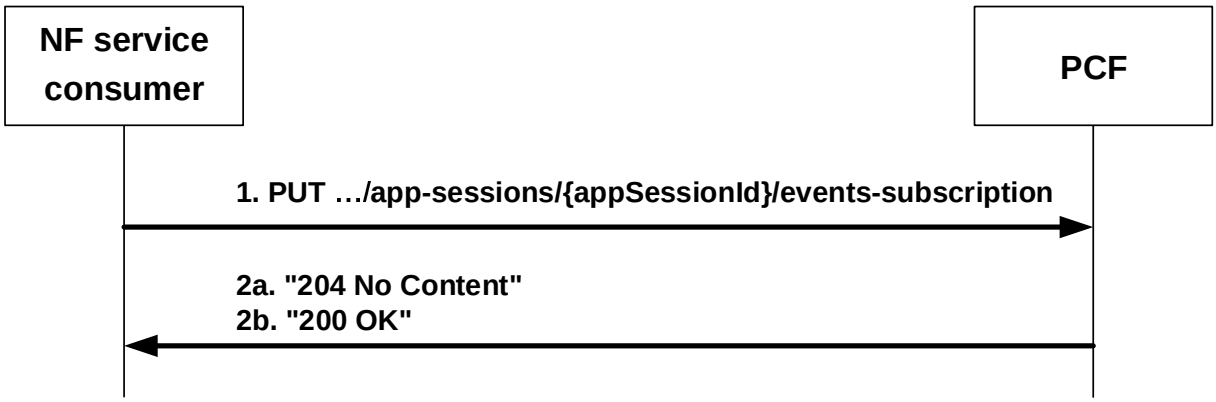


**Figure 4.2.6.2-2: Modification of events subscription information using HTTP PUT**

When the NF service consumer decides to create a subscription to one or more events for the existing application session context or to modify an existing subscription previously created by itself at the PCF, the NF service consumer shall invoke the Npcf_PolicyAuthorization_Subscribe service operation by sending the HTTP PUT request to the resource URI representing the "Events Subscription" sub-resource in the PCF, as shown in figure 4.2.6.2-1, step 1 and figure 4.2.6.2-2, step 1. The NF service consumer shall provide in the "EventsSubscReqData" data type of the body of the HTTP PUT request:

- the "events" attribute with the list of events to be subscribed; and
- the "notifUri" attribute that includes the Notification URI to indicate to the PCF where to send the notification of the subscribed events.

NOTE 1: The "notifUri" attribute within the EventsSubscReqData data structure can be modified to request that subsequent notifications are sent to a new NF service consumer.

Upon the reception of the HTTP PUT request from the NF service consumer, the PCF shall decide whether the received HTTP PUT request is accepted.

If the HTTP PUT request from the NF service consumer is rejected, the PCF shall indicate in the HTTP response the cause for the rejection as specified in clause 5.7.

If the feature "ES3XX" is supported, and the PCF determines the received HTTP PUT request needs to be redirected, the PCF shall send an HTTP redirect response as specified in clause 6.10.9 of 3GPP TS 29.500 [5].

If the PCF accepted the HTTP PUT request to create a subscription to events, the PCF shall create the "Events Subscription" sub-resource and shall send the HTTP response message to the NF service consumer as shown in figure 4.2.6.2-1, step 2. The PCF shall include in the "201 Created" response:

- a Location header field that shall contain the URI of the created "Events Subscription" sub-resource i.e. "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription"; and
- a response body with the "EventsSubscPutData" data type, that contains the attributes of the "EventsSubscReqData" data type, representing the created "Events Subscription" sub-resource.

If the PCF determines that one or more of the subscribed events are already met in the PCF, the PCF may also include the attributes of the "EventsNotification" data type within the "EventsSubscPutData" data type to notify about the already met events in the PCF.

If the PCF accepted the HTTP PUT request to modify the events subscription, the PCF shall modify the "Events Subscription" sub-resource and shall send to the NF service consumer:

- the HTTP "204 No Content" response (as shown in figure 4.2.6.2-2, step 2a); or
- the HTTP "200 OK" response (as shown in figure 4.2.6.2-2, step 2b) including in the "EventsSubscPutData" data type the updated representation of the "Events Subscription" sub-resource encoded within the attributes of the

"EventsSubscReqData" data type and, if one or more of the updated subscribed events are already met in the PCF, the notification of these events by including the attributes of the "EventsNotification" data type.

The PCF shall include in the "evsNotif" attribute:

- if the NF service consumer subscribed to the "PLMN_CHG" event in the HTTP PUT request, the "event" attribute set to "PLMN_CHG" and the "plmnId" attribute including the PLMN Identifier or the SNPN Identifie if the PCF has previously requested to be updated with this information in the SMF; and

NOTE 2: The SNPN Identifier consists of the PLMN Identifier and the NID.

- if the NF service consumer subscribed to the "ACCESS_TYPE_CHANGE" event in the HTTP PUT request, the "event" attribute set to "ACCESS_TYPE_CHANGE" and:

  i. the "accessType" attribute including the access type, and the "ratType" attribute including the RAT type when applicable for the notified access type; and

  ii. if the "ATSSS" feature is supported, the "addAccessInfo" attribute with the additional access type information if available, where the access type is encoded in the "accessType" attribute, and the RAT type is encoded in the "ratType" attribute when applicable for the notified access type; and

NOTE 3: For a MA PDU session, if the "ATSSS" feature is not supported by the NF service consumer the PCF includes the "accessType" attribute and the "ratType" attribute with a currently active combination of access type and RAT type (when applicable for the notified access type). When both 3GPP and non-3GPP accesses are available, the PCF includes the information corresponding to the 3GPP access.

  iii. the "anGwAddr" attribute including access network gateway address when available,

  if the PCF has previously requested to be updated with this information in the SMF.

Based on the received subscription information from the NF service consumer, the PCF may create a subscription to event notifications or may modify the existing subscription to event notifications, for a related PDU session from the SMF, as described in 3GPP TS 29.512 [8].

### 4.2.6.3 Initial subscription to events without provisioning of service information

The NF service consumer may subscribe with the PCF to events notification without providing service information.

NOTE 1: This service operation is intended to create a resource that enables to handle subscription to events without provisioning service information. For the scenarios where it is known the NF service consumer, after creating a subscription without service information, could require an application session context with the PCF with required service information, the NF service consumer needs to create an Individual Application Session context as described in clause 4.2.2.2.

Figure 4.2.6.3-1 illustrates the initial subscription to events without provisioning of service information.

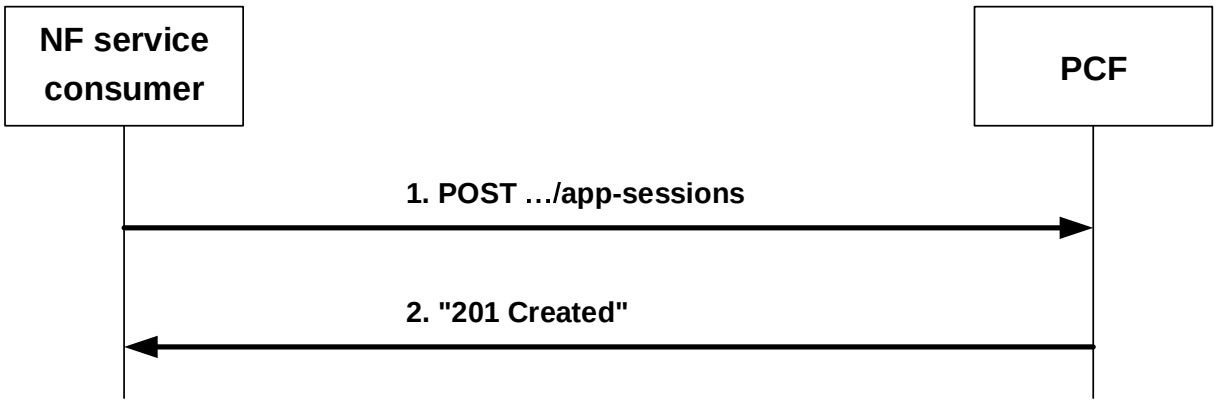


**Figure 4.2.6.3-1: Initial Subscription to events without provisioning of service information**

When a NF service consumer establishes an application session context with the PCF to subscribe to events and does not require PCC control for the related media, the NF service consumer shall invoke the Npcf_PolicyAuthorization_Subscribe service operation by sending the HTTP POST request to the resource URI representing the "Application Sessions" collection resource of the PCF, as shown in figure 4.2.6.3-1, step 1.

The NF service consumer shall include in the "ascReqData" attribute of the "AppSessionContext" data type in the payload body of the HTTP POST request:

- either the "ueMac" attribute containing the UE MAC address, or the "ueIpv4" attribute or "ueIpv6" attribute containing the UE IPv4 or the IPv6 address;
- the "notifUri" attribute containing the URI where the PCF shall request to the NF service consumer the deletion of the "Individual Application Session Context" resource"; and
- the "evSubsc" attribute of "EventsSubscReqData" data type to request the notification of certain user plane events. The NF service consumer shall include:
    a. the events to subscribe to in the "events" attribute; and
    b. the notification URI where to address the notification of the met events within the "notifUri" attribute.

The NF service consumer may provide in the "AppSessionContext" data type the DNN in the "dnn" attribute, SUPI in the "supi" attribute or other information if available.

If the PCF cannot successfully fulfil the received HTTP POST request due to the internal PCF error or due to the error in the HTTP POST request, the PCF shall send the HTTP error response as specified in clause 5.7.

Otherwise, when the PCF receives the HTTP POST request from the NF service consumer, the PCF shall apply session binding as described in 3GPP TS 29.513 [7]. The PCF identifies the PDU session for which the HTTP POST request applies as described in clause 4.2.2.2.

The information required for session binding (UE MAC address, or UE Ipv4 or IPv6 address, DNN, SUPI and other available information, such as S-NSSAI and/or IPv4 address domain identifier) is provisioned in the "Individual Application Session Context" resource. The events subscription is provisioned in the "Events Subscription" sub-resource.

Based on the received subscription information from the NF service consumer, the PCF may create a subscription to event notifications for a related PDU session from the SMF, as described in 3GPP TS 29.512 [8].

If the PCF created the "Events Subscription" sub-resource within the "Individual Application Session Context" resource, the PCF shall send to the NF service consumer a "201 Created" response to the HTTP POST request, as shown in figure 4.2.6.3-1, step 2. The PCF shall include in the "201 Created" response:

- a Location header field; and
- an "AppSessionContext" data type in the payload body.

The Location header field shall contain the URI of the created events subscription sub-resource i.e. "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription".

The "AppSessionContext" data type payload body shall contain the representation of the created "Individual Application Session Context" resource and "Events Subscription" sub-resource.

The PCF shall include in the "evsNotif" attribute:

- if the NF service consumer subscribed to the event "PLMN_CHG" in the HTTP POST request, the "event" attribute set to "PLMN_CHG" and the "plmnId" attribute including the PLMN Identifier or the SNPN Identifier if the PCF has previously requested to be updated with this information in the SMF;

NOTE 2: The SNPN Identifier consists of the PLMN Identifier and the NID.

- if the NF service consumer subscribed to the event "ACCESS_TYPE_CHANGE" in the HTTP POST request, the "event" attribute set to "ACCESS_TYPE_CHANGE" and:
    i. the "accessType" attribute including the access type, and the "ratType" attribute including the RAT type when applicable for the notified access type; and

ii. if the "ATSSS" feature is supported, the "addAccessInfo" attribute with the additional access type information if available, where the access type is encoded in the "accessType" attribute, and the RAT type is encoded in the "ratType" attribute when applicable for the notified access type; and

NOTE 3: For a MA PDU session, if the "ATSSS" feature is not supported by the NF service consumer the PCF includes the "accessType" attribute and the "ratType" attribute with a currently active combination of access type and RAT type (if applicable for the notified access type). When both 3GPP and non-3GPP accesses are available, the PCF includes the information corresponding to the 3GPP access.

iii. the "anGwAddr" attribute including access network gateway address when available,

if the PCF has previously requested to be updated with this information in the SMF; and

- if the "IMS_SBI" feature is supported and if the NF service consumer subscribed to the event "CHARGING_CORRELATION" in the HTTP POST request, the "event" attribute set to "CHARGING_CORRELATION" and may include the "anChargIds" attribute containing the access network charging identifier(s) and the "anChargAddr" attribute containing the access network charging address.

NOTE 4: Due to the resource structure, as result of the Npcf_PolicyAuthorization_Subscribe service operation using POST methods, the PCF creates an Individual Application Session context resource which can only be deleted via Npcf_PolicyAuthorization_Delete service operation.

### 4.2.6.4 Subscription to usage monitoring of sponsored data connectivity

This procedure is used by a NF service consumer to subscribe with the PCF to usage monitoring of sponsored data connectivity or to provide updated usage thresholds for the existing application session context, when the "Sponsored Connectivity" feature is supported.

The NF service consumer shall include in the HTTP PUT request message described in clause 4.2.6.2 the "EventsSubscReqData" data type, that shall contain:

- the "events" attribute with a new entry of the "AfEventSubscription" data type with the "event" attribute set to "USAGE_REPORT"; and
- the "usgThres" attribute with the usage thresholds to apply.

The PCF shall reply to the NF service consumer as described in clause 4.2.6.2.

### 4.2.6.5 Void

### 4.2.6.6 Request of access network information

This procedure is used by a NF service consumer to request the PCF to report the access network information (i.e. user location and/or user timezone information) without providing service information when the "NetLoc" feature is supported.

The NF service consumer can request access network information without providing service information:

- at initial subscription to events, using the HTTP POST request message as described in clause 4.2.6.3; and
- at modification of the subscription to events, using the HTTP PUT request message as described in clause 4.2.6.2.

The NF service consumer shall include in the HTTP request message:

- an entry of the "AfEventSubscription" data type in the "events" attribute with:

  a) the "event" attribute set to the value "ANI_REPORT"; and

  b) the "notifMethod" attribute set to the value "ONE_TIME"; and

- the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

When the PCF determines that the access network does not support the access network information reporting because the SMF does not support the NetLoc feature, the PCF shall respond to the NF service consumer including in the "EventsNotification" data type the "noNetLocSupp" attribute set to "ANR_NOT_SUPPORTED" value. Otherwise, the PCF shall immediately configure the SMF to provide such access information, as specified in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer with the HTTP POST response as described in clause 4.2.6.3 and with the HTTP PUT response as described in clause 4.2.6.2.

### 4.2.6.7 Subscription to notification of signalling path status

When the feature "IMS_SBI" is supported, this procedure is used by a NF service consumer to subscribe to notifications of the status of the AF signalling transmission path.

The NF service consumer shall create a new "Individual Application Session Context" resource with the PCF for the AF signalling using the Npcf_PolicyAuthorization_Create service operation.

The NF service consumer shall provide:

- the IP address (IPv4 or IPv6) of the UE in the "ueIpv4" or "ueIpv6" attribute;
- within the "evSubsc" attribute, the "event" attribute set to "FAILED_RESOURCES_ALLOCATION"; and
- a media component within the "medComponents" attribute including:
  - the "medCompN" attribute set to "0"; and
  - a single media subcomponent within the "medSubComps" attribute with:
    - the "flowUsage" attribute set to the value "AF_SIGNALLING"; and
    - if the procedures for NF service consumer provisioning of AF signalling flow information do not apply, the "fNum" attribute set to "0".

When the "fNum" attribute is set to "0", the rest of attributes within the related media component and media subcomponent shall not be used.

The PCF shall perform session binding as described in 3GPP TS 29.513 [7] and shall reply to the NF service consumer as described in clause 4.2.6.3.

PCC rules related to AF signalling IP flows should be provisioned to SMF using the corresponding procedures specified at 3GPP TS 29.512 [8] at an earlier stage (e.g. typically at the establishment of the QoS flow dedicated for AF signalling IP flows). The PCF may install the corresponding dynamic PCC rules for the AF signalling IP flows if none has been installed before.

NOTE 1: Well-known ports (e.g. 3GPP TS 24.229 [32] for SIP) or wildcard ports can be used by PCF to derive the dynamic PCC for the AF signalling IP flows.

If the "Individual Application Session Context" resource is only used for subscription to notification of AF signalling path status, the NF service consumer may cancel the subscription to notifications of the status of the AF signalling transmission path removing the resource as described in clause 4.2.4.2.

NOTE 2: The "Individual Application Session Context" resource created for the AF signalling can also be used when the NF service consumer requests notifications of access type change, access network information for SMS over IP and/or when the NF service consumer provisions AF Signalling Flow Information.

### 4.2.6.8 Subscription to Service Data Flow QoS Monitoring Information

This procedure is used by NF service consumer to subscribe and/or modify the PCF subscription for notification about packet delay between UPF and UE, when the "QoSMonitoring" feature is supported.

The NF service consumer shall include in the HTTP PUT request message described in clause 4.2.6.2 the "EventsSubscReqData" data type, that shall contain:

- to create a subscription to notifications of QoS monitoring report:

  a) shall include the "events" array with an array that contains a new entry per requested notification method with the "event" attribute set to "QOS_MONITORING", and notification related information as described in clause 4.2.2.23;

  b) when the "notifMethod" of the new entry is "EVENT_DETECTION", shall include a "qosMon" attribute with the QoS monitoring information as described in clause 4.2.2.23;

  c) shall include the new requested QoS monitoring parameter(s) to be measured (i.e. DL, UL and/or round trip packet delay) within the "reqQosMonParams" attribute; and

  d) may include the notification correlation identifier assigned by the AF within the "notifCorreId" attribute;

  e) if the feature "ExposureToEAS" is supported, may include the "directNotifInd" attribute set to true to indicate the direct event notification of QoS Monitoring data from the UPF.

- to remove a subscription to QoS monitoring information:

  a) shall include the "events" array containing an array that shall omit the corresponding entry with the "event" attribute value "QOS_MONITORING"; and

  b) when the "notifMethod" of the removed entry is "EVENT_DETECTION", it shall omit the "qosMon" attribute;

  c) shall omit the "reqQosMonParams";

  d) if the feature "ExposureToEAS" is supported, shall omit the "directNotifInd" attribute;

The NF service consumer shall include other events related information that shall remain unchanged.

As result of this action, the PCF shall set the appropriate subscription to QoS monitoring information for the corresponding active PCC rule(s) as described in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer as described in clause 4.2.6.2.

### 4.2.6.9 Subscription to application detection notification

This procedure is used by a NF service consumer to request the PCF the subscription to application (e.g. start, stop) detection notifications, if the "ApplicationDetectionEvents" feature is supported.

The NF service consumer can request the subscription to notification of application detection events without providing service information:

- at initial subscription to events, using the HTTP POST request message as described in clause 4.2.6.3; and

- at modification of the subscription to events, using the HTTP PUT request message as described in clause 4.2.6.2.

The NF service consumer shall include:

- To subscribe to notifications about the detection of the start/stop of one or more application's traffic the "evSubsc" attribute within the POST request as described in clause 4.2.6.3, with:

  a. the "events" array, including an event with the "event" attribute value set to "APP_DETECTION"; and

  b. the "afAppIds" attribute, with the list of AF application identifier(s) that refer to the applications' traffic to detect.

- To modify the subscription to notifications of application's traffic detection the "EventsSubscReqData" data type within the PUT request as described in clause 4.2.6.2, including an event with the "event" attribute value set to "APP_DETECTION" and an updated list of AF application identifiers within the "afAppIds" attribute.

- To remove the subscription to notifications about the start and stop of the applications traffic, an "events" array within the PUT request as described in clause 4.2.6.2, without including any event with the "event" attribute value "APP_DETECTION" and omitting the "afAppIds" attribute.

The PCF shall reply to the NF service consumer with the HTTP POST response as described in clause 4.2.6.3 and with the HTTP PUT response as described in clause 4.2.6.2.

The PCF shall set the appropriate subscription to Application Detection for the corresponding PCC rule(s) as described in 3GPP TS 29.512 [8].

In this release of the specification application detection applies only to the application(s) with IP traffic.

#### 4.2.6.10 Subscription to satellite backhaul category changes

When the feature "SatelliteBackhaul" is supported, this procedure is used by NF service consumer to subscribe and/or modify the PCF subscription to receive a notification when the satellite backhaul category changes and when the backhaul category changes between satellite backhaul and non-satellite backhaul.

The NF service consumer shall include in the HTTP PUT request message described in clause 4.2.6.2 the "EventsSubscReqData" data type, or in the HTTP POST request message described in clause 4.2.6.3 the "evSubsc" attribute, that shall contain the "events" array, with a new entry with the "event" attribute set to "SAT_CATEGORY_CHG" to indicate the creation of a subscription to backhaul category changes.

The NF service consumer shall include other events related information that shall remain unchanged.

As result of this action, the PCF shall set the appropriate subscription to satellite backhaul changes for the PDU session as described in in 3GPP TS 29.512 [8].

The PCF shall reply to the NF service consumer as described in clause 4.2.6.2 or in clause 4.2.6.3. The PCF shall include the "evsNotif" attribute with an entry in the "evNotifs" array with the "event" attribute set to "SAT_CATEGORY_CHG" and the "satBackhaulCategory" attribute including the satellite backhaul category or the indication of non-satellite backhaul if the PCF has previously subscribed with the SMF to changes in this information.

### 4.2.7 Npcf_PolicyAuthorization_Unsubscribe service operation

#### 4.2.7.1 General

The Npcf_PolicyAuthorization_Unsubscribe service operation enables NF service consumers to remove subscription to all subscribed events for the existing application session context. Subscription to events shall be removed:

- by invoking the Npcf_PolicyAuthorization_Unsubscribe service operation for the existing application session context, as described in clause 4.2.7.2; or
- within the application session context modification procedure by invoking the Npcf_PolicyAuthorization_Update service operation, as described in clause 4.2.3; or
- within the application session context termination procedure by invoking the Npcf_PolicyAuthorization_Delete service operation, as described in clause 4.2.4.

The following procedure using the Npcf_PolicyAuthorization_Unsubscribe service operation is supported:

- Unsubscription to events.

#### 4.2.7.2 Unsubscription to events

This procedure is used to unsubscribe to all subscribed events for the existing AF application session context, as defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [4].

Figure 4.2.7.2-1 illustrates the unsubscription to events using the HTTP DELETE method.

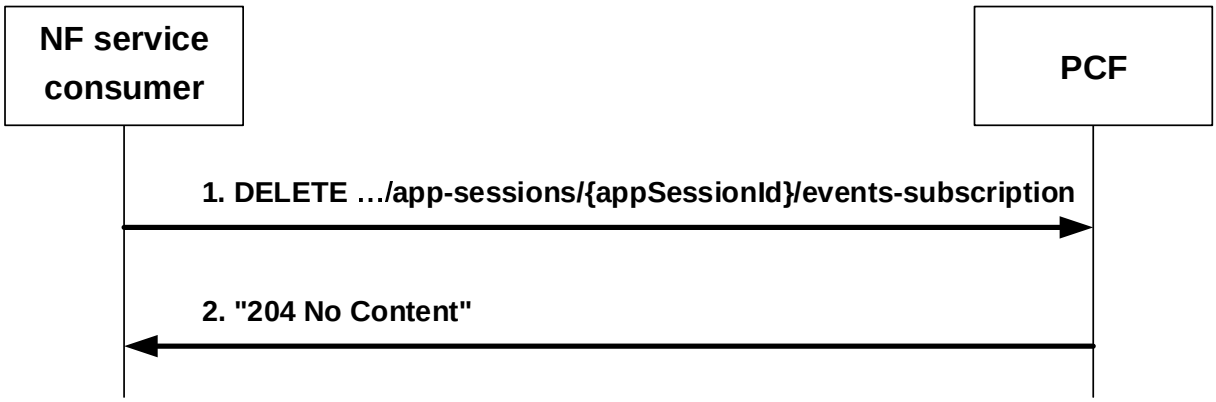


**Figure 4.2.7.2-1: Removal of events subscription information using HTTP DELETE**

When the NF service consumer decides to unsubscribe to all subscribed events for the existing application session context, the NF service consumer shall invoke the Npcf_PolicyAuthorization_Unsubscribe service operation by sending the HTTP DELETE request message to the resource URI representing the "Events Subscription" sub-resource in the PCF, as shown in figure 4.2.7.2-1, step 1.

Upon the reception of the HTTP DELETE request message from the NF service consumer, the PCF shall decide whether the received HTTP request message is accepted.

If the HTTP DELETE request message from the NF service consumer is accepted, the PCF shall delete "Events Subscription" sub-resource and shall send to the NF service consumer a HTTP "204 No Content" response message. The PCF may delete the existing subscription to event notifications for the related PDU session from the SMF as described in 3GPP TS 29.512 [8].

If the HTTP DELETE request message from the NF service consumer is rejected, the PCF shall indicate in the HTTP response message the cause for the rejection as specified in clause 5.7.

# 5 Npcf_PolicyAuthorization Service API

## 5.1 Introduction

The Npcf_PolicyAuthorization Service shall use the Npcf_PolicyAuthorization API.

The API URI of the Npcf_PolicyAuthorization API shall be:

**{apiRoot}/<apiName>/<apiVersion>**

The request URIs used in each HTTP requests from the NF service consumer towards the PCF shall have the Resource URI structure defined in clause 4.4.1 of 3GPP TS 29.501 [6], i.e.:

**{apiRoot}/<apiName>/<apiVersion>/<apiSpecificResourceUriPart>**

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [6].
- The <apiName> shall be "npcf-policyauthorization".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 5.3.

# 5.2 Usage of HTTP

## 5.2.1 General

HTTP/2, IETF RFC 7540 [9], shall be used as specified in clause 5.2 of 3GPP TS 29.500 [5].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [5].

The OpenAPI [11] specification of HTTP messages and content bodies for the Npcf_PolicyAuthorization service is contained in Annex A.

## 5.2.2 HTTP standard headers

### 5.2.2.1 General

See clause 5.2.2 of 3GPP TS 29.500 [5] for the usage of HTTP standard headers.

### 5.2.2.2 Content type

JSON, IETF RFC 8259 [10], shall be used as content type of the HTTP bodies specified in the present specification, as specified in clause 5.4 of 3GPP TS 29.500 [5]. The use of the JSON format shall be signalled by the content type "application/json".

JSON object used in the HTTP PATCH request shall be encoded according to "JSON Merge Patch" and shall be signalled by the content type "application/merge-patch+json", as defined in IETF RFC 7396 [21].

"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 7807 [24].

## 5.2.3 HTTP custom headers

The Npcf_PolicyAuthorization API shall support mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [5] and may support optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [5].

In this Release of the specification, no specific custom headers are defined for the Npcf_PolicyAuthorization API.

# 5.3 Resources

## 5.3.1 Resource Structure

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 5.3.1-1 depicts the resource URIs structure for the Npcf_PolicyAuthorization API.

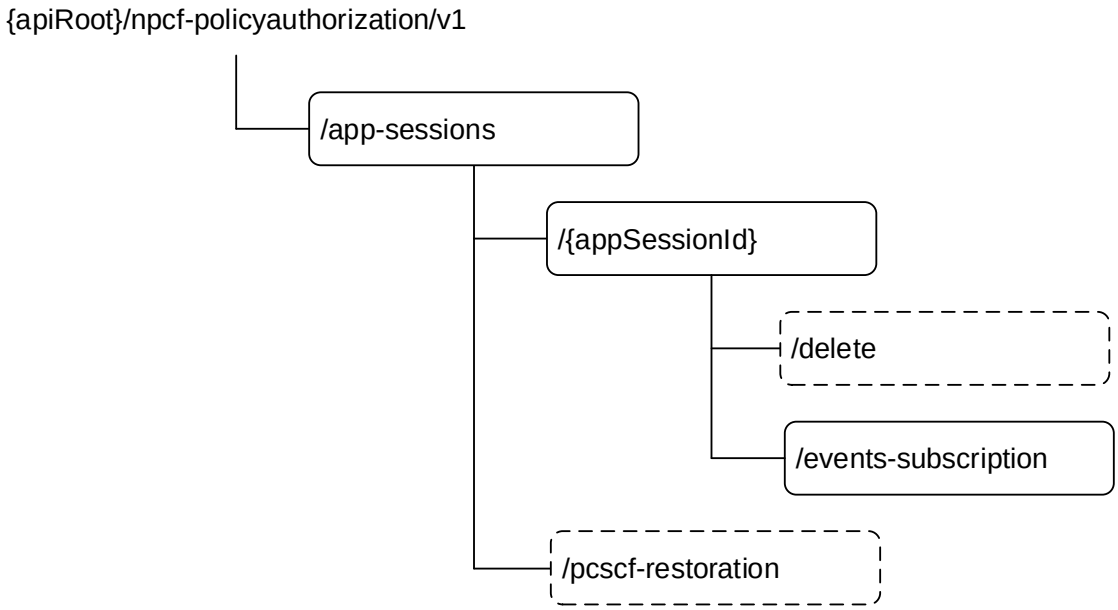


**Figure 5.3.1-1: Resource URI structure of the Npcf_PolicyAuthorization API**

Table 5.3.1-1 provides an overview of the resources and applicable HTTP methods.

**Table 5.3.1-1: Resources and methods overview**

| Resource name | Resource URI | HTTP method or custom operation | Description |
|---|---|---|---|
| Application Sessions | /app-sessions | POST | Npcf_PolicyAuthorization_Create. Creates a new Individual Application Session Context resource and may create the child Events Subscription sub-resource. |
| | /app-sessions/pcscf-restoration | PcscfRestoration (POST) | P-CSCF restoration. It indicates that P-CSCF restoration needs to be performed. |
| Individual Application Session Context | /app-sessions/{appSessionId} | PATCH | Npcf_PolicyAuthorization_Update. Updates an existing Individual Application Session Context resource. It can also update an Events Subscription sub-resource. |
| | | GET | Reads an existing Individual Application Session Context resource. |
| | /app-sessions/{appSessionId}/delete | delete (POST) | Npcf_PolicyAuthorization_Delete. Deletes an existing Individual Application Session Context resource and the child Events Subscription sub-resource. |
| Events Subscription | /app-sessions/{appSessionId} /events-subscription | PUT | Npcf_PolicyAuthorization_Subscribe. Creates a new Events Subscription sub-resource or modifies an existing Events Subscription sub-resource. |
| | | DELETE | Npcf_PolicyAuthorization_Unsubscribe. Deletes an Events Subscription sub-resource. |

## 5.3.2 Resource: Application Sessions (Collection)

### 5.3.2.1 Description

The Application Sessions resource represents all application session contexts that exist in the Npcf_PolicyAuthorization service at a given PCF instance.

### 5.3.2.2 Resource definition

Resource URI: **{apiRoot}/npcf-policyauthorization/v1/app-sessions**

This resource shall support the resource URI variables defined in table 5.3.2.2-1.

**Table 5.3.2.2-1: Resource URI variables for this resource**

| Name | Data type | Definition |
|---|---|---|
| apiRoot | string | See clause 5.1 |

### 5.3.2.3 Resource Standard Methods

#### 5.3.2.3.1 POST

This method shall support the URI query parameters specified in table 5.3.2.3.1-1.

**Table 5.3.2.3.1-1: URI query parameters supported by the POST method on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| n/a | | | | |

This method shall support the request data structures specified in table 5.3.2.3.1-2 and the response data structures and response codes specified in table 5.3.2.3.1-3.

**Table 5.3.2.3.1-2: Data structures supported by the POST Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| AppSessionContext | M | 1 | Contains the information for the creation of a new Individual Application Session Context resource. |

**Table 5.3.2.3.1-3: Data structures supported by the POST Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| AppSessionContext | M | 1 | 201 Created | Successful case.<br>The creation of an Individual Application Session Context resource is confirmed and a representation of that resource is returned. |
| n/a | | | 303 See Other | The result of the HTTP POST request would be equivalent to the existing Application Session Context.<br>The HTTP response shall contain a Location header field set to the URI of the existing individual Application Session Context resource. |
| ProblemDetails | O | 0..1 | 400 Bad Request | (NOTE 2) |
| ExtendedProblemDetails | O | 0..1 | 403 Forbidden | (NOTE 2) |
| ProblemDetails | O | 0..1 | 500 Internal Server Error | (NOTE 2) |
| NOTE 1: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the POST method shall also apply.<br>NOTE 2: Failure cases are described in clause 5.7. | | | | |

**Table 5.3.2.3.1-4: Headers supported by the 201 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | Contains the URI of the newly created resource, according to the structure: {apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId} |

**Table 5.3.2.3.1-5: Headers supported by the 303 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | Contains the URI of the existing individual Application Session Context resource. |

**Table 5.3.2.3.1-6: Headers supported by the 403 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Retry-After | string or integer | M | 1 | Indicates the time the NF service consumer has to wait before making a new request. |

## 5.3.2.4 Resource Custom Operations

### 5.3.2.4.1 Overview

**Table 5.3.2.4.1-1: Custom operations**

| Operation name | Custom operation URI | Mapped HTTP method | Description |
|---|---|---|---|
| PcscfRestoration | /app-sessions/pcscf-restoration | POST | The P-CSCF Restoration custom operation invokes P-CSCF restoration. It does not create an Individual Application Session Context resource. |

### 5.3.2.4.2 Operation: PcscfRestoration

#### 5.3.2.4.2.1 Description

#### 5.3.2.4.2.2 Operation Definition

This custom operation invokes P-CSCF restoration in the PCF and does not create an Individual Application Session Context resource.

This operation shall support the request data structure specified in table 5.3.2.4.2.2-1 and the response data structure and response codes specified in table 5.3.2.4.2.2-2.

**Table 5.3.2.4.2.2-1: Data structures supported by the POST Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| PcscfRestorationRequestData | O | 0..1 | P-CSCF restoration data to be sent by the NF service consumer to request the P-CSCF restoration to the PCF. |

**Table 5.3.2.4.2.2-2: Data structures supported by the POST Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| n/a | | | 204 No Content | Successful case.<br>The P-CSCF restoration has been successfully invoked. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during P-CSCF restoration. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during P-CSCF restoration. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| ProblemDetails | O | 0..1 | 500 Internal Server Error | (NOTE 2) |
| NOTE 1: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the POST method shall also apply.<br>NOTE 2: Failure cases are described in subclause 5.7. | | | | |

**Table 5.3.2.4.2.2-3: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

**Table 5.3.2.4.2.2-4: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

## 5.3.3 Resource: Individual Application Session Context (Document)

### 5.3.3.1 Description

The Individual Application Session Context resource represents a single application session context that exists in the Npcf_PolicyAuthorization service.

### 5.3.3.2 Resource definition

Resource URI: **{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}**

This resource shall support the resource URI variables defined in table 5.3.2.2-1.

**Table 5.3.3.2-1: Resource URI variables for this resource**

| Name | Data type | Definition |
|---|---|---|
| apiRoot | string | See clause 5.1 |
| appSessionId | string | Identifies an application session context formatted according to IETF RFC 3986 [19]. |

### 5.3.3.3 Resource Standard Methods

#### 5.3.3.3.1 GET

This method shall support the URI query parameters specified in table 5.3.3.3.1-1.

**Table 5.3.3.3.1-1: URI query parameters supported by the GET method on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| n/a | | | | |

This method shall support the request data structures specified in table 5.3.3.3.1-2 and the response data structures and response codes specified in table 5.3.3.3.1-3.

**Table 5.3.3.3.1-2: Data structures supported by the GET Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| n/a | | | |

**Table 5.3.3.3.1-3: Data structures supported by the GET Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| AppSessionContext | M | 1 | 200 OK | A representation of an Individual Application Session Context resource is returned. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during Individual Application Session Context retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during Individual Application Session Context retrieval. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| ProblemDetails | O | 0..1 | 404 Not Found | (NOTE 2) |
| NOTE 1: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the GET method shall also apply.<br>NOTE 2: Failure cases are described in clause 5.7. | | | | |

**Table 5.3.3.3.1-4: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

**Table 5.3.3.3.1-5: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

#### 5.3.3.3.2 PATCH

This method shall support the URI query parameters specified in table 5.3.3.3.2-1.

**Table 5.3.3.3.2-1: URI query parameters supported by the PATCH method on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| n/a | | | | |

This method shall support the request data structures specified in table 5.3.3.3.2-2 and the response data structures and response codes specified in table 5.3.3.3.2-3.

**Table 5.3.3.3.2-2: Data structures supported by the PATCH Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| AppSessionContextUpdateDataPatch | M | 1 | Contains the modification(s) to apply to the Individual Application Session Context resource. |

**Table 5.3.3.3.2-3: Data structures supported by the PATCH Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| AppSessionContext | M | 1 | 200 OK | Successful case.<br>The Individual Application Session Context resource was modified and a representation of that resource is returned. |
| n/a | | | 204 No Content | Successful case.<br>The Individual Application session context resource was modified. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during Individual Application Session Context modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during Individual Application Session Context modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| ProblemDetails | O | 0..1 | 400 Bad Request | (NOTE 2) |
| ExtendedProblemDetails | O | 0..1 | 403 Forbidden | (NOTE 2) |
| ProblemDetails | O | 0..1 | 404 Not Found | (NOTE 2) |
| NOTE 1: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the PATCH method shall also apply.<br>NOTE 2: Failure cases are described in clause 5.7. | | | | |

**Table 5.3.3.3.2-4: Headers supported by the 403 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Retry-After | string or integer | M | 1 | Indicates the time the NF service consumer has to wait before making a new request. |

**Table 5.3.3.3.2-5: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

**Table 5.3.3.3.2-6: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

## 5.3.3.4 Resource Custom Operations

### 5.3.3.4.1 Overview

**Table 5.3.3.4.1-1: Custom operations**

| Operation name | Custom operation URI | Mapped HTTP method | Description |
|---|---|---|---|
| delete | /app-sessions/{appSessionId}/delete | POST | Npcf_PolicyAuthorization_Delete. Deletes an existing Individual Application Session Context resource and the child Events Subscription sub-resource. |

### 5.3.3.4.2 Operation: delete

#### 5.3.3.4.2.1 Description

#### 5.3.3.4.2.2 Operation Definition

This custom operation deletes an existing Individual Application Session Context resource and the child Events Subscription sub-resource in the PCF.

This operation shall support the request data structures specified in table 5.3.3.4.2.2-1 and the response data structure and response codes specified in table 5.3.3.4.2.2-2.

**Table 5.3.3.4.2.2-1: Data structures supported by the POST Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| EventsSubscReqData | O | 0..1 | Events subscription information to be sent by the NF service consumer to request event notification when the Individual Application Session Context resource is deleted. |

**Table 5.3.3.4.2.2-2: Data structures supported by the POST Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| n/a | | | 204 No Content | Successful case.<br>The Individual Application session context resource was deleted. |
| AppSessionContext | M | 1 | 200 OK | Successful case.<br>The Individual Application Session Context resource was deleted and a partial representation of that resource containing event notification information is returned. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during Individual Application Session Context termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during Individual Application Session Context termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| ProblemDetails | O | 0..1 | 404 Not Found | (NOTE 2) |

NOTE 1: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the POST method shall also apply.
NOTE 2: Failure cases are described in clause 5.7.

**Table 5.3.3.4.2.2-3: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

**Table 5.3.3.4.2.2-4: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

## 5.3.4 Resource: Events Subscription (Document)

### 5.3.4.1 Description

The Events Subscription sub-resource represents a subscription to events for an application session context that exists in the Npcf_PolicyAuthorization service.

### 5.3.4.2 Resource definition

Resource URI: **{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription**

This resource shall support the resource URI variables defined in table 5.3.4.2-1.

**Table 5.3.4.2-1: Resource URI variables for this resource**

| Name | Data type | Definition |
|---|---|---|
| apiRoot | string | See clause 5.1 |
| appSessionId | string | Identifies an application session context formatted according to IETF RFC 3986 [19]. |

### 5.3.4.3 Resource Standard Methods

#### 5.3.4.3.1 PUT

This method shall support the URI query parameters specified in table 5.3.4.3.1-1.

**Table 5.3.4.3.1-1: URI query parameters supported by the PUT method on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| n/a | | | | |

This method shall support the request data structures specified in table 5.3.4.3.1-2 and the response data structures and response codes specified in table 5.3.4.3.1-3.

