ETSI TS 129 514 V15.2.0 (2019-04)

TECHNICAL SPECIFICATION

**5G;
5G System;
Policy Authorization Service;
Stage 3
(3GPP TS 29.514 version 15.2.0 Release 15)**

Reference

RTS/TSGC-0329514vf20

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Copyright Notification

ETSI

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://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 3.0.0 Specification", https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md.

[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".

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 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.

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].

AF	Application Function
DEI	Drop Eligible Indicator
DNAI	DN Access Identifier
DNN	Data Network Name
E-UTRA	Evolved Universal Terrestrial Radio Access
H-PCF	PCF in the HPLMN
JSON	JavaScript Object Notation
MPS	Multimedia Priority Service
NEF	Network Exposure Function
NR	New Radio

NRF	Network Repository Function
NWDAF	Network Data Analytics Function
PCC	Policy and Charging Control
PCF	Policy Control Function
PCP	Priority Code Point
PRA	Presence Reporting Area
QoS	Quality of Service
RFSP	RAT Frequency Selection Priority
RTCP	Real Time Control Protocol
SDF	Service Data Flow
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SUPI	Subscription Permanent Identifier
UDR	Unified Data Repository
UPF	User Plane Function
URSP	UE Route Selection Policy
VID	VLAN Identifier
VLAN	Virtual Local Area Network
V-PCF	PCF in the VPLMN

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 an AF 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 allows the NF service consumer to subscribe/unsubscribe to the notification of events (e.g. Access Type and RAT type, PLMN identifier, usage 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) and the Network Exposure Function (NEF).

The Npcf_PolicyAuthorization service is provided by the PCF and consumed by the AF and the NEF, 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.
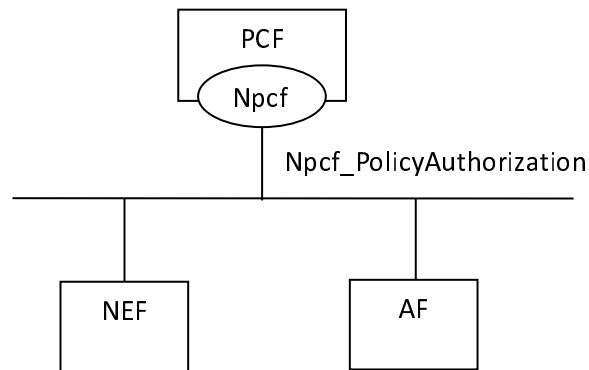
Figure 4.1.2-1: Npcf_PolicyAuthorization service Architecture, SBI representation
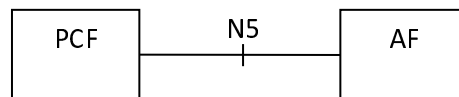
Figure 4.1.2-2: Npcf_PolicyAuthorization service Architecture, reference point representation

The NEF can act as an AF using N5 reference point.

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 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 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].

4.1.3.2   NF Service Consumers

The known NF service consumers are the AF and the NEF, as defined in 3GPP TS 23.502 [3].

The AF is an element offering applications that require the Policy and Charging Control of traffic plane resources. The AF uses the Npcf_PolicyAuthorization service to provide service information to the PCF.

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 subclause 5.20 of 3GPP TS 23.501 [2].

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

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.	AF, NEF
Npcf_PolicyAuthorization_Update	Determines and updates the policy according to the modified service information provided by an authorized NF service consumer.	AF, NEF
Npcf_PolicyAuthorization_Delete	Provides means to delete the application session context of the NF service consumer.	AF, NEF
Npcf_PolicyAuthorization_Notify	Notifies NF service consumer of the subscribed events.	PCF
Npcf_PolicyAuthorization_Subscribe	Allows NF service consumers to subscribe to the notification of events.	AF, NEF
Npcf_PolicyAuthorization_Unsubscribe	Allows NF service consumers to unsubscribe to the notification of events.	AF, NEF

NOTE: The NEF and the AF use the Npcf_PolicyAuthorization service in the same way. To improve the readability of the service procedures, only the AF is mentioned in the following subclauses.

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.

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.
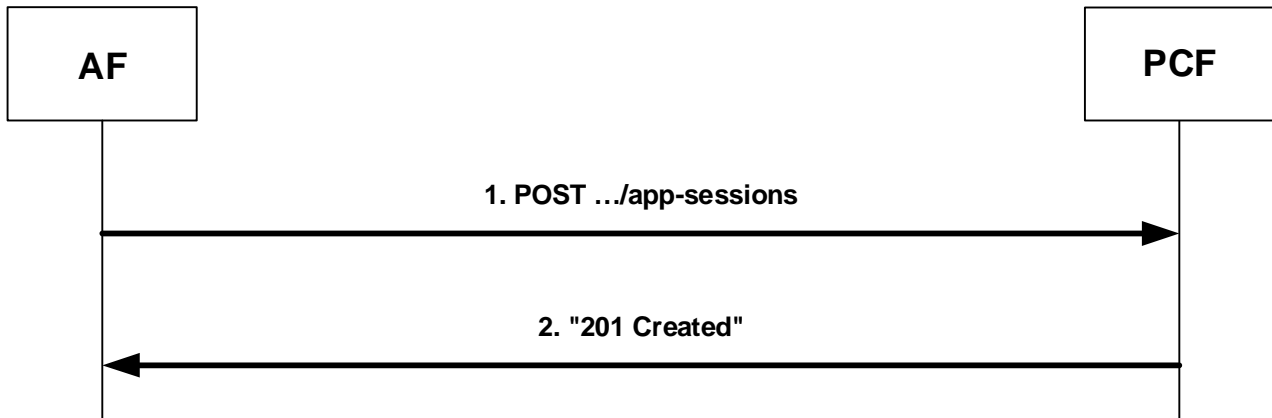
Figure 4.2.2.2-1: Initial provisioning of service information

When a new AF application session context is being established and media information for this application session context is available at the AF and the related media requires PCC control, the AF 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 AF 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 AF 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.

The AF 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.

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].

The AF may include the AF charging identifier in the "afChargId" attribute for charging correlation purposes.

The AF may also include the "evSubsc" attribute of "EventsSubscReqData" data type to request the notification of certain user plane events. The AF 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 subclause 5.7.

Otherwise, when the PCF receives the HTTP POST request from the AF, 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 AF 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 AF may provide DNN in the "dnn" attribute, SUPI in the "supi" attribute, the S-NSSAI in the "sliceInfo" attribute if available for session binding. The AF may also provide the domain identity in the "ipDomain" attribute.

NOTE 1: The "ipDomain" attribute is helpful in the following scenario: Within a network slice instance, 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. An AF 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 AF. If a NAT is used, the AF 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 AF supplies an "ipDomain" attribute denoting the IP address domain behind the NAT in addition. The AF 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 2: The "sliceInfo" attribute is helpful in the scenario where multiple network slice instances are deployed in the same DNN, and the same IPv4 address may be allocated to UE PDU sessions in different network slice instances. If one PCF controls several network slices, the UE IP address is not sufficient for the session binding. The AF supplies "sliceInfo" attribute denoting the network slice instance that allocated the IPv4 address of the UE PDU session. How the AF derives S-NSSAI is out of the scope of this specification.

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), 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 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 AF receives the retry interval within the "Retry-After" HTTP header field, the AF 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] subclause 5.2.2.2.

To allow the PCF and SMF/UPF to perform PCC rule authorization and QoS flow binding for the described service data flows, the AF 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 AF may specify the ToS traffic class within the "tosTrCl" attribute for the described service data flows together with the "fDescs" attribute.

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

- if the AF subscribed to the event "ACCESS_TYPE_CHG" in the HTTP POST request, the "event" attribute set to "ACCESS_TYPE_CHG" and the attributes "accessType" including the access type, "ratType" including the RAT type when applicable for the notified access type, and the "anGwAddr" including access network gateway address when available, if the PCF has previously requested to be updated with this information in the SMF.

The AF subscription to other specific events using the Npcf_PolicyAuthorization_Create request is described in the related subclauses. Notification of events when the applicable information is not available in the PCF when receiving the Npcf_PolicyAuthorization_Create request is described in subclause 4.2.5.

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

NOTE 3: The behaviour when the AF 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 AF 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 "medSubComponents" attributes.

If a "medSubComponents" 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 AF as described in subclause 4.2.2.2.

4.2.2.4 Initial Background Data Transfer policy indication

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

The AF may include in the HTTP POST request message described in subclause 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 AF 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 AF 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 AF 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 AF as described in subclause 4.2.2.2.

4.2.2.5 Initial provisioning of sponsored connectivity information

This procedure is used by an AF to indicate sponsored data connectivity when Sponsored Connectivity feature is supported.

The AF shall provide in the "AppSessionContext" data type of the HTTP POST request message described in subclause 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 AF 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 AF may subscribe with the PCF to the notification of usage threshold reached. The AF 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 AF 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 AF indicated to enable sponsored data connectivity, and the UE is roaming in a VPLMN, the following procedures apply:

- If the AF 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 AF 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 AF 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 AF as described in subclause 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 an AF 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 AF shall use the "EventsSubscReqData" data type as described in subclause 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 "QOS_NOTIF".

The PCF shall reply to the AF as described in subclause 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 an AF 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 AF shall use the "EventsSubscReqData" data type as described in subclause 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 "FAILED_RESOURCES_ALLOCATION".

The PCF shall reply to the AF as described in subclause 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 an AF 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 "Influence on Traffic Routing" feature is supported.

NOTE 1: The AF uses the Npcf_PolicyAuthorization service for requests targeting specific on-going PDU sessions of individual UE(s). The AF 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 AF shall include in the HTTP POST request message described in subclause 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 AF may include traffic routing requirements together with service information.

The AF may request to influence SMF traffic routing decisions to a DNAI. The AF 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

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

The AF may include in the "afRoutReq" attribute:

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

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

c) Spatial validity during which the AF 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".

The AF may also subscribe to notifications about UP path management events. The AF 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 AF is receiving the Nsmf_EventExposure_Notify service operation in the "notificationUri" attribute; and

- the notification correlation identifier assigned by the AF in the "notifCorrelId" attribute.

The PCF shall reply to the AF as described in subclause 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 2: The AF receives the notification about UP path management events by the Nsmf_EventExposure_Notify service operation as defined in subclause 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 an AF to subscribe to notifications when the resources associated to the corresponding service information have been allocated and/or cannot be allocated.

The AF shall use the "EventsSubscReqData" data type as described in subclause 4.2.2.2 and shall include in the HTTP POST request message:

-    if the AF 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 AF 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 AF as described in subclause 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

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

The AF 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 AF 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 subclause 6.8.2 of 3GPP TS 29.500 [5].

NOTE: If the AF supports the SBI Message Priority mechanism for an MPS session, the AF 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].

4.2.2.13   Support of content versioning

The support of the media component versioning is optional. When the "Media Component Versioning" feature is supported, the AF and the PCF shall comply with the procedures specified in this subclause.

If required by operator policies, the AF 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], subclause 4.2.6.2.14.

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.

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].

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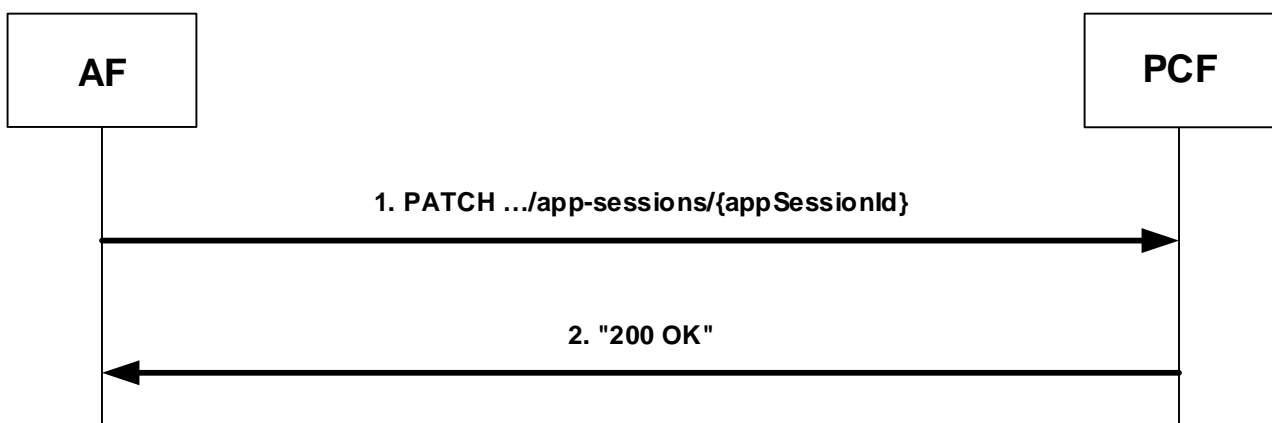
Figure 4.2.3.2-1: Modification of service information using HTTP PATCH

The AF may modify the application session context information at any time (e.g. due to an AF session modification or internal AF 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 "AppSessionContextUpdateData" data type and shall be encoded according to "JSON Merge Patch", as defined in IETF RFC 7396 [21].