**Table 5.3.4.3.1-2: Data structures supported by the PUT Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| EventsSubscReqData | M | 1 | Contains information for the modification of the Events Subscription sub-resource. |

**Table 5.3.4.3.1-3: Data structures supported by the PUT Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| EventsSubscPutData | M | 1 | 201 Created | Successful case.<br>The Events Subscription sub-resource was created.<br>The properties of the EventsSubscReqData data type shall be included. The properties of the EventsNotification data type shall be included when the notification for one or more created events is already available in the PCF. |
| EventsSubscPutData | M | 1 | 200 OK | Successful case.<br>The Events Subscription sub-resource was modified and a representation of that sub-resource is returned.<br>The properties of the EventsSubscReqData data type shall be included. The properties of the EventsNotification data type shall be included when the notification for one or more updated events is already available in the PCF. |
| n/a | | | 204 No Content | Successful case.<br>The Events Subscription sub-resource was modified. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during Events Subscription modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during Events Subscription modification. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| ProblemDetails | O | 0..1 | 403 Forbidden | (NOTE 2) |
| ProblemDetails | O | 0..1 | 404 Not Found | (NOTE 2) |
| NOTE 1: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the PUT method shall also apply.<br>NOTE 2: Failure cases are described in clause 5.7. | | | | |

**Table 5.3.4.3.1-4: Headers supported by the 201 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | Contains the URI of the newly created resource, according to the structure: {apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription |

**Table 5.3.4.3.1-5: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

**Table 5.3.4.3.1-6: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

#### 5.3.4.3.2 DELETE

This method shall support the URI query parameters specified in table 5.3.4.3.2-1.

**Table 5.3.4.3.2-1: URI query parameters supported by the DELETE method on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| n/a | | | | |

This method shall support the request data structures specified in table 5.3.4.3.2-2 and the response data structures and response codes specified in table 5.3.4.3.2-3.

**Table 5.3.4.3.2-2: Data structures supported by the DELETE Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| n/a | | | |

**Table 5.3.4.3.2-3: Data structures supported by the DELETE Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| n/a | | | 204 No Content | Successful case.<br>The Events Subscription sub-resource was deleted. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during Events Subscription termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during Events Subscription termination. The response shall include a Location header field containing an alternative URI of the resource located in an alternative PCF (service) instance.<br>Applicable if the feature "ES3XX" is supported. |
| ProblemDetails | O | 0..1 | 404 Not Found | (NOTE 2) |
| NOTE 1: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the DELETE method shall also apply.<br>NOTE 2: Failure cases are described in clause 5.7. | | | | |

**Table 5.3.4.3.2-4: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

**Table 5.3.4.3.2-5: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI of the resource located in an alternative PCF (service) instance. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the request is redirected |

### 5.3.3.4 Resource Custom Operations

None.

# 5.4 Custom Operations without associated resources

No custom operation is defined in this Release of the specification.

# 5.5 Notifications

## 5.5.1 General

Notifications shall comply to clause 6.2 of 3GPP TS 29.500 [5] and clause 4.6.2.3 of 3GPP TS 29.501 [6].

**Table 5.5.1-1: Notifications overview**

| Notification | Callback URI | HTTP method or custom operation | Description (service operation) |
|---|---|---|---|
| Event Notification | {notifUri}/notify | notify (POST) | PCF event notification. |
| Termination Request | {notifUri}/terminate | terminate (POST) | Request for termination of an Individual Application Session Context. |
| Notification about new 5GS Bridge | {notifUri}/new-bridge | new-bridge (POST) | Notification about new 5GS Bridge |
| Notification about PDU session events | {notifUri}/pdu-session | pdu-session (POST) | Notification about PDU session events not bound to an Individual Application Session Context. |

## 5.5.2 Event Notification

### 5.5.2.1 Description

The Event Notification is used by the PCF to report one or several observed application session context events to the NF service consumer that has subscribed to such notifications via the Events Subscription sub-resource.

### 5.5.2.2 Target URI

The Callback URI **"{notifUri}/notify"** shall be used with the callback URI variables defined in table 5.5.2.2-1.

**Table 5.5.2.2-1: Callback URI variables**

| Name | Data type | Definition |
|---|---|---|
| notifUri | Uri | The Notification Uri as assigned within the Events Subscription sub-resource and described within the EventsSubscReqData type (see table 5.6.2.6-1). |

### 5.5.2.3 Standard Methods

#### 5.5.2.3.1 POST

This method shall support the URI query parameters specified in table 5.5.2.3.1-1.

**Table 5.5.2.3.1-1: URI query parameters supported by the POST method on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| n/a | | | | |

This method shall support the request data structures specified in table 5.5.2.3.1-2 and the response data structures and response codes specified in table 5.5.2.3.1-3.

**Table 5.5.2.3.1-2: Data structures supported by the POST Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| EventsNotification | M | 1 | Provides Information about observed events. |

**Table 5.5.2.3.1-3: Data structures supported by the POST Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| n/a | | | 204 No Content | The receipt of the Notification is acknowledged. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during event notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent.<br>Applicable if the feature "ES3XX" is supported. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during event notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent.<br>Applicable if the feature "ES3XX" is supported. |
| NOTE: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the POST method shall also apply. | | | | |

**Table 5.5.2.3.1-4: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the notification request is redirected |

**Table 5.5.2.3.1-5: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the notification request is redirected |

## 5.5.3 Termination Request

### 5.5.3.1 Description

The Termination Request is used by the PCF to request the NF service consumer the deletion of the Individual Application Session Context resource.

### 5.5.3.2 Target URI

The Callback URI **"{notifUri}/terminate"** shall be used with the callback URI variables defined in table 5.5.3.2-1.

**Table 5.5.3.2-1: Callback URI variables**

| Name | Data type | Definition |
|---|---|---|
| notifUri | Uri | The Notification Uri as assigned within the Individual Application Session Context resource and described within the AppSessionContextReqData Data type (see table 5.6.2.3-1). |

## 5.5.3.3 Standard Methods

### 5.5.3.3.1 POST

This method shall support the URI query parameters specified in table 5.5.3.3.1-1.

**Table 5.5.3.3.1-1: URI query parameters supported by the POST method on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| n/a | | | | |

This method shall support the request data structures specified in table 5.5.3.3.1-2 and the response data structures and response codes specified in table 5.5.3.3.1-3.

**Table 5.5.3.3.1-2: Data structures supported by the POST Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| TerminationInfo | M | 1 | Provides information about the deletion of the resource. |

**Table 5.5.3.3.1-3: Data structures supported by the POST Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| n/a | | | 204 No Content | The receipt of the Notification is acknowledged. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during event notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent.<br>Applicable if the feature "ES3XX" is supported. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during event notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent.<br>Applicable if the feature "ES3XX" is supported. |
| NOTE: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the POST method shall also apply. | | | | |

**Table 5.5.3.3.1-4: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the notification request is redirected |

**Table 5.5.3.3.1-5: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the notification request is redirected |

## 5.5.4 Detected 5GS Bridge for a PDU session

### 5.5.4.1 Description

The detected TSC user plane node for a PDU session operation is used by the PCF to notify the NF service consumer about the detection of TSC user plane node information in the context of a PDU session and to trigger in the NF service consumer (i.e. TSN AF or TSCTSF) the creation of a new Individual Application Session Context to associate it with the detected TSC user plane node for the PDU session.

The PCF shall use the locally configured notification URI of the NF service consumer (i.e. TSN AF or TSCTSF) or the notification URI of the NF service consumer (i.e. TSCTSF) discovered via Nnrf_NFDiscovery service as defined in 3GPP TS 29.510 [27], if not configured, as request URI of the notification request. The "callback" definition in the OpenAPI specification is associated to the "ApplicationSessions" resource.

### 5.5.4.2 Target URI

The Callback URI **"{notifUri}/new-bridge"** shall be used with the callback URI variables defined in table 5.5.4.2-1.

**Table 5.5.4.2-1: Callback URI variables**

| Name | Data type | Definition |
|---|---|---|
| notifUri | Uri | It is locally configured in the PCF or discovered via Nnrf_NFDiscovery service. |

### 5.5.4.3 Standard Methods

#### 5.5.4.3.1 POST

This method shall support the URI query parameters specified in table 5.5.4.3.1-1.

**Table 5.5.4.3.1-1: URI query parameters supported by the POST method on this resource**

| Name | | Data type | P | Cardinality | Description |
|---|---|---|---|---|---|
| n/a | | | | | |

This method shall support the request data structures specified in table 5.5.4.3.1-2 and the response data structures and response codes specified in table 5.5.4.3.1-3.

**Table 5.5.4.3.1-2: Data structures supported by the POST Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| PduSessionTsnBridge | M | 1 | Provides information about the UP node of the reported PDU session. |

**Table 5.5.4.3.1-3: Data structures supported by the POST Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| n/a | | | 204 No Content | The receipt of the notification is acknowledged. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during PDU session TSC user plane nodenotification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent.<br>Applicable if the feature "ES3XX" is supported. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during PDU session TSC user plane node notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent.<br>Applicable if the feature "ES3XX" is supported. |
| NOTE: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the POST method shall also apply. | | | | |

**Table 5.5.4.3.1-4: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the notification request is redirected |

**Table 5.5.4.3.1-5: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the notification request is redirected |

## 5.5.5 Notification about PDU session event

### 5.5.5.1 Description

The Notification about PDU session events not bound to an Individual Application Session Context (eventNotificationPduSession) is used by the PCF to notify the NF service consumer (e.g., the PCF for a UE) about the PDU session events.

The PCF shall use the NF service consumer (e.g. PCF for a UE) callback URI implicitly subscribed (e.g. contained in the SM Policy Association of the related PDU session) as request URI of the notification request, and append the "pdu-session" segment path at the end of the URI. The "callback" definition in the OpenAPI specification is associated to the "ApplicationSessions" resource.

### 5.5.5.2 Target URI

The Callback URI **"{notifUri}/pdu-session"** shall be used with the callback URI variables defined in table 5.5.5.2-1.

**Table 5.5.5.2-1: Callback URI variables**

| Name | Data type | Definition |
|---|---|---|
| notifUri | Uri | It is the PCF for a UE callback URI stored in the SM Policy Association. |

## 5.5.5.3 Standard Methods

### 5.5.5.3.1 POST

This method shall support the URI query parameters specified in table 5.5.5.3.1-1.

**Table 5.5.5.3.1-1: URI query parameters supported by the POST method on this resource**

| Name | | Data type | P | Cardinality | Description |
|---|---|---|---|---|---|
| n/a | | | | | |

This method shall support the request data structures specified in table 5.5.5.3.1-2 and the response data structures and response codes specified in table 5.5.5.3.1-3.

**Table 5.5.5.3.1-2: Data structures supported by the POST Request Body on this resource**

| Data type | P | Cardinality | Description |
|---|---|---|---|
| PduSessionEventNotification | M | 1 | Provides information about the PDU session related event implicitly subscribed. |

**Table 5.5.5.3.1-3: Data structures supported by the POST Response Body on this resource**

| Data type | P | Cardinality | Response codes | Description |
|---|---|---|---|---|
| n/a | | | 204 No Content | The receipt of the Notification is acknowledged. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection, during PDU session established/terminated notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent. |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection, during PDU session established/terminated notification. The response shall include a Location header field containing an alternative URI representing the end point of an alternative NF consumer (service) instance where the notification should be sent. |
| NOTE: In addition, the HTTP status codes which are specified as mandatory in table 5.2.7.1-1 of 3GPP TS 29.500 [5] for the POST method shall also apply. | | | | |

**Table 5.5.5.3.1-4: Headers supported by the 307 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the notification request is redirected |

**Table 5.5.5.3.1-5: Headers supported by the 308 Response Code on this resource**

| Name | Data type | P | Cardinality | Description |
|---|---|---|---|---|
| Location | string | M | 1 | An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification should be redirected. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance towards which the notification request is redirected |

# 5.6 Data Model

## 5.6.1 General

This clause specifies the application data model supported by the API.

Table 5.6.1-1 specifies the data types defined for the Npcf_PolicyAuthorization service based interface protocol.

**Table 5.6.1-1: Npcf_PolicyAuthorization specific Data Types**

| Data type | Section defined | Description | Applicability |
|---|---|---|---|
| AcceptableServiceInfo | 5.6.2.30 | Acceptable maximum requested bandwidth. | |
| AccessNetChargingIdentifier | 5.6.2.32 | Contains the access network charging identifier. | IMS_SBI |
| AfAppId | 5.6.3.2 | Contains an AF application identifier. | |
| AfEvent | 5.6.3.7 | Represents an event to notify to the NF service consumer. | |
| AfEventNotification | 5.6.2.11 | Represents the notification of an event. | |
| AfEventSubscription | 5.6.2.10 | Represents the subscription to events. | |
| AfNotifMethod | 5.6.3.8 | Represents the notification methods that can be subscribed for an event. | |
| AfRequestedData | 5.6.3.18 | Represents the information the NF service consumer requested to be exposed. | IMS_SBI |
| AfRoutingRequirement | 5.6.2.13 | Describes the routing requirements for the application traffic flows. | InfluenceOnTrafficRouting |
| AfRoutingRequirementRm | 5.6.2.24 | This data type is defined in the same way as the "AfRoutingRequirement" data type, but with the OpenAPI "nullable: true" property. | InfluenceOnTrafficRouting |
| AlternativeServiceRequirementsData | 5.6.2.47 | Contains alternative QoS related parameter sets. | AltSerReqsWithIndQoS |
| AnGwAddress | 5.6.2.20 | Carries the control plane address of the access network gateway. | |
| AppDetectionReport | 5.6.2.44 | Indicates the start or stop of the detected application traffic and the detected AF application identifier. | ApplicationDetectionEvents |
| AppDetectionNotifType | 5.6.3.23 | Represents the types of reports bound to the notification of application detection information. | ApplicationDetectionEvents |
| AppSessionContext | 5.6.2.2 | Represents an Individual Application Session Context resource. | |
| AppSessionContextReqData | 5.6.2.3 | Represents the Individual Application Session Context resource data received in an HTTP POST request message. | |
| AppSessionContextRespData | 5.6.2.4 | Represents the Individual Application Session Context resource data produced by the server and returned in an HTTP response message. | |
| AppSessionContextUpdateData | 5.6.2.5 | Describes the modifications to the "ascReqData" property of an Individual Application Session Context resource. | |
| AppSessionContextUpdateDataPatch | 5.6.2.43 | Describes the modifications to an Individual Application Session Context resource | PatchCorrection |
| AspId | 5.6.3.2 | Contains an identity of an application service provider. | SponsoredConnectivity |
| CodecData | 5.6.3.2 | Contains a codec related information. | |
| ContentVersion | 5.6.3.2 | Represents the version of a media component. | MediaComponentVersioning |
| EthFlowDescription | 5.6.2.17 | Defines a packet filter for an Ethernet flow. | |
| EventsNotification | 5.6.2.9 | Describes the notification about the events occurred within an Individual Application Session Context resource. | |
| EventsSubscPutData | 5.6.2.42 | Identifies the events the application subscribes to within an Events Subscription sub-resource data. It may also include the attributes of the notification about the events already met at the time of subscription.<br>It is represented as a non-exclusive list of two data types: EventsSubscReqData and EventsNotification. | |
| EventsSubscReqData | 5.6.2.6 | Identifies the events the application subscribes to within an Individual Application Session Context resource. | |
| EventsSubscReqDataRm | 5.6.2. 25 | This data type is defined in the same way as the "EventsSubscReqData" data type, but with the OpenAPI "nullable: true" property. | |

| Data type | Section defined | Description | Applicability |
|---|---|---|---|
| ExtendedProblemDetails | 5.6.2.29 | Data type that extends ProblemDetails. | |
| FlowDescription | 5.6.3.2 | Defines a packet filter for an IP flow. | |
| Flows | 5.6.2.21 | Identifies the flows related to a media component. | |
| FlowStatus | 5.6.3.12 | Describes whether the IP flow(s) are enabled or disabled. | |
| FlowUsage | 5.6.3.14 | Describes the flow usage of the flows described by a media subcomponent. | |
| MediaComponent | 5.6.2.7 | Contains service information for a media component of an AF session. | |
| MediaComponentRm | 5.6.2.26 | This data type is defined in the same way as the "MediaComponent" data type, but with the OpenAPI "nullable: true" property. | |
| MediaComponentResourcesStatus | 5.6.3.13 | Indicates whether the media component is active or inactive. | |
| MediaSubComponent | 5.6.2.8 | Contains the requested bitrate and filters for the set of IP flows identified by their common flow identifier. | |
| MediaSubComponentRm | 5.6.2.27 | This data type is defined in the same way as the "MediaSubComponent" data type, but with the OpenAPI "nullable: true" property. | |
| MediaType | 5.6.3.3 | Indicates the media type of a media component. | |
| MpsAction | 5.6.3.22 | Indicates whethe it is an invocation, a revocation or an invocation with authorization of the MPS for DTS service. | MPSforDTS |
| OutOfCreditInformation | 5.6.2.33 | Indicates the service data flows without available credit and the corresponding termination action. | IMS_SBI |
| PcfAddressingInfo | 5.6.2.46 | Contains PCF address information. | |
| PcscfRestorationRequestData | 5.6.2.36 | Indicates P-CSCF restoration. | PCSCF-Restoration-Enhancement |
| PduSessionEventNotification | 5.6.2.45 | Indicates PDU session information for the established/terminated PDU session. | |
| PduSessionStatus | 5.6.3.24 | Indicates whether the PDU session is established or terminated. | |
| PduSessionTsnBridge | 5.6.2.40 | Contains the TSC user plane node Information and DS-TT port and/or NW-TT ports management information of a new detected TSC user plane node in the context of a new PDU session. | TimeSensitiveNetworking |
| PreemptionControlInformation | 5.6.3.19 | Pre-emption control information. | MCPTT-Preemption |
| PreemptionControlInformationRm | 5.6.3.21 | This data type is defined in the same way as the "PreemptionControlInformation" data type, but with the OpenAPI "nullable: true" property. | MCPTT-Preemption |
| PrioritySharingIndicator | 5.6.3.20 | Priority sharing indicator. | PrioritySharing |
| QosMonitoringInformation | 5.6.2.34 | QoS monitoring for UL, DL or round trip delay. | QoSMonitoring |
| QosMonitoringInformationRm | 5.6.2.41 | This data type is defined in the same way as the "QosMonitoringInformation" data type, but with the OpenAPI "nullable: true" property. | QoSMonitoring |
| QosMonitoringReport | 5.6.2.37 | Contains QoS monitoring reporting information. | QoSMonitoring |
| QosNotificationControlInfo | 5.6.2.15 | Indicates whether the QoS targets related to certain media component are not guaranteed or are guaranteed again. | |
| QosNotifType | 5.6.3.9 | Indicates type of notification for QoS Notification Control. | |
| RequiredAccessInfo | 5.6.3.15 | Indicates the access network information required for an AF session. | NetLoc |
| ReservPriority | 5.6.3.4 | Indicates the reservation priority. | |
| ResourcesAllocationInfo | 5.6.2.14 | Indicates the status of the PCC rule(s) related to certain media component. | |

| Data type | Section defined | Description | Applicability |
|---|---|---|---|
| ServAuthInfo | 5.6.3.5 | Indicates the result of the Policy Authorization service request from the NF service consumer. | |
| ServiceInfoStatus | 5.6.3.16 | Preliminary or final service information status. | IMS_SBI |
| ServiceUrn | 5.6.3.2 | Service URN. | IMS_SBI |
| SipForkingIndication | 5.6.3.17 | Describes if several SIP dialogues are related to an "Individual Application Session Context" resource. | IMS_SBI |
| SpatialValidity | 5.6.2.16 | Describes the spatial validity of an NF service consumer request for influencing traffic routing. | InfluenceOnTrafficRouting |
| SpatialValidityRm | 5.6.2.28 | This data type is defined in the same way as the "SpatialValidity" data type, but with the OpenAPI "nullable: true" property. | InfluenceOnTrafficRouting |
| SponId | 5.6.3.2 | Contains an Identity of a sponsor. | SponsoredConnectivity |
| SponsoringStatus | 5.6.3.6 | Represents whether sponsored data connectivity is enabled or disabled/not enabled. | SponsoredConnectivity |
| TemporalValidity | 5.6.2.22 | Indicates the time interval during which the NF service consumer request is to be applied. | InfluenceOnTrafficRouting |
| TerminationCause | 5.6.3.10 | Indicates the cause for requesting the deletion of the Individual Application Session Context resource. | |
| TerminationInfo | 5.6.2.12 | Includes information related to the termination of the Individual Application Session Context resource. | |
| TosTrafficClass | 5.6.3.2 | Contains the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the ToS/Traffic Class mask field. | |
| TosTrafficClassRm | 5.6.3.2 | This data type is defined in the same way as the "TosTrafficClass" data type, but with the OpenAPI "nullable: true" property. | |
| TscPriorityLevel | 5.6.3.2 | Priority of TSC Flows | TimeSensitiveNetworking |
| TscPriorityLevelRm | 5.6.3.2 | This data type is defined in the same way as the "TscPriorityLevel" data type, but with the OpenAPI "nullable: true" property | TimeSensitiveNetworking |
| TscaiInputContainer | 5.6.2.39 | TSCAI Input information container. | TimeSensitiveNetworking |
| TsnQosContainer | 5.6.2.35 | TSC traffic QoS parameters. | TimeSensitiveNetworking |
| TsnQosContainerRm | 5.6.2.38 | This data type is defined in the same way as the "TsnQosContainer" data type, but with the OpenAPI "nullable: true" property. | TimeSensitiveNetworking |
| UeIdentityInfo | 5.6.2.31 | Represents 5GS-Level UE Identities. | IMS_SBI |

Table 5.6.1-2 specifies data types re-used by the Npcf_PolicyAuthorization service based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Npcf_PolicyAuthorization service based interface.

**Table 5.6.1-2: Npcf_PolicyAuthorization re-used Data Types**

| Data type | Reference | Comments | Applicability |
|---|---|---|---|
| AccNetChargingAddress | 3GPP TS 29.512 [8] | Indicates the IP address of the network entity within the access network performing charging. | IMS_SBI |
| AccessType | 3GPP TS 29.571 [12] | The identification of the type of access network. | |
| AccumulatedUsage | 3GPP TS 29.122 [15] | Accumulated Usage. | SponsoredConnectivity |
| AdditionalAccessInfo | 3GPP TS 29.512 [8] | Indicates the combination of additional Access Type and RAT Type for MA PDU session | ATSSS |
| AfSigProtocol | 3GPP TS 29.512 [8] | Represents the protocol used for signalling between the UE and the NF service consumer. | ProvAFsignalFlow |
| ApplicationChargingId | 3GPP TS 29.571 [12] | Application provided charging identifier allowing correlation of charging information. | IMS_SBI |
| BdtReferenceId | 3GPP TS 29.122 [15] | Identifies transfer policies. | |
| BitRate | 3GPP TS 29.571 [12] | Specifies bitrate in kbits per second. | |
| BitRateRm | 3GPP TS 29.571 [12] | This data type is defined in the same way as the "BitRate" data type, but with the OpenAPI "nullable: true" property. | |
| BridgeManagementContainer | 3GPP TS 29.512 [8] | Contains TSC user plane node management information. | TimeSensitiveNetworking |
| Bytes | 3GPP TS 29.571 [12] | String with format "byte". | |
| ChargingId | 3GPP TS 29.571 [12] | Charging identifier allowing correlation of charging information. | IMS_SBI |
| DateTime | 3GPP TS 29.571 [12] | String with format "date-time" as defined in OpenAPI Specification [11]. | InfluenceOnTrafficRouting, TimeSensitiveNetworking |
| Dnn | 3GPP TS 29.571 [12] | Data Network Name. | |
| DurationSec | 3GPP TS 29.571 [12] | Identifies a period of time in units of seconds. | TimeSensitiveNetworking, EnhancedSubscriptionToNotification, SimultConnectivity |
| DurationSecRm | 3GPP TS 29.571 [12] | This data type is defined in the same way as the "DurationSec" data type, but with the OpenAPI "nullable: true" property. | SimultConnectivity |
| EasIpReplacementInfo | 3GPP TS 29.571 [12] | Contains EAS IP replacement information for a Source and a Target EAS. | EASIPreplacement |
| FinalUnitAction | 3GPP TS 32.291 [22] | Indicates the action to be taken when the user's account cannot cover the service cost. | |
| Float | 3GPP TS 29.571 [12] | Number with format "float" as defined in OpenAPI Specification [11]. | FLUS |
| FloatRm | 3GPP TS 29.571 [12] | This data type is defined in the same way as the "Float" data type, but with the OpenAPI "nullable: true" property. | FLUS |
| FlowDirection | 3GPP TS 29.512 [8] | Flow Direction. | |
| Fqdn | 3GPP TS 29.571 [12] | Contains a FQDN | |
| ExtMaxDataBurstVol | 3GPP TS 29.571 [12] | Maximum Burst Size. | TimeSensitiveNetworking |
| ExtMaxDataBurstVolRm | 3GPP TS 29.571 [12] | This data type is defined in the same way as the "ExtMaxDataBurstVol" data type, but with the OpenAPI "nullable: true" property | TimeSensitiveNetworking |
| Gpsi | 3GPP TS 29.571 [12] | Identifies the GPSI. | |
| Ipv4Addr | 3GPP TS 29.571 [12] | Identifies an IPv4 address. | |
| Ipv6Addr | 3GPP TS 29.571 [12] | Identifies an IPv6 address. | |
| IpEndPoint | 3GPP TS 29.510 [27] | Contains a NF IPv4 and/or IPv6 end points. | |
| MacAddr48 | 3GPP TS 29.571 [12] | MAC Address. | |

| Data type | Reference | Comments | Applicability |
|---|---|---|---|
| NetLocAccessSupport | 3GPP TS 29.512 [8] | Indicates the access network does not support the report of the requested access network information. | NetLoc |
| NullValue | 3GPP TS 29.571 [12] | JSON's null value, used as an explicit value of an enumeration. | MCPTT-Preemption |
| PacketDelBudget | 3GPP TS 29.571 [12] | Packet Delay Budget. | TimeSensitiveNetworking |
| PacketDelBudgetRm | 3GPP TS 29.571 [12] | This data type is defined in the same way as the "PacketDelBudget" data type, but with the OpenAPI "nullable: true" property | TimeSensitiveNetworking |
| PacketLossRateRm | 3GPP TS 29.571 [12] | This data type is defined in the same way as the "PacketLossRate" data type, but with the OpenAPI "nullable: true" property. | CHEM |
| Pei | 3GPP TS 29.571 [12] | Identifies the PEI. | IMS_SBI |
| PlmnIdNid | 3GPP TS 29.571 [12] | Identifies the network: the PLMN Identifier (the mobile country code and the mobile network code) or the SNPN Identifier (the PLMN Identifier and the NID). | |
| PreemptionCapability | 3GPP TS 29.571 [12] | Pre-emption capability. | MCPTT-Preemption |
| PreemptionVulnerability | 3GPP TS 29.571 [12] | Pre-emption vulnerability. | MCPTT-Preemption |
| PreemptionCapabilityRm | 3GPP TS 29.571 [12] | It is defined in the same way as the "PreemptionCapability" data type, but with the OpenAPI "nullable: true" property. | MCPTT-Preemption |
| PreemptionVulnerabilityRm | 3GPP TS 29.571 [12] | It is defined in the same way as the "PreemptionVulnerability" data type, but with the OpenAPI "nullable: true" property. | MCPTT-Preemption |
| PresenceInfo | 3GPP TS 29.571 [12] | Represents an area of interest, e.g. a Presence Reporting Area. | InfluenceOnTrafficRouting |
| PortManagementContainer | 3GPP TS 29.512 [8] | Contains port management information for a related port. | TimeSensitiveNetworking |
| ProblemDetails | 3GPP TS 29.571 [12] | Contains a detailed information about an error. | |
| RanNasRelCause | 3GPP TS 29.512 [8] | Indicates RAN and/or NAS release cause code information. | RAN-NAS-Cause |
| RedirectResponse | 3GPP TS 29.571 [12] | Contains redirection related information. | ES3XX |
| RequestedQosMonitoringParameter | 3GPP TS 29.512 [8] | Indicate the UL packet delay, DL packet delay or round trip packet delay between the UE and the UPF is to be monitored when the QoS Monitoring for URLLC is enabled for the service data flow. | QoSMonitoring |
| RatType | 3GPP TS 29.571 [12] | RAT Type. | |
| RouteToLocation | 3GPP TS 29.571 [12] | Identifies routes to locations of applications. | InfluenceOnTrafficRouting |
| SatelliteBackhaulCategory | 3GPP TS 29.571 [12] | Indicates the satellite or non-satellite backhaul category | SatelliteBackhaul |
| Snssai | 3GPP TS 29.571 [12] | Identifies the S-NSSAI. | |
| Supi | 3GPP TS 29.571 [12] | Identifies the SUPI. | |
| SupportedFeatures | 3GPP TS 29.571 [12] | Used to negotiate the applicability of the optional features defined in table 5.8-1. | |
| TimeZone | 3GPP TS 29.571 [12] | Time Zone. | NetLoc |
| TsnBridgeInfo | 3GPP TS 29.512 [8] | TSC user plane node information. | TimeSensitiveNetworking |
| Uint32 | 3GPP TS 29.571 [12] | Unsigned 32-bit integers, i.e. only value 0 and 32-bit integers above 0 are permissible. | ResourceSharing |
| Uint32Rm | 3GPP TS 29.571 [12] | This data type is defined in the same way as the "Uint32" data type, but with the OpenAPI "nullable: true" property. | ResourceSharing |
| Uinteger | 3GPP TS 29.571 [12] | Unsigned Integer, i.e. only value 0 and integers above 0 are permissible. Minimum = 0. | TimeSensitiveNetworking |

| Data type | Reference | Comments | Applicability |
|---|---|---|---|
| UpPathChgEvent | 3GPP TS 29.512 [8] | Contains the subscription information to be delivered to SMF for the UP path management events. | InfluenceOnTrafficRouting |
| Uri | 3GPP TS 29.571 [12] | String providing an URI. | |
| UsageThreshold | 3GPP TS 29.122 [15] | Usage Thresholds. | SponsoredConnectivity |
| UsageThresholdRm | 3GPP TS 29.122 [15] | This data type is defined in the same way as the "UsageThreshold" data type, but with the OpenAPI "nullable: true" property. | SponsoredConnectivity |
| UserLocation | 3GPP TS 29.571 [12] | User Location(s). | NetLoc |

## 5.6.2 Structured data types

### 5.6.2.1 Introduction

This clause defines the structures to be used in resource representations.

### 5.6.2.2 Type AppSessionContext

**Table 5.6.2.2-1: Definition of type AppSessionContext**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| ascReqData | AppSessionContextReqData | C | 0..1 | Identifies the service requirements of an Individual Application Session Context. It shall be present in HTTP POST request messages for the creation of the resource and may be included in the HTTP response messages. | |
| ascRespData | AppSessionContextRespData | C | 0..1 | Describes the authorization data of an Individual Application Session Context created by the PCF. It may be present in the HTTP response messages. | |
| evsNotif | EventsNotification | O | 0..1 | Describes information related to the notification of events. | |

### 5.6.2.3 Type AppSessionContextReqData

**Table 5.6.2.3-1: Definition of type AppSessionContextReqData**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| afAppId | AfAppId | O | 0..1 | AF application identifier. | |
| afChargId | ApplicationChargingId | O | 0..1 | AF charging identifier. This information may be used for charging correlation with QoS flow. | IMS_SBI |
| afReqData | AfRequestedData | O | 0..1 | Represents the NF service consumer requested data to be exposed. | IMS_SBI |
| afRoutReq | AfRoutingRequirement | C | 0..1 | Indicates the AF traffic routing requirements. It shall be included if Influence on Traffic Routing feature is supported. | InfluenceOnTrafficRouting |
| aspId | AspId | C | 0..1 | Application service provider identity. It shall be included if "SponsoredConnectivity" feature is supported. | SponsoredConnectivity |
| bdtRefId | BdtReferenceId | O | 0..1 | Reference to a transfer policy negotiated for background data traffic. | |
| dnn | Dnn | C | 0..1 | Data Network Name, a full DNN with both the Network Identifier and Operator Identifier, or a DNN with the Network Identifier only. It shall be present when the "afRoutReq" attribute is present. | |
| evSubsc | EventsSubscReqData | O | 0..1 | Identifies the events the application subscribes to at creation of an Individual Application Session Context resource. | |
| ipDomain | string | O | 0..1 | Indicates the IPv4 address domain information that assists session binding. | |
| mcpttId | string | O | 0..1 | Indicates that the created Individual Application Session Context resource relates to an MCPTT session prioritized call.<br>It includes either one of the namespace values used for MCPTT (see IETF RFC 8101 [42]) and it may include the name of the MCPTT service provider. | MCPTT |
| mcVideoId | string | O | 0..1 | Indicates that the created Individual Application Session Context resource relates to an MCVideo session prioritized call.<br>It includes either one of the namespace values used for MCPTT (see IETF RFC 8101 [42]) and it may include the name of the MCVideo service provider. | MCVideo |
| medComponents | map(MediaComponent) | O | 1..N | Media Component information. The key of the map is the attribute "medCompN". | |
| mpsAction | MpsAction | O | 0..1 | Indicates a request to invoke an MPS action. | MPSforDTS |
| mpsId | string | O | 0..1 | Indicates that the created Individual Application Session Context resource relates to an MPS service. It contains the national variant for MPS service name. | |
| mcsId | string | O | 0..1 | Indicates that the created Individual Application Session Context resource relates to an MCS service. It contains the national variant for MCS service name. | |
| preemptControlInfo | PreemptionControlInformation | O | 0..1 | Pre-emption control information. | MCPTT-Preemption |
| resPrio | ReservPriority | O | 0..1 | Indicates the reservation priority. | |

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| servInfStatus | ServiceInfoStatus | O | 0..1 | Indicates whether the service information is preliminary or final. When the attribute is not provided the default value is "FINAL". | IMS_SBI |
| notifUri | Uri | M | 1 | Notification URI for Application Session Context termination requests. | |
| servUrn | ServiceUrn | O | 0..1 | Service URN. | IMS_SBI |
| sliceInfo | Snssai | O | 0..1 | Identifies the S-NSSAI. | |
| sponId | SponId | C | 0..1 | Sponsor identity. It shall be included if "SponsoredConnectivity" feature is supported. | SponsoredConnectivity |
| sponStatus | SponsoringStatus | O | 0..1 | Indication of whether sponsored connectivity is enabled or disabled/not enabled. The absence of the attribute indicates that the sponsored connectivity is enabled. | SponsoredConnectivity |
| supi | Supi | O | 0..1 | Subscription Permanent Identifier. | |
| gpsi | Gpsi | O | 0..1 | Generic Public Subscription Identifier. | |
| suppFeat | SupportedFeatures | M | 1 | This IE represents a list of Supported features used as described in clause 5.8. It shall be supplied by the NF service consumer in the POST request that requests a creation of an Individual Application Session Context resource. | |
| ueIpv4 | Ipv4Addr | C | 0..1 | The IPv4 address of the served UE. | |
| ueIpv6 | Ipv6Addr | C | 0..1 | The IPv6 address of the served UE. | |
| ueMac | MacAddr48 | C | 0..1 | The MAC address of the served UE. When the feature "TimeSensitiveNetworking" is supported this attribute represents the DS-TT port MAC address. | |
| tsnBridgeManCont | BridgeManagementContainer | O | 0..1 | Transports TSC user plane node management information. | TimeSensitiveNetworking |
| tsnPortManContDstt | PortManagementContainer | O | 0..1 | Transports port management information for the DS-TT port. | TimeSensitiveNetworking |
| tsnPortManContNwtts | array(PortManagementContainer) | O | 1..N | Transports port management information for one or more NW-TT ports. | TimeSensitiveNetworking |
| NOTE: Only one of the served UE addressing parameters (the IPv4 address or the IPv6 address or MAC address) shall always be included. | | | | | |

### 5.6.2.4 Type AppSessionContextRespData

**Table 5.6.2.4-1: Definition of type AppSessionContextRespData**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| servAuthInfo | ServAuthInfo | O | 0..1 | Indicates additional information related with the result of the authorization for a service request. | |
| ueIds | array(UeIdentityInfo) | O | 1..N | Represents the 5GS-Level UE identities available for an AF session context. | IMS_SBI |
| suppFeat | SupportedFeatures | C | 0..1 | This IE represents a list of Supported features used as described in clause 5.8. It shall be supplied by the PCF in the response to the POST request that requested a creation of an Individual Application Session Context resource. | |

### 5.6.2.5 Type AppSessionContextUpdateData

**Table 5.6.2.5-1: Definition of type AppSessionContextUpdateData**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| afAppId | AfAppId | O | 0..1 | AF application identifier. | |
| afRoutReq | AfRoutingRequirementRm | O | 0..1 | Indicates the AF traffic routing requirements. | InfluenceOnTrafficRouting |
| aspId | AspId | O | 0..1 | Application service provider identity. | SponsoredConnectivity |
| bdtRefId | BdtReferenceId | O | 0..1 | Reference to a transfer policy negotiated for background data traffic. | |
| evSubsc | EventsSubscReqDataRm | O | 0..1 | Identifies the events the application subscribes to at modification of an Individual Application Session Context resource. | |
| mcpttId | string | O | 0..1 | Indicates that the updated Individual Application Session Context resource relates to an MCPTT session prioritized call.<br>It includes either one of the namespace values used for MCPTT (see IETF RFC 8101 [42]) and it may include the name of the MCPTT service provider. | MCPTT |
| mcVideoId | string | O | 0..1 | Indicates that the updated Individual Application Session Context resource relates to an MCVideo session prioritized call.<br>It includes either one of the namespace values used for MCPTT (see IETF RFC 8101 [42]) and it may include the name of the MCVideo service provider. | MCVideo |
| medComponents | map(MediaComponentRm) | O | 1..N | Media Component information.<br>The key of the map is the "medCompN" attribute. | |
| mpsAction | MpsAction | O | 0..1 | Indicates a request to invoke or revoke MPS for DTS. | MPSforDTS |
| mpsId | string | O | 0..1 | Indicates that the modified Individual Application Session Context resource relates to an MPS service. It contains the national variant for MPS service name. | |
| mcsId | string | O | 0..1 | Indicates that the updated Individual Application Session Context resource relates to an MCS service. It contains the national variant for MCS service name. | |
| preemptControlInfo | PreemptionControlInformationRm | O | 0..1 | Preemption control information. | MCPTT-Preemption |
| resPrio | ReservPriority | O | 0..1 | Indicates the reservation priority. | |
| servInfStatus | ServiceInfoStatus | O | 0..1 | Indicates whether the service information is preliminary or final. | IMS_SBI |
| sipForkInd | SipForkingIndication | O | 0..1 | Describes if several SIP dialogues are related to an "Individual Application Session Context" resource. | IMS_SBI |
| sponId | SponId | O | 0..1 | Sponsor identity. | SponsoredConnectivity |
| sponStatus | SponsoringStatus | O | 0..1 | Indication of whether sponsored connectivity is enabled or disabled/not enabled. | SponsoredConnectivity |
| tsnBridgeManCont | BridgeManagementContainer | O | 0..1 | Transports TSC user plane node management information. | TimeSensitive Networking |
| tsnPortManContDstt | PortManagementContainer | O | 0..1 | Transports port management information for the DS-TT port. | TimeSensitive Networking |
| tsnPortManContNwtts | array(PortManagementContainer) | O | 1..N | Transports port management information for one or more NW-TT ports. | TimeSensitive Networking |