The AF may include the updated service information in the "medComponents" attribute.

The AF may include in the "AppSessionContextUpdateData" data type 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].

The AF 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 AF 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; and the "notifUri" attribute with the notification URI where the PCF shall send the notifications.

The AF shall update existing event subscription information by including in the "AppSessionContextUpdateData" data type and updated value of the "evSubsc" attribute of the "EventsSubscReqData" data type.

The AF shall remove existing event subscription information by setting to null the "evSubsc" attribute included in the "AppSessionContextUpdateData" data type.

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 subclause 5.7.

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), the PCF shall include in an HTTP "403 Forbidden" response message the "cause" attribute set to "REQUESTED_SERVICE_NOT_AUTHORIZED". 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 AF receives the retry interval within the "Retry-After" HTTP header field, the AF 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] subclause 5.2.2.2.

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

- if the AF subscribed to the "ACCESS_TYPE_CHG" event in the HTTP PATCH request, the "event" attribute set to "ACCESS_TYPE_CHG" and the attributes "accessType" including the access type, "ratType" including the RAT type when applicable for the notified access type, and the "anGwAddr" including access network gateway address when available, if the PCF has previously requested to be updated with this information in the SMF.

The AF subscription to other specific events using the Npcf_PolicyAuthorization_Update request is described in the related subclauses. Notification of events when the applicable information is not available in the PCF when receiving the Npcf_PolicyAuthorization_Update request is described in subclause 4.2.5.

The HTTP response message towards the AF 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 an AF to modify in the PCF the service data flow(s) that are to be enabled or disabled to pass through the PDU session.

The AF shall use the HTTP PATCH method to modify the gate control information.

The AF shall include in the HTTP PATCH request message described in subclause 4.2.3.2 the "fStatus" attribute for the flows to be enabled or disabled with the appropriate value.

If a "medSubComponents" 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 AF as described in subclause 4.2.3.2.

4.2.3.4 Background Data Transfer policy indication at policy authorization update

This procedure is used by an AF 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 AF may include in the HTTP PATCH request message described in subclause 4.2.3.2 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 AF 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 AF 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 AF 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 AF as described in subclause 4.2.3.2.

4.2.3.5 Modification of sponsored connectivity information

This procedure is used by an AF to modify sponsored data connectivity when Sponsored Connectivity feature is supported.

The AF shall use the HTTP PATCH method to modify the sponsored connectivity information.

The AF shall include in the HTTP PATCH request message described in subclause 4.2.3.2 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 AF requests to enable sponsored data connectivity the AF shall change the "sponStatus" attribute value to "SPONSOR_ENABLED".

If the AF requests to disable sponsored data connectivity the AF 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 AF may also include in the HTTP PATCH a new or modified "evSubsc" attribute of "EventsSubscReqData" 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 AF 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 data connectivity information.

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

- If the AF 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 AF 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 AF 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 AF as described in subclause 4.2.3.2.

4.2.3.6   Modification of Subscription to Service Data Flow QoS notification control

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

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

The AF shall include in the HTTP PATCH request message described in subclause 4.2.3.2 the updated values of the "EventsSubscReqData" data type, which either include in the "events" attribute a new element with the "event" attribute set to "QOS_NOTIF" or remove in the "events" attribute an existing element with the "event" attribute set to "QOS_NOTIF".

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 AF as described in subclause 4.2.3.2.

4.2.3.7   Modification of Subscription to Service Data Flow Deactivation

This procedure is used by an AF 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 AF shall use the HTTP PATCH method to update the "Events Subscription" sub-resource together with the modifications to the "Individual Application Session" sub-resource.

The AF shall include in the HTTP PATCH request message described in subclause 4.2.3.2 the updated values of the "EventsSubscReqData" data type, which either include in the "events" attribute a new element with the "event" attribute set to "FAILED_RESOURCES_ALLOCATION" or remove in the "events" attribute an existing element with the "event" attribute set to "FAILED_RESOURCES_ALLOCATION".

The PCF shall reply to the AF as described in subclause 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 an AF 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 "Influence on Traffic Routing" feature is supported.

The AF shall use the HTTP PATCH method.

To modify traffic routing information, the AF shall include in the HTTP PATCH request message described in subclause 4.2.3.2 an updated "afRoutReq" attribute(s) with the modified traffic routing information.

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

The PCF shall reply to the AF as described in subclause 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 AF to modify in the PCF the subscription to notification about resources allocation outcome.

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

The AF shall include in the HTTP PATCH request message described in subclause 4.2.3.2 the updated values of the "EventsSubscReqData" 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 AF may include 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 AF supports the SBI message priority mechanism for an MPS session, the AF shall include the "3gpp-Sbi-Message-Priority" custom HTTP header towards the PCF as described in subclause 4.2.2.12.

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].

4.2.3.13 Support of content versioning

The support of the media component versioning is optional. When the "Media Component Versioning" feature is supported, the AF and the PCF shall comply with the procedures specified in this subclause.

Upon each media component modification, if the content version was previously assigned to a media component, the AF 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 AF 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], subclause 4.2.6.2.14.

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.

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.
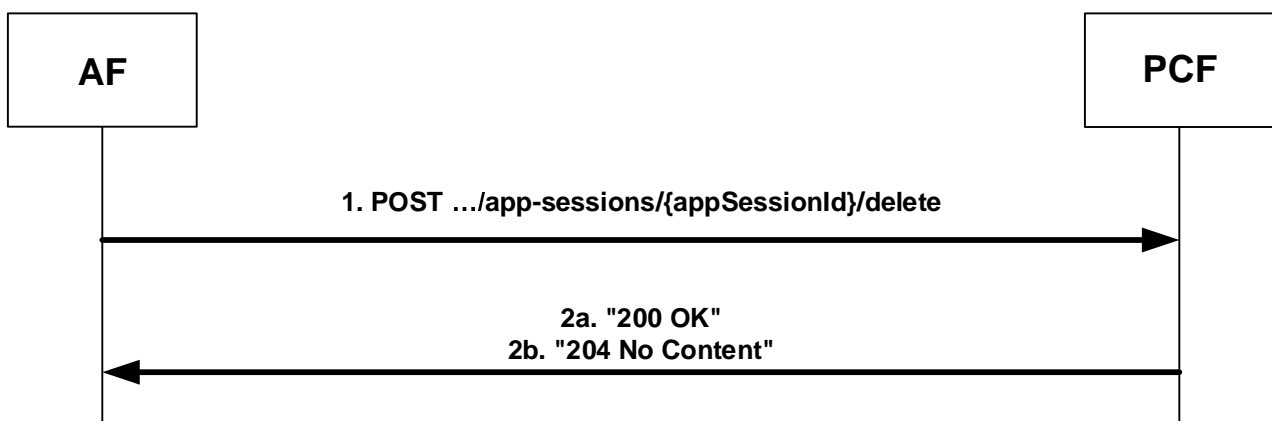
Figure 4.2.4.2-1: Application session context termination

When an AF session is terminated, and if the AF application session context was created as described in subclause 4.2.2, the AF 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 AF shall set the request URI to "{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/delete".

The AF 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 AF, 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 AF is accepted, the PCF shall send to the AF a "200 OK" response to HTTP POST request, as shown in figure 4.2.4.2-1, step 2a, including in the "EventsNotification" data type the "evNotifs" attribute indicating the event to report to the AF, as described in subclause 4.2.5.2. Otherwise the PCF shall send to the AF 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 following the corresponding procedures specified in 3GPP TS 29.512 [8].

If the HTTP POST request from the AF is rejected, the PCF shall indicate in the response to HTTP POST request the cause for the rejection as specified in subclause 5.7.

4.2.4.3 Reporting usage for sponsored data connectivity

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

This procedure is initiated when:

- the "Individual Application Session Context" is deleted by the AF; or

- the PCF requests the deletion of the "Individual Application Session Context" to the AF, as described in subclause 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.

The PCF shall notify the AF by including the "EventsNotification" data type in the response of the HTTP POST request as described in subclause 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].

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.

4.2.5.2 Notification about application session context event

This procedure is invoked by the PCF to notify the AF 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.
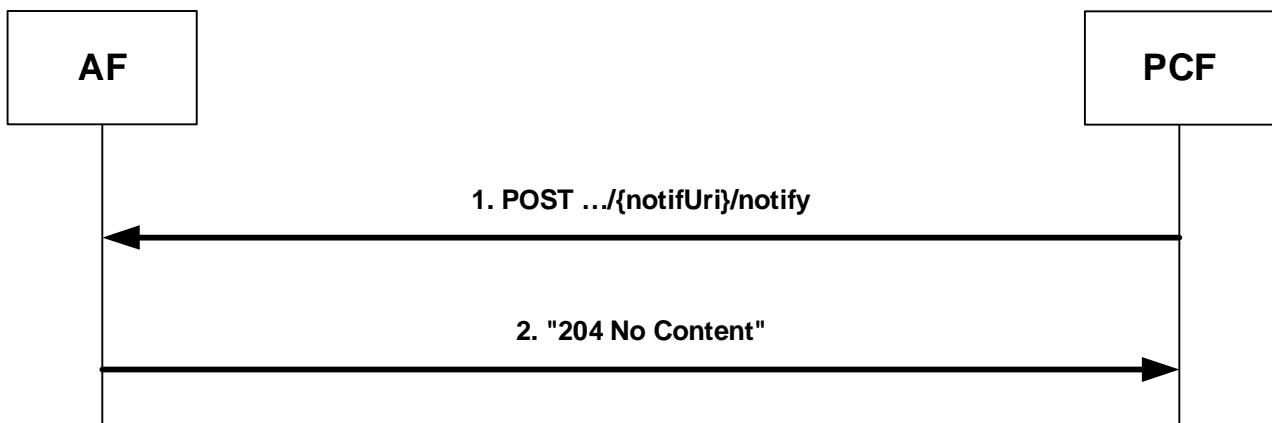
Figure 4.2.5.2-1: Notification about application session context event

When the PCF determines that the event for the existing AF application session context, to which the AF 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 AF using the notification URI received in the subscription creation (or modification), as specified in subclause 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 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 AF subscribed to the "PLMN_CHG" event, the "event" attribute set to "PLMN_CHG" and the "plmnId" attribute including the PLMN identifier if the PCF has requested to be updated with this information in the SMF; and

- if the AF subscribed to the "ACCESS_TYPE_CHG" event, the "event" attribute set to "ACCESS_TYPE_CHG" and the attributes "accessType" including the access type, "ratType" including the RAT type when applicable for the notified access type, and the "anGwAddr" including access network gateway address when available.

The AF notification of other specific events using the Npcf_PolicyAuthorization_Notify request is described in the related subclauses.

Upon the reception of the HTTP POST request from the PCF indicating that the PDU session and/or service related event occurred, the AF 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 AF 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 AF shall indicate in the response to HTTP POST request the cause for the rejection as specified in subclause 5.7.

4.2.5.3 Notification about application session context termination

This procedure is invoked by the PCF to notify the AF 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.
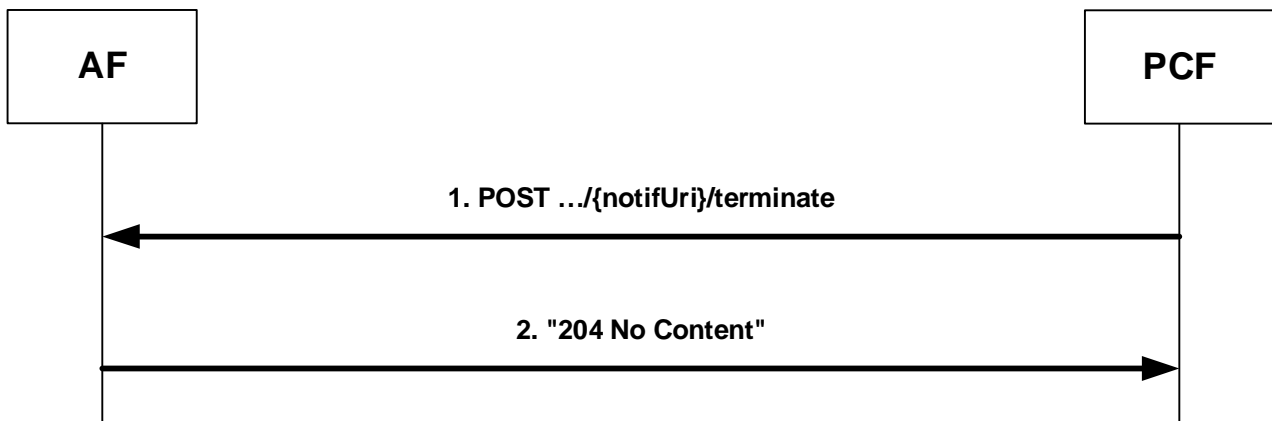
Figure 4.2.5.3-1: Notification about application session context termination

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 subclause 4.2.2, and appending the "termination" segment path at the end of the URI, to trigger the AF to request the application session context termination (see subclause 4.2.4.2). The PCF shall provide in the body of the HTTP POST request the "TerminationInfo" data type including:

- the application session context identifier in the "resUri" attribute; and

- the application session context termination cause in the "termCause" attribute of the "TerminationCause" data type, indicating either "PDU_SESSION_TERMINATION" or "ALL_SDF_DEACTIVATION".