### 5.6.2.6 Type EventsSubscReqData

**Table 5.6.2.6-1: Definition of type EventsSubscReqData**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| events | array(AfEventSubscription) | M | 1..N | Subscribed Events. | |
| notifUri | Uri | O | 0..1 | Notification URI. | |
| reqQosMonParams | array(RequestedQosMonitoringParameter) | O | 1..N | Indicates the UL packet delay, DL packet delay and/or round trip packet delay between the UE and the UPF is to be monitored when the QoS Monitoring for URLLC is enabled for the service data flow. | QoSMonitoring |
| qosMon | QosMonitoringInformation | O | 0..1 | Qos Monitoring information. It can be present when the event "QOS_MONITORING" is subscribed. | QoSMonitoring |
| reqAnis | array(RequiredAccessInfo) | C | 1..N | Represents the required access network information. It shall be present when the event "ANI_REPORT" is subscribed. | NetLoc |
| usgThres | UsageThreshold | O | 0..1 | Includes the volume and/or time thresholds for sponsored data connectivity. | SponsoredConnectivity |
| notifCorreId | string | O | 0..1 | It is used to set the value of Notification Correlation ID in the corresponding notification. | EnhancedSubscriptionToNotification |
| afAppIds | array(AfAppId) | O | 1..N | AF application identifier(s). It shall be present when the event "APP_DETECTION" is subscribed. | ApplicationDetectionEvents |
| directNotifInd | boolean | O | 0..1 | Indicates that the event notification of QoS Monitoring data is sent by the UPF to Local NEF or AF if it is included and set to true. It may be present when the event "QOS_MONITORING" is subscribed.<br>The default value "false" shall apply, if the attribute is not present. | ExposureToEAS |

### 5.6.2.7 Type MediaComponent

**Table 5.6.2.7-1: Definition of type MediaComponent**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| afAppId | AfAppId | O | 0..1 | Contains information that identifies the particular service the AF session belongs to. | |
| afRoutReq | AfRoutingRequirement | O | 0..1 | Indicates the AF traffic routing requirements. | InfluenceOnTrafficRouting |
| qosReference | string | O | 0..1 | Identifies a pre-defined QoS information. | AuthorizationWithRequiredQoS |
| altSerReqs | array(string) | O | 1..N | Ordered list of alternative service requirements that include a set of QoS references. The lower the index of the array for a given entry, the higher the priority.(NOTE) | AuthorizationWithRequiredQoS |
| altSerReqsData | array(AlternativeServiceRequirementsData) | O | 1..N | Ordered list of alternative service requirements that include individual QoS parameter sets. The lower the index of the array for a given entry, the higher the priority. (NOTE) | AltSerReqsWithIndQoS |
| disUeNotif | boolean | O | 0..1 | Indicates to disable QoS flow parameters signalling to the UE when the SMF is notified by the NG-RAN of changes in the fulfilled QoS situation when it is included and set to "true". The fulfilled situation is either the QoS profile or an Alternative QoS Profile. The default value "false" shall apply, if the attribute is not present and has not been supplied previously. | DisableUENotification |
| contVer | ContentVersion | O | 0..1 | Represents the content version of a media component. | MediaComponentVersioning |
| desMaxLatency | Float | O | 0..1 | Indicates a maximum desirable transport level packet latency in milliseconds. | FLUS, QoSHint |
| desMaxLoss | Float | O | 0..1 | Indicates the maximum desirable transport level packet loss rate in percent (without "%" sign). | FLUS, QoSHint |
| flusId | string | O | 0..1 | Indicates that the media component is used for FLUS media.<br>It is derived from the media level attribute "a=label:" (see IETF RFC 4574 [50]) obtained from the SDP body. It contains the string after "a=label:" starting with "flus" and may be followed by more characters as described in 3GPP TS 26.238 [51]. | FLUS |
| medCompN | integer | M | 1 | Identifies the media component number, and it contains the ordinal number of the media component. | |
| medSubComps | map(MediaSubComponent) | O | 1..N | Contains the requested bitrate and filters for the set of service data flows identified by their common flow identifier. The key of the map is the attribute "fNum". | |
| medType | MediaType | O | 0..1 | Indicates the media type of the service. | |
| marBwUl | BitRate | O | 0..1 | Maximum requested bandwidth for the Uplink. | |
| marBwDl | BitRate | O | 0..1 | Maximum requested bandwidth for the Downlink. | |
| maxPacketLossRateDl | PacketLossRateRm | O | 0..1 | Indicates the downlink maximum rate for lost packets that can be tolerated for the service data flow. | CHEM |
| maxPacketLossRateUl | PacketLossRateRm | O | 0..1 | Indicates the uplink maximum rate for lost packets that can be tolerated for the service data flow. | CHEM |
| maxSuppBwDl | BitRate | O | 0..1 | Maximum supported bandwidth for the Downlink. | IMS_SBI |

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| maxSuppBwUl | BitRate | O | 0..1 | Maximum supported bandwidth for the Uplink. | IMS_SBI |
| minDesBwDl | BitRate | O | 0..1 | Minimum desired bandwidth for the Downlink. | IMS_SBI |
| minDesBwUl | BitRate | O | 0..1 | Minimum desired bandwidth for the Uplink. | IMS_SBI |
| mirBwUl | BitRate | O | 0..1 | Minimum requested bandwidth for the Uplink. | |
| mirBwDl | BitRate | O | 0..1 | Minimum requested bandwidth for the Downlink. | |
| fStatus | FlowStatus | O | 0..1 | Indicates whether the status of the service data flows is enabled, or disabled. | |
| preemptCap | PreemptionCapability | O | 0..1 | Defines whether the media flow may get resources that were already assigned to another media flow with a lower priority level. It may be included together with "prioSharingInd" for ARP decision. | MCPTT-Preemption |
| preemptVuln | PreemptionVulnerability | O | 0..1 | Defines whether the media flow may lose the resources assigned to it in order to admit a media flow with higher priority level. It may be included together with "prioSharingInd" for ARP decision. | MCPTT-Preemption |
| prioSharingInd | PrioritySharingIndicator | O | 0..1 | Indicates that the media flow is allowed to use the same ARP as media flows belonging to other "Individual Application Session Context" resources bound to the same PDU session. | PrioritySharing |
| resPrio | ReservPriority | O | 0..1 | Indicates the reservation priority. | |
| rrBw | BitRate | O | 0..1 | Indicates the maximum required bandwidth in bits per second for RTCP receiver reports within the session component as specified in IETF RFC 3556 [37]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP. | IMS_SBI |
| rsBw | BitRate | O | 0..1 | Indicates the maximum required bandwidth in bits per second for RTCP sender reports within the session component as specified in IETF RFC 3556 [37]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP. | IMS_SBI |
| sharingKeyDl | Uint32 | O | 0..1 | Identifies which media components share resources in the downlink direction. If resource sharing applies between media components across "Individual Application Session Context" resources for the same PDU session, the same value of the "sharingKeyDl" attribute shall be used. If resource sharing does not apply among media components across "Individual Application Session Context" resources for the same PDU session, a different value for the "sharingKeyDl" attribute shall be used. | ResourceSharing |

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| sharingKeyUl | Uint32 | O | 0..1 | Identifies which media components share resources in the uplink direction. If resource sharing applies between media components across "Individual Application Session Context" resources for the same PDU session, the same value of the "sharingKeyUl" attribute shall be used. If resource sharing does not apply among media components across "Individual Application Session Context" resources for the same PDU session, a different value for the "sharingKeyUl" attribute shall be used. | ResourceSharing |
| codecs | array(CodecData) | O | 1..2 | Indicates the codec data. | |
| tsnQos | TsnQoSContainer | O | 0..1 | Transports QoS parameters for TSC traffic. | TimeSensitiveNetworking |
| tscaiInputUl | TscaiInputContainer | O | 0..1 | Transports TSCAI input parameters for TSC traffic at the ingress interface of the DS-TT/UE (uplink flow direction). | TimeSensitiveNetworking |
| tscaiInputDl | TscaiInputContainer | O | 0..1 | Transports TSCAI input parameters for TSC traffic at the ingress of the NW-TT (downlink flow direction). | TimeSensitiveNetworking |
| tscaiTimeDom | Uinteger | O | 0..1 | Indicates the (g)PTP domain that the (TSN)AF is located in. | TimeSensitiveCommunication |
| NOTE: The attributes "altSerReqs" and "altSerReqsData" are mutually exclusive. Of the two, only the attribute "altSerReqs" may be provided if the attribute "qosReference" is provided, while only the attribute "altSerReqsData" may be provided if the attribute "qosReference" is not provided. | | | | | |

All IP flows within a "MediaSubComponent" data type are permanently disabled by supplying "FlowStatus" data type with a deletion indication.

Bandwidth information and the "fStatus" attribute provided within the MediaComponent applies to all those IP flows within the media component, for which no corresponding information is being provided within the "medSubComps" attribute. As defined in 3GPP TS 29.513 [7], the bandwidth information within the media component level "marBwUl" and "marBwDl" attributes applies separately to each media subcomponent except for media subcomponents with a "flowUsage" attribute with the value "RTCP". The mapping of bandwidth information for RTCP media subcomponent is defined in 3GPP TS 29.513 [7] clause 7.3.3.

### 5.6.2.8 Type MediaSubComponent

**Table 5.6.2.8-1: Definition of type MediaSubComponent**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| afSigProtocol | AfSigProtocol | O | 0..1 | Indicates the protocol used for signalling between the UE and the NF service consumer. It may be included only if the "flowUsage" attribute is set to the value "AF_SIGNALLING". | ProvAFsignalFlow |
| ethfDescs | array(EthFlowDescription) | O | 1..2 | Contains the flow description for the Uplink and/or Downlink Ethernet flows. | |
| fNum | integer | M | 1 | Identifies the ordinal number of the service data flow. | |
| fDescs | array(FlowDescription) | O | 1..2 | Contains the flow description for the Uplink and/or Downlink IP flows. | |
| fStatus | FlowStatus | O | 0..1 | Indicates whether the status of the service data flows is enabled or disabled. | |
| flowUsage | FlowUsage | O | 0..1 | Flow usage of the flows (e.g. RTCP, AF signalling). | |
| marBwUl | BitRate | O | 0..1 | Maximum requested bandwidth for the Uplink. | |
| marBwDl | BitRate | O | 0..1 | Maximum requested bandwidth for the Downlink. | |
| tosTrCl | TosTrafficClass | O | 0..1 | Type of Service or Traffic Class. | |

The bit rate information and flow status information provided within the "MediaSubComponent" data type takes precedence over information provided within "MediaComponent" data type.

All service data flows within a "MediaSubComponent" data type are permanently disabled by supplying "FlowStatus" data type with a deletion indication.

### 5.6.2.9 Type EventsNotification

**Table 5.6.2.9-1: Definition of type EventsNotification**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| adReports | array(AppDetection Report) | C | 0..1 | Includes the detected application report. It shall be present when the notified event is "APP_DETECTION". | ApplicationDet ectionEvents |
| accessType | AccessType | C | 0..1 | Includes the access type. It shall be present when the notified event is "ACCESS_TYPE_CHANGE". | |
| addAccessInfo | AdditionalAccessInf o | O | 0..1 | Indicates the additional combination of Access Type and RAT Type available for MA PDU session. It may be present when the notified event is "ACCESS_TYPE_CHANGE" and the PDU session is a Multi-Access PDU session. | ATSSS |
| relAccessInfo | AdditionalAccessInf o | O | 0..1 | Indicates the released combination of Access Type and RAT Type previously available for MA PDU session. It may be present when the notified event is "ACCESS_TYPE_CHANGE" and the PDU session is a Multi-Access PDU session. | ATSSS |
| anChargAddr | AccNetChargingAdd ress | O | 0..1 | Includes the access network charging address. It shall be present if available when the notified event is "CHARGING_CORRELATION". | IMS_SBI |
| anChargIds | array(AccessNetCh argingIdentifier) | C | 1..N | Includes the access network charging identifier(s). It shall be present when the notified event is "CHARGING_CORRELATION". | IMS_SBI |
| anGwAddr | AnGwAddress | O | 0..1 | Access network Gateway Address. It carries the IP address of the ePDG used as IPSec tunnel endpoint with the UE for EPC/ePDG and 5GS interworking. It shall be present, if applicable, when the notified event is "ACCESS_TYPE_CHANGE". | |
| evSubsUri | Uri | M | 1 | The Events Subscription URI. Identifies the Events Subscription sub-resource that triggered the notification. (NOTE 1) | |
| evNotifs | array(AfEventNotific ation) | M | 1..N | Notifications about individual events. | |
| failedResourcAllo cReports | array(ResourcesAllo cationInfo) | C | 1..N | Indicates the status of the PCC rule(s) related to certain failed media components. It shall be included when the event trigger is "FAILED_RESOURCES_ALLOCATION". | |
| succResourcAlloc Reports | array(ResourcesAllo cationInfo) | O | 1..N | Indicates the alternative service requirement the NG-RAN can guarantee to certain media components. It may be included when the event trigger is "SUCCESSFUL_RESOURCES_ALLOC ATION". | Authorization WithRequired QoS |
| noNetLocSupp | NetLocAccessSupp ort | O | 0..1 | Indicates the access network does not support the report of the requested access network information. | NetLoc |
| outOfCredReports | array(OutOfCreditInf ormation) | C | 1..N | Out of credit information per service data flow. It shall be present when the notified event is "OUT_OF_CREDIT". | IMS_SBI |

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| plmnId | PlmnIdNid | C | 0..1 | PLMN Identifier or the SNPN Identifier. It shall be present when the notified event is "PLMN_CHG" or, if location information is required but is not available when the notified event is "ANI_REPORT". It shall be present if available when the notified event is "RAN_NAS_CAUSE". (NOTE 2) | |
| qncReports | array(QosNotificationControlInfo) | C | 1..N | QoS notification control information. It shall be present when the notified event is "QOS_NOTIF". | |
| qosMonReports | array(QosMonitoringReport) | C | 1..N | QoS Monitoring reporting information. It shall be present when the notified event is "QOS_MONITORING". | QoSMonitoring |
| ranNasRelCauses | array(RanNasRelCause) | C | 1..N | RAN-NAS release cause. It shall be present if available when the notified event is "RAN_NAS_CAUSE". | RAN-NAS-Cause |
| ratType | RatType | O | 0..1 | RAT type. It shall be present, if applicable, when the notified event is "ACCESS_TYPE_CHANGE". | |
| satBackhaulCategory | SatelliteBackhaulCategory | C | 0..1 | Indicates the satellite or non-satellite backhaul category of the PDU session. It shall be present, if applicable, when the notified event is "SAT_CATEGORY_CHG". | SatelliteBackhaul |
| ueLoc | UserLocation | O | 0..1 | E-UTRA, or NR, and/or non-3GPP trusted and untrusted access user location information. "n3gppTai" and "n3IwfId" attributes within the "N3gaLocation" data type shall not be supplied. It shall be present if required and available when the notified event is "ANI_REPORT". It shall be present if available when the notified event is "RAN_NAS_CAUSE". (NOTE 3) (NOTE 4) | NetLoc, RAN-NAS-Cause |
| ueLocTime | DateTime | O | 0..1 | Contains the NTP time at which the UE was last known to be in the location. (NOTE 3) | NetLoc |
| ueTimeZone | TimeZone | O | 0..1 | UE time zone. It shall be present if required and available when the notified event is "ANI_REPORT". It shall be present if available when the notified event is "RAN_NAS_CAUSE". | NetLoc, RAN-NAS-Cause |
| usgRep | AccumulatedUsage | C | 0..1 | Indicates the measured volume and/or time for sponsored data connectivity. It shall be present when the notified event is "USAGE_REPORT". | SponsoredConnectivity |
| tsnBridgeManCont | BridgeManagementContainer | O | 0..1 | Transports TSC user plane node management information. | TimeSensitiveNetworking |
| tsnPortManContDstt | PortManagementContainer | O | 0..1 | Transports port management information for the DS-TT port. | TimeSensitiveNetworking |
| tsnPortManContNwtts | array(PortManagementContainer) | O | 1..N | Transports port management information for one or more NW-TT ports. | TimeSensitiveNetworking |

NOTE 1: Either the complete resource URI included in the "evSubsUri" attribute or the "apiSpecificResourceUriPart" component (see clause 5.1) of the resource URI included in the "evSubsUri" attribute may be used by the NF service consumer for the identification of the Individual Application Session Context resource related to the notification.
NOTE 2: The SNPN Identifier consists of the PLMN Identifier and the NID.
NOTE 3: Whether the "ueLoc" attribute also encodes the age of location is implementation specific.
NOTE 4: When the "ueLoc" attribute contains both, the 3GPP and the non-3GPP UE location, the "ueLocTime" attribute contains the age of the last known 3GPP UE location.

### 5.6.2.10 Type AfEventSubscription

**Table 5.6.2.10-1: Definition of type AfEventSubscription**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| event | AfEvent | M | 1 | Subscribed Event. | |
| notifMethod | AfNotifMethod | O | 0..1 | If notifMethod is not supplied, the default value "EVENT_DETECTION" applies. | |
| repPeriod | DurationSec | O | 0..1 | Indicates the time interval between successive event notifications. It is supplied for notification method "PERIODIC".<br>If the feature "PacketDelayFailureReport" is supported, it also indicates the time interval at which a measurement failure needs to be reported if no measurement result is provided. It is supplied for notification methods "PERIODIC" and "EVENT_DETECTION". | EnhancedSubscriptionToNotification<br>PacketDelayFailureReport |
| waitTime | DurationSec | O | 0..1 | Indicates the minimum waiting time between subsequent reports. Only applicable when the notification is set to "EVENT_DETECTION". | EnhancedSubscriptionToNotification |

### 5.6.2.11 Type AfEventNotification

**Table 5.6.2.11-1: Definition of type AfEventNotification**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| event | AfEvent | M | 1 | Notified Event. | |
| flows | array(Flows) | O | 1..N | Affected Service Data Flows. | |

### 5.6.2.12 Type TerminationInfo

**Table 5.6.2.12-1: Definition of type TerminationInfo**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| termCause | TerminationCause | M | 1 | Indicates the cause for requesting the deletion of the Individual Application Session Context resource. | |
| resUri | Uri | M | 1 | Identifies the Individual Application Session Context that triggered the termination notification.<br>(NOTE) | |
| NOTE: Either the complete resource URI included in the "resUri" attribute or the "apiSpecificResourceUriPart" component (see clause 5.1) of the resource URI included in the "resUri" attribute may be used by the NF service consumer for the identification of the Individual Application Session Context resource related to the termination notification. | | | | | |

### 5.6.2.13 Type AfRoutingRequirement

**Table 5.6.2.13-1: Definition of type AfRoutingRequirement**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| appReloc | boolean | O | 0..1 | Indication of application relocation possibility.<br>When it is included and set to "true", it indicates that the application cannot be relocated once a location of the application is selected by the 5GC. The default value is "false". | InfluenceOnTrafficRouting |
| routeToLocs | array(RouteToLocation) | O | 1..N | A list of traffic routes to applications locations. | InfluenceOnTrafficRouting |
| spVal | SpatialValidity | O | 0..1 | Indicates where the traffic routing requirements apply. The absence of this attribute indicates no spatial restrictions. | InfluenceOnTrafficRouting |
| tempVals | array(TemporalValidity) | O | 1..N | Indicates the time interval(s) during which the NF service consumer request is to be applied. | InfluenceOnTrafficRouting |
| upPathChgSub | UpPathChgEvent | O | 0..1 | Subscription to UP path management events. | InfluenceOnTrafficRouting |
| addrPreserInd | boolean | O | 0..1 | Indicates whether UE IP address should be preserved.<br>This attribute shall set to "true" if preserved, otherwise, set to "false".<br>Default value is false if omitted. | URLLC |
| simConnInd | boolean | O | 0..1 | Indication of simultaneous connectivity temporarily maintained for the source and target PSA. If it is included and set to "true", temporary simultaneous connectivity should be kept. The default value "false" applies, if the attribute is not present and has not been supplied previously. | SimultConnectivity |
| simConnTerm | DurationSec | C | 0..1 | Indication of the minimum time interval to be considered for inactivity of the traffic routed via the source PSA during the edge re-location procedure.<br>It may be included when the "simConnInd" attribute is set to true. | SimultConnectivity |
| maxAllowedUpLat | Uinteger | O | 0..1 | Indicates the target user plane latency in units of milliseconds. | AF_latency |
| easIpReplaceInfos | array(EasIpReplacementInfo) | O | 1..N | Contains EAS IP replacement information. | EASIPreplacement |
| easRedisInd | boolean | O | 0..1 | Indicates the EAS rediscovery is required for the application if it is included and set to "true". Default value is "false" if omitted.<br>The indication shall be invalid after it was applied unless it is provided again. | EASDiscovery |

### 5.6.2.14 Type ResourcesAllocationInfo

**Table 5.6.2.14-1: Definition of type ResourcesAllocationInfo**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| mcResourcStatus | MediaComponentResourcesStatus | C | 0..1 | Indicates the status of the PCC rule(s) related to the media components identified by the "flows" attribute. | |
| flows | array(Flows) | C | 1..N | Identification of the flows.<br>It shall be included if "MediaComponentVersioning" feature is supported.<br>When "MediaComponentVersioning" feature is not supported, if no flows are provided, the status in the "mcResourcStatus" applies for all flows within the AF session. | |
| altSerReq | string | O | 0..1 | When present, indicates the alternative service requirement the NG-RAN can guarantee for the indicated "flows". | AuthorizationWithRequiredQoS |
| NOTE: The "mcResourcStatus" attribute shall be included if AuthorizationWithRequiredQoS feature is not supported. | | | | | |

### 5.6.2.15 Type QosNotificationControlInfo

**Table 5.6.2.15-1: Definition of type QosNotificationControlInfo**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| notifType | QosNotifType | M | 1 | Indicates whether the GBR targets for the indicated SDFs are "NOT_GUARANTEED" or "GUARANTEED" again. | |
| flows | array(Flows) | C | 1..N | Identification of the flows. It shall be included if "MediaComponentVersioning" feature is supported. When "MediaComponentVersioning" feature is not supported, if no flows are provided, the notification in the "notifType" applies for all flows within the AF session. | |
| altSerReq | string | O | 0..1 | Indicates the alternative service requirement the NG-RAN can guarantee. | AuthorizationWithRequiredQoS |

### 5.6.2.16 Type SpatialValidity

**Table 5.6.2.16-1: Definition of type SpatialValidity**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| presenceInfoList | map(PresenceInfo) | M | 1..N | Defines the presence information provisioned by the NF service consumer. The "presenceState" attribute within the "PresenceInfo" data type shall not be supplied. The "praId" attribute within the PresenceInfo data type shall also be the key of the map. | InfluenceOnTrafficRouting |

### 5.6.2.17 Type EthFlowDescription

**Table 5.6.2.17-1: Definition of type EthFlowDescription**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| destMacAddr | MacAddr48 | O | 0..1 | Destination MAC address. | |
| ethType | string | M | 1 | A two-octet string that represents the Ethertype, as described in IEEE 802.3 [16] and IETF RFC 7042 [18] in hexadecimal representation.<br>Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the ethType shall appear first in the string, and the character representing the 4 least significant bits of the ethType shall appear last in the string. | |
| fDesc | FlowDescription | C | 0..1 | Contains the flow description for the Uplink or Downlink IP flow. It shall be present when the Ethertype is IP. (NOTE 3) | |
| fDir | FlowDirection | O | 0..1 | Contains the packet filter direction. Only the "DOWNLINK" or "UPLINK" value is applicable. (NOTE 2) | |
| sourceMacAddr | MacAddr48 | O | 0..1 | Source MAC address. | |
| vlanTags | array(string) | O | 1..2 | Customer-VLAN and/or Service-VLAN tags containing the VID, PCP/DEI fields as defined in IEEE 802.1Q [17] and IETF RFC 7042 [18]. The first/lower instance in the array stands for the Customer-VLAN tag and the second/higher instance in the array stands for the Service-VLAN tag.<br><br>Each field is encoded as a two-octet string in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the PCP/DEI field shall appear first in the string, followed by character representing the 4 most significant bits of the VID field, and the character representing the 4 least significant bits of the VID field shall appear last in the string.<br><br>If only Service-VLAN tag is provided, empty string for Customer-VLAN tag shall be provided. | |
| srcMacAddrEnd | MacAddr48 | O | 0..1 | Source MAC address end. If this attribute is present, the sourceMacAddr attribute specifies the source MAC address start. E.g. srcMacAddrEnd with value 00-10-A4-23-3E-FE and sourceMacAddr with value 00-10-A4-23-3E-02 means all MAC addresses from 00-10-A4-23-3E-02 up to and including 00-10-A4-23-3E-FE. | MacAddressRange |
| destMacAddrEnd | MacAddr48 | O | 0..1 | Destination MAC address end. If this attribute is present, the destMacAddr attribute specifies the destination MAC address start. | MacAddressRange |

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| NOTE 1: The "srcMacAddrEnd" attribute may only be present if the "sourceMacAddr" attribute is present; the "destMacAddrEnd" attribute may only be present if the "destMacAddr" attribute is present.<br>NOTE 2: If the "UPLINK" is included within the "fDir" attribute, the "sourceMacAddr" attribute and "srcMacAddrEnd" attribute (if MacAddressRange feature is supported) contain the UE address and "destMacAddr" attribute and "destMacAddrEnd" attribute (if MacAddressRange feature is supported)contain the remote address; otherwise if the "DOWNLINK" is included within the "fDir" attribute or the "fDir" attribute is never provided, the "sourceMacAddr" attribute and "srcMacAddrEnd" attribute (if MacAddressRange feature is supported) contain the remote address and "destMacAddr" attribute and "destMacAddrEnd" attribute (if MacAddressRange feature is supported) contain the UE address.<br>NOTE 3: The direction of the "fDesc" attribute shall be set to "in" if the "UPLINK" is included within the "fDir" attribute; the direction of the "fDesc" attribute shall be set to "out" if the "DOWNLINK" is included within the "fDir" attribute or the "fDir" attribute is never provided. | | | | | |

### 5.6.2.18 Void

### 5.6.2.19 Void

### 5.6.2.20 Type AnGwAddress

**Table 5.6.2.20-1: Definition of type AnGwAddress**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| anGwIpv4addr | Ipv4Addr | O | 0..1 | Includes the IPv4 address of the access network gateway control node. | |
| anGwIpv6addr | Ipv6Addr | O | 0..1 | Includes the IPv6 address of the access network gateway control node. | |
| NOTE: At least one address of the access network gateway control node (the IPv4 address or the IPv6 address or both if both addresses are available) shall be included. | | | | | |

### 5.6.2.21 Type Flows

**Table 5.6.2.21-1: Definition of type Flows**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| contVers | array(ContentVersion) | C | 1..N | Represents the content version of the content of a media component. If "MediaComponentVersioning" feature is supported, the content version shall be included if it was included when the corresponding media component was provided or modified. | MediaComponentVersioning |
| fNums | array(integer) | O | 1..N | Indicates the service data flows via their flow identifier. If no flow identifier is supplied, the Flows data type refers to all the flows matching the media component number. | |
| medCompN | integer | M | 1 | Identifies the media component number, and it contains the ordinal number of the media component. | |

### 5.6.2.22 Type TemporalValidity

**Table 5.6.2.22-1: Definition of type TemporalValidity**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| startTime | DateTime | O | 0..1 | Indicates the time from which the traffic routing requirements start to apply. The absence of this attribute indicates the traffic routing requirements apply immediately. | InfluenceOnTraffic Routing |
| stopTime | DateTime | O | 0..1 | Indicates the time when the traffic routing requirements cease to apply. The absence of this attribute indicates the traffic routing requirements do not cease at any time. | InfluenceOnTraffic Routing |

### 5.6.2.23 Void

### 5.6.2.24 Type AfRoutingRequirementRm

This data type is defined in the same way as the "AfRoutingRequirement" data type, but:

- with the OpenAPI "nullable: true" property;
- the removable attribute "spVal" is defined with the data type "SpatialValidityRm"; and
- the removable attributes "tempVals", "routeToLocs", "addrPreserInd", "simConnInd", "simConnTerm" and "easIpReplaceInfos" are defined as nullable in the OpenAPI.

**Table 5.6.2.24-1: Definition of type AfRoutingRequirementRm**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| appReloc | boolean | O | 0..1 | Indication of application relocation possibility. When it is set to "true", it indicates that the application cannot be relocated once a location of the application is selected by the 5GC. | InfluenceOnTrafficRouting |
| routeToLocs | array(RouteToLocation) | O | 1..N | A list of traffic routes to applications locations. | InfluenceOnTrafficRouting |
| spVal | SpatialValidityRm | O | 0..1 | Indicates where the traffic routing requirements apply. | InfluenceOnTrafficRouting |
| tempVals | array(TemporalValidity) | O | 1..N | Indicates the time interval(s) during which the NF service consumer request is to be applied. | InfluenceOnTrafficRouting |
| upPathChgSub | UpPathChgEvent | O | 0..1 | Subscription to UP path management events. | InfluenceOnTrafficRouting |
| addrPreserInd | boolean | O | 0..1 | Indicates whether UE IP address should be preserved. | URLLC |
| simConnInd | boolean | O | 0..1 | Indication of simultaneous connectivity temporarily maintained for the source and target PSA. If it is included and set to "true", temporary simultaneous connectivity should be kept. | SimultConnectivity |
| simConnTerm | DurationSecRm | C | 0..1 | Indication of the minimum time interval to be considered for inactivity of the traffic routed via the source PSA during the edge re-location procedure. | SimultConnectivity |
| maxAllowedUpLat | UintegerRm | O | 0..1 | Indicates the target user plane latency in units of milliseconds. | AF_latency |
| easIpReplaceInfos | array(EasIpReplacementInfo) | O | 1..N | Contains EAS IP replacement information. | EASIPreplacement |
| easRedisInd | boolean | O | 0..1 | Indicates the EAS rediscovery is required for the application if it is included and set to "true". Default value is "false" if omitted. The indication shall be invalid after it was applied unless it is provided again. | EASDiscovery |

### 5.6.2.25 Type EventsSubscReqDataRm

This data type is defined in the same way as the "EventsSubscReqData" data type, but:

- with the OpenAPI "nullable: true" property; and
- the removable attribute "usgThres" is defined with the removable data type "UsageThresholdRm"; and removable attribute "qosMon" is defined with the removable data type "QosMonitoringInformationRm".

**Table 5.6.2.25-1: Definition of type EventsSubscReqDataRm**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| events | array(AfEventSubscription) | M | 1..N | Subscribed Events. | |
| notifUri | Uri | O | 0..1 | Notification URI. | |
| reqQosMonParams | array(RequestedQosMonitoringParameter) | O | 1..N | Indicates the UL packet delay, DL packet delay and/or round trip packet delay between the UE and the UPF is to be monitored when the QoS Monitoring for URLLC is enabled for the service data flow. | QoSMonitoring |
| qosMon | QosMonitoringInformationRm | O | 0..1 | Qos Monitoring information. It can be present when the event "QOS_MONITORING" is subscribed. | QoSMonitoring |
| reqAnis | array(RequiredAccessInfo) | C | 1..N | Represents the required access network information. It shall be present when the event "ANI_REPORT" is subscribed. (NOTE) | NetLoc |
| usgThres | UsageThresholdRm | O | 0..1 | Includes the volume and/or time thresholds for sponsored data connectivity. | SponsoredConnectivity |
| notifCorreId | string | O | 0..1 | It is used to set the value of Notification Correlation ID in the corresponding notification. | EnhancedSubscriptionToNotification |
| directNotifInd | boolean | C | 0..1 | Indicates that the event notification of QoS Monitoring data is sent by the UPF to Local NEF or AF if it is included and set to true. It may be present when the event "QOS_MONITORING" is subscribed. | ExposureToEAS |

NOTE: "ANI_REPORT" is the one-time reported event and thus the attribute "reqAnis" is not defined as removable attribute (i.e. with the removable data type "RequiredAccessInfoRm"). Once the access network information is reported to the NF service consumer the subscription to this event is automatically terminated in the PCF and the related information is removed.

### 5.6.2.26 Type MediaComponentRm

This data type is defined in the same way as the "MediaComponent" data type, but:

- with the OpenAPI "nullable: true" property; and
- the removable attributes "afRoutReq" is defined with the removable data type "AfRoutingRequirementRm"; "maxPacketLossRateDl" and "maxPacketLossRateUl" are defined with the removable data type "PacketLossRateRm"; "medSubComps" is defined with the removable data type "MediaSubComponentRm"; "preemptCap" is defined with the removable data type "PreemptionCapabilityRm"; "preemptVuln" is defined with the removable data type "PreemptionVulnerabilityRm"; "marBwDl", "marBwUl", "minDesBwDl", "minDesBwUl", "mirBwDl", "mirBwUl", "maxSuppBwDl", "maxSuppBwUl", "rrBw", "rsBw" are defined with the removable data type "BitRateRm"; "sharingKeyDl", "sharingKeyUl", and "tsnQos" are defined with the removable data types , "Uint32Rm" and "TsnQosContainerRm"; the removable attributes "desMaxLatency" and "desMaxLoss" are defined with the removable data type "FloatRm"; the removable attribute "flusId" is defined as nullable in the OpenAPI.
- the removable attributes "qosReference" and "altSerReqs" are defined as nullable.

**Table 5.6.2.26-1: Definition of type MediaComponentRm**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| afAppId | AfAppId | O | 0..1 | Contains information that identifies the particular service the AF session belongs to. | |
| afRoutReq | AfRoutingRequirementRm | O | 0..1 | Indicates the AF traffic routing requirements. | InfluenceOnTrafficRouting |
| qosReference | string | O | 0..1 | Identifies a pre-defined QoS information. | AuthorizationWithRequiredQoS |
| altSerReqs | array(string) | O | 1..N | Ordered list of alternative service requirements that include a set of QoS references. The lower the index of the array for a given entry, the higher the priority. (NOTE) | AuthorizationWithRequiredQoS |
| altSerReqsData | array(AlternativeServiceRequirementsData) | O | 1..N | Ordered list of alternative service requirements that include individual QoS parameter sets. The lower the index of the array for a given entry, the higher the priority. (NOTE) | AltSerReqsWithIndQoS |
| disUeNotif | boolean | O | 0..1 | Indicates to disable QoS flow parameters signalling to the UE when the SMF is notified by the NG-RAN of changes in the fulfilled QoS situation when it is included and set to "true". The fulfilled situation is either the QoS profile or an Alternative QoS Profile. The default value "false" shall apply, if the attribute is not present and has not been supplied previously. | DisableUENotification |
| contVer | ContentVersion | O | 0..1 | Represents the content version of a media component. | MediaComponentVersioning |
| desMaxLatency | FloatRm | O | 0..1 | Indicates a maximum desirable transport level packet latency in milliseconds. | FLUS, QoSHint |
| desMaxLoss | FloatRm | O | 0..1 | Indicates the maximum desirable transport level packet loss rate in percent (without "%" sign). | FLUS, QoSHint |
| flusId | string | O | 0..1 | Indicates that the media component is used for FLUS media.<br>It is derived from the media level attribute "a=label:" (see IETF RFC 4574 [50]) obtained from the SDP body. It contains the string after "a=label:" starting with "flus" and may be followed by more characters as described in 3GPP TS 26.238 [51]. | FLUS |
| maxPacketLossRateDl | PacketLossRateRm | O | 0..1 | Indicates the downlink maximum rate for lost packets that can be tolerated for the service data flow. | CHEM |
| maxPacketLossRateUl | PacketLossRateRm | O | 0..1 | Indicates the uplink maximum rate for lost packets that can be tolerated for the service data flow. | CHEM |
| medCompN | integer | M | 1 | Identifies the media component number, and it contains the ordinal number of the media component. | |
| medSubComps | map(MediaSubComponentRm) | O | 1..N | Contains the requested bitrate and filters for the set of service data flows identified by their common flow identifier. The key of the map is the attribute "fNum". | |
| medType | MediaType | O | 0..1 | Indicates the media type of the service. | |
| marBwUl | BitRateRm | O | 0..1 | Maximum requested bandwidth for the Uplink. | |
| marBwDl | BitRateRm | O | 0..1 | Maximum requested bandwidth for the Downlink. | |
| maxSuppBwDl | BitRateRm | O | 0..1 | Maximum supported bandwidth for the Downlink. | IMS_SBI |

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| maxSuppBwUl | BitRateRm | O | 0..1 | Maximum supported bandwidth for the Uplink. | IMS_SBI |
| minDesBwDl | BitRateRm | O | 0..1 | Minimum desired bandwidth for the Downlink. | IMS_SBI |
| minDesBwUl | BitRateRm | O | 0..1 | Minimum desired bandwidth for the Uplink. | IMS_SBI |
| mirBwUl | BitRateRm | O | 0..1 | Minimum requested bandwidth for the Uplink. | |
| mirBwDl | BitRateRm | O | 0..1 | Minimum requested bandwidth for the Downlink. | |
| fStatus | FlowStatus | O | 0..1 | Indicates whether the status of the service data flows is enabled, or disabled. | |
| preemptCap | PreemptionCapabilityRm | O | 0..1 | Defines whether the media flow may get resources that were already assigned to another media flow with a lower priority level. | MCPTT-Preemption |
| preemptVuln | PreemptionVulnerabilityRm | O | 0..1 | Defines whether the media flow may lose the resources assigned to it in order to admit a media flow with higher priority level. | MCPTT-Preemption |
| prioSharingInd | PrioritySharingIndicator | O | 0..1 | Indicates that the media flow is allowed to use the same ARP as media flows belonging to other "Individual Application Session Context" resources bound to the same PDU session. | PrioritySharing |
| resPrio | ReservPriority | O | 0..1 | Indicates the reservation priority. | |
| rrBw | BitRateRm | O | 0..1 | Indicates the maximum required bandwidth in bits per second for RTCP receiver reports within the session component as specified in IETF RFC 3556 [37]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP. | IMS_SBI |
| rsBw | BitRateRm | O | 0..1 | Indicates the maximum required bandwidth in bits per second for RTCP sender reports within the session component as specified in IETF RFC 3556 [37]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP. | IMS_SBI |
| codecs | array(CodecData) | O | 1..2 | Indicates the codec data. | |
| sharingKeyDl | Uint32Rm | O | 0..1 | Identifies which media components share resources in the downlink direction.<br>If resource sharing applies between media components across "Individual Application Session Context" resources for the same PDU session, the same value of the "sharingKeyDl" attribute shall be used. If resource sharing does not apply among media components across "Individual Application Session Context" resources for the same PDU session, a different value for the "sharingKeyDl" attribute shall be used. If resource sharing does no longer apply for this media component, the "sharingKeyDl" attribute shall be set to "null". | ResourceSharing |

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| sharingKeyUl | Uint32Rm | O | 0..1 | Identifies which media components share resources in the uplink direction. If resource sharing applies between media components across "Individual Application Session Context" resources for the same PDU session, the same value of the "sharingKeyUl" attribute shall be used. If resource sharing does not apply among media components across "Individual Application Session Context" resources for the same PDU session, a different value for the "sharingKeyUl" attribute shall be used. If resource sharing does no longer apply for this media component, the "sharingKeyUl" attribute shall be set to "null". | ResourceSharing |
| tsnQos | TsnQoSContainerRm | O | 0..1 | Transports QoS parameters for TSC traffic. | TimeSensitiveNetworking |
| tscaiInputUl | TscaiInputContainer | O | 0..1 | Transports TSCAI input parameters for TSC traffic at the ingress interface of the DS-TT/UE (uplink flow direction). | TimeSensitiveNetworking |
| tscaiInputDl | TscaiInputContainer | O | 0..1 | Transports TSCAI input parameters for TSC traffic at the ingress of the NW-TT (downlink flow direction). | TimeSensitiveNetworking |
| tscaiTimeDom | Uinteger | O | 0..1 | Indicates the (g)PTP domain that the (TSN)AF is located in. | TimeSensitiveCommunication |
| NOTE: The attributes "altSerReqs" and "altSerReqsData" are mutually exclusive. | | | | | |

### 5.6.2.27 Type MediaSubComponentRm

This data type is defined in the same way as the "MediaSubComponent" data type, but:

- with the OpenAPI "nullable: true" property;
- the removable attributes "marBwDl", "marBwUl", defined with the removable data type "BitRateRm"; the removable attribute "tosTrCl", defined with the removable data type "TosTrafficClassRm"; and
- the removable attributes "ethfDescs" and "fDescs" are defined as nullable in the OpenAPI.