Upon the reception of the HTTP POST request from the PCF requesting the application session context termination, the AF 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 AF 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 subclause 4.2.4.

If the HTTP POST request from the PCF is not accepted, the AF shall indicate in the response to HTTP POST request the cause for the rejection as specified in subclause 5.7.

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 AF accordingly if the AF has previously subscribed as described in subclauses 4.2.2.6 and 4.2.3.6.

The PCF shall notify the AF by including the "EventsNotification" data type in the body of the HTTP POST request as described in subclause 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; and

    b) the identification of the affected service flows (if not all the flows are affected) encoded in the "flows" attribute.

If "Media Component Versioning" 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 subclause 4.2.6.2.14 in 3GPP TS 29.512 [8].

When the AF receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF. The AF 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 AF accordingly if the AF has previously subscribed as described in subclauses 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 AF by including the "EventsNotification" data type in the body of the HTTP POST request as described in subclause 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.

If the "Media Component Versioning" feature is supported, and if the content version was included when the corresponding media component was provisioned as described in subclause 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.

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 subclause 4.2.6.2.14 in 3GPP TS 29.512 [8].

When the AF receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF. The AF 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 AF by sending a notification about application session context termination as defined in subclause 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 Sponsored Connectivity is supported, the AF enabled sponsored data connectivity and the AF provided usage thresholds for such sponsor to the PCF, the PCF shall report accumulated usage to the AF using the Npcf_PolicyAuthorization_Notify service operation when:

- the PCF detects that the usage threshold provided by the AF has been reached; or

- the AF disables the sponsored data connectivity.

The PCF shall notify the AF of the accumulated usage by including the "EventsNotification" data type in the body of the HTTP POST request as described in subclause 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 AF receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the PCF. The AF may terminate the AF session sending an HTTP POST as described in subclause 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 subclause 4.2.3.5 or an HTTP PUT request to the PCF as described in subclause 4.2.6.4.

NOTE: After the PCF reports the accumulated usage to the AF, the AF can provide a new usage threshold to the PCF. The monitoring will not start until the PCF receives the new threshold from the AF 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 AF accordingly if the AF has previously subscribed to the "SUCCESSFUL_RESOURCES_ALLOCATION" event as described in subclauses 4.2.2.10 and 4.2.3.10. The PCF shall notify the AF by including the "EventsNotification" data type in the body of the HTTP POST request as described in subclause 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 "Media Component Versioning" 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 AF accordingly if the AF has previously subscribed to the "FAILED_RESOURCES_ALLOCATION" event as described in subclauses 4.2.2.10 and 4.2.3.10. The PCF shall notify the AF by including the "EventsNotification" data type in the body of the HTTP POST request as described in subclause 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 "mcResourceStatus" attribute, and (if not all the flows are affected) the identification of the related media components in the "flows" attribute. If the "Media Component Versioning" 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 subclause 4.2.6.2.14 in 3GPP TS 29.512 [8].

NOTE: The AF 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 AF handles such situations is out of scope of this specification.

When the AF 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

4.2.6 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 subclause 4.2.2; or

- within the application session context modification procedure by invoking the Npcf_PolicyAuthorization_Update service operation, as described in subclause 4.2.3; or

- by invoking the Npcf_PolicyAuthorization_Subscribe service operation for the existing application session context, as described in subclause 4.2.6.2.

The following procedure 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.

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.
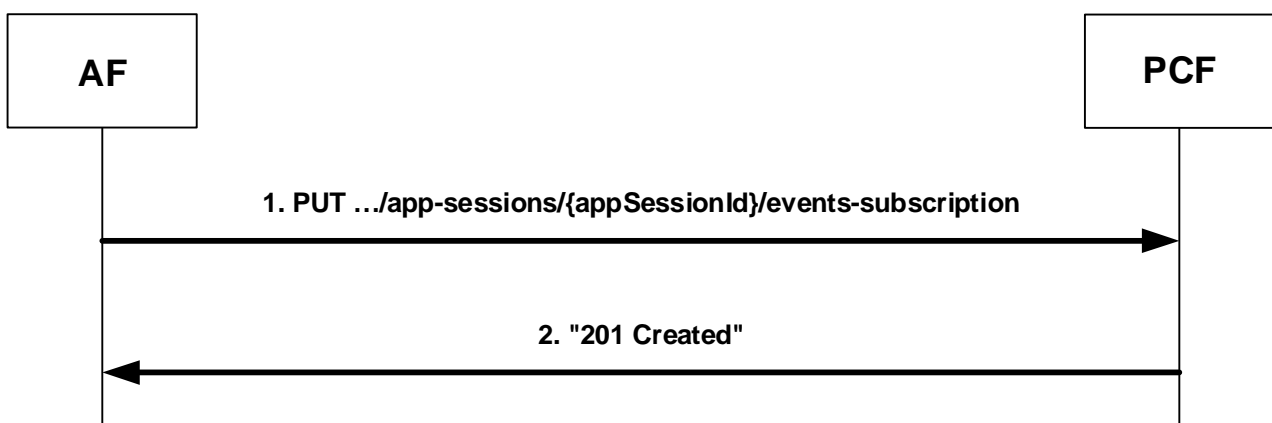
Figure 4.2.6.2-1: Creation or modification of events subscription information using HTTP PUT

Figure 4.2.6.2-2 illustrates the modification of events subscription information using HTTP PUT method.
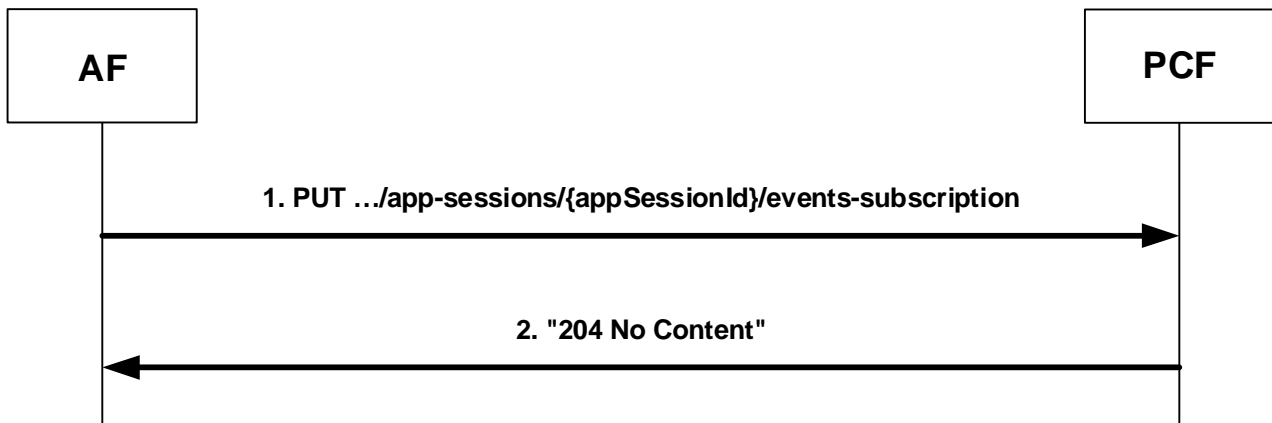
Figure 4.2.6.2-2: Modification of events subscription information using HTTP PUT