**Table 5.6.2.27-1: Definition of type MediaSubComponentRm**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| afSigProtocol | AfSigProtocol | O | 0..1 | Indicates the protocol used for signalling between the UE and the NF service consumer. It may be included only if the "flowUsage" attribute is set to the value "AF_SIGNALLING". | ProvAFsignalFlow |
| ethfDescs | array(EthFlowDescription) | O | 1..2 | Contains the flow description for the Uplink and/or Downlink Ethernet flows. | |
| fNum | integer | M | 1 | Identifies the ordinal number of the IP flow. | |
| fDescs | array(FlowDescription) | O | 1..2 | Contains the flow description for the Uplink and/or Downlink IP flows. | |
| fStatus | FlowStatus | O | 0..1 | Indicates whether the status of the service data flows is enabled or disabled. | |
| flowUsage | FlowUsage | O | 0..1 | Flow usage of the flows (e.g. RTCP, AF signalling). | |
| marBwUl | BitRateRm | O | 0..1 | Maximum requested bandwidth for the Uplink. | |
| marBwDl | BitRateRm | O | 0..1 | Maximum requested bandwidth for the Downlink. | |
| tosTrCl | TosTrafficClassRm | O | 0..1 | Type of Service or Traffic Class. | |

### 5.6.2.28 Type SpatialValidityRm

This data type is defined in the same way as the "SpatialValidity" data type, but with the OpenAPI "nullable: true" property.

### 5.6.2.29 Type ExtendedProblemDetails

This data type is the "ProblemDetails" data type defined in 3GPP TS 29.571 [12] but extended with the attribute "acceptableServInfo" of data type "AcceptableServiceInfo".

**Table 5.6.2.29-1: Definition of type ExtendedProblemDetails**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| acceptableServInfo | AcceptableServiceInfo | O | 0..1 | Describes information related to the acceptable service information, i.e., the maximum acceptable bandwidth for an AF session and/or for specific media components. | |
| NOTE: ExtendedProblemDetails data type also contains all the properties defined for ProblemDetails data type in 3GPP TS 29.571[12]. | | | | | |

### 5.6.2.30 Type AcceptableServiceInfo

**Table 5.6.2.30-1: Definition of type AcceptableServiceInfo**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| accBwMedComps | map(MediaComponent) | O | 1..N | Indicates the maximum bandwidth that shall be authorized by the PCF for each media component of the map.<br>Each media component of the map shall only include the "medCompN" attribute and the "marBwDl" and/or "marBwUl" attributes indicating the maximum acceptable bandwidth.<br>The key of the map is the media component number. | |
| marBwUl | BitRate | O | 0..1 | Maximum acceptable bandwidth for the Uplink for the AF session. | |
| marBwDl | BitRate | O | 0..1 | Maximum acceptable bandwidth for the Downlink for the AF session. | |
| NOTE: When the acceptable bandwidth applies to one or more media components, only the "accBwMedComps" attribute shall be provided. When the acceptable bandwidth applies to the whole AF session, only the "marBwDl" and "marBwUl" attributes shall be present. | | | | | |

### 5.6.2.31 Type UeIdentityInfo

**Table 5.6.2.31-1: Definition of type UeIdentityInfo**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| gpsi | Gpsi | O | 0..1 | Represents the GPSI. | |
| pei | Pei | O | 0..1 | Represents the PEI. | |
| supi | Supi | O | 0..1 | Represents the SUPI. | |
| NOTE: At least one of the "gpsi", "supi" and "pei" attributes shall be present. More than one attribute may be present simultaneously. | | | | | |

### 5.6.2.32 Type AccessNetChargingIdentifier

**Table 5.6.2.32-1: Definition of type AccessNetChargingIdentifier**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| accNetChaIdValue | ChargingId | C | 0..1 | Contains a charging identifier.<br>(NOTE 1) | |
| accNetChargIdString | string | C | 0..1 | A character string containing the charging identifier (see clause 5.1.9.1 of 3GPP TS 32.255 [35]).<br>(NOTE 1) | AccNetChargId_String |
| flows | array(Flows) | O | 1..N | Identifications of the flows transported within the corresponding QoS flow. If no flows are provided, the charging identifier applies for all flows within the AF session. | |
| NOTE 1: The "accNetChaIdValue" shall be used to encode the charging identifier when the charging identifier is within the Uint32 value range. The "accNetChargIdString" attribute shall be used to encode the charging identifier when the "AccNetChargId_String" feature is supported by the AF and the PCF and the charging identifier is out of the Uint32 range.<br>NOTE 2: When the "AccNetChargId_String" feature is not supported and the value of the charging identifier is out of the ChargingId data type value range (Uint32) it is not possible to ensure a proper charging correlation using value of the "accNetChaIdValue" attribute. | | | | | |

### 5.6.2.33 Type OutOfCreditInformation

**Table 5.6.2.33-1: Definition of type OutOfCreditInformation**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| finUnitAct | FinalUnitAction | M | 1 | Indicates the termination action to be taken when the user's account cannot cover the service cost. | |
| flows | array(Flows) | O | 1..N | Identifications of the flows without available credit. If no flows are provided, the termination action in "finUnitAct" attribute applies for all flows within the AF session. | |

### 5.6.2.34 Type QosMonitoringInformation

**Table 5.6.2.34-1: Definition of type QosMonitoringInformation**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| repThreshDl | integer | O | 0..1 | Indicates the threshold in units of milliseconds for DL packet delay. Only applicable when the "notifMethod" attribute is not supplied or the "notifMethod" is supplied and set to "EVENT_DETECTION".<br>Minimum = 0. | |
| repThreshUl | integer | O | 0..1 | Indicates the threshold in units of milliseconds for UL packet delay. Only applicable when the "notifMethod" attribute is not supplied or the "notifMethod" is supplied and set to "EVENT_DETECTION".<br>Minimum = 0. | |
| repThreshRp | integer | O | 0..1 | Indicates the threshold in units of milliseconds for round trip packet delay. Only applicable when the "notifMethod" attribute is not supplied or the "notifMethod" is supplied and set to "EVENT_DETECTION".<br>Minimum = 0. | |
| NOTE: The "repThreshDl" attribute and/or the "repThreshUl" attribute and/or the "repThreshRp" attribute shall be present. | | | | | |

### 5.6.2.35 Type TsnQosContainer

**Table 5.6.2.35-1: Definition of type TsnQosContainer**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| maxTscBurstSize | ExtMaxDataBurstVol | O | 0..1 | Maximum burst size of the TSC traffic in units of Bytes.<br>Minimum = 4096, Maximum = 2000000. | |
| tscPackDelay | PacketDelBudget | O | 0..1 | Delay of the TSC traffic. | |
| tscPrioLevel | TscPriorityLevel | O | 0..1 | TSC traffic priority in relation to other TSC and non-TSC traffic. | |
| NOTE: At least one of the attributes shall be present in an instance of the TsnQosContainer. | | | | | |

### 5.6.2.36 Type PcscfRestorationRequestData

**Table 5.6.2.36-1: Definition of type PcscfRestorationRequestData**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| dnn | Dnn | C | 0..1 | Data Network Name, a full DNN with both the Network Identifier and Operator Identifier, or a DNN with the Network Identifier only. It shall be present when the "afRoutReq" attribute is present. | |
| ipDomain | string | O | 0..1 | Indicates the IPv4 address domain information that assists session binding. | |
| sliceInfo | Snssai | O | 0..1 | Identifies the S-NSSAI. | |
| supi | Supi | O | 0..1 | Subscription Permanent Identifier. | |
| ueIpv4 | Ipv4Addr | C | 0..1 | The IPv4 address of the served UE. | |
| ueIpv6 | Ipv6Addr | C | 0..1 | The IPv6 address of the served UE. | |
| NOTE: When present, only one of the served UE addressing parameters (the IPv4 address or the IPv6 address) shall always be included. | | | | | |

### 5.6.2.37 Type QosMonitoringReport

**Table 5.6.2.37-1: Definition of type QosMonitoringReport**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| flows | array(Flows) | C | 1..N | Identification of the flows. It shall be included if "MediaComponentVersioning" feature is supported. When "MediaComponentVersioning" feature is not supported, if no flows are provided, the packet delay applies for all flows within the AF session. | |
| ulDelays | array(integer) | O | 1..N | Uplink packet delay in units of milliseconds. (NOTE 1) | |
| dlDelays | array(integer) | O | 1..N | Downlink packet delay in units of milliseconds. (NOTE 1) | |
| rtDelays | array(integer) | O | 1..N | Round trip delay in units of milliseconds. (NOTE 1) | |
| pdmf | boolean | O | 0..1 | Packet delay measurement failure indicator. When set to true, it indicates that a packet delay failure has occurred. Default value is false if omitted. (NOTE 2) | PacketDelayFailureReport |
| NOTE 1: In this release of the specification one element may be included in the array, as specified in clause 4.2.5.14..<br>NOTE 2: When the "pdmf" attribute is set to true, "ulDelays", "dlDelays" and "rtDelays" shall not be present. | | | | | |

### 5.6.2.38 Type TsnQosContainerRm

This data type is defined in the same way as the "TsnQoSContainer" data type, but with the OpenAPI "nullable: true" property.

### 5.6.2.39 Type TscaiInputContainer

**Table 5.6.2.39-1: Definition of type TscaiInputContainer**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| periodicity | Uinteger | O | 0..1 | Unsigned 64-bit integer identifying a period of time in units of microseconds, i.e. 0 to (2^64)-1.<br>Minimum = 0.<br>Maximum = 18446744073709551615.<br>Identifications of the time period between the start of two bursts in reference to the external GM. | |
| burstArrivalTime | DateTime | O | 0..1 | Indicates the arrival time of the data burst in reference to the external GM. | |
| surTimeInNumMsg | Uinteger | O | 0..1 | Unsigned 32-bit integer indicates the survival time in terms of maximum number of messages an application can survive without any burst. A message is equivalent to a burst, i.e. 0 to (2^32)-1.<br>Minimum = 0.<br>Maximum = 4294967295. | TimeSensitive Communicatio n |
| surTimeInTime | Uinteger | O | 0..1 | Unsigned 64-bit integer indicates the survival time in terms of time units of microseconds an application can survive without any burst, i.e. 0 to (2^64)-1.<br>Minimum = 0.<br>Maximum = 18446744073709551615. | TimeSensitive Communicatio n |

### 5.6.2.40 Type PduSessionTsnBridge

**Table 5.6.2.40-1: Definition of type PduSessionTsnBridge**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| tsnBridgeInfo | TsnBridgeInfo | M | 1 | Reports the TSC user plane node information. | |
| tsnBridgeManCont | BridgeManagementContainer | O | 0..1 | Transports TSC user plane node management information. | |
| tsnPortManContDstt | PortManagementContainer | O | 0..1 | Transports port management information for the DS-TT port. | |
| tsnPortManContNwtts | array(PortManagementContainer) | O | 1..N | Transports port management information for one or more NW-TT ports. | |
| ueIpv4Addr | Ipv4Addr | O | 0..1 | It represents the identifier of the PDU session related to the reported UP node information, and contains the UE IPv4 address.<br>It might be present for PDU sessions of IP type.<br>(NOTE) | TimeSensitiveCommunication |
| dnn | Dnn | O | 0..1 | The DNN of the PDU session, a full DNN with both the Network Identifier and Operator Identifier, or a DNN with the Network Identifier only. | TimeSensitiveCommunication |
| snssai | Snssai | O | 0..1 | Identifies the S-NSSAI. | TimeSensitiveCommunication |
| ipDomain | string | O | 0..1 | IPv4 address domain identifier. | TimeSensitiveCommunication |
| ueIpv6AddrPrefix | Ipv6Prefix | O | 0..1 | It represents the identifier of the PDU session related to the reported UP node information, and contains the UE IPv6 address prefix.<br>It might be present for PDU sessions of IP type.<br>(NOTE) | TimeSensitiveCommunication |
| NOTE: For PDU sessions of IP type, either the ueIpv4Addr or the ueIpv6AddrPrefix shall be present in this release of the specification. | | | | | |

### 5.6.2.41 Type QosMonitoringInformationRm

This data type is defined in the same way as the "QosMonitoringInformation" data type, but with the OpenAPI "nullable: true" property.

### 5.6.2.42 Type EventsSubscPutData

**Table 5.6.2.42-1: Definition of type EventsSubscPutData**

| Data Type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|
| EventsSubscReqData | C | 0..1 | Identifies the events the application subscribes to and represents the Events Subscription sub-resource data.<br>It shall be present in the response to PUT requests as specified in table 5.3.4.3.1-3. | |
| EventsNotification | C | 0..1 | Describes the notification about the events already met at the time of subscription. It shall be present if available. | |
| NOTE: EventsSubscPutData data type is represented as a non-exclusive list of two data types: EventsSubscReqData and EventsNotification. | | | | |

### 5.6.2.43 Type AppSessionContextUpdateDataPatch

**Table 5.6.2.43-1: Definition of type AppSessionContextUpdateDataPatch**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| ascReqData | AppSessionContext UpdateData | O | 0..1 | Describes the requested update to the services requirements of an Individual Application Session Context. | |

### 5.6.2.44 Type AppDetectionReport

**Table 5.6.2.44-1: Definition of type AppDetectionReport**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| adNotifType | AppDetectionNotifTyp e | M | 1 | Indicates whether the report is about the detection of application start or application stop. | |
| afAppId | AfAppId | M | 1 | It indicates the application identifier of the detected traffic. | |

### 5.6.2.45 Type PduSessionEventNotification

**Table 5.6.2.45-1: Definition of PduSessionEventNotification**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| evNotif | AfEventNotific ation | M | 1 | Indicates the reported event (e.g. "PDU_SESSION_STATUS"). | |
| supi | Supi | C | 0..1 | Contains the SUPI of the PDU session. It shall be present for the "PDU_SESSION_STATUS" event. | |
| ueIpv4 | Ipv4Addr | C | 0..1 | The IPv4 address of the served UE for the reported PDU session. | |
| ueIpv6 | Ipv6Addr | C | 0..1 | The IPv6 address of the served UE for the reported PDU session. | |
| ueMac | MacAddr48 | C | 0..1 | The MAC address of the served UE for the reported PDU session. | |
| status | PduSessionSt atus | C | 0..1 | It shall be present for the "PDU_SESSION_STATUS" event. Indicates whether the PDU session is "ESTABLISHED" or "TERMINATED". | |
| pcfInfo | PcfAddressing Info | C | 0..1 | Contains PCF addressing information. It may be present for the "PDU_SESSION_STATUS" event. It shall be included when the PDU session operation is "ESTABLISHED". | |
| dnn | Dnn | C | 0..1 | Contains the DNN of the PDU session. It shall be included when the event is "PDU_SESSION_STATUS" and the PDU session operation is "ESTABLISHED". | |
| snssai | Snssai | C | 0..1 | Contains the S-NSSAI of the PDU session. It shall be included when the event is "PDU_SESSION_STATUS" and the PDU session operation is "ESTABLISHED". | |
| gpsi | Gpsi | O | 0..1 | Contains the GPSI of the PDU session. It shall be included, if available, when the event is "PDU_SESSION_STATUS" and the PDU session operation is "ESTABLISHED". | |
| NOTE: Only one of the served UE addressing parameters (the IPv4 address or the IPv6 address or MAC address) shall always be included. | | | | | |

### 5.6.2.46 Type PcfAddressingInfo

**Table 5.6.2.46-1: Definition of type PcfAddressingInfo**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| pcfFqdn | Fqdn | C | 0..1 | FQDN of the PCF hosting the Npcf_PolicyAuthorization service. It shall be provided if available. (NOTE) | |
| pcfIpEndPoints | array(IpEndPoint) | C | 1..N | IP end points of the PCF hosting the Npcf_PolicyAuthorization service. It shall be provided if available. (NOTE) | |
| bindingInfo | string | O | 0..1 | This IE shall be present, if available.<br><br>When present, this IE shall contain the Binding indications of the PCF indicated by the pcfFqdn IE and/or pcfIpEndPoints IE, and shall be set to the value of the 3gpp-Sbi-Binding header defined in clause 5.2.3.2.6 of 3GPP TS 29.500 [25], without the header name and including only binding indications for "nf-instance" or "nf-set" binding levels. | |
| NOTE: The pcfFqdn and/or the pcfIpEndPoints shall always be included. | | | | | |

### 5.6.2.47 Type AlternativeServiceRequirementsData

**Table 5.6.2.47-1: Definition of type AlternativeServiceRequirementsData**

| Attribute name | Data type | P | Cardinality | Description | Applicability |
|---|---|---|---|---|---|
| altQosParamSetRef | string | M | 1 | It contains a reference to the alternative individual QoS related parameter(s) included in this set. The value of this attribute shall only be used in QoS notification control information (see "altSerReq" attribute in Table 5.6.2.15) to indicate the alternative individual QoS related parameters that can be guaranteed (if any). | |
| gbrUl | BitRate | O | 0..1 | Indicates the guaranteed bandwidth in uplink. | |
| gbrDl | BitRate | O | 0..1 | Indicates the guaranteed bandwidth in downlink. | |
| pdb | PacketDelBudget | O | 0..1 | Unsigned integer. It indicates the Packet Delay Budget expressed in milliseconds. | |
| NOTE: The "pdb" attribute, the combination of the "gbrUl" and "gbrDl" attributes, or both shall be provided. | | | | | |

## 5.6.3 Simple data types and enumerations

### 5.6.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

### 5.6.3.2 Simple data types

The simple data types defined in table 5.6.3.2-1 shall be supported.

**Table 5.6.3.2-1: Simple data types**

| Type Name | Type Definition | Description | Applicability |
|---|---|---|---|
| AfAppId | string | Contains an AF application identifier. | |
| AspId | string | Contains an identity of an application service provider. | SponsoredConnectivity |
| CodecData | string | Contains codec related information.<br>Refer to clause 5.3.7 of 3GPP TS 29.214 [20] for encoding. | |
| ContentVersion | integer | Unsigned 64-bit integer that indicates the version of some content, as e.g. the content of a media component. The content version shall be unique for the content and for the lifetime of that content. (NOTE) | MediaComponentVersioning |
| FlowDescription | string | Defines a packet filter for an IP flow. It contains an IpFilterRule according to clause 4.3 of IETF RFC 6733 [52].<br>Refer to clause 5.3.8 of 3GPP TS 29.214 [20] for encoding. | |
| SponId | string | Contains an identity of a sponsor. | SponsoredConnectivity |
| ServiceUrn | string | Indicates that an AF session is used for Emergency traffic.<br><br>It contains values of the service URN and it may include subservices, as defined in IETF RFC 5031 [34] or registered at IANA.<br><br>The string "urn:service:" in the beginning of the URN shall be omitted and all subsequent text shall be included. Examples of valid values of the ServiceUrn data structure are "sos", "sos.fire", "sos.police" and "sos.ambulance". | IMS_SBI |
| TosTrafficClass | string | 2-octet string, where each octet is encoded in hexadecimal representation. The first octet contains the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the second octet contains the ToS/Traffic Class mask field. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. One example is that of a TFT packet filter as defined in 3GPP TS 24.008 [36]. | |
| TosTrafficClassRm | string | This data type is defined in the same way as the "TosTrafficClass" data type, but with the OpenAPI "nullable: true" property. | |
| TscPriorityLevel | integer | Indicates the TSC traffic Priority Level, within the range 1 to 8.<br>Values are ordered in decreasing order of priority, i.e. with 1 as the highest priority and 8 as the lowest priority. | TimeSensitiveNetworking |
| TscPriorityLevelRm | integer | This data type is defined in the same way as the "TscPriorityLevel" data type, but with the OpenAPI "nullable: true" property. | TimeSensitiveNetworking |
| NOTE: The method of assigning content versions is implementation specific. | | | |

### 5.6.3.3 Enumeration: MediaType

The enumeration "MediaType" represents the media type of a media component.

**Table 5.6.3.3-1: Enumeration MediaType**

| Enumeration value | Description | Applicability |
|---|---|---|
| AUDIO | The type of media is audio. | |
| VIDEO | The type of media is video. | |
| DATA | The type of media is data. | |
| APPLICATION | The type of media is application data. | |
| CONTROL | The type of media is control. | |
| TEXT | The type of media is text. | |
| MESSAGE | The type of media is message | |
| OTHER | Other type of media. | |

### 5.6.3.4 Enumeration: ReservPriority

The enumeration "ReservPriority" represents the reservation priority. The lowest priority shall be indicated with the "PRIO_1" value, the next after the lowest with the "PRIO_2" value, and so on up to the highest priority which shall be indicated with "PRIO_16".

**Table 5.6.3.4-1: Enumeration ReservPriority**

| Enumeration value | Description | Applicability |
|---|---|---|
| PRIO_1 | | |
| PRIO_2 | | |
| PRIO_3 | | |
| PRIO_4 | | |
| PRIO_5 | | |
| PRIO_6 | | |
| PRIO_7 | | |
| PRIO_8 | | |
| PRIO_9 | | |
| PRIO_10 | | |
| PRIO_11 | | |
| PRIO_12 | | |
| PRIO_13 | | |
| PRIO_14 | | |
| PRIO_15 | | |
| PRIO_16 | | |

### 5.6.3.5 Enumeration: ServAuthInfo

The enumeration "ServAuthInfo" represents the result of the Npcf_PolicyAuthorization service request from the NF service consumer.

**Table 5.6.3.5-1: Enumeration ServAuthInfo**

| Enumeration value | Description | Applicability |
|---|---|---|
| TP_NOT_KNOWN | Indicates the transfer policy is not known. | |
| TP_EXPIRED | Indicates the transfer policy has expired. | |
| TP_NOT_YET_OCCURRED | Indicates the time window of the transfer policy has not yet occurred. | |
| ROUT_REQ_NOT_AUTHORIZED | Indicates the AF influence on traffic routing request is not allowed for the concerned PDU session. | RoutingReqOutcome |

### 5.6.3.6 Enumeration: SponsoringStatus

The enumeration "SponsoringStatus" represents whether the sponsored data connectivity is enabled or disabled/not-enabled.

**Table 5.6.3.6-1: Enumeration SponsoringStatus**

| Enumeration value | Description | Applicability |
|---|---|---|
| SPONSOR_DISABLED | Sponsored data connectivity is disabled or not enabled. | SponsoredConnectivity |
| SPONSOR_ENABLED | Sponsored data connectivity is enabled. | SponsoredConnectivity |

### 5.6.3.7 Enumeration: AfEvent

The enumeration "AfEvent" represents the traffic events the PCF can notify to the NF service consumer.

**Table 5.6.3.7-1: Enumeration AfEvent**

| Enumeration value | Description | Applicability |
|---|---|---|
| ACCESS_TYPE_CHANGE | Access type change. | |
| ANI_REPORT | Access Network Information Report requested. | NetLoc |
| APP_DETECTION | Application detection report is requested. | ApplicationDetectionEvents |
| CHARGING_CORRELATION | Access Network Charging Correlation Information. | IMS_SBI |
| UP_PATH_CHG_FAILURE | Indicates that the enforcement of the AF required routing requirements (i.e. DNAI change) failed. | RoutingReqOutcome |
| EPS_FALLBACK | Indicates that the establishment of the QoS flow for the requested voice media type was rejected due to fallback to EPS. | EPSFallbackReport |
| FAILED_QOS_UPDATE | Indicates that the invocation/revocation indication included in the mpsAction requested by the NF service consumer has failed. | MPSforDTS |
| FAILED_RESOURCES_ALLOCATION | Indicates that one or more of the SDFs of an Individual Application Session Context are deactivated at the SMF. It also indicates that the resources requested for a particular service information cannot be successfully allocated. | |
| OUT_OF_CREDIT | Out of credit. | IMS_SBI |
| PDU_SESSION_STATUS | Indicates the status of the PDU session (established/terminated). It only applies to notifications to the PCF for a UE as specified in clause 4.2.5.22. | |
| PLMN_CHG | This trigger indicates PLMN change. | |
| QOS_NOTIF | The GBR QoS targets of a SDF are not guaranteed or are guaranteed again. | |
| QOS_MONITORING | Indicates PCF to enable Qos Monitoring for the Service Data Flow. | QoSMonitoring |
| RAN_NAS_CAUSE | This trigger indicates RAN-NAS release cause information is available in the PCF from the SMF.<br>This event does not require explicit subscription. | RAN-NAS-Cause |
| REALLOCATION_OF_CREDIT | Credit has been reallocated after a former out of credit indication. | IMS_SBI, ReallocationOfCredit |
| SAT_CATEGORY_CHG | Indicates that the SMF has detected a change between different satellite backhaul category, or non-satellite backhaul. | SatelliteBackhaul |
| SUCCESSFUL_QOS_UPDATE | Indicates that the invocation/revocation indication included in the mpsAction requested by the NF service consumer has been successful. | MPSforDTS |
| SUCCESSFUL_RESOURCES_ALLOCATION | Indicates that the resources requested for particular service information have been successfully allocated. | |
| TSN_BRIDGE_INFO | 5GS Bridge information (UMIC and/or PMIC(s)) received by the PCF from the SMF. | TimeSensitiveNetworking |
| USAGE_REPORT | Volume and/or time usage for sponsored data connectivity. | SponsoredConnectivity |

### 5.6.3.8 Enumeration: AfNotifMethod

The enumeration "AfNotifMethod" represents the notification methods that can be subscribed by an NF service consumer.

**Table 5.6.3.8-1: Enumeration AfNotifMethod**

| Enumeration value | Description | Applicability |
|---|---|---|
| EVENT_DETECTION | Event is reported whenever the event is met and the subscription is alive. | |
| ONE_TIME | Events are reported once the event is met and are not reported again unless the AF refreshes the subscription. | |
| PERIODIC | The notification is periodically sent. | EnhancedSubscriptionToNotification |

### 5.6.3.9 Enumeration: QosNotifType

The enumeration "QosNotifType" represents the types of reports bound to the notification of QoS Notification Control.

**Table 5.6.3.9-1: Enumeration QosNotifType**

| Enumeration value | Description | Applicability |
|---|---|---|
| GUARANTEED | The QoS targets of one or more SDFs are guaranteed again. | |
| NOT_GUARANTEED | The QoS targets of one or more SDFs are not being guaranteed. | |

### 5.6.3.10 Enumeration: TerminationCause

The enumeration "TerminationCause" represents the types of causes the PCF can report when requesting to the NF service consumer the deletion of the "Individual Application Session Context" resource.

**Table 5.6.3.10-1: Enumeration TerminationCause**

| Enumeration value | Description | Applicability |
|---|---|---|
| ALL_SDF_DEACTIVATION | All the SDFs of an Individual Application Session Context are deactivated at the SMF. It also indicates the case that the all resource allocation of an Individual Application Session Context fails. | |
| PDU_SESSION_TERMINATION | The PDU session is terminated. | |
| PS_TO_CS_HO | Indication of PS to CS handover is received from the SMF. | IMS_SBI |
| INSUFFICIENT_SERVER_RESOURCES | Indicates that the server is overloaded and needs to release the Individual Application Session Context resource. | |
| INSUFFICIENT_QOS_FLOW_RESOURCES | Indicates that the QoS flow has been deactivated due to insufficient QoS flow resources (e.g. the maximum number of QoS flows for the PDU session is reached). | |
| SPONSORED_DATA_CONNECTIVITY_DISALLOWED | Indicates that due to operator policy (e.g. disallowing the UE accessing the sponsored data connectivity in the roaming case) the Individual Application Session Context resource needs to be terminated. | |

### 5.6.3.11 Void

### 5.6.3.12 Enumeration: FlowStatus

The enumeration "FlowStatus" represents whether the service data flow(s) are enabled or disabled.

**Table 5.6.3.12-1: Enumeration FlowStatus**

| Enumeration value | Description | Applicability |
|---|---|---|
| ENABLED-UPLINK | Indicates to enable associated uplink service data flow(s) and to disable associated downlink service data flow(s). | |
| ENABLED-DOWNLINK | Indicates to enable associated downlink service data flow(s) and to disable associated uplink service data flow(s). | |
| ENABLED | Indicates to enable all associated service data flow(s) in both directions. | |
| DISABLED | Indicates to disable all associated service data flow(s) in both directions. | |
| REMOVED | Indicates to remove all associated service data flow(s). The IP Filters for the associated service data flow(s) shall be removed. The associated service data flows shall not be taken into account when deriving the authorized QoS. | |

### 5.6.3.13 Enumeration: MediaComponentResourcesStatus

The enumeration "MediaComponentResourcesStatus" indicates whether the PCC rule(s) related to certain media component are active or inactive.

**Table 5.6.3.13-1: Enumeration MediaComponentResourcesStatus**

| Enumeration value | Description | Applicability |
|---|---|---|
| ACTIVE | Indicates that the PCC rule(s) related to certain media component are active. | |
| INACTIVE | Indicates that the PCC rule(s) related to certain media component are inactive. | |

### 5.6.3.14 Enumeration: FlowUsage

The enumeration "FlowUsage" represents the flow usage of the flows described by a media subcomponent.

**Table 5.6.3.14-1: Enumeration FlowUsage**

| Enumeration value | Description | Applicability |
|---|---|---|
| NO_INFO | This value is used to indicate that no information about the usage of the IP flow is being provided. This is the default value. | |
| RTCP | This value is used to indicate that an IP flow is used to transport RTCP. | |
| AF_SIGNALLING | This value is used to indicate that the IP flow is used to transport AF Signalling Protocols (e.g. SIP/SDP). | IMS_SBI |

NOTE: A NF service consumer can choose not to identify RTCP flows, e.g. in order to avoid that RTCP flows are always enabled by the server.

### 5.6.3.15 Enumeration: RequiredAccessInfo

The enumeration "RequiredAccessInfo" represents the access network information required for the "Individual Application Session Context" resource.

**Table 5.6.3.15-1: Enumeration RequiredAccessInfo**

| Enumeration value | Description | Applicability |
|---|---|---|
| USER_LOCATION | Indicates that the user location information shall be reported. | |
| UE_TIME_ZONE | Indicates that the user timezone shall be reported. | |

### 5.6.3.16 Enumeration: ServiceInfoStatus

The enumeration "ServiceInfoStatus" represents whether the NF service consumer provided service information is preliminary or final.

**Table 5.6.3.16-1: Enumeration ServiceInfoStatus**

| Enumeration value | Description | Applicability |
|---|---|---|
| FINAL | This value is used to indicate that the service has been fully negotiated between the two ends and service information provided is the result of that negotiation. | |
| PRELIMINARY | This value is used to indicate that the service information that the AF has provided to the PCF is preliminary and needs to be further negotiated between the two ends (e.g. for IMS when the service information is sent based on the SDP offer). | |

### 5.6.3.17 Enumeration: SipForkingIndication

The enumeration "SipForkingIndication" describes if several SIP dialogues are related to an "Individual Application Session Context" resource.

**Table 5.6.3.17-1: Enumeration SipForkingIndication**

| Enumeration value | Description | Applicability |
|---|---|---|
| SINGLE_DIALOGUE | This value is used to indicate that the "Individual Application Session Context" resource relates to a single SIP dialogue. This is the default value. | |
| SEVERAL_DIALOGUES | This value is used to indicate that the "Individual Application Session Context" resource relates to several SIP dialogues. | |

### 5.6.3.18 Enumeration: AfRequestedData

The enumeration "AfRequestedData" represents the information the NF service consumer requested to be exposed.

**Table 5.6.3.18-1: Enumeration AfRequestedData**

| Enumeration value | Description | Applicability |
|---|---|---|
| UE_IDENTITY | Indicates that the NF service consumer requests the PCF to provide the 5GS-level UE identities (SUPI, GPSI, PEI) available for that PDU session. | |

### 5.6.3.19 Enumeration: PreemptionControlInformation

The enumeration "PreemptionControlInformation" represents how to perform pre-emption among multiple potential media flow candidates of same priority.

**Table 5.6.3.19-1: Enumeration PreemptionControlInformation**

| Enumeration value | Description | Applicability |
|---|---|---|
| MOST_RECENT | Indicates the most recent added flow is to be pre-empted. | |
| LEAST_RECENT | Indicates the least recent added flow is to be pre-empted. | |
| HIGHEST_BW | Indicates the highest bandwidth flow is to be pre-empted. | |

### 5.6.3.20 Enumeration: PrioritySharingIndicator

The enumeration "PrioritySharingIndicator" represents whether the media component is enabled or disabled for priority sharing with other media components which are assigned the same 5QI and belong to other "Individual Application Session Context" resource bound to the same PDU session.

**Table 5.6.3.20-1: Enumeration PrioritySharingIndicator**

| Enumeration value | Description | Applicability |
|---|---|---|
| ENABLED | Indicates the media component is allowed to share ARP with other medias which are assigned the same 5QI and belong to other "Individual Application Session Context" resources bound to the same PDU session. | |
| DISABLED | Indicates the media component is not allowed to share ARP with other media components. This is the default value when omitted. | |

### 5.6.3.21 Enumeration: PreemptionControlInformationRm

This data type is defined in the same way as the "PreemptionControlInformation" data type but also allows null value (specified as "NullValue" data type).

### 5.6.3.22 Enumeration: MpsAction

The enumeration "MpsAction" indicates the type of action for an MPS request.

**Table 5.6.3.22-1: Enumeration MpsAction**

| Enumeration value | Description | Applicability |
|---|---|---|
| DISABLE_MPS_FOR_DTS | Disable MPS for DTS. | |
| ENABLE_MPS_FOR_DTS | Enable MPS for DTS. | |
| AUTHORIZE_AND_ENABLE_MPS_FOR_DTS | Check the UE's MPS subscription and enable MPS for DTS. | |

### 5.6.3.23 Enumeration: AppDetectionNotifType

The enumeration "AppDetectionNotifType" represents the types of reports bound to the notification of application detection information.

**Table 5.6.3.23-1: Enumeration AppDetectionNotifType**

| Enumeration value | Description | Applicability |
|---|---|---|
| APP_START | The start of application's traffic is detected. | |
| APP_STOP | The stop of application's traffic is detected. | |

### 5.6.3.24 Enumeration: PduSessionStatus

The enumeration "PduSessionStatus" represents the notification is about PDU session established or terminated.

**Table 5.6.3.24-1: Enumeration PduSessionStatus**

| Enumeration value | Description | Applicability |
|---|---|---|
| ESTABLISHED | The PDU session is established. | |
| TERMINATED | The PDU session is terminated. | |

## 5.7 Error handling

### 5.7.1 General

HTTP error handling shall be supported as specified in clause 5.2.4 of 3GPP TS 29.500 [5].

For the Npcf_PolicyAuthorization API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [6].

Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [5] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in table 5.2.7.1-1 of 3GPP TS 29.500 [5].

In addition, the requirements in the following clauses shall apply.

## 5.7.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the Npcf_PolicyAuthorization API.

## 5.7.3 Application Errors

The application errors defined for the Npcf_PolicyAuthorization API are listed in table 5.7.3-1.

**Table 5.7.3-1: Application errors**

| Application Error | HTTP status code | Description |
|---|---|---|
| INVALID_SERVICE_INFORMATION | 400 Bad Request | The HTTP request is rejected because the service information is invalid or insufficient for the PCF to perform the requested action, e.g. invalid media type or invalid QoS reference. (NOTE 1) |
| FILTER_RESTRICTIONS | 400 Bad Request | The HTTP request is rejected because the IP flow descriptions cannot be handled by the PCF because the restrictions defined in clause 5.3.8 of 3GPP TS 29.214 [20] are not observed. (NOTE 1) |
| DUPLICATED_AF_SESSION | 400 Bad Request | The HTTP request is rejected because the new Individual Application Session Context relates to an AF session with another related active Individual Application Session Context, e.g. if the AF provided the same AF charging identifier for this new Individual Application Session Context that is already in use for the other ongoing Individual Application Session Context. (NOTE 2) |
| REQUESTED_SERVICE_NOT_AUTHORIZED | 403 Forbidden | The service information provided in the request is rejected. (NOTE 1) |
| REQUESTED_SERVICE_TEMPORARILY_NOT_AUTHORIZED | 403 Forbidden | The service information provided in the request is temporarily rejected. (NOTE 2) |
| UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY | 403 Forbidden | The request for sponsored data connectivity is not authorized. (NOTE 3) |
| UNAUTHORIZED_NON_EMERGENCY_SESSION | 403 Forbidden | The PCF rejects a new AF session context setup because the session binding function associated a non-Emergency IMS session to a PDU session established to an Emergency DNN. |
| TEMPORARY_NETWORK_FAILURE | 403 Forbidden | The PCF rejects new or modified service information because there is a temporary failure in the access network (e.g. the SGW has failed) |
| APPLICATION_SESSION_CONTEXT_NOT_FOUND | 404 Not Found | The HTTP request is rejected because the specified Individual Application Session Context does not exist. (NOTE 4) |
| PDU_SESSION_NOT_AVAILABLE | 500 Internal Server Error | The PCF failed in executing session binding. (NOTE 5) |

NOTE 1: This application error is included in the response to the POST request (see clauses 4.2.2.2 and 4.2.2.5) and to the PATCH request (see clauses 4.2.3.2 and 4.2.3.5).
NOTE 2: This application error is included in the response to the POST request (see clause 4.2.2.2) and to the PATCH request (see clause 4.2.3.2).
NOTE 3: This application error is included in the response to the POST request (see clause 4.2.2.5) and to the PATCH request (see clause 4.2.3.5).
NOTE 4: This application error is included in the responses to the GET, PATCH and delete custom operation requests to the Individual Application Session Context resource, and to the PUT and DELETE requests to the Events Subscription resource.
NOTE 5: This application error is included in the response to the POST request (see clauses 4.2.2.2, 4.2.6.3 and 4.2.2.27).
NOTE 6: Including a "ProblemDetails" data structure with the "cause" attribute in the HTTP response is optional unless explicitly mandated in the service operation clauses.

## 5.8 Feature negotiation

The optional features in table 5.8-1 are defined for the Npcf_PolicyAuthorization API. They shall be negotiated using the extensibility mechanism defined in clause 6.6.2 of 3GPP TS 29.500 [5].

When requesting the PCF to create an Individual Application Session Context resource the NF service consumer shall indicate the optional features the NF service consumer supports for the Npcf_PolicyAuthorization service by including the "suppFeat" attribute in the "AppSessionContextReqData" data type of the HTTP POST request.

The PCF shall determine the supported features for the created Individual Application Session Context resource as specified in clause 6.6.2 of 3GPP TS 29.500 [5]. The PCF shall indicate the supported features in the HTTP response confirming the creation of the Individual Application Session Context resource by including the "suppFeat" attribute in the "AppSessionContextRespData" data type.

**Table 5.8-1: Supported Features**

| Feature number | Feature Name | Description |
|---|---|---|
| 1 | InfluenceOnTrafficRouting | Indicates support of Application Function influence on traffic routing. If the PCF supports this feature, the NF service consumer may influence SMF routing to applications or subscribe to notifications of UP path management for the traffic flows of an active PDU session. |
| 2 | SponsoredConnectivity | Indicates support of sponsored data connectivity. If the PCF supports this feature, the NF service consumer may provide sponsored data connectivity to the SUPI. |
| 3 | MediaComponentVersioning | Indicates the support of the media component versioning. |
| 4 | URLLC | Indicates support of Ultra-Reliable Low-Latency Communication (URLLC) requirements, i.e. AF application relocation acknowledgement and UE address(es) preservation. The InfluenceOnTrafficRouting feature shall be supported in order to support this feature. |
| 5 | IMS_SBI | Indicates support of the communication with the 5GC IMS NF service consumer via Service Based Interfaces. |
| 6 | NetLoc | Indicates the support of access network information reporting. |
| 7 | ProvAFsignalFlow | This indicates support for the feature of provisioning of AF signalling flow information as described in clauses 4.2.2.16 and 4.2.3.17. If the PCF supports this feature the NF service consumer may provision AF signalling flow information.<br><br>NOTE: This feature is used by the IMS Restoration Procedures to provide to the SMF the address of the P-CSCF selected by the UE, refer to 3GPP TS 23.380 [39].<br><br>The IMS_SBI feature shall be supported in order to support this feature. |
| 8 | ResourceSharing | This feature indicates the support of resource sharing across several "Individual Application Session Context" resources. The IMS_SBI feature shall be supported in order to support this feature. |
| 9 | MCPTT | This feature indicates the support of Mission Critical Push To Talk services as described in 3GPP TS 24.379 [41]. |
| 10 | MCVideo | This feature indicates the support of Mission Critical Video services as described in 3GPP TS 24.281 [43]. |
| 11 | PrioritySharing | This feature indicates that Priority Sharing is supported as described in 3GPP TS 23.503 [4], clause 6.1.3.15. |
| 12 | MCPTT-Preemption | This feature indicates the support of service pre-emption based on the information provided by the NF service consumer. It requires that both PrioritySharing and MCPTT features are also supported. |
| 13 | MacAddressRange | Indicates the support of a set of MAC addresses with a specific range in the traffic filter. |
| 14 | RAN-NAS-Cause | This feature indicates the support for the release cause code information from the access network. |
| 15 | EnhancedSubscriptionToNotification | Indicates the support of:<br>- Subscription to periodic notifications.<br>- Definition of a waiting time between the reporting of two event triggered events.<br>- Indication of whether the event has to be reported at PDU Session termination.<br>- Notification Correlation Id for a subscription to an event. |
| 16 | QoSMonitoring | Indicates the support of QoS monitoring information. This feature requires the support of the EnhancedSubscriptionToNotification feature. |
| 17 | AuthorizationWithRequiredQoS | Indicates support of policy authorization for the AF session with required QoS. |
| 18 | TimeSensitiveNetworking | Indicates that the 5G System is integrated within the external network as a TSN bridge. |
| 19 | PCSCF-Restoration-Enhancement | This feature indicates support of P-CSCF Restoration Enhancement. It is used for the PCF and the P-CSCF to indicate if they support P-CSCF Restoration Enhancement. |
| 20 | CHEM | This feature indicates the support of Coverage and Handover Enhancements for Media (CHEM). |

| Feature number | Feature Name | Description |
|---|---|---|
| 21 | FLUS | This feature indicates the support of FLUS functionality as described in 3GPP TS 26.238 [51]. |
| 22 | EPSFallbackReport | This feature indicates the support of the report of EPS Fallback as defined in clauses 4.2.2.30, 4.2.3.29 and 4.2.5.15. |
| 23 | ATSSS | Indicates the support of the report of the multiple access types of a MA PDU session. |
| 24 | QoSHint | This feature indicates the support of specific QoS hint parameters as described in 3GPP TS 26.114 [30], clause 6.2.10. |
| 25 | ReallocationOfCredit | This feature indicates the support of notifications of reallocation of credits events. It requires the support of IMS_SBI feature. |
| 26 | ES3XX | Extended Support for 3xx redirections. This feature indicates the support of redirection for any service operation, according to Stateless NF procedures as specified in clauses 6.5.3.2 and 6.5.3.3 of 3GPP TS 29.500 [5] and according to HTTP redirection principles for indirect communication, as specified in clause 6.10.9 of 3GPP TS 29.500 [5]. |
| 27 | DisableUENotification | Indicates the support of disabling QoS flow parameters signalling to the UE when the SMF is notified by the NG-RAN of changes in the fulfilled QoS situation. This feature requires that the AuthorizationWithRequiredQoS featute is also supported. |
| 28 | PatchCorrection | Indicates support of the correction to the PATCH method:<br>When this feature is not supported, the interoperability between a NF service consumer and the PCF can only be ensured when it is not required the update of the Individual Application Session Context resource. |
| 29 | MPSforDTS | Indicates support for MPS for DTS as described in clauses 4.2.2.12.2 and 4.2.3.12. |
| 30 | ApplicationDetectionEvents | This feature indicates the support of the subscription to notifications of the detection of the start and stop of an application's traffic. |
| 31 | TimeSensitiveCommunication | Indicates that the 5G System is integrated within the external network as a TSC user plane node to enable the Time Sensitive Communications and Time Synchronization. This feature requires that the TimeSensitiveNetworking feature is also supported. |
| 32 | ExposureToEAS | This feature indicates the support of the indication of direct event notification of QoS monitoring events from the UPF to the Local NEF or AF in 5GC. This indication requires that the QoSMonitoring feature is supported. |
| 33 | SatelliteBackhaul | Indicates the support of the report of the satellite or non-satellite backhaul category of the PDU session. |
| 34 | RoutingReqOutcome | Indicates the support of:<br>- the report of UP path change failures; and<br>- the indication of whether AF routing requirements are applied.<br>It requires the support of InfluenceOnTrafficRouting feature. |
| 35 | EASDiscovery | This feature indicates the support of EAS (re)discovery. |
| 36 | AltSerReqsWithIndQoS | Indicates the support of provisioning Alternative Service Requirements with individual QoS parameters. This feature requires that the AuthorizationWithRequiredQoS feature is also supported. |
| 37 | SimultConnectivity | This feature indicates the support of the indication of temporary simultaneous connectivity over source and target PSA at edge relocation. This indication requires that the InfluenceOnTrafficRouting feature is supported. |
| 38 | EASIPreplacement | This feature indicates the support of provisioning of EAS IP replacement info. This support requires that InfluenceOnTrafficRouting feature is also supported |
| 39 | AccNetChargId_String | This feature indicates the support of long character strings as access network charging identifier. |
| 40 | WLAN_Location | This feature indicates the support of the report of the WLAN location information received from the ePDG/EPC, if available. It is only applicable to EPS interworking scenarios as described in 3GPP TS 29.512 [8], Annex B. |

| Feature number | Feature Name | Description |
|---|---|---|
| 41 | AF_latency | This feature indicates support for edge relocation considering user plane latency. |
| 44 | PacketDelayFailureReport | Indicates the support of packet delay failure report as part of QoS Monitoring procedures. This feature requires that QoSMonitoring feature is supported. |

## 5.9 Security

As indicated in 3GPP TS 33.501 [25] and 3GPP TS 29.500 [5], the access to the Npcf_PolicyAuthorization API, based on local configuration, may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [26]), using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [27]) plays the role of the authorization server.

If OAuth2 authorization is used, an NF service consumer, prior to consuming services offered by the Npcf_PolicyAuthorization API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [27], clause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF service consumer used for discovering the Npcf_PolicyAuthorization service.

The Npcf_PolicyAuthorization API defines a single scope "npcf-policyauthorization" for OAuth2 authorization (as specified in 3GPP TS 33.501 [25]) for the entire API, and it does not define any additional scopes at resource or operation level.

# Annex A (normative): OpenAPI specification

## A.1 General

The present Annex contains an OpenAPI [11] specification of HTTP messages and content bodies used by the Npcf_PolicyAuthorization API.

This Annex shall take precedence when being discrepant to other parts of the specification with respect to the encoding of information elements and methods within the API.

NOTE: The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

Informative copies of the OpenAPI specification file contained in this 3GPP Technical Specification are available on a Git-based repository that uses the GitLab software version control system (see clause 5B of the 3GPP TR 21.900 [28] and clause 5.3.1 of the 3GPP TS 29.501 [6] for further information).

## A.2 Npcf_PolicyAuthorization API

```
openapi: 3.0.0
info:
  title: Npcf_PolicyAuthorization Service API
  version: 1.2.3
  description: |
    PCF Policy Authorization Service.
    © 2023, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.514 V17.9.0; 5G System; Policy Authorization Service; Stage 3.
  url: 'https://www.3gpp.org/ftp/Specs/archive/29_series/29.514/'
#
servers:
  - url: '{apiRoot}/npcf-policyauthorization/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501

security:
  - {}
  - oAuth2ClientCredentials:
    - npcf-policyauthorization
paths:
  /app-sessions:
    post:
      summary: Creates a new Individual Application Session Context resource
      operationId: PostAppSessions
      tags:
        - Application Sessions (Collection)
      requestBody:
        description: Contains the information for the creation the resource.
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/AppSessionContext'
      responses:
        '201':
          description: Successful creation of the resource
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AppSessionContext'
```

```
          headers:
            Location:
              description: >
                Contains the URI of the created individual application session context resource,
                according to the structure
                {apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}
                or the URI of the created events subscription sub-resource,
                according to the structure
                {apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-
subscription}
              required: true
              schema:
                type: string
        '303':
          description: See Other. The result of the HTTP POST request would be equivalent to the
existing Application Session Context.
          headers:
            Location:
              description: Contains the URI of the existing individual Application Session Context
resource.
              required: true
              schema:
                type: string
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          description: Forbidden
          content:
            application/problem+json:
              schema:
                $ref: '#/components/schemas/ExtendedProblemDetails'
          headers:
            Retry-After:
              description: >
                Indicates the time the AF has to wait before making a new request. It can be a
                non-negative integer (decimal number) indicating the number of seconds the AF
                has to wait before making a new request or an HTTP-date after which the AF can
                retry a new request.
              schema:
                anyOf:
                  - type: integer
                  - type: string
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      callbacks:
        terminationRequest:
          '{$request.body#/ascReqData/notifUri}/terminate':
            post:
              requestBody:
                description: Request of the termination of the Individual Application Session
Context.
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/TerminationInfo'
              responses:
                '204':
                  description: The receipt of the notification is acknowledged.
                '307':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/307'
                '308':
```

```
            $ref: 'TS29571_CommonData.yaml#/components/responses/308'
          '400':
            $ref: 'TS29571_CommonData.yaml#/components/responses/400'
          '401':
            $ref: 'TS29571_CommonData.yaml#/components/responses/401'
          '403':
            $ref: 'TS29571_CommonData.yaml#/components/responses/403'
          '404':
            $ref: 'TS29571_CommonData.yaml#/components/responses/404'
          '411':
            $ref: 'TS29571_CommonData.yaml#/components/responses/411'
          '413':
            $ref: 'TS29571_CommonData.yaml#/components/responses/413'
          '415':
            $ref: 'TS29571_CommonData.yaml#/components/responses/415'
          '429':
            $ref: 'TS29571_CommonData.yaml#/components/responses/429'
          '500':
            $ref: 'TS29571_CommonData.yaml#/components/responses/500'
          '503':
            $ref: 'TS29571_CommonData.yaml#/components/responses/503'
          default:
            $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  eventNotification:
    '{$request.body#/ascReqData/evSubsc/notifUri}/notify':
      post:
        requestBody:
          description: Notification of an event occurrence in the PCF.
          required: true
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/EventsNotification'
        responses:
          '204':
            description: The receipt of the notification is acknowledged.
          '307':
            $ref: 'TS29571_CommonData.yaml#/components/responses/307'
          '308':
            $ref: 'TS29571_CommonData.yaml#/components/responses/308'
          '400':
            $ref: 'TS29571_CommonData.yaml#/components/responses/400'
          '401':
            $ref: 'TS29571_CommonData.yaml#/components/responses/401'
          '403':
            $ref: 'TS29571_CommonData.yaml#/components/responses/403'
          '404':
            $ref: 'TS29571_CommonData.yaml#/components/responses/404'
          '411':
            $ref: 'TS29571_CommonData.yaml#/components/responses/411'
          '413':
            $ref: 'TS29571_CommonData.yaml#/components/responses/413'
          '415':
            $ref: 'TS29571_CommonData.yaml#/components/responses/415'
          '429':
            $ref: 'TS29571_CommonData.yaml#/components/responses/429'
          '500':
            $ref: 'TS29571_CommonData.yaml#/components/responses/500'
          '503':
            $ref: 'TS29571_CommonData.yaml#/components/responses/503'
          default:
            $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  detected5GsBridgeForPduSession:
    '{$request.body#/ascReqData/evSubsc/notifUri}/new-bridge':
      post:
        requestBody:
          description: Notification of a new TSC user plane node detected in the PCF.
          required: true
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/PduSessionTsnBridge'
        responses:
          '204':
            description: The receipt of the notification is acknowledged.
          '307':
            $ref: 'TS29571_CommonData.yaml#/components/responses/307'
          '308':
```

```
                $ref: 'TS29571_CommonData.yaml#/components/responses/308'
              '400':
                $ref: 'TS29571_CommonData.yaml#/components/responses/400'
              '401':
                $ref: 'TS29571_CommonData.yaml#/components/responses/401'
              '403':
                $ref: 'TS29571_CommonData.yaml#/components/responses/403'
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '411':
                $ref: 'TS29571_CommonData.yaml#/components/responses/411'
              '413':
                $ref: 'TS29571_CommonData.yaml#/components/responses/413'
              '415':
                $ref: 'TS29571_CommonData.yaml#/components/responses/415'
              '429':
                $ref: 'TS29571_CommonData.yaml#/components/responses/429'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              '503':
                $ref: 'TS29571_CommonData.yaml#/components/responses/503'
              default:
                $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      eventNotificationPduSession:
        '{$request.body#/ascReqData/evSubsc/notifUri}/pdu-session':
          post:
            requestBody:
              description: Notification of PDU session established or terminated.
              required: true
              content:
                application/json:
                  schema:
                    $ref: '#/components/schemas/PduSessionEventNotification'
            responses:
              '204':
                description: The receipt of the notification is acknowledged.
              '307':
                $ref: 'TS29571_CommonData.yaml#/components/responses/307'
              '308':
                $ref: 'TS29571_CommonData.yaml#/components/responses/308'
              '400':
                $ref: 'TS29571_CommonData.yaml#/components/responses/400'
              '401':
                $ref: 'TS29571_CommonData.yaml#/components/responses/401'
              '403':
                $ref: 'TS29571_CommonData.yaml#/components/responses/403'
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '411':
                $ref: 'TS29571_CommonData.yaml#/components/responses/411'
              '413':
                $ref: 'TS29571_CommonData.yaml#/components/responses/413'
              '415':
                $ref: 'TS29571_CommonData.yaml#/components/responses/415'
              '429':
                $ref: 'TS29571_CommonData.yaml#/components/responses/429'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              '503':
                $ref: 'TS29571_CommonData.yaml#/components/responses/503'
              default:
                $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  /app-sessions/pcscf-restoration:
    post:
      summary: "Indicates P-CSCF restoration and does not create an Individual Application Session
Context"
      operationId: PcscfRestoration
      tags:
        - PCSCF Restoration Indication
      requestBody:
        description: PCSCF Restoration Indication.
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/PcscfRestorationRequestData'
      responses:
        '204':
```

```
          description: The deletion is confirmed without returning additional data.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
#
  /app-sessions/{appSessionId}:
    get:
      summary: "Reads an existing Individual Application Session Context"
      operationId: GetAppSession
      tags:
        - Individual Application Session Context (Document)
      parameters:
        - name: appSessionId
          description: String identifying the resource.
          in: path
          required: true
          schema:
            type: string
      responses:
        '200':
          description: A representation of the resource is returned.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AppSessionContext'
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29571_CommonData.yaml#/components/responses/406'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
    patch:
      summary: "Modifies an existing Individual Application Session Context"
      operationId: ModAppSession
      tags:
        - Individual Application Session Context (Document)
      parameters:
        - name: appSessionId
          description: String identifying the resource.
```

```
          in: path
          required: true
          schema:
            type: string
      requestBody:
        description: Modification of the resource.
        required: true
        content:
          application/merge-patch+json:
            schema:
              $ref: '#/components/schemas/AppSessionContextUpdateDataPatch'
      responses:
        '200':
          description: Successful modification of the resource and a representation of that resource
is returned.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AppSessionContext'
        '204':
          description: The successful modification.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          description: Forbidden
          content:
            application/problem+json:
              schema:
                $ref: '#/components/schemas/ExtendedProblemDetails'
          headers:
            Retry-After:
              description: >
                Indicates the time the AF has to wait before making a new request. It can be a
                non-negative integer (decimal number) indicating the number of seconds the AF has
                to wait before making a new request or an HTTP-date after which the AF can retry
                a new request.
              schema:
                anyOf:
                  - type: integer
                  - type: string
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      callbacks:
        eventNotification:
          '{$request.body#/ascReqData/evSubsc/notifUri}/notify':
            post:
              requestBody:
                description: Notification of an event occurrence in the PCF.
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/EventsNotification'
              responses:
                '204':
                  description: The receipt of the notification is acknowledged
                '307':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/307'
```

```
                '308':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/308'
                '400':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/400'
                '401':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/401'
                '403':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/403'
                '404':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/404'
                '411':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/411'
                '413':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/413'
                '415':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/415'
                '429':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/429'
                '500':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/500'
                '503':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/503'
                default:
                  $ref: 'TS29571_CommonData.yaml#/components/responses/default'
#
#
  /app-sessions/{appSessionId}/delete:
    post:
      summary: "Deletes an existing Individual Application Session Context"
      operationId: DeleteAppSession
      tags:
        - Individual Application Session Context (Document)
      parameters:
        - name: appSessionId
          description: String identifying the Individual Application Session Context resource.
          in: path
          required: true
          schema:
            type: string
      requestBody:
        description: Deletion of the Individual Application Session Context resource, req
notification.
        required: false
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EventsSubscReqData'
      responses:
        '200':
          description: The deletion of the resource is confirmed and a resource is returned.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/AppSessionContext'
        '204':
          description: The deletion is confirmed without returning additional data.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
```

```
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
#
  /app-sessions/{appSessionId}/events-subscription:
    put:
      summary: "creates or modifies an Events Subscription subresource"
      operationId: updateEventsSubsc
      tags:
        - Events Subscription (Document)
      parameters:
        - name: appSessionId
          description: String identifying the Events Subscription resource.
          in: path
          required: true
          schema:
            type: string
      requestBody:
        description: Creation or modification of an Events Subscription resource.
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/EventsSubscReqData'
      responses:
        '201':
          description: The creation of the Events Subscription resource is confirmed and its
representation is returned.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/EventsSubscPutData'
          headers:
            Location:
              description: >
                Contains the URI of the created Events Subscription resource,
                according to the structure
                {apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-
subscription}
              required: true
              schema:
                type: string
        '200':
          description: The modification of the Events Subscription resource is confirmed its
representation is returned.
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/EventsSubscPutData'
        '204':
          description: The modification of the Events Subscription subresource is confirmed without
returning additional data.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
```

```
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      callbacks:
        eventNotification:
          '{$request.body#/notifUri}/notify':
           post:
             requestBody:
               description: Contains the information for the notification of an event occurrence in
the PCF.
               required: true
               content:
                 application/json:
                   schema:
                     $ref: '#/components/schemas/EventsNotification'
             responses:
               '204':
                 description: The receipt of the notification is acknowledged.
               '307':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/307'
               '308':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/308'
               '400':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/400'
               '401':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/401'
               '403':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/403'
               '404':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/404'
               '411':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/411'
               '413':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/413'
               '415':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/415'
               '429':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/429'
               '500':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/500'
               '503':
                 $ref: 'TS29571_CommonData.yaml#/components/responses/503'
               default:
                 $ref: 'TS29571_CommonData.yaml#/components/responses/default'
    delete:
      summary: deletes the Events Subscription subresource
      operationId: DeleteEventsSubsc
      tags:
        - Events Subscription (Document)
      parameters:
        - name: appSessionId
          description: String identifying the Individual Application Session Context resource.
          in: path
          required: true
          schema:
            type: string
      responses:
        '204':
          description: The deletion of the of the Events Subscription sub-resource is confirmed
without returning additional data.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
```

```
components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            npcf-policyauthorization: Access to the Npcf_PolicyAuthorization API
  schemas:
    AppSessionContext:
      description: Represents an Individual Application Session Context resource.
      type: object
      properties:
        ascReqData:
          $ref: '#/components/schemas/AppSessionContextReqData'
        ascRespData:
          $ref: '#/components/schemas/AppSessionContextRespData'
        evsNotif:
          $ref: '#/components/schemas/EventsNotification'
    AppSessionContextReqData:
      description: Identifies the service requirements of an Individual Application Session Context.
      type: object
      required:
        - notifUri
        - suppFeat
      oneOf:
        - required: [ueIpv4]
        - required: [ueIpv6]
        - required: [ueMac]
      properties:
        afAppId:
          $ref: '#/components/schemas/AfAppId'
        afChargId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ApplicationChargingId'
        afReqData:
          $ref: '#/components/schemas/AfRequestedData'
        afRoutReq:
          $ref: '#/components/schemas/AfRoutingRequirement'
        aspId:
          $ref: '#/components/schemas/AspId'
        bdtRefId:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/BdtReferenceId'
        dnn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        evSubsc:
          $ref: '#/components/schemas/EventsSubscReqData'
        mcpttId:
          description: Indication of MCPTT service request.
          type: string
        mcVideoId:
          description: Indication of MCVideo service request.
          type: string
        medComponents:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MediaComponent'
          minProperties: 1
          description: Contains media component information. The key of the map is the medCompN
attribute.
        ipDomain:
          type: string
        mpsAction:
          $ref: '#/components/schemas/MpsAction'
        mpsId:
          description: Indication of MPS service request.
          type: string
        mcsId:
          description: Indication of MCS service request.
          type: string
        preemptControlInfo:
          $ref: '#/components/schemas/PreemptionControlInformation'
        resPrio:
          $ref: '#/components/schemas/ReservPriority'
        servInfStatus:
          $ref: '#/components/schemas/ServiceInfoStatus'
        notifUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
```

```
        servUrn:
          $ref: '#/components/schemas/ServiceUrn'
        sliceInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        sponId:
          $ref: '#/components/schemas/SponId'
        sponStatus:
          $ref: '#/components/schemas/SponsoringStatus'
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
        ueIpv4:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ueIpv6:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
        ueMac:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
        tsnBridgeManCont:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/BridgeManagementContainer'
        tsnPortManContDstt:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/PortManagementContainer'
        tsnPortManContNwtts:
          type: array
          items:
            $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/PortManagementContainer'
          minItems: 1
    AppSessionContextRespData:
      description: Describes the authorization data of an Individual Application Session Context
created by the PCF.
      type: object
      properties:
        servAuthInfo:
          $ref: '#/components/schemas/ServAuthInfo'
        ueIds:
          type: array
          items:
            $ref: '#/components/schemas/UeIdentityInfo'
          minItems: 1
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
    AppSessionContextUpdateDataPatch:
      description: Identifies the modifications to an Individual Application Session Context and/or
the modifications to the sub-resource Events Subscription.
      type: object
      properties:
        ascReqData:
          $ref: '#/components/schemas/AppSessionContextUpdateData'
    AppSessionContextUpdateData:
      description: >
        Identifies the modifications to the "ascReqData" property of an Individual Application
        Session Context which may include the modifications to the sub-resource Events Subscription.
      type: object
      properties:
        afAppId:
          $ref: '#/components/schemas/AfAppId'
        afRoutReq:
          $ref: '#/components/schemas/AfRoutingRequirementRm'
        aspId:
          $ref: '#/components/schemas/AspId'
        bdtRefId:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/BdtReferenceId'
        evSubsc:
          $ref: '#/components/schemas/EventsSubscReqDataRm'
        mcpttId:
          description: Indication of MCPTT service request.
          type: string
        mcVideoId:
          description: Indication of modification of MCVideo service.
          type: string
        medComponents:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MediaComponentRm'
          minProperties: 1
```

```
          description: Contains media component information. The key of the map is the medCompN
attribute.
        mpsAction:
          $ref: '#/components/schemas/MpsAction'
        mpsId:
          description: Indication of MPS service request.
          type: string
        mcsId:
          description: Indication of MCS service request.
          type: string
        preemptControlInfo:
          $ref: '#/components/schemas/PreemptionControlInformationRm'
        resPrio:
          $ref: '#/components/schemas/ReservPriority'
        servInfStatus:
          $ref: '#/components/schemas/ServiceInfoStatus'
        sipForkInd:
          $ref: '#/components/schemas/SipForkingIndication'
        sponId:
          $ref: '#/components/schemas/SponId'
        sponStatus:
          $ref: '#/components/schemas/SponsoringStatus'
        tsnBridgeManCont:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/BridgeManagementContainer'
        tsnPortManContDstt:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/PortManagementContainer'
        tsnPortManContNwtts:
          type: array
          items:
            $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/PortManagementContainer'
          minItems: 1
    EventsSubscReqData:
      description: Identifies the events the application subscribes to.
      type: object
      required:
        - events
      properties:
        events:
          type: array
          items:
            $ref: '#/components/schemas/AfEventSubscription'
          minItems: 1
        notifUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        reqQosMonParams:
          type: array
          items:
            $ref:
'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/RequestedQosMonitoringParameter'
          minItems: 1
        qosMon:
          $ref: '#/components/schemas/QosMonitoringInformation'
        reqAnis:
          type: array
          items:
            $ref: '#/components/schemas/RequiredAccessInfo'
          minItems: 1
        usgThres:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/UsageThreshold'
        notifCorreId:
          type: string
        afAppIds:
          type: array
          items:
            $ref: '#/components/schemas/AfAppId'
          minItems: 1
        directNotifInd:
          type: boolean
    EventsSubscReqDataRm:
      description: This data type is defined in the same way as the EventsSubscReqData data type,
but with the OpenAPI nullable property set to true.
      type: object
      required:
        - events
      properties:
        events:
          type: array
          items:
```

```
            $ref: '#/components/schemas/AfEventSubscription'
          notifUri:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
          reqQosMonParams:
            type: array
            items:
              $ref:
'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/RequestedQosMonitoringParameter'
            minItems: 1
          qosMon:
            $ref: '#/components/schemas/QosMonitoringInformationRm'
          reqAnis:
            type: array
            items:
              $ref: '#/components/schemas/RequiredAccessInfo'
            minItems: 1
          usgThres:
            $ref: 'TS29122_CommonData.yaml#/components/schemas/UsageThresholdRm'
          notifCorreId:
            type: string
          directNotifInd:
            type: boolean
            nullable: true
        nullable: true
      MediaComponent:
        description: Identifies a media component.
        type: object
        required:
          - medCompN
        properties:
          afAppId:
            $ref: '#/components/schemas/AfAppId'
          afRoutReq:
            $ref: '#/components/schemas/AfRoutingRequirement'
          qosReference:
            type: string
          disUeNotif:
            type: boolean
          altSerReqs:
            type: array
            items:
              type: string
            minItems: 1
          altSerReqsData:
            type: array
            items:
              $ref: '#/components/schemas/AlternativeServiceRequirementsData'
            minItems: 1
            description: Contains alternative service requirements that include individual QoS
parameter sets.
          contVer:
            $ref: '#/components/schemas/ContentVersion'
          codecs:
            type: array
            items:
              $ref: '#/components/schemas/CodecData'
            minItems: 1
            maxItems: 2
          desMaxLatency:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Float'
          desMaxLoss:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Float'
          flusId:
            type: string
          fStatus:
            $ref: '#/components/schemas/FlowStatus'
          marBwDl:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
          marBwUl:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
          maxPacketLossRateDl:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketLossRateRm'
          maxPacketLossRateUl:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketLossRateRm'
          maxSuppBwDl:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
          maxSuppBwUl:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
```

```
        medCompN:
          type: integer
        medSubComps:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MediaSubComponent'
          minProperties: 1
          description: Contains the requested bitrate and filters for the set of service data flows
identified by their common flow identifier. The key of the map is the fNum attribute.
        medType:
          $ref: '#/components/schemas/MediaType'
        minDesBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        minDesBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        mirBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        mirBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        preemptCap:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PreemptionCapability'
        preemptVuln:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PreemptionVulnerability'
        prioSharingInd:
          $ref: '#/components/schemas/PrioritySharingIndicator'
        resPrio:
          $ref: '#/components/schemas/ReservPriority'
        rrBw:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        rsBw:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        sharingKeyDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uint32'
        sharingKeyUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uint32'
        tsnQos:
          $ref: '#/components/schemas/TsnQosContainer'
        tscaiInputDl:
          $ref: '#/components/schemas/TscaiInputContainer'
        tscaiInputUl:
          $ref: '#/components/schemas/TscaiInputContainer'
        tscaiTimeDom:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
    MediaComponentRm:
      description: This data type is defined in the same way as the MediaComponent data type, but
with the OpenAPI nullable property set to true.
      type: object
      required:
        - medCompN
      properties:
        afAppId:
          $ref: '#/components/schemas/AfAppId'
        afRoutReq:
          $ref: '#/components/schemas/AfRoutingRequirementRm'
        qosReference:
          type: string
          nullable: true
        altSerReqs:
          type: array
          items:
            type: string
          minItems: 1
          nullable: true
        altSerReqsData:
          type: array
          items:
            $ref: '#/components/schemas/AlternativeServiceRequirementsData'
          minItems: 1
          description: Contains removable alternative service requirements that include individual
QoS parameter sets.
          nullable: true
        disUeNotif:
          type: boolean
        contVer:
          $ref: '#/components/schemas/ContentVersion'
        codecs:
          type: array
          items:
```

```
            $ref: '#/components/schemas/CodecData'
          minItems: 1
          maxItems: 2
        desMaxLatency:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/FloatRm'
        desMaxLoss:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/FloatRm'
        flusId:
          type: string
          nullable: true
        fStatus:
          $ref: '#/components/schemas/FlowStatus'
        marBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        marBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        maxPacketLossRateDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketLossRateRm'
        maxPacketLossRateUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketLossRateRm'
        maxSuppBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        maxSuppBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        medCompN:
          type: integer
        medSubComps:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MediaSubComponentRm'
          minProperties: 1
          description: Contains the requested bitrate and filters for the set of service data flows
identified by their common flow identifier. The key of the map is the fNum attribute.
        medType:
          $ref: '#/components/schemas/MediaType'
        minDesBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        minDesBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        mirBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        mirBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        preemptCap:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PreemptionCapabilityRm'
        preemptVuln:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PreemptionVulnerabilityRm'
        prioSharingInd:
          $ref: '#/components/schemas/PrioritySharingIndicator'
        resPrio:
          $ref: '#/components/schemas/ReservPriority'
        rrBw:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        rsBw:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        sharingKeyDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uint32Rm'
        sharingKeyUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uint32Rm'
        tsnQos:
          $ref: '#/components/schemas/TsnQosContainerRm'
        tscaiInputDl:
          $ref: '#/components/schemas/TscaiInputContainer'
        tscaiInputUl:
          $ref: '#/components/schemas/TscaiInputContainer'
        tscaiTimeDom:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
      nullable: true
    MediaSubComponent:
      description: Identifies a media subcomponent.
      type: object
      required:
        - fNum
      properties:
        afSigProtocol:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/AfSigProtocol'
        ethfDescs:
          type: array
```

```
        items:
          $ref: '#/components/schemas/EthFlowDescription'
        minItems: 1
        maxItems: 2
      fNum:
        type: integer
      fDescs:
        type: array
        items:
          $ref: '#/components/schemas/FlowDescription'
        minItems: 1
        maxItems: 2
      fStatus:
        $ref: '#/components/schemas/FlowStatus'
      marBwDl:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
      marBwUl:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
      tosTrCl:
        $ref: '#/components/schemas/TosTrafficClass'
      flowUsage:
        $ref: '#/components/schemas/FlowUsage'
  MediaSubComponentRm:
    description: >
      This data type is defined in the same way as the MediaSubComponent data type, but with the
      OpenAPI nullable property set to true. Removable attributes marBwDl and marBwUl are defined
      with the corresponding removable data type.
    type: object
    required:
      - fNum
    properties:
      afSigProtocol:
        $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/AfSigProtocol'
      ethfDescs:
        type: array
        items:
          $ref: '#/components/schemas/EthFlowDescription'
        minItems: 1
        maxItems: 2
        nullable: true
      fNum:
        type: integer
      fDescs:
        type: array
        items:
          $ref: '#/components/schemas/FlowDescription'
        minItems: 1
        maxItems: 2
        nullable: true
      fStatus:
        $ref: '#/components/schemas/FlowStatus'
      marBwDl:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
      marBwUl:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
      tosTrCl:
        $ref: '#/components/schemas/TosTrafficClassRm'
      flowUsage:
        $ref: '#/components/schemas/FlowUsage'
    nullable: true
  EventsNotification:
    description: Describes the notification of a matched event.
    type: object
    required:
      - evSubsUri
      - evNotifs
    properties:
      adReports:
        type: array
        items:
          $ref: '#/components/schemas/AppDetectionReport'
        minItems: 1
        description: Includes the detected application report.
      accessType:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
      addAccessInfo:
        $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/AdditionalAccessInfo'
      relAccessInfo:
```

```
        $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/AdditionalAccessInfo'
      anChargAddr:
        $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/AccNetChargingAddress'
      anChargIds:
        type: array
        items:
          $ref: '#/components/schemas/AccessNetChargingIdentifier'
        minItems: 1
      anGwAddr:
        $ref: '#/components/schemas/AnGwAddress'
      evSubsUri:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
      evNotifs:
        type: array
        items:
          $ref: '#/components/schemas/AfEventNotification'
        minItems: 1
      failedResourcAllocReports:
        type: array
        items:
          $ref: '#/components/schemas/ResourcesAllocationInfo'
        minItems: 1
      succResourcAllocReports:
        type: array
        items:
          $ref: '#/components/schemas/ResourcesAllocationInfo'
        minItems: 1
      noNetLocSupp:
        $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/NetLocAccessSupport'
      outOfCredReports:
        type: array
        items:
          $ref: '#/components/schemas/OutOfCreditInformation'
        minItems: 1
      plmnId:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnIdNid'
      qncReports:
        type: array
        items:
          $ref: '#/components/schemas/QosNotificationControlInfo'
        minItems: 1
      qosMonReports:
        type: array
        items:
          $ref: '#/components/schemas/QosMonitoringReport'
        minItems: 1
      ranNasRelCauses:
        type: array
        items:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/RanNasRelCause'
        minItems: 1
        description: Contains the RAN and/or NAS release cause.
      ratType:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
      satBackhaulCategory:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SatelliteBackhaulCategory'
      ueLoc:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
      ueLocTime:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
      ueTimeZone:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
      usgRep:
        $ref: 'TS29122_CommonData.yaml#/components/schemas/AccumulatedUsage'
      tsnBridgeManCont:
        $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/BridgeManagementContainer'
      tsnPortManContDstt:
        $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/PortManagementContainer'
      tsnPortManContNwtts:
        type: array
        items:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/PortManagementContainer'
        minItems: 1
  AfEventSubscription:
    description: Describes the event information delivered in the subscription.
    type: object
    required:
      - event
```

```
      properties:
        event:
          $ref: '#/components/schemas/AfEvent'
        notifMethod:
          $ref: '#/components/schemas/AfNotifMethod'
        repPeriod:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        waitTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
    AfEventNotification:
      description: Describes the event information delivered in the notification.
      type: object
      required:
        - event
      properties:
        event:
          $ref: '#/components/schemas/AfEvent'
        flows:
          type: array
          items:
            $ref: '#/components/schemas/Flows'
          minItems: 1
    TerminationInfo:
      description: Indicates the cause for requesting the deletion of the Individual Application
Session Context resource.
      type: object
      required:
        - termCause
        - resUri
      properties:
        termCause:
          $ref: '#/components/schemas/TerminationCause'
        resUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
    AfRoutingRequirement:
      description: Describes the event information delivered in the subscription.
      type: object
      properties:
        appReloc:
          type: boolean
        routeToLocs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/RouteToLocation'
          minItems: 1
        spVal:
          $ref: '#/components/schemas/SpatialValidity'
        tempVals:
          type: array
          items:
            $ref: '#/components/schemas/TemporalValidity'
          minItems: 1
        upPathChgSub:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/UpPathChgEvent'
        addrPreserInd:
          type: boolean
        simConnInd:
          type: boolean
          description: Indicates whether simultaneous connectivity should be temporarily maintained
for the source and target PSA.
        simConnTerm:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        easIpReplaceInfos:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/EasIpReplacementInfo'
          minItems: 1
          description: Contains EAS IP replacement information.
        easRedisInd:
          type: boolean
          description: Indicates the EAS rediscovery is required.
        maxAllowedUpLat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
    SpatialValidity:
      description: Describes explicitly the route to an Application location.
      type: object
      required:
        - presenceInfoList
```

```
      properties:
        presenceInfoList:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
          minProperties: 1
          description: Defines the presence information provisioned by the AF. The praId attribute
within the PresenceInfo data type is the key of the map.
    SpatialValidityRm:
      description: This data type is defined in the same way as the SpatialValidity data type, but
with the OpenAPI nullable property set to true.
      type: object
      required:
        - presenceInfoList
      properties:
        presenceInfoList:
          type: object
          additionalProperties:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
          minProperties: 1
          description: Defines the presence information provisioned by the AF. The praId attribute
within the PresenceInfo data type is the key of the map.
      nullable: true
    AfRoutingRequirementRm:
      description: >
        This data type is defined in the same way as the AfRoutingRequirement data type, but with
        the OpenAPI nullable property set to true and the spVal and tempVals attributes defined as
        removable.
      type: object
      properties:
        appReloc:
          type: boolean
        routeToLocs:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/RouteToLocation'
          minItems: 1
          nullable: true
        spVal:
          $ref: '#/components/schemas/SpatialValidityRm'
        tempVals:
          type: array
          items:
            $ref: '#/components/schemas/TemporalValidity'
          minItems: 1
          nullable: true
        upPathChgSub:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/UpPathChgEvent'
        addrPreserInd:
          type: boolean
          nullable: true
        simConnInd:
          type: boolean
          nullable: true
          description: Indicates whether simultaneous connectivity should be temporarily maintained
for the source and target PSA.
        simConnTerm:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSecRm'
        easIpReplaceInfos:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/EasIpReplacementInfo'
          minItems: 1
          description: Contains EAS IP replacement information.
          nullable: true
        easRedisInd:
          type: boolean
          description: Indicates the EAS rediscovery is required.
        maxAllowedUpLat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UintegerRm'
      nullable: true
    AnGwAddress:
      description: Describes the address of the access network gateway control node.
      type: object
      anyOf:
        - required: [anGwIpv4Addr]
        - required: [anGwIpv6Addr]
      properties:
```

```
        anGwIpv4Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        anGwIpv6Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
    Flows:
      description: Identifies the flows.
      type: object
      required:
        - medCompN
      properties:
        contVers:
          type: array
          items:
            $ref: '#/components/schemas/ContentVersion'
          minItems: 1
        fNums:
          type: array
          items:
            type: integer
          minItems: 1
        medCompN:
          type: integer
    EthFlowDescription:
      description: Identifies an Ethernet flow.
      type: object
      required:
        - ethType
      properties:
        destMacAddr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
        ethType:
          type: string
        fDesc:
          $ref: '#/components/schemas/FlowDescription'
        fDir:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/FlowDirection'
        sourceMacAddr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
        vlanTags:
          type: array
          items:
            type: string
          minItems: 1
          maxItems: 2
        srcMacAddrEnd:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
        destMacAddrEnd:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'


    ResourcesAllocationInfo:
      description: Describes the status of the PCC rule(s) related to certain media components.
      type: object
      properties:
        mcResourcStatus:
          $ref: '#/components/schemas/MediaComponentResourcesStatus'
        flows:
          type: array
          items:
            $ref: '#/components/schemas/Flows'
          minItems: 1
        altSerReq:
          type: string
    TemporalValidity:
      description: Indicates the time interval(s) during which the AF request is to be applied.
      type: object
      properties:
        startTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        stopTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
#
    QosNotificationControlInfo:
      description: Indicates whether the QoS targets for a GRB flow are not guaranteed or guaranteed
again.
      type: object
      required:
        - notifType
```

```
      properties:
        notifType:
          $ref: '#/components/schemas/QosNotifType'
        flows:
          type: array
          items:
            $ref: '#/components/schemas/Flows'
          minItems: 1
        altSerReq:
          type: string
#
    AcceptableServiceInfo:
      description: Indicates the maximum bandwidth that shall be authorized by the PCF.
      type: object
      properties:
        accBwMedComps:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MediaComponent'
          description: Indicates the maximum bandwidth that shall be authorized by the PCF for each
media component of the map. The key of the map is the media component number.
          minProperties: 1
        marBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        marBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'

    UeIdentityInfo:
      description: Represents 5GS-Level UE identities.
      type: object
      anyOf:
        - required: [gpsi]
        - required: [pei]
        - required: [supi]
      properties:
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
        pei:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Pei'
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
#
    AccessNetChargingIdentifier:
      description: Describes the access network charging identifier.
      type: object
      oneOf:
        - required: [accNetChaIdValue]
        - required: [accNetChargIdString]
      properties:
        accNetChaIdValue:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ChargingId'
        accNetChargIdString:
          type: string
          description: A character string containing the access network charging identifier.
        flows:
          type: array
          items:
            $ref: '#/components/schemas/Flows'
          minItems: 1
#
    OutOfCreditInformation:
      description: Indicates the SDFs without available credit and the corresponding termination
action.
      type: object
      required:
        - finUnitAct
      properties:
        finUnitAct:
          $ref: 'TS32291_Nchf_ConvergedCharging.yaml#/components/schemas/FinalUnitAction'
        flows:
          type: array
          items:
            $ref: '#/components/schemas/Flows'
          minItems: 1
#
    QosMonitoringInformation:
      description: Indicates the QoS Monitoring information to report, i.e. UL and/or DL and or
round trip delay.
```

```
      type: object
      properties:
        repThreshDl:
          type: integer
        repThreshUl:
          type: integer
        repThreshRp:
          type: integer
#
#
    PduSessionTsnBridge:
      description: Contains the new TSC user plane node information and may contain the DS-TT port
and/or NW-TT port management information.
      type: object
      required:
        - tsnBridgeInfo
      properties:
        tsnBridgeInfo:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/TsnBridgeInfo'
        tsnBridgeManCont:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/BridgeManagementContainer'
        tsnPortManContDstt:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/PortManagementContainer'
        tsnPortManContNwtts:
          type: array
          items:
            $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/PortManagementContainer'
          minItems: 1
        ueIpv4Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        dnn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        snssai:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        ipDomain:
          type: string
          description: IPv4 address domain identifier.
        ueIpv6AddrPrefix:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'

#
    QosMonitoringInformationRm:
      description: This data type is defined in the same way as the QosMonitoringInformation data
type, but with the OpenAPI nullable property set to true.
      type: object
      properties:
        repThreshDl:
          type: integer
        repThreshUl:
          type: integer
        repThreshRp:
          type: integer
      nullable: true
#
    PcscfRestorationRequestData:
      description: Indicates P-CSCF restoration.
      type: object
      oneOf:
        - required: [ueIpv4]
        - required: [ueIpv6]
      properties:
        dnn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        ipDomain:
          type: string
        sliceInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        ueIpv4:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ueIpv6:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'

#
#
    QosMonitoringReport:
      description: QoS Monitoring reporting information.
```

```
      type: object
      properties:
        flows:
          type: array
          items:
            $ref: '#/components/schemas/Flows'
          minItems: 1
        ulDelays:
          type: array
          items:
            type: integer
          minItems: 1
        dlDelays:
          type: array
          items:
            type: integer
          minItems: 1
        rtDelays:
          type: array
          items:
            type: integer
          minItems: 1
        pdmf:
          type: boolean
          description: Represents the packet delay measurement failure indicator.
#
    TsnQosContainer:
      description: Indicates TSC Traffic QoS.
      type: object
      properties:
        maxTscBurstSize:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ExtMaxDataBurstVol'
        tscPackDelay:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketDelBudget'
        tscPrioLevel:
          $ref: '#/components/schemas/TscPriorityLevel'
#
#
    TsnQosContainerRm:
      description: Indicates removable TSC Traffic QoS.
      type: object
      properties:
        maxTscBurstSize:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ExtMaxDataBurstVolRm'
        tscPackDelay:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketDelBudgetRm'
        tscPrioLevel:
          $ref: '#/components/schemas/TscPriorityLevelRm'
      nullable: true
#
    TscaiInputContainer:
      description: Indicates TSC Traffic pattern.
      type: object
      properties:
        periodicity:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
        burstArrivalTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        surTimeInNumMsg:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
        surTimeInTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
      nullable: true
#
#
    AppDetectionReport:
      description: Indicates the start or stop of the detected application traffic and the
application identifier of the detected application traffic.
      type: object
      required:
        - adNotifType
        - afAppId
      properties:
        adNotifType:
          $ref: '#/components/schemas/AppDetectionNotifType'
        afAppId:
          $ref: '#/components/schemas/AfAppId'
#
```

```
#
    PduSessionEventNotification:
      description: Indicates PDU session information for the concerned established/terminated PDU
session.
      type: object
      required:
        - evNotif
      properties:
        evNotif:
          $ref: '#/components/schemas/AfEventNotification'
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        ueIpv4:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ueIpv6:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
        ueMac:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
        status:
          $ref: '#/components/schemas/PduSessionStatus'
        pcfInfo:
          $ref: '#/components/schemas/PcfAddressingInfo'
        dnn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        snssai:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
#
#
    PcfAddressingInfo:
      description: Contains PCF address information.
      type: object
      properties:
        pcfFqdn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Fqdn'
        pcfIpEndPoints:
          type: array
          items:
            $ref: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/IpEndPoint'
          minItems: 1
          description: IP end points of the PCF hosting the Npcf_PolicyAuthorization service.
        bindingInfo:
          type: string
          description: contains the binding indications of the PCF.
#
    AlternativeServiceRequirementsData:
      description: Contains an alternative QoS related parameter set.
      type: object
      required:
        - altQosParamSetRef
      properties:
        altQosParamSetRef:
          type: string
          description: Reference to this alternative QoS related parameter set.
        gbrUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        gbrDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        pdb:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketDelBudget'
#
    EventsSubscPutData:
      description: >
        Identifies the events the application subscribes to within an Events Subscription
        sub-resource data. It may contain the notification of the already met events.
      anyOf:
        - $ref: '#/components/schemas/EventsSubscReqData'
        - $ref: '#/components/schemas/EventsNotification'
#
# EXTENDED PROBLEMDETAILS
#
    ExtendedProblemDetails:
      description: Extends ProblemDetails to also include the acceptable service info.
      allOf:
        - $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
        - type: object
          properties:
```

```
            acceptableServInfo:
              $ref: '#/components/schemas/AcceptableServiceInfo'

#
# SIMPLE DATA TYPES
#
    AfAppId:
      description: Contains an AF application identifier.
      type: string
    AspId:
      description: Contains an identity of an application service provider.
      type: string
    CodecData:
      description: Contains codec related information.
      type: string
    ContentVersion:
      description: Represents the content version of some content.
      type: integer
    FlowDescription:
      description: Defines a packet filter of an IP flow.
      type: string
    SponId:
      description: Contains an identity of a sponsor.
      type: string
    ServiceUrn:
      description: Contains values of the service URN and may include subservices.
      type: string
    TosTrafficClass:
      description: >
        2-octet string, where each octet is encoded in hexadecimal representation. The first octet
        contains the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the second octet
        contains the ToS/Traffic Class mask field.
      type: string
    TosTrafficClassRm:
      description: This data type is defined in the same way as the TosTrafficClass data type, but
with the OpenAPI nullable property set to true.
      type: string
      nullable: true
    TscPriorityLevel:
      description: Represents the priority level of TSC Flows.
      type: integer
      minimum: 1
      maximum: 8
    TscPriorityLevelRm:
      description: This data type is defined in the same way as the TscPriorityLevel data type, but
with the OpenAPI nullable property set to true.
      type: integer
      minimum: 1
      maximum: 8
      nullable: true
#
# ENUMERATIONS DATA TYPES
#
    MediaType:
      description: Indicates the media type of a media component.
      anyOf:
        - type: string
          enum:
            - AUDIO
            - VIDEO
            - DATA
            - APPLICATION
            - CONTROL
            - TEXT
            - MESSAGE
            - OTHER
        - type: string
#
    MpsAction:
      description: Indicates whether it is an invocation, a revocation or an invocation with
authorization of the MPS for DTS service.
      anyOf:
        - type: string
          enum:
            - DISABLE_MPS_FOR_DTS
            - ENABLE_MPS_FOR_DTS
            - AUTHORIZE_AND_ENABLE_MPS_FOR_DTS
        - type: string
```

```
#
    ReservPriority:
      description: Indicates the reservation priority.
      anyOf:
        - type: string
          enum:
            - PRIO_1
            - PRIO_2
            - PRIO_3
            - PRIO_4
            - PRIO_5
            - PRIO_6
            - PRIO_7
            - PRIO_8
            - PRIO_9
            - PRIO_10
            - PRIO_11
            - PRIO_12
            - PRIO_13
            - PRIO_14
            - PRIO_15
            - PRIO_16
        - type: string
#
    ServAuthInfo:
      description: Indicates the result of the Policy Authorization service request from the AF.
      anyOf:
      - type: string
        enum:
          - TP_NOT_KNOWN
          - TP_EXPIRED
          - TP_NOT_YET_OCURRED
          - ROUT_REQ_NOT_AUTHORIZED
      - type: string
#
    SponsoringStatus:
      description: Indicates whether sponsored data connectivity is enabled or disabled/not enabled.
      anyOf:
      - type: string
        enum:
          - SPONSOR_DISABLED
          - SPONSOR_ENABLED
      - type: string
#
    AfEvent:
      description: Represents an event to notify to the AF.
      anyOf:
      - type: string
        enum:
          - ACCESS_TYPE_CHANGE
          - ANI_REPORT
          - APP_DETECTION
          - CHARGING_CORRELATION
          - EPS_FALLBACK
          - FAILED_QOS_UPDATE
          - FAILED_RESOURCES_ALLOCATION
          - OUT_OF_CREDIT
          - PDU_SESSION_STATUS
          - PLMN_CHG
          - QOS_MONITORING
          - QOS_NOTIF
          - RAN_NAS_CAUSE
          - REALLOCATION_OF_CREDIT
          - SAT_CATEGORY_CHG
          - SUCCESSFUL_QOS_UPDATE
          - SUCCESSFUL_RESOURCES_ALLOCATION
          - TSN_BRIDGE_INFO
          - UP_PATH_CHG_FAILURE
          - USAGE_REPORT
      - type: string
#
    AfNotifMethod:
      description: Represents the notification methods that can be subscribed for an event.
      anyOf:
      - type: string
        enum:
          - EVENT_DETECTION
          - ONE_TIME
```

```
          - PERIODIC
      - type: string
#
    QosNotifType:
      description: Indicates the notification type for QoS Notification Control.
      anyOf:
      - type: string
        enum:
          - GUARANTEED
          - NOT_GUARANTEED
      - type: string
#
    TerminationCause:
      description: Indicates the cause behind requesting the deletion of the Individual Application
Session Context resource.
      anyOf:
      - type: string
        enum:
          - ALL_SDF_DEACTIVATION
          - PDU_SESSION_TERMINATION
          - PS_TO_CS_HO
          - INSUFFICIENT_SERVER_RESOURCES
          - INSUFFICIENT_QOS_FLOW_RESOURCES
          - SPONSORED_DATA_CONNECTIVITY_DISALLOWED
      - type: string
#
    MediaComponentResourcesStatus:
      description: Indicates whether the media component is active or inactive.
      anyOf:
      - type: string
        enum:
          - ACTIVE
          - INACTIVE
      - type: string
#
#
    FlowUsage:
      description: Describes the flow usage of the flows described by a media subcomponent.
      anyOf:
      - type: string
        enum:
          - NO_INFO
          - RTCP
          - AF_SIGNALLING
      - type: string


    FlowStatus:
      description: Describes whether the IP flow(s) are enabled or disabled.
      anyOf:
      - type: string
        enum:
          - ENABLED-UPLINK
          - ENABLED-DOWNLINK
          - ENABLED
          - DISABLED
          - REMOVED
      - type: string
#
    RequiredAccessInfo:
      description: Indicates the access network information required for an AF session.
      anyOf:
      - type: string
        enum:
          - USER_LOCATION
          - UE_TIME_ZONE
      - type: string
#
    SipForkingIndication:
      description: Indicates whether several SIP dialogues are related to an "Individual Application
Session Context" resource.
      anyOf:
        - type: string
          enum:
            - SINGLE_DIALOGUE
            - SEVERAL_DIALOGUES
        - type: string
#
```

```
    AfRequestedData:
      description: Represents the information that the AF requested to be exposed.
      anyOf:
        - type: string
          enum:
            - UE_IDENTITY
        - type: string
#
    ServiceInfoStatus:
      description: Represents the preliminary or final service information status.
      anyOf:
        - type: string
          enum:
            - FINAL
            - PRELIMINARY
        - type: string
#
    PreemptionControlInformation:
      description: Represents Pre-emption control information.
      anyOf:
        - type: string
          enum:
            - MOST_RECENT
            - LEAST_RECENT
            - HIGHEST_BW
        - type: string
#
    PrioritySharingIndicator:
      description: Represents the Priority sharing indicator.
      anyOf:
        - type: string
          enum:
            - ENABLED
            - DISABLED
        - type: string
#
    PreemptionControlInformationRm:
      description: This data type is defined in the same way as the PreemptionControlInformation
data type, but with the OpenAPI nullable property set to true.
      anyOf:
        - $ref: '#/components/schemas/PreemptionControlInformation'
        - $ref: 'TS29571_CommonData.yaml#/components/schemas/NullValue'
#
    AppDetectionNotifType:
      description: Indicates the notification type for Application Detection Control.
      anyOf:
      - type: string
        enum:
          - APP_START
          - APP_STOP
      - type: string
#
    PduSessionStatus:
      description: Indicates whether the PDU session is established or terminated.
      anyOf:
      - type: string
        enum:
          - ESTABLISHED
          - TERMINATED
      - type: string
```