When the AF 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 AF 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 AF shall provide in the "EventsSubscReqData" data type of the body of the HTTP PUT request:

-    the "evSubsc" 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 if not provided before.

Upon the reception of the HTTP PUT request from the AF, the PCF shall decide whether the received HTTP PUT request is accepted.

If the HTTP PUT request from the AF is rejected, the PCF shall indicate in the HTTP response the cause for the rejection as specified in subclause 5.7.

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 AF 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

-    an "EventsSubscReqData" data type and may include the "EventsNotification"data type in the payload body containing the representation of the created "Events Subscription" sub-resource.

The PCF shall include in the "evsNotif" attribute:

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

-    if the AF subscribed to the "ACCESS_TYPE_CHG" event in the HTTP PUT request, the "event" attribute set to "ACCESS_TYPE_CHG" and the attributes "accessType" including the access type, "ratType" including the RAT type when applicable for the notified access type, and the "anGwAddr" including access network gateway address when available, if the PCF has previously requested to be updated with this information in the SMF.

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 the HTTP "204 No Content" response to the AF as shown in figure 4.2.6.2-2, step 2. Based on the received subscription information from the AF, 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 AF may subscribe with the PCF to events notification without providing service information. Figure 4.2.6.3-1 illustrates the initial subscription to events without provisioning of service information.
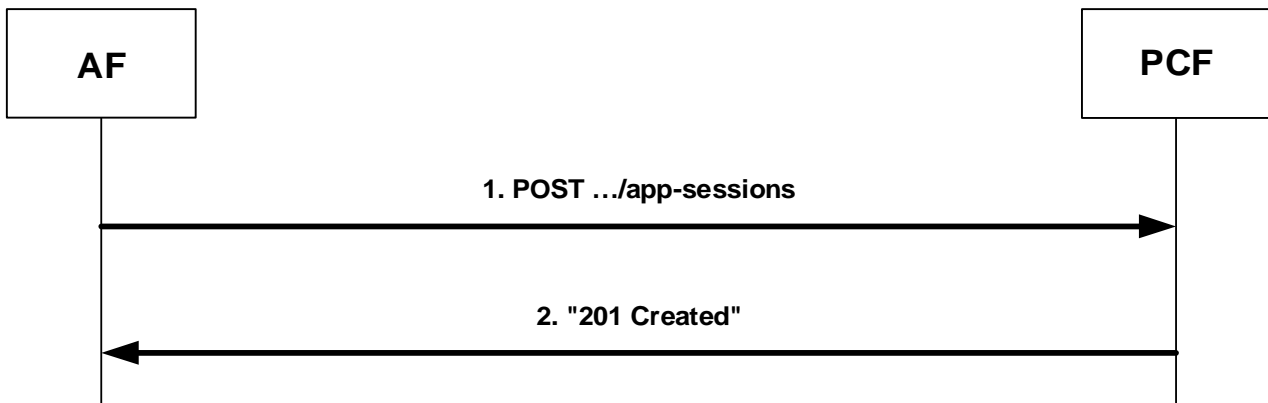
Figure 4.2.6.3-1: Initial Subscription to events without provisioning of service information

When an AF establishes an application session context with the PCF to subscribe to events and does not require PCC control for the related media, the AF 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 AF shall include in 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; and

- the "evSubsc" attribute of "EventsSubscReqData" data type to request the notification of certain user plane events. The AF shall include the events to subscribe to in the "eventSubsc" attribute, and the notification URI where to address the Npcf_PolicyAuthorization_Notify service operation in the "notifUri" attribute.

The AF 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 subclause 5.7.

Otherwise, when the PCF receives the HTTP POST request from the AF, 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 subclause 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 AF, 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 AF 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 AF 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 if the PCF has previously requested to be updated with this information in the SMF; and

- if the AF subscribed to the event "ACCESS_TYPE_CHG" in the HTTP POST request, the "event" attribute set to "ACCESS_TYPE_CHG" and the attributes "accessType" including the access type, "ratType" including the RAT type when applicable for the notified access type, and the "anGwAddress" including access network gateway address when available, if the PCF has previously requested to be updated with this information in the SMF.

4.2.6.4 Subscription to usage monitoring of sponsored data connectivity

This procedure is used by an AF 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 AF shall include in the HTTP PUT request message described in subclause 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 AF as described in subclause 4.2.6.2.

4.2.6.5 Void

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 subclause 4.2.7.2; or

- within the application session context modification procedure by invoking the Npcf_PolicyAuthorization_Update service operation, as described in subclause 4.2.3; or

- within the application session context termination procedure by invoking the Npcf_PolicyAuthorization_Delete service operation, as described in subclause 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.
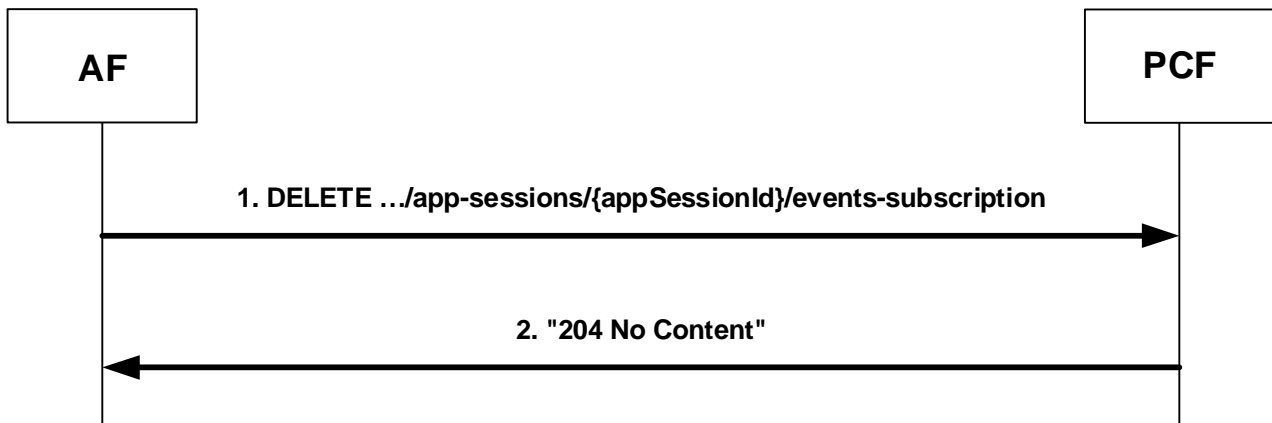
Figure 4.2.7.2-1: Removal of events subscription information using HTTP DELETE

When the AF decides to unsubscribe to all subscribed events for the existing application session context, the AF 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 AF, the PCF shall decide whether the received HTTP request message is accepted.