# Annex B (normative): IMS Related P-CSCF Procedures over N5

## B.1 Provision of Service Information at P-CSCF

When the "IMS_SBI" feature is supported, the P-CSCF shall send service information to the PCF upon every SIP message that includes an SDP answer payload for the purpose of authorizing the IP flows and the QoS resources required for a negotiated IMS session, unless the SDP payload only relates to a circuit-switched bearer (i.e. "c=" line set to "PSTN" and an "m=" line set to "PSTN", refer to 3GPP TS 24.292 [29]). The service information shall be derived both from the SDP offer and the SDP answer. This ensures that the PCF receives proper information to perform media authorization for all possible IMS session set-up scenarios, and that the PCF is also capable of handling session modifications. The P-CSCF may include "servInfStatus" attribute set to "FINAL".

Additionally, the P-CSCF may send service information to the PCF when receiving a SIP message that includes an SDP offer payload for the purpose of performing an early bandwidth authorization check, or for enabling pre-authorization for a UE terminated IMS session establishment or modification with UE initiated resource reservation, or for the retrieval of network provided access network information (see clause B.8.2).

The P-CSCF shall send service information to the PCF when receiving a SIP message that includes an SDP offer payload when the IMS session is an MPS session that requires priority treatment. For a UE terminated session the P-CSCF may send the service information derived from the SDP offer when the SDP offer either does not include any preconditions information or includes preconditions information indicating that the local preconditions (i.e. the preconditions related to the remote peer) are already met. In this case, the P-CSCF shall derive the service information only from the SDP offer and shall include "servInfStatus" attribute set to "PRELIMINARY".

NOTE 1: For a UE terminated session setup, when the SDP offer either does not include any preconditions information or includes preconditions information indicating that the local preconditions (i.e. the preconditions related to the remote peer) are already met, the terminating UE can request a resource modification prior to sending the SDP answer. Even if the IP address and port information in the session information derived from the SDP offer can be insufficient for PCC rule authorization, the policy to handle such UE initiated requests at the PCF can take into account the fact that an IMS session establishment is ongoing, for instance in deciding whether to authorize the request and in selecting an appropriate charging key and a gating policy.

The P-CSCF shall derive the value of the "fDescs" attribute within the service information from the SDP as follows:

- An uplink entry in the "fDescs" attribute shall be formed as follows: The destination address shall be taken from the SDP information received by the P-CSCF in downlink direction, while the source IP address may be formed from the address present in the SDP received by the P-CSCF in uplink direction (taking into account only the 64 bit prefix of the Ipv6 address) Source and destination ports shall be derived according to rules provided in 3GPP TS 29.513 [7] clause 7.2.

EXAMPLE 1: Assuming UE A sends an SDP to UE B, the PCF of UE B uses the address present in this SDP for the destination address of UE B's uplink entry in the "fDescs" attribute, while the PCF of the UE A uses the 64 bit prefix of the same address for the source address of UE A's uplink entry in the "fDescs" attribute. If the source address is not formed from the 64 bit prefix, the source address shall be wildcarded.

- A downlink entry in the "fDescs" attribute shall be formed as follows: The destination address shall be taken from the SDP information received by the P-CSCF in uplink direction, while the source IP address may be formed (in order to reduce the possibilities of QoS flow misuse) from the destination address in the SDP received by the P-CSCF in downlink direction (taking into account only the 64 bit prefix of the Ipv6 address) Source and destination ports shall be derived according to rules provided in 3GPP TS 29.513 [7] clause 7.2.

EXAMPLE 2: Assuming UE A sends an SDP to UE B, the PCF of UE A uses the address present in this SDP for the destination address of UE A's downlink entry in the "fDescs" attribute, while the PCF of UE B uses the 64 bit prefix of the same address for the source address of UE B's downlink entry in the "fDescs" attribute. If the source address is not formed from the 64 bit prefix, the source address shall be wildcarded.

The P-CSCF shall derive the bandwidth information within the service information, from the "b=AS" SDP parameter and "a=bw-info" SDP parameter, if available. If "a=bw-info" is used for bandwidth derivation, the P-CSCF shall use the SDP attribute line that contains the bandwidth properties for the IP version used by the UE, as detailed in 3GPP TS 29.513 [7] clause 7.2. If the received "a=bw-info" SDP attribute line(s) contain only bandwidth properties for an IP version that is not used by the UE, the P-CSCF shall re-compute the bandwidth properties for the used IP version and use that value for the bandwidth derivation as defined in 3GPP TS 26.114 [30].

NOTE 2: If no IP version is included for any of the "a=bw-info" SDP attribute lines related to a certain payload type and direction then IPv6 is assumed for all bandwidth properties related to the same direction and payload type, on all of the related "a=bw-info" SDP attribute lines, see clause 19 of 3GPP TS 26.114 [30].

If "a=bw-info" is used for bandwidth derivation and it includes both known and unknown bandwidth properties, the P-CSCF shall only consider the known bandwidth properties to derive the bandwidth information and ignore the unknown ones. If the" a=bw-info" line is received with an unknown directionality, then the entire "a=bw-info" line shall be ignored.

For the possibly associated RTCP IP flows, the P-CSCF shall use the SDP "b=RR" and "b=RS" parameters, if present, as specified in 3GPP TS 29.513 [7] clause 7.2. The "b=AS", "b=RR" and "b=RS" parameters in the SDP contain all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTCP payload, or IP, UDP and RTCP.

For multiplexed RTP/RTCP flows (as negotiated using the "a=rtcp-mux" SDP attribute defined in IETF RFC 5761 [31], a P-CSCF supporting RTP/RTCP transport multiplexing shall derive the bandwidth information within the service information as specified in 3GPP TS 29.513 [7] clause 7.2.

However, if service information is received containing the "b=TIAS" SDP parameter that corresponds to an SDP answer payload, and if the P-CSCF supports this parameter, the P-CSCF may derive the bandwidth from this parameter rather than from the "b=AS" SDP parameter, as detailed in 3GPP TS 29.513 [7] clause 7.2.

When available, the P-CSCF shall also indicate to PCF, as a complement to the Service Information, the IMS Communication Service Identifier within the "afAppId" attribute. The originating P-CSCF shall take the IMS Communication Service Identifier value from the SIP response. The terminating P-CSCF shall take the IMS Communication Service Identifier value from the SIP request. Otherwise, the P-CSCF may not be able to provide an IMS Communication Service Identifier value to the PCF. The format and specific headers where IMS communication service identifiers are transported within SIP are defined in 3GPP TS 24.229 [32].

NOTE 3: In order to indicate the IMS Communication Service Identifier to the PCF, the originating P-CSCF sets the "afAppId" attribute to the ICSI contained in the topmost occurrence of the "+g.3gpp.icsi-ref" header field parameter of the Feature-Caps header field(s) of 18x or 2xx SIP response (Feature-Caps: *;+g.3gpp.icsi-ref="urn%Aurn-7%A3gpp-service.ims.icsi.mmtel") and the terminating P-CSCF sets the "afAppId" attribute to the ICSI of the P-Asserted-Service header information received in the SIP request (e.g. P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel). Since the headers and the format of the ICSI can vary depending on the case, the PCF has to be prepared to accept the complete ICSI information received in different formats, as described in clause 7.2A.8.2 in 3GPP TS 24.229 [32].

Additionally, if "ResourceSharing" feature is supported, the P-CSCF may include the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute within a media component of the "medComponents" attribute in order to indicate the PCF that resource sharing should apply for the media components in the related direction with the same value for the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute.

Additionally, if "PrioritySharing" feature is supported, the P-CSCF may provide the "prioSharingInd" attribute within a media component of the "medComponents" attribute as described in clause 4.2.2.21 and 4.2.3.21.

NOTE 4: The P-CSCF obtains this information from the Application Server as described in 3GPP TS 23.228 [33], clause 5.4.7.9.

NOTE 5: RTCP flows are not subject to resource sharing. This requirement cannot be met for multiplexed RTP/RTCP flows as in this case there is no mechanism in the current release to distinguish between RTP and RTCP flows.

For IMS emergency services provided by a PLMN or an SNPN if the "servUrn" attribute does not include an emergency service URN, i.e. a top-level service type of "sos" as specified in IETF RFC 5031 [34] and possibly additional sub-service information on the type of the emergency service and the PCF binds the IMS service session to a PDU session established to an Emergency DNN, the PCF shall return the application error UNAUTHORIZED_NON_EMERGENCY_SESSION to the P-CSCF. Upon receiving an application error

UNAUTHORIZED_NON_EMERGENCY_SESSION the P-CSCF shall apply the procedures defined in 3GPP TS 24.229 [32].

NOTE 6: The PCF determines whether a PDU session is established to an Emergency DNN based on the information received over N7 and operator configuration.

If the "afReqData" attribute is provided in the "ascReqData" attribute indicating "5GS-level UE Identities required", the PCF shall provide the available user information for the PDU session in the serving network (either a PLMN or an SNPN) within the "ueIds" attribute included in the "ascRespData" attribute, where each entry shall contain the IMSI (for PLMN access) or either IMSI or NAI (for SNPN access) within the "supi", and/or the MSISDN within the "gpsi" and/or the IMEI(SV) within the "pei" attributes.

The PCF may decide not to authorize requested service information. The PCF will indicate it to the P-CSCF by rejecting the HTTP request with an HTTP "403 Forbidden" response message including the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED". Upon receiving an HTTP "403 Forbidden" response message including the "cause" attribute set to the value "REQUESTED_SERVICE_NOT_AUTHORIZED" the P-CSCF shall apply the procedures defined in 3GPP TS 24.229 [32].

# B.2 Enabling of IP Flows

## B.2.1 General

Prior to the completion of the SIP session set-up, i.e. until the 2xx response to the INVITE request is received, the P-CSCF may enable or disable media IP flows depending on operator policy, thus allowing or forbidding early media in forward and/or backward direction. The P-CSCF may set the values of the "fStatus" attribute derived from the SDP direction attributes as defined in 3GPP TS 29.513 [7] clause 7.3.3 or set the values of the "fStatus" attributes considering the em-param of the P-Early-Media header field according to clause B.2.2 or downgrade the values of the "fStatus" attribute derived from the SDP direction attribute based on the configuration in the P-CSCF according to clause B.2.3. However for multiplexed RTP/RTCP flows (as negotiated using the "a=rtcp-mux" SDP attribute defined in IETF RFC 5761 [31]), a P-CSCF supporting RTP/RTCP transport multiplexing shall set the "fStatus" attribute to "ENABLED" to prevent that RTCP is blocked. If the P-CSCF chooses to modify the values of the "fStatus" as received from the SDP direction attribute, the P-CSCF shall store the last received SDP.

When a 2xx response is received, the P-CSCF shall enable all media IP flows according to the direction attribute within the last received SDP, as specified in 3GPP TS 29.513 [7] clause 7.3.3. When a 2xx response is received and the P-CSCF previously provided the values of the "fStatus" attributes different from the value derived from the SDP direction attribute in the session information, the P-CSCF shall provide service information with values of the "fStatus" attributes corresponding to the last received SDP.

NOTE: In most cases a 2xx response is a 200 (OK) response.

If the P-CSCF receives SDP answers after the completion of the SIP session set-up, i.e. after the 2xx response to the INVITE request is received, the P-CSCF shall provide the "fStatus" attribute, based on the last received SDP answer. The "fStatus" attribute shall be derived from the SDP according to 3GPP TS 29.513 [7] clause 7.3.3.

## B.2.2 Gate control procedures considering the P-Early-Media header field

Prior to the completion of the SIP session set-up, the P-CSCF may use the em-param of the P-Early-Media header field defined in IETF RFC 5009 [35] in order to enable or disable early media in forward and/or backward direction. If the P-CSCF uses the em-param of the P-Early-Media header field for the gate control of early media, the P-CSCF shall perform the following procedures.

In the terminating P-CSCF, when a SIP message with the P-Early-Media header field is received from the UE and the policies configured in the P-CSCF indicate that the UE is authorized to send early media, then:

1) the P-CSCF shall set the "fStatus" attribute to "ENABLED" if:

- the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the UE is "sendrecv" or no SDP direction attribute has been received; or

2) the P-CSCF shall set the "fStatus" attribute to "ENABLED-UPLINK" if:

- the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the UE is "sendonly"; or

- the received em-param(s) in the P-Early-Media header field includes "sendonly" and the last received SDP direction attribute from the UE is "sendrecv" or "sendonly" or no SDP direction attribute has been received; or

3) the P-CSCF shall set the "fStatus" attribute to "ENABLED-DOWNLINK" if:

- the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the UE is "recvonly"; or

- the received em-param(s) in the P-Early-Media header field includes "recvonly" and the last received SDP direction attribute from the UE is "sendrecv" or "recvonly" or no SDP direction attribute has been received; or

4) the P-CSCF shall set the "fStatus" attribute to "DISABLED" if either the received em-param(s) in the P-Early-Media header field or the last received SDP direction attribute from the UE includes "inactive"; or

5) the P-CSCF may set the "fStatus" attribute to "DISABLED" or apply the rules defined in clause B.2.2 if the received em-param(s) in the P-Early-Media header field includes "sendonly" or "recvonly" and the last received SDP direction attribute from the UE is "recvonly" or "sendonly" respectively.

NOTE 1: If the UE is authorized to send early media, the P-CSCF will not remove or modify the P-Early-Media header field according to 3GPP TS 24.229 [32].

When a SIP message with the P-Early-Media header field is received from the functional entity within the trust domain, and if:

- the P-Early-Media header field includes the "gated" parameter, then the P-CSCF may decide not to perform the gate control of early media; or

- the P-Early-Media header field does not include the "gated" parameter, then the P-CSCF shall perform the following procedures:

1) the P-CSCF shall set the "fStatus" attribute to "ENABLED" if:

- the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the functional entity is "sendrecv" or no SDP direction attribute has been received; or

2) the P-CSCF shall set the "fStatus" attribute to "ENABLED-DOWNLINK" if:

- the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the functional entity is "sendonly"; or

- the received em-param(s) in the P-Early-Media header field includes "sendonly" and the last received SDP direction attribute from the functional entity is "sendrecv" or "sendonly" or no SDP direction parameter has been received; or

3) the P-CSCF shall set the "fStatus" attribute to "ENABLED-UPLINK" if:

- the received em-param(s) in the P-Early-Media header field includes "sendrecv" and the last received SDP direction attribute from the functional entity is "recvonly"; or

- the received em-param(s) in the P-Early-Media header field includes "recvonly" and the last received SDP direction attribute from the functional entity is "sendrecv" or "recvonly" or no SDP direction parameter has been received; or

4) the P-CSCF shall set the "fStatus" attribute to "DISABLED" if either the received em-param(s) in the P-Early-Media header field or the last received SDP direction attribute from the functional entity includes "inactive"; or

5) the P-CSCF may set the "fStatus" attribute to "DISABLED" or apply the rules defined in clause A.2.2 if the received em-param(s) in the P-Early-Media header field includes "sendonly" or "recvonly" and the last received SDP direction attribute from the functional entity is "recvonly" or "sendonly" respectively.

NOTE 2: According to IETF RFC 5009 [35], the non-direction parameter "gated" can be included after the direction parameter (e.g. "sendrecv") in the parameter list. The proxy performing gating of early media can add the parameter before forwarding the SIP message.

When a SIP message without the P-Early-Media header field is received from either the functional entity within the trust domain or the UE that is authorized to send early media, then the P-CSCF may set the "fStatus" attribute to "DISABLED" or apply the rules defined in clause B.2.3 or apply the rules defined in 3GPP TS 29.513 [7] clause 7.3.3.

NOTE 3: As indicated in IETF RFC 5009 [35] the applicable preconditions need to be met in order to allow early media in a particular direction.

When a SIP message is received from the functional entity other than the functional entity within the trust domain or the UE that is authorized to send early media, then the P-CSCF shall not use the received em-param(s) in the P-Early-Media header field and may apply the rules defined in clause B.2.2 or apply the rules defined in 3GPP TS 29.513 [7] clause 7.3.3.

NOTE 4: The P-CSCF will remove or modify the P-Early-Media header field in the above case.

### B.2.3 Gate control procedures based on the configuration in the P-CSCF

Prior to the completion of the SIP session set-up, the P-CSCF may downgrade the values of the "fStatus" attributes derived from the SDP direction attributes based on the configuration in the P-CSCF. If the P-CSCF has the configuration for the gate control of early media, the P-CSCF shall perform the following procedures.

NOTE: The gate control of early media can be configured in the P-CSCF per UE basis.

When the "fStatus" attribute derived from the SDP direction attribute is "ENABLED", then the P-CSCF may downgrade the value of the "fStatus" attribute to the value "DISABLED", "ENABLED_UPLINK", or "ENABLED_DOWNLINK" based on the configuration in the P-CSCF.

When the "fStatus" attribute derived from the SDP direction attribute is "ENABLED_UPLINK" or "ENABLED_DOWNLINK", then the P-CSCF may downgrade the value of the "fStatus" attribute to the value "DISABLED" based on the configuration in the P-CSCF.

## B.3 Support for SIP forking

### B.3.0 General

The P-CSCF shall be able to handle forking when PCC is applied and the "IMS_SBI" feature is supported. Forking can occur as specified in 3GPP TS 23.228 [33]. The related UE procedures are described in 3GPP TS 24.229 [32].

### B.3.1 PCC rule provisioning for early media for forked responses

When a SIP session has been originated by a connected UE, the P-CSCF may receive multiple provisional responses due to forking before the first final answer is received. Multiple early media session may be established during this process.

The UE and the P-CSCF become aware of the forking only when a subsequent provisional response arrives for a new early dialogue. After the first early media session is established, for each subsequent provisional response establishing

an additional early media session, the P-CSCF shall use an Npcf_PolicyAuthorization_Update service operation containing the "sipForkInd" attribute with value "SEVERAL_DIALOGUES" and include the service information derived from the latest provisional response.

The P-CSCF shall also provision the service information derived from any subsequent SDP offer-answer exchange within an early dialogue (e.g. in PRACK and OK(PRACK), or UPDATE and OK(UPDATE) ) using an Npcf_PolicyAuthorization_Update service operation containing the "sipForkInd" attribute with value "SEVERAL_DIALOGUES" and the derived service information.

When receiving an Npcf_PolicyAuthorization_Update service operation containing the "sipForkInd" attribute with value "SEVERAL_DIALOGUES", the PCF shall identify the existing "Individual Application Session Context" resource with existing authorization information.

The PCF shall send additional PCC Rules or individual service data flow filters to already provided PCC rules as required by the "fDescs" attribute within the AF session context information to the SMF. The PCF shall authorize any additional media components and any increased QoS requirements for the previously authorized media components, as requested within the service information.

The PCF shall authorize the maximum bandwidth required by any of the dialogues, but not the sum of the bandwidths required by all dialogues. Thus, the QoS authorized for a media component is equal to the highest QoS requested for that media component by any of the forked responses.

The PCF shall open or close the gates for service flows depending on the flow status that is being provisioned. However, if a flow ID has been enabled in uplink or downlink direction or both way within previous service information, it shall remain enabled even if the PCF receives service information that disable this flow ID within an Npcf_PolicyAuthorization_Update service operation containing the "sipForkInd" attribute with value "SEVERAL_DIALOGUES".

If the P-CSCF provides one or more media components within the "medComponents" attribute with the "fStatus" attribute set to "REMOVED" for previously authorized media component(s) the media component shall remain as authorized and the PCF shall not take any action on that media component(s).

NOTE: There can be cases where a forked response could not support some of the media components included in the SDP Offer (e.g. when early session disposition SDP as described in Annex B.6 applies, the forked response related to the early session could include the port set to zero for those media components not related to the early session or when a subsequent SDP Offer-Answer to indicate that some media is disabled). For those cases the P-CSCF will indicate the PCF about the removal of the corresponding media component. However this media component is already supported by other UEs and the PCF needs to maintain the corresponding PCC rules until the final SDP answer is received in the P-CSCF in order to avoid the release of resources in the network.

## B.3.2 Updating the provisioned PCC rules at the final answer

The P-CSCF shall store the SDP information for each early dialogue separately till the first final SIP answer is received. Then the related early dialogue is progressed to an established dialogue to establish the final SIP session. All the other early dialogues are terminated. The service information for the SIP session is updated to match the requirements of the remaining early dialogue only.

When receiving the first final SIP response, the P-CSCF shall send an Npcf_PolicyAuthorization_Update service operation setting to null the "sipForkInd" attribute and shall include the service information derived from the SDP corresponding to the dialogue of the final response. The P-CSCF shall provision the full service information including the applicable "fDescs" attribute and "fStatus" attribute.

When receiving an Npcf_PolicyAuthorization_Update service operation with a "sipForkInd" attribute with value "SINGLE_DIALOGUE", the PCF shall update installed PCC Rules information and Authorized-QoS information to match only the requirements of the service information within this Npcf_PolicyAuthorization_Update service operation. The PCF should immediately remove PCC Rule(s) or individual service data flow filters not matching IP flow(s) in the updated Service Information, to reduce the risk for initial clipping of the media stream, and to minimize possible misuse of resources. The PCF shall also open or close the gates for service flows according to the flow status in the received service information.

## B.4 Notification of AF Signalling Transmission Path Status

When the P-CSCF receives an initial REGISTER SIP message from an attached UE, the P-CSCF may subscribe to notifications of the status of the AF signalling transmission path using the procedures specified in clause 4.2.6.7. Once the P-CSCF has subscribed, the P-CSCF may receive notifications from the PCF according to clause 4.2.5.10.

NOTE: This procedure is not applicable for IMS registrations for Emergency sessions.

The P-CSCF shall cancel the subscription to notification of the status of the AF signalling transmission path when the AF signalling to that particular user is terminated (i.e. when the user is de-REGISTERED from the IM CN subsystem).

When the P-CSCF receives a notification of loss of signalling connectivity from the PCF, the P-CSCF shall behave as defined in 3GPP TS 24.229 [32].

## B.5 Indication of Emergency Registration and Session Establishment

When the P-CSCF receives an initial REGISTER SIP message for an IMS emergency registration or an INVITE SIP message for an emergency session and the P-CSCF determines that there are no IMS-level roaming interfaces, and the "IMS_SBI" feature is supported the P-CSCF may request the PCF to provide the 5GS-Level UE identities (GPSI, SUPI, PEI) available for that PDU session in the serving network (either a PLMN or an SNPN) using the procedure as specified in this clause (for an IMS emergency registration) or B.1 (for an IMS emergency session establishment).

A P-CSCF may request the PCF to provide the 5GS-level identities (GPSI, SUPI, PEI) available for that PDU session when no service information is available in the P-CSCF. To do so, the P-CSCF shall create an "Individual Application Session Context" resource in the PCF for the AF signalling using an Npcf_PolicyAuthorization_Create service operation. The P-CSCF shall provide the UE's IP address (using either the "ueIpv4" attribute or the "ueIpv6" attribute) and the "afReqData" attribute set to "UE_IDENTITY". The P-CSCF shall include the "servUrn" attribute set to the value "sos", in order to indicate that the new AF session context relates to emergency traffic that is not related to a specific emergency service.

If the P-CSCF supports the SBI Message Priority mechanism for an emergency session, it shall include the "3gpp-Sbi-Message-Priority" custom HTTP header towards the PCF as described in clause 6.8.2 of 3GPP TS 29.500 [5].

NOTE 1: If the P-CSCF supports the SBI Message Priority mechanism for an emergency session, the P-CSCF includes the "3gpp-Sbi-Message-Priority" custom HTTP header based on P-CSCF policies in relation to valid values of the "servUrn" attribute. The highest user priority value is mapped to the corresponding lowest value of the "3gpp-Sbi-Message-Priority" custom HTTP header.

When the PCF receives an Npcf_PolicyAuthorization_Create service operation as described in the preceding paragraphs from the P-CSCF, the PCF shall perform session binding as described in 3GPP TS 29.513 [7]. When the PCF receives the "servUrn" attribute indicating an emergency session, the PCF may apply special policies, for instance prioritising service flows relating to the AF session context or allowing these service flows free of charge.

When the "servUrn" attribute indicates that the AF session context relates to emergency traffic and the "afReqData" attribute is received indicating "UE_IDENTITY", the PCF shall provide the requested available user information (MSISDN, IMSI (for PLMN access) or either IMSI or NAI (for SNPN access), IMEI(SV)) for the PDU session within "ueIds" attribute within the "ascRespData" in the HTTP "201 Created" response.

When the P-CSCF receives the HTTP "201 Created" response with the 5GS-level UE identities from the PCF, the P-CSCF stores the "ueIds" received within "Individual Application Session Context" resource returned in the HTTP "201 Created" response and behaves as defined in 3GPP TS 24.229 [32].

NOTE 2: The user information received within the "ueIds" attribute can be used to support PSAP callback functionality for anonymous IMS emergency sessions. See 3GPP TS 23.167 [40] for further information.

The P-CSCF may decide to delete the "Individual Application Session Context" resource at any time. In that case, the Npcf_PolicyAuthorization_Delete service operation, as described in clause 4.2.4.2.

A SIP INVITE request can contain a service URN as defined in IETF RFC 5031 [34] within the request URI. If the service within this URN is "sos", possibly with additional sub-service information, the P-CSCF shall provision this service and sub-service information within the "servUrn" attribute towards the PCF. The P-CSCF may also provision possible information about other services received within the service URN.

# B.6 Support for Early Session disposition SDP

## B.6.1 General

As a network option, when the "IMS_SBI" feature is supported, the P-CSCF may support the PCC procedures in the present clause to handle "early session" disposition type SDP, as standardised in IETF RFC 3959 [38].

## B.6.2 Service Information Provisioning for Early Media

The P-CSCF can receive "early session" disposition SDP in addition to "session" disposition SDP in SIP early dialogues.

The P-CSCF shall then provision service information derived both from the "early session" disposition SDP and "session" disposition SDP applying the procedures in clauses B.1, B.2, and B.3, and in the present clause.

The P-CSCF shall apply the mapping rules in Annex C to derive the flow identifiers from "early session" disposition SDP.

If a single media line with one media type (e.g. "audio" or "video") is contained in "early session" disposition SDP and a single media line with the same media type is contained in the "session" disposition SDP of the same SIP dialogue, and both media lines describe service flows of the same directionality (uplink, downlink, or bidirectional), the P-CSCF should describe those SDP media lines in the same session information media component (with the same flow ID).

The "early session" disposition SDP can also contain media lines of a type not included in the "session" disposition SDP, or several media lines of the same type. Such media components shall be described in own media components in the service information.

If the P-CSCF desires to invoke special policies or separate event notifications for an "early session" disposition media line, it may choose to provision a separate session information media component even if a media line with the same media type and directionality is contained in "session" disposition SDP.

NOTE 1: A PCF is then likely to supply separate PCC rules for early media and the corresponding final media. This may lead to an over provisioning of resources during call establishment and a subsequent reconfiguration of the radio bearer, or even to a call failure if the extra resources are not authorized or available.

If the P-CSCF receives "early session" disposition SDP before any "session" disposition SDP and supplies service information derived from the "early session" disposition SDP at this point of time, it shall use dedicated media components relating only to the "early session" disposition SDP in the service information.

NOTE 2: The "session" disposition SDP offer will frequently occur before the "early session" disposition SDP offer, but can also occur in parallel or in exceptional cases afterwards. The "session" disposition SDP answer can be contained in the same SIP message as the "early session" disposition SDP offer, or can be sent in a 200 OK (INVITE), i.e. after the "early session" disposition SDP answer.

If the P-CSCF includes any media component relating both to "early session" disposition SDP and "session" disposition SDP in the service information, the P-CSCF shall:

- provision the service information derived from "early session" disposition SDP and the service information derived from "session" disposition SDP in separate Npcf_PolicyAuthorization_Update requests (to the same "Individual Application Session Context" resource), and shall send a new Npcf_PolicyAuthorization_Update request only after any previous Npcf_PolicyAuthorization_Update request has been acknowledged; and

- provision the first service information (either derived from "early session" disposition SDP or "session" disposition SDP) without the "sipForkInd" attribute, or with "sipForkInd" attribute with value "SINGLE_DIALOGUE"; and

- provision all subsequent service information during ongoing call establishment with the "sipForkInd" attribute with value SEVERAL_DIALOGUES; and

- if an SDP answer has been received and codecs are provisioned within the "codecs" attribute included in a media component of the "medComponents" attribute, provision within a "codecs" attribute the codec derived from the corresponding offer together with a codec derived from the SDP answer.

NOTE 3: The P-CSCF needs to provision the service information derived from "early session" disposition SDP and the service information derived from "session" disposition SDP in separate Npcf_PolicyAuthorization_Update requests because the encoding of the media component does not allow for the simultaneous provisioning of two corresponding filters.

NOTE 4: The PCF will treat service information containing the "sipForkInd" attribute as described in clause B.3.

### B.6.3 Updating the Provisioned Service Information when Dialogue is established

The P-CSCF shall store the SDP information for the "session" disposition type until the first final SIP answer is received. Then the early media described in the "early session" disposition type SDP are terminated.

The P-CSCF shall then update the service information to match the requirements of the media described in the "session" disposition type SDP only:

- If the P-CSCF included any media component relating both to "early session" disposition SDP and "session" disposition SDP in the service information, the P-CSCF shall send an Npcf_PolicyAuthorization_Update request without the "sipForkInd" attribute or with a "sipForkInd" attribute with value SINGLE_DIALOGUE and shall include the service information derived from the "session" disposition SDP. The P-CSCF shall provision the full service information including the applicable "fDescs" attribute and "fStatus" attribute.

- The P-CSCF shall disable any media component(s) in the service information that relate to early media only by setting their flow status to "REMOVED".

## B.7 Provision of Signalling Flow Information at P-CSCF

When the P-CSCF has successfully concluded the initial registration of an attached UE, i.e., when the P-CSCF has sent to the UE a SIP 200 (OK) response to the SIP REGISTER request, the P-CSCF may provision information about the SIP signalling flows between the UE and itself using the procedure specified in clause 4.2.2.16. If the P-CSCF already has created an "Individual Application Session Context" resource with the PCF related to the signalling with the UE, e.g. one that has been opened according to the procedure described in clause B.4, the P-CSCF shall reuse the already open session to provision the SIP Signalling IP Flow information using the procedure specified in clause 4.2.3.17.

NOTE: This procedure is not applicable for IMS registrations for Emergency sessions.

If the P-CSCF provisions information about SIP signalling flows, the P-CSCF shall ensure that for each signalling IP flow information it provides, the flow descriptions within the "fDescs" attribute shall accurately reflect the IP flow information as seen in the IP header 'on the wire'. The P-CSCF shall set the value of the "afSigProtocol" attribute to "SIP".

When the P-CSCF de-registers the UE and terminates SIP Signalling to the UE, the P-CSCF shall de-provision the SIP Signalling IP flow information from the PCRF as described in clauses 4.2.2.16 and 4.2.3.17.

# B.8 Retrieval of network provided location information

## B.8.1 General

According to clause E.7 of 3GPP TS 23.228 [33], the P-CSCF can use PCC to retrieve network provided location information. Information flows related to the distribution of network provided location information within the IMS are provided in Annex R of 3GPP TS 23.228 [33].

The following clauses provide optional PCC procedures to support the retrieval of network provided location information.

The originating P-CSCF can, depending on operator policy, retrieve the user location and/or UE Time Zone information either before sending the INVITE or MESSAGE towards the terminating side or upon reception of the SDP answer from the terminating side.

The terminating P-CSCF can, depending on operator policy, retrieve the user location and/or UE Time Zone information either upon reception of a SIP INVITE or upon reception of a SIP response.

The originating and terminating P-CSCF can, depending on operator policy, retrieve the user location and/or UE Time Zone information at mid call. e.g., when the P-CSCF learns about the access type change.

## B.8.2 Retrieval of network provided location information at originating P-CSCF for inclusion in SIP Request

If the originating P-CSCF is required by operator policy to retrieve network provided location information before forwarding a SIP INVITE request, upon reception of the SIP INVITE/UPDATE request, the P-CSCF shall invoke:

- the Npcf_PolicyAuthorization_Create service operation according to clause 4.2.2.14 (SIP INVITE request); or
- the Npcf_PolicyAuthorization_Update service operation according to clause 4.2.3.14 or the Npcf_PolicyAuthorization_Subscribe service operation according to clause 4.2.6.6 (SIP INVITE/UPDATE request);

including in the corresponding HTTP request:

- an entry of the "AfEventSubscription" data type in the "events" attribute with:
  a) the "event" attribute set to the value "ANI_REPORT"; and
  b) the "notifMethod" attribute set to the value "ONE_TIME"; and
- the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

If the SIP INVITE request is an initial SIP INVITE request, the P-CSCF shall create a new "Individual Application Session Context" for the new SIP session with the Npcf_PolicyAuthorization_Subscribe service operation according to clause 4.2.6.6 (if no session information is included) or with the Npcf_PolicyAuthorization_Create service operation according to clause 4.2.2.14 (if preliminary session information is included).

The P-CSCF will receive the access network information from the PCF within the Npcf_PolicyAuthorization_Notify service operation as described in clause 4.2.5.11 and should include this access network information in the SIP INVITE/UPDATE requests that it forwards. When the retrieved access network information corresponds to the "tnapId" or "twapId" attribute, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in clause E.8 of 3GPP TS 23.228 [33].

If the originating P-CSCF is required by operator policy to retrieve network provided location information before forwarding a SIP MESSAGE request, upon reception of a MESSAGE request, the P-CSCF shall invoke the Npcf_PolicyAuthorization_Subscribe service operation including in the corresponding HTTP request:

- the IP address (IPv4 or IPv6) of the UE in the "ueIpv4" or "ueIpv6" attribute;

- a media component within the "medComponents" attribute including:

  a) the "medCompN" attribute set to "0"; and

  b) a single media subcomponent within the "medSubComps" attribute with:

     i. the "flowUsage" attribute set to the value "AF_SIGNALLING"; and

     ii. if the procedures for AF provisioning of AF signalling flow information do not apply, the "fNum" attribute set to "0".

- an entry of the "AfEventSubscription" data type in the "events" attribute with:

  a) the "event" attribute set to the value "ANI_REPORT"; and

  b) the "notifMethod" attribute set to the value "ONE_TIME"; and

- the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

The P-CSCF will receive the access network information from the PCF within the Npcf_PolicyAuthorization_Notify service operation as described in clause 4.2.5.11 and should include this access network information in the SIP MESSAGE requests that it forwards. When the retrieved access network information corresponds to the "tnapId" or "twapId" attribute, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in clause E.8 of 3GPP TS 23.228 [33].

If the AF application session context is only used for retrieval of network provided location information, at reception of this information, the AF may delete the context of application session information using the Npcf_PolicyAuthorization_ Delete service operation.

## B.8.3 Retrieval of network provided location information at originating P-CSCF for inclusion in SIP response confirmation

If an originating P-CSCF is required by operator policy to retrieve network provided location information before forwarding an SDP answer, the P-CSCF shall apply the following procedures.

Upon reception of an SDP offer, the P-CSCF may invoke the Npcf_PolicyAuthorization_Create service operation to the PCF according to clause B.1 and may include in the corresponding HTTP POST request:

- an entry of the "AfEventSubscription" data type in the "events" attribute with:

  a) the "event" attribute set to the value "ANI_REPORT"; and

  b) the "notifMethod" attribute set to the value "ONE_TIME"; and

- the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

Upon reception of an SDP answer, the P-CSCF will invoke the Npcf_PolicyAuthorization_Update service operation to the PCF according to clause B.1. If the P-CSCF has not requested access network information upon reception of the SDP offer, the P-CSCF shall include in the corresponding HTTP PATCH request:

- an entry of the "AfEventSubscription" data type in the "events" attribute with:

  a) the "event" attribute set to the value "ANI_REPORT"; and

  b) the "notifMethod" attribute set to the value "ONE_TIME"; and

- the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

The P-CSCF will receive the access network information from the PCF in the Npcf_PolicyAuthorization_Notify service operation and should include this access network information in the SIP message with the response confirmation before

forwarding it. When the retrieved access network information corresponds to the "tnapId" or "twapId" attribute, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in clause E.8 of 3GPP TS 23.228 [33].

## B.8.4 Retrieval of network provided location information at terminating P-CSCF

If a terminating P-CSCF is required by operator policy to retrieve network provided location information at session establishment and/or modification, the P-CSCF shall apply the following procedures.

The terminating P-CSCF may request network provided location information upon reception of a SIP INVITE request in the following manner:

- if the SIP INVITE request is an initial SIP INVITE request, the P-CSCF shall create a new "Individual Application Session Context" for the new SIP session with the Npcf_PolicyAuthorization_Subscribe service operation according to clause 4.2.6.6 (if no session information is included) or with the Npcf_PolicyAuthorization_Create service operation according to clause 4.2.2.14 (if preliminary session information is included);

- if the SIP INVITE contains an SDP offer, the P-CSCF shall include in the corresponding HTTP request:

  a) an entry of the "AfEventSubscription" data type in the "events" attribute with:

     (i) the "event" attribute set to the value "ANI_REPORT"; and

     (ii) the "notifMethod" attribute set to the value "ONE_TIME";

  b) the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information);

  c) service information derived from the SDP offer; and

  d) the "servInfStatus" attribute with the value set to "PRELIMINARY"; and

- if the SIP INVITE does not contain an SDP offer, the P-CSCF shall include in the corresponding HTTP request:

  a) an entry of the "AfEventSubscription" data type in the "events" attribute with:

     (i) the "event" attribute set to the value "ANI_REPORT"; and

     (ii) the "notifMethod" attribute set to the value "ONE_TIME"; and

  b) the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

Upon reception of a SIP response that requires the inclusion of access network information, if the P-CSCF has not already requested network provided location information upon reception of the corresponding SIP INVITE request, the P-CSCF shall request network provided location information in the following manner:

- if an "Individual Application Session Context" related to service data has not yet been created, the P-CSCF shall create an "Individual Application Session Context" for the new SIP session with the Npcf_PolicyAuthorization_Subscribe service operation according to clause 4.2.6.6 (if no session information is included) or with the Npcf_PolicyAuthorization_Create service operation according to clause 4.2.2.14 (if session information is included);

- if the SIP response includes an SDP answer, the P-CSCF shall send an HTTP request to the PCF according to clause B.1; the P-CSCF shall include in this HTTP request:

  a) an entry of the "AfEventSubscription" data type in the "events" attribute with:

     (i) the "event" attribute set to the value "ANI_REPORT"; and

     (ii) the "notifMethod" attribute set to the value "ONE_TIME"; and

b) the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information);

- if the SIP response does not contain an SDP body, the P-CSCF shall include in the corresponding HTTP request:

a) an entry of the "AfEventSubscription" data type in the "events" attribute with:

(i) the "event" attribute set to the value "ANI_REPORT"; and

(ii) the "notifMethod" attribute set to the value "ONE_TIME"; and

b) the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information); and

- if the SIP response includes an SDP offer, the P-CSCF shall include in the corresponding HTTP request:

- a) an entry of the "AfEventSubscription" data type in the "events" attribute with:

(i) the "event" attribute set to the value "ANI_REPORT"; and

(ii) the "notifMethod" attribute set to the value "ONE_TIME";

b) the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information);

c) service information derived from the SDP offer; and

d) the "servInfStatus" attribute with the value set to "PRELIMINARY".

The P-CSCF will receive the access network information from the PCF in the Npcf_PolicyAuthorization_Notify service operation and should include this access network information in the appropriate SIP response before forwarding it. When the retrieved access network information corresponds to the "tnapId" or "twapId" attribute, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in clause E.8 of 3GPP TS 23.228 [33].

If the terminating P-CSCF is required by operator policy to retrieve network provided location information upon reception of a SIP MESSAGE response, the P-CSCF shall behave according to B.8.2.

## B.8.5 Provisioning of network provided location information at SIP session release

If a P-CSCF is required by operator policy to include network provided location information in SIP session release signalling, the P-CSCF shall apply the following procedures:

Upon reception of a SIP session release request that requires the inclusion of network provided location information, the P-CSCF will invoke the Npcf_PolicyAuthorization_Delete service operation to the PCF according to clause 4.2.4.6 and shall include in the HTTP request:

- an entry of the "AfEventSubscription" data type in the "events" attribute with:

a) the "event" attribute set to the value "ANI_REPORT"; and

b) the "notifMethod" attribute set to the value "ONE_TIME"; and

- the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information).

The P-CSCF will receive the access network information from the PCF in the Npcf_PolicyAuthorization_Delete service operation according to clause 4.2.4.6 and shall include this access network information in the appropriate SIP message before forwarding it. When the retrieved access network information corresponds to the "tnapId" or "twapId" attribute, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in clause E.8 of 3GPP TS 23.228 [33].

### B.8.6 Provisioning of network provided location information at mid call

If a P-CSCF is required by operator policy to include network provided location information at mid call, the P-CSCF shall apply the following procedures:

Upon reception of a trigger (e.g., when the P-CSCF learns about the access change) that requires the inclusion of network provided location information in a SIP message, the P-CSCF will invoke the Npcf_PolicyAuthorization_Update and shall include in the corresponding HTTP request:

a) an entry of the "AfEventSubscription" data type in the "events" attribute with:

   (i) the "event" attribute set to the value "ANI_REPORT"; and

   (ii) the "notifMethod" attribute set to the value "ONE_TIME";

b) the "reqAnis" attribute, with the required access network information, i.e. user location and/or user time zone information);

c) service information related to the service according to clause 4.2.3.2.

The P-CSCF will receive the access network information from the PCF in the Npcf_PolicyAuthorization_Notify service operation, and should include this access network information in the appropriate SIP message before forwarding it. When the retrieved access network information corresponds to the "tnapId" or "twapId" attribute, the P-CSCF may also map the retrieved access network information to a Geographical Identifier for routing, as specified in clause E.8 of 3GPP TS 23.228 [33].

## B.9 Resource Sharing

The P-CSCF may indicate to the PCF that media of an "Individual Application Session Context" resource may share resources with media belonging to other "Individual Application Session Context" resources according to 3GPP TS 23.228 [33].

If the P-CSCF determines that resource sharing is possible, it may at creation of a new "Individual Application Session Context" resource, include the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute indicating that media resources may be shared in the related direction. The P-CSCF shall assign a distinct value for the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute for each media component within the "medComponents" attribute.

NOTE 1: When resource sharing applies to both directions for a certain media component, the P-CSCF can assign the same value for "sharingKeyUl" attribute and "sharingKeyDl" attribute within the same media component.

The P-CSCF shall not include the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute within the media components in the "medComponents" attribute when the "Individual Application Session Context" resource relates to an Emergency Session.

The PCF shall not include the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute for those PCC/QoS Rules related to the RTCP traffic.

Trigger conditions that require applying or stopping resource sharing are described in 3GPP TS 24.229 [32].

NOTE 2: When P-CSCF needs to stop sharing according to the procedures described in 3GPP TS 24.229 [32], the P-CSCF will provide "null" value for the "sharingKeyUl" attribute and/or "sharingKeyDl" attribute within the media component in the "medComponents" attribute.

# B.10 Handling of MCPTT priority call

## B.10.1 General

Within the framework of MCPTT, when the SIP Core (3GPP TS 24.379 [41]) is implemented by an IMS core network, if the P-CSCF receives a SIP request message including a Resource-Priority header field with a namespace field and priority value defined for MCPTT for adjusting the priority of an MCPTT session, the P-CSCF shall provide the "resPrio" attribute and the "mcpttId" in the Npcf_PolicyAuthorization_Create request as defined in clause B.13.2 to allow the PCF to set the corresponding PCC rule(s) according to the prioritized MCPTT service. Additionally, if "PrioritySharing" feature is supported, the P-CSCF may provide the "prioSharingInd" attribute within the media component included in the "medComponents" attribute as described in clause B.1. For MCPTT the service priority and the priority sharing indicator are defined in 3GPP TS 24.379 [41].

NOTE 1: The process of adjusting priority may occur several times during the course of one session, e.g. a normal MCPTT group call elevated to an MCPTT emergency group call, returned to a normal priority MCPTT group call, elevated to an MCPTT imminent peril group call and returned to a normal priority MCPTT group call.

NOTE 2: Upon reception of a request that requires the adjustment of the MCPTT priority, the PCF is expected to derive the PCC Rules corresponding to the this MCPTT session, as appropriate according to operator policies.

NOTE 3: The PCF can identify an MCPTT call using the IMS Communication Service Identifier specific to MCPTT, which is provided by the P-CSCF in the "afAppId" attribute in the Npcf_PolicyAuthorization_Create request sent to PCF.

## B.10.2 Determination of MCPTT priority parameter values

When the P-CSCF receives an authorized Resource-Priority header field containing an appropriate namespace and priority value used for MCPTT in SIP signalling, the P-CSCF shall include the "mcpttId" attribute and the "resPrio" attribute in the corresponding Npcf_PolicyAuthorization service operation towards the PCF.

The "mcpttId" attribute shall include the namespace defined for MCPTT as received within the Resource-Priority header field.

NOTE: Two different values are defined for the MCPTT-Identifier AVP, one for each namespace value defined for MCPTT (see IETF RFC 8101 [42]).

The "resPrio" attribute shall contain the priority value of the Resource-Priority header; the lowest priority shall be mapped to PRIO_1 (Resource-Priority header value 0), the next after the lowest to PRIO_2 (Resource-Priority header value 1), and so on up to the highest priority which shall be mapped to PRIO_16 (Resource-Priority header value 15).

Additionally, when the P-CSCF receives information about priority sharing from an MCPTT server that supports simultaneous sessions and that needs to share a common priority for several MCPTT sessions and if "PrioritySharing" feature is supported, the P-CSCF may include the "prioSharingInd" attribute within the media component received in the "medComponents" attribute in the corresponding Npcf_PolicyAuthorization service operation. See 3GPP TS 24.379 [41] for further information.

# B.11 Handling of MCVideo priority call

## B.11.1 General

Within the framework of MCVideo, when the SIP Core (3GPP TS 23.281 [34]) is implemented by an IMS core network, if the P-CSCF receives a SIP request message including a Resource-Priority header field with a namespace field and priority value defined for MCVideo for adjusting the priority of an MCVideo session, the P-CSCF shall provide the "resPrio" attribute and the "mcVideoId" in the Npcf_PolicyAuthorization_Create request as defined in clause B.15.2 to allow the PCF to set the corresponding PCC rule(s) according to the prioritized MCVideo service.

NOTE 1: The process of adjusting priority may occur several times during the course of one session, e.g. a normal MCVideo group call elevated to an MCVideo emergency group call and returned to a normal priority MCVideo group call, elevated to an MCVideo imminent peril group call and returned to a normal priority MCVideo group call.

NOTE 2: Upon reception of a request that requires the adjustment of the MCVideo priority, the PCF is expected to derive the PCC Rules corresponding to the this MCVideo session, as appropriate according to operator policies.

NOTE 3: The PCF can identify an MCVideo call using the IMS Communication Service Identifier specific to MCVideo, which is provided by the P-CSCF in the "afAppId" attribute in the Npcf_PolicyAuthorization_Create request sent to PCF.

## B.11.2 Determination of MCVideo priority parameter values

When the P-CSCF receives an authorized Resource-Priority header field containing an appropriate namespace and priority value used for MCVideo in SIP signalling, the P-CSCF shall include the "mcVideoId" attribute and the "resPrio" attribute in the corresponding Npcf_PolicyAuthorization service operation towards the PCF.

The "mcVideoId" attribute shall include the namespace defined for MCVideo as received within the Resource-Priority header field.

The "resPrio" attribute shall contain the priority value of the Resource-Priority header; the lowest priority shall be mapped to PRIO_1 (Resource-Priority header value 0), the next after the lowest to PRIO_2 (Resource-Priority header value 1), and so on up to the highest priority which shall be mapped to PRIO_16 (Resource-Priority header value 15).

# B.12 Notification Access Type Change

When the P-CSCF receives an initial SIP REGISTER message or a SIP INVITE message from an attached UE, the P-CSCF may request from the PCF the information about the access type the UE is attached to using the procedure specified in clauses 4.2.2.2, 4.2.3.2 and 4.2.6.2.

NOTE 1: This procedure is not applicable for IMS registrations for Emergency sessions.

NOTE 2: The P-CSCF can request information about the access type as part of the SIP session setup when it is only interested in the related information when the IMS session is ongoing.

If the P-CSCF requests information about the access type, the P-CSCF shall also subscribe within the same Npcf_PolicyAuthorization service operation to notifications for changes of the access type used by the UE. The P-CSCF shall include an entry of the "AfEventSubscription" data type in the "events" attribute with the "event" attribute set to the value "ACCESS_TYPE_CHANGE".

When the P-CSCF receives from the PCF the access type:

- in the subscription request response within the HTTP response; or
- in the notification of access type change in an HTTP POST request from the PCF,

the P-CSCF shall store the access type information received within the "accessType" attribute and the RAT type information received within "ratType" attribute and use the received information as per P-CSCF procedures in 3GPP TS 24.229 [32].

The P-CSCF may receive subsequent notifications for changes of the access type from the PCF according to clause 4.2.5.2. When the P-CSCF receives a notification of the change of the access type used by the UE, the P-CSCF shall store the new access type information and RAT type information and use the received information as per P-CSCF procedures in 3GPP TS 24.229 [32].

NOTE 3: The subscription to receive information about the access type will be cancelled when the corresponding Individual Application Session Context resource is removed by the P-CSCF (i.e. when the UE is de-REGISTERED or the related SIP call is released).

# B.13 Notification of PLMN Change

When the P-CSCF receives an initial SIP REGISTER message from an attached UE, the P-CSCF may subscribe to notifications of PLMN changes corresponding to the identity of the network (either a PLMN or an SNPN) where the UE is located using the procedure specified in clauses 4.2.2.2, 4.2.3.2 and 4.2.6.2.

NOTE: For a UE located in an SNPN the SNPN Identifier consisting of the PLMN Identifier and the NID is provided.

When the P-CSCF receives the subscription request response in an HTTP response or the notification of PLMN change in an HTTP POST request from the PCF, the P-CSCF shall store the PLMN Identifier and, if available, the NID received within the "plmnId" attribute and use the received information as per P-CSCF procedures in 3GPP TS 24.229 [32].

The P-CSCF shall cancel the subscription to notification for changes of the PLMN used by the UE when the user is de-registered from the IM CN subsystem.

# B.14 Coverage and Handoff Enhancements using Multimedia error robustness feature (CHEM)

As a network option, the P-CSCF may support the PCC procedures in the present clause to handle the Coverage and Handoff Enhancements using Multimedia error robustness feature (CHEM).

NOTE: When the CHEM feature is supported, improved error robustness might be enabled by packet-loss handling procedures of the codec, codec mode, or codec configuration to avoid, delay, or reduce the need to handoff a terminal due to degradation in the media quality. Communicating the level of robustness of the media to the network enables the eNB to use this information to determine a threshold for when the terminal should be handed off to another cell, domain (circuit-switched vs. packet-switched), or radio access technology.

When a session is initiated or modified the P-CSCF supporting the CHEM feature shall derive the "maxPacketLossRateDl" attribute and "maxPacketLossRateUl" attribute based on the PLR_adapt and maxe2e-PLR attribute values in both the SDP offer and/or SDP answer to determine the maximum tolerable end-to-end PLR budget distributed across the uplink and downlink in a media transport path as described in 3GPP TS 29.513 [7] clause 7.2.3.

Upon reception of SDP offer and answer, the P-CSCF should check whether "a= PLR_adapt" line is present in both SDP offer and answer to derive "maxPacketLossRateDl" attribute and "maxPacketLossRateUl" attribute in "medComponents" attribute else "maxPacketLossRateDl" and "maxPacketLossRateUl" attributes are not included by the P-CSCF.

The originating P-CSCF should derive "maxPacketLossRateDl" attribute to the maximum value of MaxPacketLossRateDl among all the RTP payload types. For each RTP payload type MaxPacketLossRateDl is computed as described in 3GPP TS 29.513 [7] clause 7.2.3.

- If maxe2e-PLR is included in the SDP offer then the MaxPacketLossRateDl for a payload type is derived as value of maxe2e-PLR in the SDP offer minus maxUL-PLR in the SDP answer if present else the MaxPacketLossRateDlis ½ maxe2e-PLR value present in the SDP offer.

- If maxe2e-PLR is not included in the SDP offer then the MaxPacketLossRateDl for a payload type is derived from the default value in end-to-end Maximum End-to-End Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [30]clause X.1.2 for application layer redundancy or X.1.1 for partial redundancy minus maxUL-PLR in the SDP answer if present else the MaxPacketLossRateDl ½ default value in end-to-end Maximum End-to-End Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [30] clause X.1.2 for application layer redundancy or X.1.1 for partial redundancy.

The originating P-CSCF should derive "maxPacketLossRateUl" attribute to the maximum value of MaxPacketLossRateUl among all the RTP payload types. For each RTP payload type MaxPacketLossRateUl is computed as described in 3GPP TS 29.513 [7] clause 7.2.3.

- If maxe2e-PLR is included in the SDP answer then the MaxPacketLossRateUl for a payload type is derived as value of maxe2e-PLR in the SDP answer minus maxDL-PLR in the SDP answer if present else the MaxPacketLossRateUl is ½ maxe2e-PLR value present in the SDP answer.

- If maxe2e-PLR is not included in the SDP answer then the MaxPacketLossRateUl for a payload type is derived as the ½ default value in end-to-end Maximum End-to-End Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [30] clause X.1.2 for application layer redundancy or X.1.1 for partial redundancy.

The terminating P-CSCF should derive "maxPacketLossRateDl" attribute to the maximum value of MaxPacketLossRateDl among all the RTP payload types. For each RTP payload type MaxPacketLossRateDl is computed as described in 3GPP TS 29.513 [7] clause 7.2.3.

- If maxe2e-PLR is included in the SDP answer then the MaxPacketLossRateDl for a payload type is derived as value of maxDL-PLR in the SDP answer if present else the MaxPacketLossRateDl is ½ maxe2e-PLR value present in the SDP answer.

- If maxe2e-PLR is not included in the SDP answer then the MaxPacketLossRateDl for a payload type is derived as the ½ default value in end-to-end Maximum End-to-End Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [30] clause X.1.2 for application layer redundancy or X.1.1 for partial redundancy.

The terminating P-CSCF should derive "maxPacketLossRateUl" attribute to the maximum value of MaxPacketLossRateUl among all the RTP payload types. For each RTP payload type MaxPacketLossRateUl is computed as described in 3GPP TS 29.513 [7] clause 7.2.3.

- If maxe2e-PLR is included in the SDP offer then the MaxPacketLossRateUl for a payload type is derived as value of maxUL-PLR in the SDP answer if present else the MaxPacketLossRateUl is ½ maxe2e-PLR value present in the SDP offer.

- If maxe2e-PLR is not included in the SDP offer then the MaxPacketLossRateUl for a payload type is derived as the ½ default value in end-to-end Maximum End-to-End Packet Loss Rate for the decoder of the RTP payload type as recommended in 3GPP TS 26.114 [30] clause X.1.2 for application layer redundancy or X.1.1 for partial redundancy.

## B.15 Handling of a FLUS session

If the P-CSCF receives a SIP request that requires provisioning of a service information to the PCF, the "FLUS" feature is supported and an SDP attribute "a=label:flus…" is included in one or more of the received SDP media descriptions, the P-CSCF shall provide the string after "a=label:" starting with "flus" within the "flusId" attribute for each affected media components within the "medComponents" attribute in the corresponding Npcf_PolicyAuthorization service operation towards the PCF.

NOTE: During the first interaction with the PCF, the P-CSCF does not know if the "FLUS" feature is supported by the PCF. In this case the P-CSCF will include the information as if the feature is supported.

If additionally the P-CSCF receives the "a=3gpp-qos-hint" media-level SDP attribute in the SIP request, the P-CSCF shall provide the PCF with the "desMaxLatency" attribute and/or "desMaxLoss" attribute as described in 3GPP TS 29.513 [7], clause 7.2.3.

Upon receiving the information from the P-CSCF and if the "FLUS" feature is supported, the PCF shall derive the QoS information as described in 3GPP TS 29.513 [7], clause 7.3.3.

## B.16 QoS hint support for data channel media

If the P-CSCF receives a SIP request that requires provisioning of a service information to the PCF, the QoSHint feature is supported and an SDP attribute "a=3gpp-qos-hint" is included in one or more of the received data channel media descriptions, the P-CSCF may provide the "desMaxLatency" attribute and/or "desMaxLoss" attribute for each affected application media component within the "medComponents" attribute in the corresponding Npcf_PolicyAuthorization service operation towards the PCF.

NOTE: During the first interaction with the PCF, the P-CSCF does not know if the QoSHint feature is supported by the PCF. In this case the P-CSCF will include the information as if the feature is supported.

Upon receiving the information from the P-CSCF and if the QoSHint feature is supported, the PCF shall derive the QoS information as described in 3GPP TS 29.513 [7], clause 7.3.3.

# B.17 Handling of MPS Session

When the P-CSCF receives an authorised Resource-Priority header field or when the P-CSCF adds a temporarily authorised Resource-Priority header field containing an appropriate namespace and priority value in SIP signaling, and recognizes the need for priority treatment as specified in 3GPP TS 24.229 [32], and the "IMS_SBI" feature is supported, the P-CSCF shall include the "mpsId" attribute and the "resPrio" attribute in the corresponding Npcf_PolicyAuthorization service operation towards the PCF. The "mpsId" attribute shall contain the national variant for MPS service name indicating an MPS session. The "resPrio" attribute shall be determined based on the resource value received in the "wps" namespace of the SIP Resource-Priority header field, and shall be included at "AppSessionContextReqData" data type level as well as the "MediaComponent" data type level. The "resPrio" attribute shall be populated with a default value if the priority value is unknown.

NOTE 1: Various mechanisms can be applied to recognize the need for priority treatment in the P-CSCF (e.g., based on the dialled digits), according to national regulation and network configuration, as stated in 3GPP TS 24.229 [32].

NOTE 2: Highest user priority level (lowest numerical resource value of the SIP Resource-Priority header field) is mapped to the highest enumerated value of the "resPrio" attribute.

If the P-CSCF supports the SBI Message Priority mechanism for an MPS session, the P-CSCF shall include the "3gpp-Sbi-Message-Priority" custom HTTP header with a priority value based on the value of the "resPrio" attribute. The highest "resPrio" value is mapped to the corresponding lowest value of the "3gpp-Sbi-Message-Priority" custom HTTP header.

Upon reception of a request that requires MPS treatment, the PCF shall derive the PCC rules corresponding to the MPS session, as appropriate. The PCF shall take specific actions on the corresponding PDU session to ensure that the MPS session is prioritized, as described in 3GPP TS 29.512 [8], clause 4.2.6.2.12.3.

When the P-CSCF detects that the MPS session has ended, the P-CSCF deletes in the PCF the "Individual Application Session Context" resource corresponding to the MPS session. The PCF shall delete the PCC rules corresponding to the MPS session and shall revoke the actions related to the prioritization of the MPS session in the corresponding PDU session, as described in 3GPP TS 29.512 [8], clause 4.2.6.2.12.3.

# Annex C (normative): Flow identifiers: Format definition and examples

## C.1 Format of a flow identifier

### C.1.1 General

A flow identifier is expressed as a 2-tuple as follows:

> <The ordinal number of the position of the media component description in the SDI. The ordinal number of the IP flow(s) within the media component description assigned in the order of increasing downlink port numbers as detailed below.>

where both are numbered starting from 1. The encoding of the flow identifier is as indicated in 3GPP TS 24.008 [36].

The rules for the allocation of flow identifiers to IP flows are defined in 3GPP TS 29.214 [20], Annex B.1.1. Derivation of flow identifiers from SDP are described in 3GPP TS 29.214 [20], Annex B.1.2, and examples are covered in 3GPP TS 29.214 [20], Annex B2, B3, B4 and B5.

# Annex D (normative): Wireless and wireline convergence access support

## D.1 Scope

This annex provides the stage 3 definition of the Policy Authorization Service for wireless and wireline convergence access support for 5GS.

The stage 2 definition and procedures of the Policy Authorization Service for wireless and wireline convergence access support for 5GS are contained in 3GPP TS 23.316 [44].

## D.2 Npcf_PolicyAuthorization Service

### D.2.1 Service Description

#### D.2.1.1 Overview

The overview defined in clause 4.1.1 applies with the exception that the UE is replaced by the 5G-RG and the W-AGF, which is acting as a UE towards the 5GC on behalf of the FN-RG.

#### D.2.1.2 Service Architecture

The service architecture defined in clause 4.1.2 applies.

#### D.2.1.3 Network Functions

##### D.2.1.3.1 Policy Control Function (PCF)

The PCF functionality defined in clause 4.1.3.1 shall apply with the following modifications for W-5GAN and for the Npcf_PolicyAuthorization service:

- The 5G-RG and the W-AGF, acting as a UE towards the 5GC on behalf of the FN-RG, replace the UE.
- The PCF provides Policy Authorization as described in this Annex.

##### D.2.1.3.2 NF Service Consumers

The NF service consumer functionality defined in clause 4.1.3.2 shall apply with the following exceptions for the traffic of a PDU session over wireline access:

- Indication that the QoS targets can no longer (or can again) be guaranteed does not apply.
- Invocation of Multimedia Priority Services does not apply in this release of the specification.
- Indication of PLMN change does not apply.
- Indication of TSN 5GS Bridge Information does not apply.
- Reporting RAN/NAS Release Cause over wireline does not apply.
- The Maximum Packet Loss Rate for UL and DL is not forwarded to the wireline access. CHEM feature does not apply.

# D.3 Service Operations

## D.3.1 Introduction

Service procedures covered in clause 4.2.1 shall apply.

## D.3.2 Npcf_PolicyAuthorization_Create Service Operation

### D.3.2.1 General

The procedures specified in clause 4.2.2 shall apply with the following differences:

- Subscriptions to notifications of Service Data Flow QoS targets are not supported. Clause 4.2.2.6 does not apply for the traffic of a PDU session over wireline access.
- Invocation of Multimedia Priority Services is not supported. Clause 4.2.2.12 does not apply for the traffic of a PDU session over wireline access.
- The PEI that may be returned as available user information within the "ueIds" attribute described in clause 4.2.2.18 shall have one of the following representations:
  i. When the UE supports only wireline access, the PEI shall be a MAC address.
  ii. When the UE supports at least one 3GPP access technology, the PEI shall be the allocated IMEI or IMEISV.
- Subscription and notification of PLMN change does not apply for the traffic of a PDU session over wireline access.
- Indication of TSN 5GS Bridge Information does not apply. Clauses 4.2.2.24, 4.2.2.25 and 4.2.2.31 do not apply.
- The Maximum Packet Loss Rate for UL and DL is not forwarded to the wireline access. Clause 4.2.2.28, Support of CHEM feature, does not apply for the traffic of a PDU session over wireline access.
- When the NF service consumer subscribes to the Access Type Change event, the event is met, and the 5G-RG or FN-RG is connected to the 5GC via wireline access, the reported wireline transmission technology is encoded in the "ratType" attribute, within either the EventsNotification data type or the AdditionalAccessInfo data type, as applicable.

## D.3.3 Npcf_PolicyAuthorization_Update Service Operation

### D.3.3.1 General

The procedures specified in clause 4.2.3 shall apply with the following differences:

- Subscriptions to notifications of Service Data Flow QoS targets are not supported. Clause 4.2.3.6 does not apply for the traffic of a PDU session over wireline access.
- Invocation of Multimedia Priority Services is not supported. Clause 4.2.3.12 does not apply for the traffic of a PDU session over wireline access.
- Subscription and notification of PLMN change does not apply for the traffic of a PDU session over wireline access.
- Indication of TSN 5GS Bridge Information does not apply. Clauses 4.2.3.24, and 4.2.3.25 do not apply.
- The Maximum Packet Loss Rate for UL and DL is not forwarded to the wireline access. Clause 4.2.3.27, Support of CHEM feature, does not apply for the traffic of a PDU session over wireline access.

- When the NF service consumer subscribes to the Access Type Change event, the event is met, and the 5G-RG or FN-RG is connected to the 5GC via wireline access, the reported wireline transmission technology is encoded in the "ratType" attribute, within either the EventsNotification data type or the AdditionalAccessInfo data type, as applicable.

## D.3.4 Npcf_PolicyAuthorization_Delete Service Operation

### D.3.4.1 General

The procedures specified in clause 4.2.4 shall apply with the following differences:

- When the report of access network information described in clause 4.2.4.6 includes the user location information, the "n3gaLocation" attribute shall be included in the "ueLoc" attribute and shall encode:

  a) if the UE connects via W-5GBAN access:

     - shall encode the Global Line Identifier in the "gli" attribute; and

     - may include the "w5gbanLineType" attribute to indicate whether the W-5GBAN access is DSL or PON; or

  b) if the UE connects via W-5GCAN access, the HFC Node Identifier in the "hfcNodeId" attribute.

- Reporting RAN/NAS Release Cause over wireline does not apply. Clause 4.2.4.10 does not apply.

## D.3.5 Npcf_PolicyAuthorization_Notify Service Operation

### D.3.5.1 General

The procedures specified in clause 4.2.5 shall apply with the following differences:

- Subscriptions to notifications of Service Data Flow QoS targets are not supported. Clause 4.2.5.4 does not apply for the traffic of a PDU session over wireline access.

- Invocation of Multimedia Priority Services is not supported. Clause 4.2.4.5 does not apply for the traffic of a PDU session over wireline access.

- When the report of access network information described in clause 4.2.5.11 includes the user location information, the "n3gaLocation" attribute shall be included in the "ueLoc" attribute and shall encode:

  a) if the UE connects via W-5GBAN access:

     - shall encode the Global Line Identifier in the "gli" attribute; and

     - may include the "w5gbanLineType" attribute to indicate whether the W-5GBAN access is DSL or PON; or

  b) if the UE connects via W-5GCAN access, the HFC Node Identifier in the "hfcNodeId" attribute.

- Notification of PLMN changes does not apply for the traffic of a PDU session over wireline access.

- Indication of TSN 5GS Bridge Information does not apply. Clauses 4.2.5.13 and 4.2.5.16 do not apply.

- Reporting RAN/NAS Release Cause over wireline does not apply. Clauses 4.2.5.5 and 4.2.5.10 do not apply.

- When the 5G-RG or FN-RG connects to the 5GC via W-5GAN, and the Access Type Change event is met, the reported wireline transmission technology is encoded in the "ratType" attribute, within either the EventsNotification data type or the AdditionalAccessInfo data type, as applicable.

## D.3.6 Npcf_PolicyAuthorization_Subscribe Service Operation

### D.3.6.1 General

The procedures specified in clause 4.2.6 shall apply with the following differences:

- When the NF service consumer subscribes to the Access Type Change event, the event is met, and the 5G-RG or FN-RG is connected to the 5GC via wireline access, the reported wireline transmission technology is encoded in the "ratType" attribute, within either the EventsNotification data type or the AdditionalAccessInfo data type, as applicable.
- Subscription to PLMN change does not apply for the traffic of a PDU session over wireline access.

## D.3.7 Npcf_PolicyAuthorization_Unsubscribe Service Operation

### D.3.7.1 General

The procedures specified in clause 4.2.7 shall apply.