If the HTTP DELETE request message from the AF is accepted, the PCF shall delete "Events Subscription" sub-resource and shall send to the AF 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 AF is rejected, the PCF shall indicate in the HTTP response message the cause for the rejection as specified in subclause 5.7.

5 Npcf_PolicyAuthorization Service API

5.1 Introduction

The Npcf_PolicyAuthorization Service shall use the Npcf_PolicyAuthorization API.

The request URI used in each HTTP request from the NF service consumer towards the PCF shall have the structure defined in subclause 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 subclause 5.3.

5.2 Usage of HTTP

5.2.1 General

HTTP/2, IETF RFC 7540 [9], shall be used as specified in subclause 5.2 of 3GPP TS 29.500 [5].

HTTP/2 shall be transported as specified in subclause 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 subclause 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 subclause 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 HTTP custom header fields specified in subclause 5.2.3.2 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

{apiRoot}/npcf-policyauthorization/v1
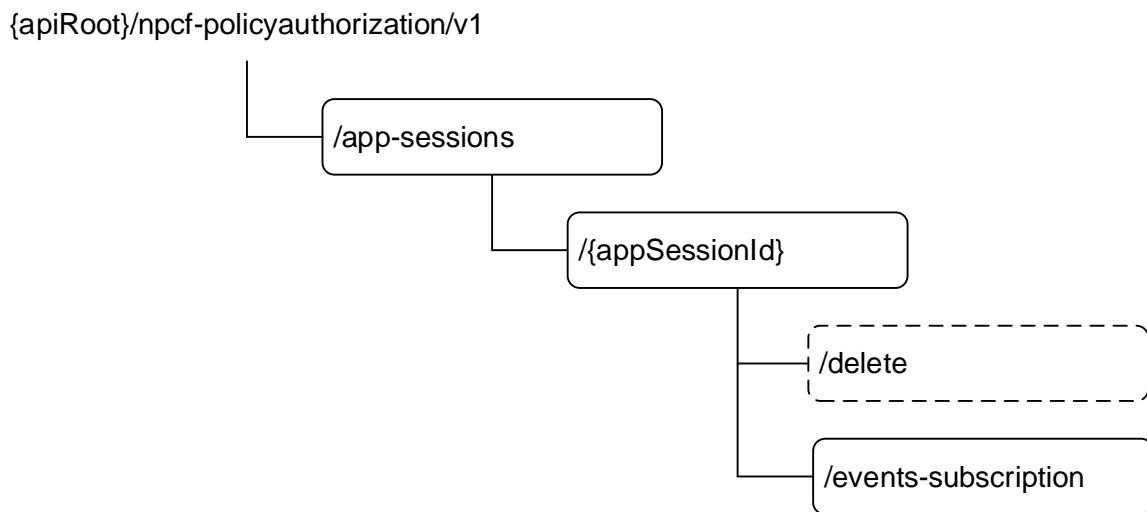
Figure 5.3.1-1: Resource URI structure of the Npcf_PolicyAuthorization API

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	{apiRoot}/ npcf-policyauthorization/v1 /app-sessions	POST	Npcf_PolicyAuthorization_Create. Creates a new Individual Application Session Context resource and may create the child Events Subscription sub-resource.
Individual Application Session Context	{apiRoot}/ npcf-policyauthorization/v1 /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.
	{apiRoot}/ npcf-policyauthorization/v1 /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	{apiRoot}/ npcf-policyauthorization/v1 /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	Definition
apiRoot	See subclause 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. 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. The HTTP response shall contain a Location header field set to the URI of the existing individual Application Session Context resource.
ProblemDetails	M	1	403 Forbidden	(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 subclause 5.7.				

5.3.2.4 Resource Custom Operations

None.

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	Definition
ApiRoot	See subclause 5.1
appSessionId	String formatted according to IETF RFC 3986 [19] identifying an application session context.

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.
ProblemDetails	M	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.				
NOTE 2: Failure cases are described in subclause 5.7.				

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
AppSessionContextUpdateData	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. The Individual Application Session Context resource was modified and a representation of that resource is returned.
n/a			204 No Content	Successful case. The Individual Application session context resource was modified.
ProblemDetails	M	1	403 Forbidden	(NOTE 2)
ProblemDetails	M	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.				
NOTE 2: Failure cases are described in subclause 5.7.				

5.3.3.4 Resource Custom Operations

5.3.3.4.1 Overview

Table 5.3.3.4.1-1: Custom operations

Custom operation URI	Mapped HTTP method	Description
{apiRoot}/ npcf-policyauthorization/v1 /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 AF 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. The Individual Application session context resource was deleted.
EventsNotification	M	1	200 OK	Successful case. The Individual Application Session Context resource was deleted and a partial representation of that resource containing event notification information is returned.
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.				

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	Definition
ApiRoot	See subclause 5.1
appSessionId	String formatted according to IETF RFC 3986 [19] identifying an application session context

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
EventsNotification	O	0..1	201 Created	Successful case. The Events Subscription sub-resource was created and events notification data is included.
EventsNotification	O	0..1	200 OK	Successful case. The Events Subscription sub-resource was modified and events notification data is included.
EventsSubscReqData	M	1	201 Created	Successful case. The Events Subscription sub-resource was created.
EventsSubscReqData	M	1	200 OK	Successful case. The Events Subscription sub-resource was modified and a representation of that sub-resource is returned.
n/a			204 No Content	Successful case. The Events Subscription sub-resource was modified.
ProblemDetails	M	1	403 Forbidden	(NOTE 2)
ProblemDetails	M	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.				
NOTE 2: Failure cases are described in subclause 5.7.				