# Annex E (informative): Change history

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2017-10 | | | | | | TS skeleton of Policy Authorization Service specification | 0.0.0 |
| 2017-03 | CT3#92 | | | | | Inclusion of pCRs agreed during CT3#92 | 0.1.0 |
| 2018-01 | CT3#94 | | | | | Inclusion of documents agreed in CT3#94:<br>C3-180036, C3-180038, C3-180212, C3-180213,<br>C3-180214, C3-180217, C3-180218, C3-180243,<br>C3-180313, C3-180314, C3-180315, C3-180316. | 0.2.0 |
| 2018-03 | CT3#95 | | | | | Inclusion of documents agreed in CT3#95:<br>C3-181229, C3-181338, C3-181231, C3-181232, C3-181339, C3-181323 | 0.3.0 |
| 2018-04 | CT3#96 | | | | | Inclusion of documents agreed in CT3#96:<br>C3-182057, C3-182333, C3-182235, C3-182334,<br>C3-182474, C3-182336, C3-182337, C3-182338,<br>C3-182339, C3-182245, C3-182475, C3-182247,<br>C3-182248, C3-182249, C3-182250, C3-182251 | 0.4.0 |
| 2018-06 | CT3#97 | | | | | Inclusion of documents agreed in CT3#97:<br>C3-183220, C3-183222, C3-183230, C3-183233,<br>C3-183234, C3-183239, C3-183281, C3-183300,<br>C3-183301, C3-183517, C3-183518, C3-183520,<br>C3-183521, C3-183522, C3-183523, C3-183524,<br>C3-183525, C3-183526, C3-183577, C3-183579,<br>C3-183580, C3-183581, C3-183582, C3-183583,<br>C3-183584, C3-183585, C3-183586, C3-183587,<br>C3-183588, C3-183589, C3-183590, C3-183591,<br>C3-183592, C3-183820, C3-183821, C3-183822,<br>C3-183879, C3-183882. | 0.5.0 |
| 2018-06 | CT#80 | | | | | TS sent to plenary for approval | 1.0.0 |
| 2018-06 | CT#80 | | | | | TS approved by plenary | 15.0.0 |
| 2018-09 | CT#81 | CP-182015 | 0001 | 2 | F | DNAI change notification type | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0002 | 1 | F | Definition of FlowStatus data type | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0003 | 2 | F | Temporal validity update | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0004 | | F | Modification of Traffic Routing Information provided at AF session level | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0005 | 1 | F | Missing AF Transaction Identifier | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0006 | 2 | B | Solution to IPv4 overlapping | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0007 | 2 | B | Subscription and notification of resources allocation outcome, data model | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0008 | 1 | B | Subscription to resources allocation outcome, service procedures | 15.1.0 |
| 2018-09 | CT#81 | CP-182101 | 0009 | 3 | B | Notification of resource allocation outcome, service procedures | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0010 | 2 | B | Subscription and notification of out of credit events, data model | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0011 | 1 | B | Subscription to out of credit notification, service procedures | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0012 | 3 | B | Out of credit notification, service procedures | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0013 | 1 | F | References to Data Types defined in 5G Technical Specifications | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0014 | 1 | F | Removal of error UNAUTHORIZED_TRAFFIC_ROUTING_REQUEST | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0015 | 3 | F | OpenAPI corrections | 15.1.0 |
| 2018-09 | CT#81 | CP-182015 | 0016 | 1 | F | Description of Structured data types | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0017 | | F | Correction on TemporalValidity | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0018 | 2 | F | Resource structure presentation | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0019 | | F | Corrections related to Feature negotiation | 15.1.0 |
| 2018-08 | CT#81 | CP-182040 | 0020 | 1 | F | Cardinality of optional arrays and maps | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0021 | | F | Application Error: SUBSCRIPTION_NOT_FOUND | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0022 | 2 | F | Completion and clarification of non-3GPP access location information | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0023 | 1 | B | Support of Priority Services | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0024 | 3 | F | Correction of PRA information | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0025 | 1 | F | Updates in clause 4.2.6.3 to detail session binding | 15.1.0 |
| 2018-08 | CT#81 | CP-182100 | 0026 | 2 | B | Support of content versioning for a media component, service procedures | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0027 | | B | Support of content versioning for a media component, data model | 15.1.0 |
| 2018-08 | CT#81 | CP-182103 | 0028 | 2 | B | Updates of QoS Notification Control description and data model | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0029 | 2 | B | Requested Service Temporarily not authorized | 15.1.0 |
| 2018-08 | CT#81 | CP-182102 | 0030 | 2 | B | Support of notification of content version during service data flow deactivation | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0031 | 1 | F | Transfer of RouteToLocation Data Type to TS 29.571 | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0032 | 2 | F | Addition of FlowUsage Information | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0033 | | F | Correction of evsNotif attribute | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0034 | 1 | F | Completing definition of re-used data types | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0035 | | F | Correction of AppSessionContextReqData | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0036 | | F | Correction of evNotif array attribute | 15.1.0 |
| 2018-08 | CT#81 | CP-182015 | 0037 | | F | Removal of Editor's note in subclause 5.6.2.6 | 15.1.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2018-08 | CT#81 | CP-182015 | 0038 | | F | Corrections on TosTrafficClass data type | 15.1.0 |
| 2018-12 | CT#82 | CP-183205 | 0043 | | F | Usage of EventsSubscReqData data type | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0044 | | F | Reference update: RFC 7396 | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0045 | | F | Supported content types | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0046 | | F | Update of sponsored data connectivity indication | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0047 | 3 | F | Npcf_PolicyAuthorization API Authorization based on OAuth2 | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0050 | 1 | F | Removal of references to 3GPP TS 29.508 | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0051 | 1 | F | Correction of 404 error | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0052 | | F | Corrections on Spatial Validity in OpenAPI | 15.2.0 |
| 2018-12 | CT#82 | CP-183125 | 0053 | 2 | F | Corrections on Data Types | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0054 | 5 | F | Adding "nullable" property to OpenAPI definitions of data types | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0055 | | F | Correction of figure 4.2.4.2-1 to include 204 status code | 15.2.0 |
| 2018-12 | CT#82 | CP-183125 | 0056 | 1 | F | Corrections on OpenAPI file | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0058 | 1 | F | Adding the externalDocs field in the OpenAPI | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0059 | | F | Default value for apiRoot | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0060 | 1 | F | Incorrect references | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0061 | 1 | F | OpenAPI: HTTP status codes alignment | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0062 | | F | OpenAPI: usage of the "tags" keyword | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0063 | | F | Presence conditions in OpenAPI file | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0064 | | F | Location header field in OpenAPI | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0065 | | F | Correction of resource URIs | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0066 | 1 | F | New data type for subscriptions to UP Path management events | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0067 | 2 | F | Mandatory traffic routing information for AF influence on traffic routing | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0068 | | F | Incorrect use of Link data type | 15.2.0 |
| 2018-12 | CT#82 | CP-183125 | 0069 | 1 | F | Corrections on QNC trigger name | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0070 | 1 | F | Miscellaneous Corrections | 15.2.0 |
| 2018-12 | CT#82 | CP-183205 | 0071 | | F | Removal of SUBSCRIPTION_NOT_FOUND error from service procedures | 15.2.0 |
| 2018-12 | CT#82 | CP-183125 | 0072 | | F | Update of supported AF events | 15.2.0 |
| 2019-03 | CT#83 | CP-190112 | 0074 | | F | Add GPSI in N5 | 15.3.0 |
| 2019-03 | CT#83 | CP-190112 | 0077 | 1 | F | Miscellaneous corrections | 15.3.0 |
| 2019-03 | CT#83 | CP-190112 | 0078 | 2 | F | Retry-After header definition in OpenAPI | 15.3.0 |
| 2019-03 | CT#83 | CP-190112 | 0079 | 1 | F | OpenAPI Version number update | 15.3.0 |
| 2019-03 | CT#83 | CP-190070 | 0076 | 1 | F | Indication of acceptable service information | 16.0.0 |
| 2019-03 | CT#83 | CP-190069 | 0080 | 3 | F | OpenAPI version update | 16.0.0 |
| 2019-06 | CT#84 | CP-191076 | 0082 | 1 | A | Correction to the encoding of the initial POST request callback URI | 16.1.0 |
| 2019-06 | CT#84 | CP-191076 | 0084 | | A | Storage of OpenAPI specification file | 16.1.0 |
| 2019-06 | CT#84 | CP-191076 | 0088 | 2 | A | Correction to EthFlowDescripiont data type | 16.1.0 |
| 2019-06 | CT#84 | CP-191076 | 0093 | 1 | A | Precedence of OpenAPI file | 16.1.0 |
| 2019-06 | CT#84 | CP-191071 | 0094 | 2 | B | AF acknowledgement to be expected | 16.1.0 |
| 2019-06 | CT#84 | CP-191071 | 0095 | 2 | B | UE IP address preservation Indication | 16.1.0 |
| 2019-06 | CT#84 | CP-191076 | 0097 | | A | Missing resPrio attribute | 16.1.0 |
| 2019-06 | CT#84 | CP-191076 | 0101 | 1 | A | Copyright Note in YAML file | 16.1.0 |
| 2019-06 | CT#84 | CP-191101 | 0105 | 2 | F | OpenAPI Version number update | 16.1.0 |
| 2019-09 | CT#85 | CP-192155 | 0109 | 1 | B | Support of “Access Network Charging Correlation Information” notification | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0110 | 1 | B | Support of “Out of credit” notification | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0111 | | B | Support of the AF charging identifier | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0112 | | B | Support of “Access Network Information Notification” | 16.2.0 |
| 2019-09 | CT#85 | CP-192202 | 0114 | 1 | B | Support a set of MAC addresses in traffic filter | 16.2.0 |
| 2019-09 | CT#85 | CP-192144 | 0116 | 1 | A | Support of Ethernet scenarios | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0117 | 1 | B | IMS related P-CSCF procedures and Service Information Status | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0118 | | B | IMS related P-CSCF procedures, setting flow status and flow number | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0119 | | B | IMS related P-CSCF procedures, Support of SIP Forking | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0120 | 1 | B | IMS related P-CSCF procedures, support of RTCP flows | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0121 | 2 | B | Subscription to notification of Signalling Path Status | 16.2.0 |
| 2019-09 | CT#85 | CP-192222 | 0122 | | B | Provisioning of Signalling Flow Information | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0123 | 1 | B | Resource Sharing Support | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0124 | | B | Support of Mission Critical Push To Talk | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0125 | 1 | B | Support of Mission Critical Video | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0126 | 1 | B | Priority Sharing Indication | 16.2.0 |
| 2019-09 | CT#85 | CP-192155 | 0127 | | B | IMS emergency services | 16.2.0 |
| 2019-09 | CT#85 | CP-192144 | 0129 | | A | Correction to Policy Authorization Update | 16.2.0 |
| 2019-09 | CT#85 | CP-192152 | 0130 | 1 | B | Support of wireline and wireless access convergence, Annex Skeleton | 16.2.0 |
| 2019-09 | CT#85 | CP-192223 | 0131 | 1 | B | Support of wireline and wireless access convergence, NFs | 16.2.0 |
| 2019-09 | CT#85 | CP-192173 | 0133 | | F | OpenAPI version update | 16.2.0 |
| 2019-12 | CT#86 | CP-193181 | 0135 | 1 | F | Open issue for AddrReservation feature | 16.3.0 |
| 2019-12 | CT#86 | CP-193186 | 0137 | | F | Correction to appReloc attribute | 16.3.0 |
| 2019-12 | CT#86 | CP-193196 | 0138 | 1 | B | P-CSCF procedures to support Access Type Change notification | 16.3.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2019-12 | CT#86 | CP-193196 | 0139 | 1 | B | P-CSCF procedures to subscribe to PLMN Change notification | 16.3.0 |
| 2019-12 | CT#86 | CP-193196 | 0140 | 2 | B | Support of the RAN-NAS Release Cause | 16.3.0 |
| 2019-12 | CT#86 | CP-193235 | 0141 | 6 | B | QoS Handling for V2X Communication | 16.3.0 |
| 2019-12 | CT#86 | CP-193181 | 0142 | 3 | B | QoS Monitoring for Service Data Flows | 16.3.0 |
| 2019-12 | CT#86 | CP-193196 | 0144 | | B | NetLoc Correction | 16.3.0 |
| 2019-12 | CT#86 | CP-193222 | 0145 | 2 | B | Transport of TSN information and containers between PCF and AF | 16.3.0 |
| 2019-12 | CT#86 | CP-193222 | 0146 | 1 | B | Transport of TSC assistance information between PCF and AF | 16.3.0 |
| 2019-12 | CT#86 | CP-193260 | 0147 | 5 | B | Indication of PS to CS Handover for 5G SRVCC | 16.3.0 |
| 2019-12 | CT#86 | CP-193215 | 0148 | 4 | B | Coverage and Handover Enhancements for Media (CHEM) | 16.3.0 |
| 2019-12 | CT#86 | CP-193197 | 0149 | 2 | B | Update of API version and TS version in OpenAPI file | 16.3.0 |
| 2019-12 | CT#86 | CP-193186 | 0151 | | A | Correct VLAN tag description | 16.3.0 |
| 2019-12 | CT#86 | CP-193186 | 0153 | | A | Corrections to several mistakes | 16.3.0 |
| 2019-12 | CT#86 | CP-193228 | 0154 | 2 | B | Report of Wireline Location Information | 16.3.0 |
| 2019-12 | CT#86 | CP-193191 | 0155 | 1 | B | Support of 5WWC, supported PEI format | 16.3.0 |
| 2019-12 | CT#86 | CP-193229 | 0156 | 2 | B | Support of Trusted non-3GPP accesses | 16.3.0 |
| 2019-12 | CT#86 | CP-193196 | 0157 | | F | Correction of AF Charging Identifier data type | 16.3.0 |
| 2019-12 | CT#86 | CP-193196 | 0158 | 2 | B | P-CSCF restoration | 16.3.0 |
| 2019-12 | CT#86 | CP-193196 | 0159 | | B | Support of Maximum Supported Bandwidth and Minimum Desired Bandwidth | 16.3.0 |
| 2019-12 | CT#86 | CP-193212 | 0161 | 1 | F | Update of API version and TS version in OpenAPI file | 16.3.0 |
| 2020-03 | CT#87e | CP-200215 | 0162 | | B | Support of Framework for Live Uplink Streaming (FLUS) in Npcf_PolicyAuthorization service | 16.4.0 |
| 2020-03 | CT#87e | CP-200207 | 0174 | | B | DNN Clarification | 16.4.0 |
| 2020-03 | CT#87e | CP-200265 | 0176 | 3 | B | Complete the QoS Monitoring | 16.4.0 |
| 2020-03 | CT#87e | CP-200206 | 0177 | | B | Network provided location information at SIP session release | 16.4.0 |
| 2020-03 | CT#87e | CP-200231 | 0180 | 1 | B | Report of EPS Fallback | 16.4.0 |
| 2020-03 | CT#87e | CP-200201 | 0181 | 1 | B | Update of the indication of PS to CS Handover | 16.4.0 |
| 2020-03 | CT#87e | CP-200254 | 0182 | 3 | B | Configuration of one or more NW-TT port management information containers | 16.4.0 |
| 2020-03 | CT#87e | CP-200218 | 0183 | | B | DS-TT port MAC address as UE MAC address | 16.4.0 |
| 2020-03 | CT#87e | CP-200218 | 0184 | 2 | B | TSCAI input container and TSN QoS container | 16.4.0 |
| 2020-03 | CT#87e | CP-200256 | 0185 | 2 | B | Notification about TSN port detection and/or port management information, AF session exists | 16.4.0 |
| 2020-03 | CT#87e | CP-200255 | 0186 | 1 | B | Notification about TSN port detection and/or port management information, no AF session exists | 16.4.0 |
| 2020-03 | CT#87e | CP-200212 | 0187 | | F | Modification of Alternative Service Requirements | 16.4.0 |
| 2020-03 | CT#87e | CP-200212 | 0188 | | F | Service Procedures for AF session with required QoS functionality | 16.4.0 |
| 2020-03 | CT#87e | CP-200207 | 0189 | | B | Adding "ProblemDetails" data type in table 5.6.1-2 | 16.4.0 |
| 2020-03 | CT#87e | CP-200214 | 0190 | | F | Enumeration PreemptionControlInformationRm and "nullable" keyword | 16.4.0 |
| 2020-03 | CT#87e | CP-200202 | 0191 | | F | Correcting 5G_URLLC errors in clause 5.6 | 16.4.0 |
| 2020-03 | CT#87e | CP-200206 | 0192 | | F | OpenAPI: property containing the pre-emption control information | 16.4.0 |
| 2020-03 | CT#87e | CP-200206 | 0193 | | F | Correcting eIMS5G_SBA errors in clause 5.6 | 16.4.0 |
| 2020-03 | CT#87e | CP-200261 | 0194 | | F | Adding info about removable attributes "maxPacketLossRateDl" and "maxPacketLossRateUl" | 16.4.0 |
| 2020-03 | CT#87e | CP-200212 | 0195 | 1 | F | Correction to QoS notification Control | 16.4.0 |
| 2020-03 | CT#87e | CP-200216 | 0197 | | F | Update of OpenAPI version and TS version in externalDocs field | 16.4.0 |
| 2020-06 | CT#88e | CP-201219 | 0199 | 1 | A | Correction to response for PUT request for Events Subscription | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0200 | 1 | F | Correction to bridge information report and port management information container provisioning | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0201 | 1 | B | Correction to TSCAI provisioning | 16.5.0 |
| 2020-06 | CT#88e | CP-201228 | 0203 | | F | Removal of MAC address | 16.5.0 |
| 2020-06 | CT#88e | CP-201228 | 0204 | | F | Solving ENs related to a global line identity | 16.5.0 |
| 2020-06 | CT#88e | CP-201228 | 0205 | | F | Solving ENs related to NetLoc support for wireline access | 16.5.0 |
| 2020-06 | CT#88e | CP-201213 | 0206 | | F | Adding QosMonitoringInformationRm in table 5.6.1-1 | 16.5.0 |
| 2020-06 | CT#88e | CP-201232 | 0207 | | F | Miscellaneous corrections | 16.5.0 |
| 2020-06 | CT#88e | CP-201246 | 0208 | | F | Support of FLUS feature | 16.5.0 |
| 2020-06 | CT#88e | CP-201246 | 0209 | | F | Names of "maxPacketLossRateDl" and "maxPacketLossRateUl" attributes | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0210 | | B | Adding support of NID | 16.5.0 |
| 2020-06 | CT#88e | CP-201228 | 0211 | | F | Correction to Access Network Information for Trusted non-3GPP access | 16.5.0 |
| 2020-06 | CT#88e | CP-201228 | 0212 | | B | Solving Editor's notes on report of location for Trusted non-3GPP access | 16.5.0 |
| 2020-06 | CT#88e | CP-201229 | 0213 | 3 | B | Access Type Report for a MA PDU session | 16.5.0 |
| 2020-06 | CT#88e | CP-201232 | 0214 | 3 | F | Correction to NetLoc feature | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0215 | 1 | B | Correction to TSCAI UL and DL description | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0216 | 3 | B | Update of TSN related events | 16.5.0 |
| 2020-06 | CT#88e | CP-201244 | 0217 | 1 | F | Storage of YAML files in ETSI Forge | 16.5.0 |
| 2020-06 | CT#88e | CP-201228 | 0218 | 3 | B | Access Type report for WWC | 16.5.0 |
| 2020-06 | CT#88e | CP-201246 | 0219 | 1 | B | Support of applications with specific QoS hints | 16.5.0 |
| 2020-06 | CT#88e | CP-201272 | 0221 | 1 | B | Introduction of Bridge management information | 16.5.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2020-06 | CT#88e | CP-201219 | 0222 | 1 | A | Correction of Policy Authorization Delete API 200 OK response body content | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0224 | 1 | B | DS-TT MAC address derivation | 16.5.0 |
| 2020-06 | CT#88e | CP-201273 | 0225 | 1 | B | Max bitrate of TSN QoS information | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0226 | 1 | B | Port management on TSN AF | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0227 | 1 | F | Service information provisioning for TSN | 16.5.0 |
| 2020-06 | CT#88e | CP-201337 | 0228 | 1 | B | TSN QoS Information derivation on the TSN AF | 16.5.0 |
| 2020-06 | CT#88e | CP-201256 | 0230 | 1 | F | URI of the Npcf_PolicyAuthorization service | 16.5.0 |
| 2020-06 | CT#88e | CP-201219 | 0232 | | A | OpenAPI: adding Location header field in 303 response | 16.5.0 |
| 2020-06 | CT#88e | CP-201228 | 0233 | 1 | B | Events not supported in wireline access | 16.5.0 |
| 2020-06 | CT#88e | CP-201270 | 0234 | 1 | B | Reallocation of credit | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0235 | 1 | B | Indication of Application Sessions resource | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0236 | 1 | B | TSN AF selection by PCF | 16.5.0 |
| 2020-06 | CT#88e | CP-201219 | 0238 | 1 | A | Correction to Subscription operation | 16.5.0 |
| 2020-06 | CT#88e | CP-201244 | 0241 | | F | Optionality of ProblemDetails | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0242 | | B | Providing NID to the P-CSCF | 16.5.0 |
| 2020-06 | CT#88e | CP-201232 | 0243 | 1 | F | "PCSCF-Restoration-Enhancement" feature corrections | 16.5.0 |
| 2020-06 | CT#88e | CP-201244 | 0244 | | F | Required field in OpenAPI file | 16.5.0 |
| 2020-06 | CT#88e | CP-201244 | 0245 | 1 | F | Supported headers, Resource Data type, Operation Name | 16.5.0 |
| 2020-06 | CT#88e | CP-201233 | 0247 | 1 | B | Description of enhanced PCC features in NF description clauses | 16.5.0 |
| 2020-06 | CT#88e | CP-201252 | 0248 | 1 | B | Description of TSN features in NF description clauses | 16.5.0 |
| 2020-06 | CT#88e | CP-201213 | 0249 | | B | Description of URLLC features in NF description clauses | 16.5.0 |
| 2020-06 | CT#88e | CP-201238 | 0250 | | B | Description of V2X features in NF description clauses | 16.5.0 |
| 2020-06 | CT#88e | CP-201255 | 0253 | | F | Update of OpenAPI version and TS version in externalDocs field | 16.5.0 |
| 2020-09 | CT#89e | CP-202065 | 0256 | 1 | F | Data type correction of the reqAni | 16.6.0 |
| 2020-09 | CT#89e | CP-202062 | 0257 | 1 | F | Removal on Editor's notes on traffic forwarding for a MA PDU session | 16.6.0 |
| 2020-09 | CT#89e | CP-202065 | 0258 | | F | Correction to Trusted Non-3GPP location information | 16.6.0 |
| 2020-09 | CT#89e | CP-202065 | 0259 | 1 | F | Correction of handling of non-3GPP location information by the P-CSCF | 16.6.0 |
| 2020-09 | CT#89e | CP-202065 | 0260 | 1 | F | Handling of MPS Session by the P-CSCF | 16.6.0 |
| 2020-09 | CT#89e | CP-202084 | 0261 | | F | Update of OpenAPI version and TS version in externalDocs field | 16.6.0 |
| 2020-12 | CT#90e | CP-203139 | 0262 | 1 | F | Essential Corrections and alignments | 16.7.0 |
| 2020-12 | CT#90e | CP-203127 | 0263 | 1 | F | SBI Message Priority mechanism for emergency session | 16.7.0 |
| 2020-12 | CT#90e | CP-203116 | 0265 | | A | Correction to ACCESS_TYPE_CHANGE | 16.7.0 |
| 2020-12 | CT#90e | CP-203150 | 0266 | 1 | F | Remove the NW-TT port from the TSN bridge info | 16.7.0 |
| 2020-12 | CT#90e | CP-203132 | 0267 | 1 | F | Correction to Alternative QoS Parameter | 16.7.0 |
| 2020-12 | CT#90e | CP-203116 | 0269 | 1 | A | Correction to referenced attributes | 16.7.0 |
| 2020-12 | CT#90e | CP-203111 | 0270 | | F | Corrections on QoS monitoring | 16.7.0 |
| 2020-12 | CT#90e | CP-203111 | 0271 | 1 | F | QoS monitoring report at PDU session termination | 16.7.0 |
| 2020-12 | CT#90e | CP-203139 | 0272 | 1 | F | Storage of YAML files in ETSI Forge | 16.7.0 |
| 2020-12 | CT#90e | CP-203110 | 0273 | 1 | F | Correction to support redirection codes | 16.7.0 |
| 2020-12 | CT#90e | CP-203152 | 0274 | | F | Update of OpenAPI version and TS version in externalDocs field | 16.7.0 |
| 2021-03 | CT#91e | CP-210210 | 0275 | 4 | F | Disable UE notifications at changes related to Alternative QoS Profiles | 16.8.0 |
| 2021-03 | CT#91e | CP-210202 | 0276 | 1 | F | Correction to location information | 16.8.0 |
| 2021-03 | CT#91e | CP-210192 | 0277 | 1 | F | mandate notifCorreId for QoS monitoring subscrtiption | 16.8.0 |
| 2021-03 | CT#91e | CP-210191 | 0278 | 3 | F | Correction to resource identifiers descriptions used in notifications | 16.8.0 |
| 2021-03 | CT#91e | CP-210237 | 0279 | 1 | F | Correction to TSN scenarios. | 16.8.0 |
| 2021-03 | CT#91e | CP-210197 | 0287 | 1 | A | Correction to PATCH method | 16.8.0 |
| 2021-03 | CT#91e | CP-210209 | 0288 | | F | Usage threshold update | 16.8.0 |
| 2021-03 | CT#91e | CP-210239 | 0291 | | F | Update of OpenAPI version and TS version in externalDocs field | 16.8.0 |
| 2021-03 | CT#91e | CP-210219 | 0280 | 1 | F | Adding "description" field for map data types | 17.0.0 |
| 2021-03 | CT#91e | CP-210218 | 0281 | | F | OpenAPI reference | 17.0.0 |
| 2021-03 | CT#91e | CP-210221 | 0283 | 1 | F | Adding some missing description fields to data type definitions in OpenAPI specification files | 17.0.0 |
| 2021-03 | CT#91e | CP-210219 | 0284 | | F | Support of optional HTTP custom header fields | 17.0.0 |
| 2021-03 | CT#91e | CP-210220 | 0285 | | F | Terminology alignment: usage of "NF service consumer" | 17.0.0 |
| 2021-03 | CT#91e | CP-210240 | 0292 | | F | Update of OpenAPI version and TS version in externalDocs field | 17.0.0 |
| 2021-06 | CT#92e | CP-211226 | 0293 | 3 | B | AF Session for control of MPS for DTS | 17.1.0 |
| 2021-06 | CT#92e | CP-211257 | 0294 | 2 | B | Adding PCF as the consumer of the Npcf_PolicyAuthorization service to support DCAMP | 17.1.0 |
| 2021-06 | CT#92e | CP-211257 | 0295 | 4 | B | Support of subscription to application detection notification for a PDU session | 17.1.0 |
| 2021-06 | CT#92e | CP-211302 | 0296 | 4 | B | Support Time Sensing Communication other than TSN | 17.1.0 |
| 2021-06 | CT#92e | CP-211272 | 0297 | 3 | B | Support survival time | 17.1.0 |
| 2021-06 | CT#92e | CP-211205 | 0302 | 2 | A | Correction on 404 Not Found | 17.1.0 |
| 2021-06 | CT#92e | CP-211261 | 0304 | | A | Correction to Data type table | 17.1.0 |
| 2021-06 | CT#92e | CP-211200 | 0306 | 1 | A | Redirect responses with "application/json" media type | 17.1.0 |
| 2021-06 | CT#92e | CP-211304 | 0308 | 3 | A | Correcting the unit of Periodicity | 17.1.0 |
| 2021-06 | CT#92e | CP-211262 | 0309 | 1 | A | Removal of tsnBridgeInfo from EventsNotification data type | 17.1.0 |
| 2021-06 | CT#92e | CP-211276 | 0314 | 1 | B | Support of Network Exposure to EAS via Local NEF. | 17.1.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2021-06 | CT#92e | CP-211217 | 0315 | 2 | B | Application error. | 17.1.0 |
| 2021-06 | CT#92e | CP-211220 | 0317 | 1 | A | Adding NWDAF as the consumer of Npcf_PolicyAuthorization service | 17.1.0 |
| 2021-06 | CT#92e | CP-211205 | 0321 | | A | Attribute and data type corrections | 17.1.0 |
| 2021-06 | CT#92e | CP-211213 | 0322 | 1 | B | Satellite backhaul change event. | 17.1.0 |
| 2021-06 | CT#92e | CP-211217 | 0323 | 1 | F | Completion of Termination Causes. | 17.1.0 |
| 2021-06 | CT#92e | CP-211274 | 0324 | 1 | B | Support of TSCAI time domain. | 17.1.0 |
| 2021-06 | CT#92e | CP-211211 | 0325 | 1 | B | AF influence on traffic routing related events and errors report. | 17.1.0 |
| 2021-06 | CT#92e | CP-211265 | 0327 | | F | Update of OpenAPI version and TS version in externalDocs field | 17.1.0 |
| 2021-09 | CT#93e | CP-212212 | 0328 | 1 | B | Authorization for MPS for DTS | 17.2.0 |
| 2021-09 | CT#93e | CP-212211 | 0329 | 1 | B | TSCTSF support for Time Sensitive Communication | 17.2.0 |
| 2021-09 | CT#93e | CP-212224 | 0330 | | F | Clarification of resource allocation failure | 17.2.0 |
| 2021-09 | CT#93e | CP-212205 | 0331 | | B | Support of IMS emergency service for SNPN | 17.2.0 |
| 2021-09 | CT#93e | CP-212200 | 0333 | 1 | A | Support of TCP and UDP ports in non-3GPP UE location | 17.2.0 |
| 2021-09 | CT#93e | CP-212211 | 0334 | 1 | F | Replacement of TSN Terminology in 29.514 | 17.2.0 |
| 2021-09 | CT#93e | CP-212190 | 0338 | | A | Corrections on modification of subscription procedure | 17.2.0 |
| 2021-09 | CT#93e | CP-212199 | 0339 | 1 | A | Correction of report of User location information time | 17.2.0 |
| 2021-09 | CT#93e | CP-212224 | 0340 | | F | Removal of network slice instance from service procedures | 17.2.0 |
| 2021-09 | CT#93e | CP-212211 | 0341 | 1 | B | Introduction of TSCTSF | 17.2.0 |
| 2021-09 | CT#93e | CP-212223 | 0342 | | F | Update of OpenAPI version and TS version in externalDocs field | 17.2.0 |
| 2021-09 | CT#93e | CP-212224 | 0344 | | F | Report of 3GPP and non-3GPP User Location | 17.2.0 |
| 2021-12 | CT#94e | CP-213239 | 0346 | | F | API URI of the Npcf_PolicyAuthorization API | 17.3.0 |
| 2021-12 | CT#94e | CP-213234 | 0347 | 1 | B | TSCTSF discovery | 17.3.0 |
| 2021-12 | CT#94e | CP-213243 | 0348 | 1 | B | Access type change report | 17.3.0 |
| 2021-12 | CT#94e | CP-213194 | 0349 | | B | Subscription to the detection of the traffic of one or more applications | 17.3.0 |
| 2021-12 | CT#94e | CP-213234 | 0350 | 1 | B | Adding QoS related parameters to the Alternative Service Requirements | 17.3.0 |
| 2021-12 | CT#94e | CP-213194 | 0351 | 1 | B | Notification of PDU session established/terminated events | 17.3.0 |
| 2021-12 | CT#94e | CP-213234 | 0352 | 1 | F | Correction to TSC QoS information | 17.3.0 |
| 2021-12 | CT#94e | CP-213234 | 0353 | 1 | F | Support of IP type and Ethernet type of PDU sessions for TSC | 17.3.0 |
| 2021-12 | CT#94e | CP-213234 | 0354 | | F | TSCTSF NF service consumer | 17.3.0 |
| 2021-12 | CT#94e | CP-213225 | 0355 | | B | Resolves the editor's note for FILTER_RESTRICTIONS application error | 17.3.0 |
| 2021-12 | CT#94e | CP-213223 | 0356 | 1 | B | Adding EAS IP replacement information in Policy Authorization | 17.3.0 |
| 2021-12 | CT#94e | CP-213228 | 0357 | 1 | B | Adding DCCF as PCF Policy Authorization NF service consumer | 17.3.0 |
| 2021-12 | CT#94e | CP-213234 | 0358 | 1 | F | Update of 5.6.1 | 17.3.0 |
| 2021-12 | CT#94e | CP-213214 | 0360 | 1 | A | Alignment of description with data type for QosMonitoringInformation | 17.3.0 |
| 2021-12 | CT#94e | CP-213249 | 0362 | | A | Alignment of description with data type for TscPriorityLevel | 17.3.0 |
| 2021-12 | CT#94e | CP-213244 | 0365 | 1 | F | Correction to QoS notification data type | 17.3.0 |
| 2021-12 | CT#94e | CP-213230 | 0366 | | B | Slice data rate control in N5 interface | 17.3.0 |
| 2021-12 | CT#94e | CP-213200 | 0367 | 1 | F | Correction of service architecture, N43 reference point | 17.3.0 |
| 2021-12 | CT#94e | CP-213223 | 0368 | 1 | B | AF Request for Simultaneous Connectivity over Source and Target PSA at Edge Relocation | 17.3.0 |
| 2021-12 | CT#94e | CP-213229 | 0369 | 1 | B | 5GS Level Identities in SNPN scenarios | 17.3.0 |
| 2021-12 | CT#94e | CP-213234 | 0370 | 1 | F | Update of service architecture | 17.3.0 |
| 2021-12 | CT#94e | CP-213238 | 0372 | | A | Correction to optionality of problem details | 17.3.0 |
| 2021-12 | CT#94e | CP-213239 | 0373 | | F | Addition of description field to MpsAction data type | 17.3.0 |
| 2021-12 | CT#94e | CP-213225 | 0374 | | F | Correction to error responses | 17.3.0 |
| 2021-12 | CT#94e | CP-213244 | 0375 | 1 | F | Miscellaneous corrections | 17.3.0 |
| 2021-12 | CT#94e | CP-213246 | 0376 | | F | Update of OpenAPI version and TS version in externalDocs field | 17.3.0 |
| 2022-03 | CT#95e | CP-220183 | 0378 | 1 | B | QoS determination for TSC | 17.4.0 |
| 2022-03 | CT#95e | CP-220185 | 0379 | 1 | B | Support of AF triggered EAS rediscovery | 17.4.0 |
| 2022-03 | CT#95e | CP-220179 | 0380 | 1 | F | Corrections to satellite backhaul category changes | 17.4.0 |
| 2022-03 | CT#95e | CP-220197 | 0381 | 1 | F | Update of 4.2.5.1 | 17.4.0 |
| 2022-03 | CT#95e | CP-220176 | 0382 | 2 | A | Alignment of "Application Errors" clause with SBI TS template | 17.4.0 |
| 2022-03 | CT#95e | CP-220183 | 0383 | 1 | B | Adding alternative QoS related parameter setsAdding alternative QoS related parameter sets | 17.4.0 |
| 2022-03 | CT#95e | CP-220185 | 0384 | 1 | F | Handling of supported features for Edge Computing | 17.4.0 |
| 2022-03 | CT#95e | CP-220195 | 0385 | | F | Handling of the indication of UE IP address preservation in Update procedures | 17.4.0 |
| 2022-03 | CT#95e | CP-220202 | 0387 | 1 | B | Support of AN-GW restoration | 17.4.0 |
| 2022-03 | CT#95e | CP-220201 | 0389 | | F | Update of FQDN data type | 17.4.0 |
| 2022-03 | CT#95e | CP-220201 | 0390 | 1 | F | Update of description fields | 17.4.0 |
| 2022-03 | CT#95e | CP-220197 | 0391 | 1 | F | Correction to notification about PDU session establishment/termination events | 17.4.0 |
| 2022-03 | CT#95e | CP-220197 | 0392 | | F | Clarification to subscription to notification of application detection | 17.4.0 |
| 2022-03 | CT#95e | CP-220195 | 0394 | 1 | F | Correction to enable retrieval of Network Provided Location information in a MESSAGE request | 17.4.0 |
| 2022-03 | CT#95e | CP-220183 | 0395 | 1 | F | Correction to notification of detected TSC user plane node information | 17.4.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2022-03 | CT#95e | CP-220183 | 0396 | | F | Removal of Editor's notes | 17.4.0 |
| 2022-03 | CT#95e | CP-220195 | 0397 | 1 | B | Correction to enable retrieval of Network Provided Location information at mid-call access change | 17.4.0 |
| 2022-03 | CT#95e | CP-220194 | 0398 | | F | Update of info and externalDocs fields | 17.4.0 |
| 2022-06 | CT#96 | CP-221159 | 0402 | 1 | F | Wording correction for consistency | 17.5.0 |
| 2022-06 | CT#96 | CP-221144 | 0404 | 2 | F | Resolve the issue related to individual QoS parameters | 17.5.0 |
| 2022-06 | CT#96 | CP-221144 | 0405 | 1 | B | DNN and S-NSSAI notification | 17.5.0 |
| 2022-06 | CT#96 | CP-221157 | 0407 | 3 | F | Correction to the charging identifier to enable uniqueness in roaming scenarios | 17.5.0 |
| 2022-06 | CT#96 | CP-221119 | 0410 | 1 | A | Correction to Npcf_PolicyAuthorization_Subscribe service operation | 17.5.0 |
| 2022-06 | CT#96 | CP-221155 | 0412 | 1 | F | Update to include a missing NOTE | 17.5.0 |
| 2022-06 | CT#96 | CP-221154 | 0413 | | F | Alignment with the SBI template | 17.5.0 |
| 2022-06 | CT#96 | CP-221158 | 0416 | 1 | F | Correction to traffic routing requirements | 17.5.0 |
| 2022-06 | CT#96 | CP-221144 | 0417 | | F | Discovery of TSCTSF notification URI | 17.5.0 |
| 2022-06 | CT#96 | CP-221161 | 0419 | 2 | A | Correction on TscaiInputContainer definition | 17.5.0 |
| 2022-06 | CT#96 | CP-221151 | 0420 | | F | Update of info and externalDocs fields | 17.5.0 |
| 2022-09 | CT#97e | CP-222125 | 0421 | | F | Untrusted WLAN location information | 17.6.0 |
| 2022-09 | CT#97e | CP-222093 | 0424 | | A | Correction to notification about application session context termination | 17.6.0 |
| 2022-09 | CT#97e | CP-222127 | 0425 | 1 | F | Correction to notification about PDU session established/terminated events | 17.6.0 |
| 2022-09 | CT#97e | CP-222113 | 0426 | | F | Correction to the notification URI | 17.6.0 |
| 2022-09 | CT#97e | CP-222099 | 0427 | 1 | F | User plane latency requirement support | 17.6.0 |
| 2022-09 | CT#97e | CP-222125 | 0428 | 1 | F | Clarification of ToS traffic class | 17.6.0 |
| 2022-09 | CT#97e | CP-222113 | 0429 | | F | Correction to time synchronization procedures during the creation of the AF session | 17.6.0 |
| 2022-09 | CT#97e | CP-222125 | 0430 | | F | Correction to QoS monitoring | 17.6.0 |
| 2022-09 | CT#97e | CP-222125 | 0432 | | F | Correction to the subscription to Access Type change | 17.6.0 |
| 2022-09 | CT#97e | CP-222121 | 0435 | | F | Update of info and externalDocs fields | 17.6.0 |
| 2022-12 | CT#98e | CP-223164 | 0443 | | A | Correction to the attribute name of media subcomponent | 17.7.0 |
| 2023-03 | CT#99 | CP-230128 | 0460 | 1 | A | Corrections to QoS monitoring | 17.8.0 |
| 2023-03 | CT#99 | CP-230173 | 0467 | 1 | F | Correction on setting Packet Delay Failure report Threshold | 17.8.0 |
| 2023-03 | CT#99 | CP-230160 | 0485 | | F | Update of info and externalDocs fields | 17.8.0 |
| 2023-06 | CT#100 | CP-231154 | 0512 | 1 | F | Wrong attribute name for the indication of direct notification | 17.9.0 |
| 2023-06 | CT#100 | CP-231147 | 0516 | | A | Removal of unspecified QoS monitoring control options | 17.9.0 |
| 2023-06 | CT#100 | CP-231161 | 0530 | | F | Update of info and externalDocs fields | 17.9.0 |
| 2023-12 | CT#102 | CP-233265 | 0581 | 1 | A | Wrong attribute name for Access Network Gateway Address | 17.10.0 |
| 2024-03 | CT#103 | CP-240170 | 0610 | | A | Corrections on QoS monitoring reports | 17.11.0 |

# History

| Document history | | |
|---|---|---|
| V17.4.0 | May 2022 | Publication |
| V17.5.0 | June 2022 | Publication |
| V17.6.0 | September 2022 | Publication |
| V17.7.0 | January 2023 | Publication |
| V17.8.0 | April 2023 | Publication |
| V17.9.0 | July 2023 | Publication |
| V17.10.0 | January 2024 | Publication |
| V17.11.0 | April 2024 | Publication |