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. The Events Subscription sub-resource was deleted.
ProblemDetails	M	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.				
NOTE 2: Failure cases are described in subclause 5.7.				

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 subclause 6.2 of 3GPP TS 29.500 [5] and subclause 4.6.2.3 of 3GPP TS 29.501 [6].

Table 5.5.1-1: Notifications

Custom operation URI	Mapped HTTP method	Description
{notifUri}/notify	POST	PCF event notification.
{notifUri}/terminate	POST	Request for termination of the 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 Notification URI **"{notifUri}/notify"** shall be used with the URI variables defined in table 5.5.2.2-1.

Table 5.5.2.2-1: URI variables

Name	Definition
notifUri	String formatted as URI with the Notification Uri as assigned within the Events Subscription sub-resource and described within the EventsSubscriptionData 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.
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.				

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 Notification URI **"{notifUri}/terminate"** shall be used with the URI variables defined in table 5.5.3.2-1.

Table 5.5.3.2-1: URI variables

Name	Definition
notifUri	String formatted as URI with 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.
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.			

5.6 Data Model

5.6.1 General

This subclause 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

Table 5.6.1-1: Npcf_PolicyAuthorization specific Data Types

Data type	Section defined	Description	Applicability
AfEvent	5.6.3.7	Represents an event to notify to the AF.	
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.	
AfRoutingRequirement	5.6.2.13	Describes the routing requirements for the application traffic flows.	Influence on Traffic Routing
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.	Influence on Traffic Routing
AnGwAddress	5.6.2.20	Carries the control plane address of the access network gateway.	
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 an Individual Application Session Context resource.	
ContentVersion	5.6.3.2	Represents the version of a media component.	Media Component Versioning
EventsNotification	5.6.2.9	Describes the notification about the events occurred within an Individual Application Session Context resource.	
EventsSubscReqData	5.6.2.6	Identifies the events the application subscribes to within an Individual Application Session Context resource.	
EventsSubscReqDataRm	5.6.2.6.25	This data type is defined in the same way as the "EventsSubscReqData" data type, but with the OpenAPI "nullable: true" property.	
EthFlowDescription	5.6.2.17	Defines a packet filter for an Ethernet flow.	
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	5.6.2.6.26	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.	
QosNotificationControlInfo	5.6.2.15	Indicates whether the QoS targets related to certain media component are not fulfilled or are fulfilled again.	
QosNotifType	5.6.3.9	Indicates type of notification for QoS Notification Control.	
ResourcesAllocationInfo	5.6.2.14	Indicates the status of the PCC rule(s) related to certain media component.	
ServAuthInfo	5.6.3.5	Indicates the result of the Policy Authorization service request from the AF.	
SpatialValidity	5.6.2.16	Describes the spatial validity of an AF request for influencing traffic routing.	Influence on Traffic Routing

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.	Influence on Traffic Routing
SponId	5.6.3.2	Contains an Identity of a sponsor.	Sponsored Connectivity
SponsoringStatus	5.6.3.6	Represents whether sponsored data connectivity is enabled or disabled/not enabled.	Sponsored Connectivity
TemporalValidity	5.6.2.22	Indicates the time interval during which the AF request is to be applied.	Influence on traffic routing
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.	

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
AccumulatedUsage	3GPP TS 29.122 [15]	Accumulated Usage.	Sponsored Connectivity
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.	
DateTime	3GPP TS 29.571 [12]	String with format "date-time" as defined in OpenAPI Specification [11].	Influence on Traffic Routing
Dnai	3GPP TS 29.571 [12]	Data network access identifier.	Influence on Traffic Routing
Dnn	3GPP TS 29.571 [12]	Data Network Name.	
FinalUnitAction	3GPP TS 32.291 [22]	Indicates the action to be taken when the user's account cannot cover the service cost.	
FlowDirection	3GPP TS 29.512 [8]	Flow Direction.	
Ipv4Addr	3GPP TS 29.571 [12]	Identifies an IPv4 address.	
Ipv6Addr	3GPP TS 29.571 [12]	Identifies an IPv6 address.	
MacAddr48	3GPP TS 29.571 [12]	MAC Address.	
PlmnId	3GPP TS 29.571 [12]	PLMN mobile country code and mobile network code.	NetLoc
PresenceInfo	3GPP TS 29.571 [12]	Represents an area of interest, e.g. a Presence Reporting Area.	Influence on Traffic Routing
RatType	3GPP TS 29.571 [12]	RAT Type.	
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
Uinteger	3GPP TS 29.571 [12]	Unsigned Integer, i.e. only value 0 and integers above 0 are permissible. In an OpenAPI Specification [11] schema, the format shall be designated as "Uinteger".	
UpPathChgEvent	3GPP TS 29.512 [8]	Contains the subscription information to be delivered to SMF for the UP path management events.	Influence on Traffic Routing
Uri	3GPP TS 29.571 [12]	String providing an URI.	
UsageThreshold	3GPP TS 29.122 [15]	Usage Thresholds.	Sponsored Connectivity
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.	Sponsored Connectivity
UserLocation	3GPP TS 29.571 [12]	User Location.	NetLoc

5.6.2   Structured data types

5.6.2.1   Introduction

This subclause 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	AppSessionContext ReqData	C	0..1	Identifies the service requirements of an Individual Application Session Context. It shall be present in HTTP POST request messages and may be included in the HTTP response messages.	
ascRespData	AppSessionContext RespData	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.	
afRoutReq	AfRoutingRequirement	C	0..1	Indicates the AF traffic routing requirements. It shall be included if Influence on Traffic Routing feature is supported.	Influence on Traffic Routing
aspId	AspId	C	0..1	Application service provider identity. It shall be included if Sponsored Connectivity feature is supported	Sponsored Connectivity
bdtRefId	BdtReferenceId	O	0..1	Reference to a transfer policy negotiated for background data traffic.	
dnn	Dnn	C	0..1	Data Network Name. 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.	
medComponents	map(MediaComponent)	O	1..N	Media Component information. The key of the map is the attribute "medCompN".	
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.	
notifUri	Uri	M	1	Notification URI for Application Session Context termination requests.	
sliceInfo	Snssai	O	0..1	Identifies the S-NSSAI.	
sponId	SponId	C	0..1	Sponsor identity. It shall be included if Sponsored Connectivity feature is supported.	Sponsored Connectivity
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.	Sponsored Connectivity
supi	Supi	O	0..1	Subscription Permanent Identifier.	
suppFeat	SupportedFeatures	M	1	This IE represents a list of Supported features used as described in subclause 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.	
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 the result of the authorization for a service request bound to a transfer policy.	
suppFeat	SupportedFeatures	C	0..1	This IE represents a list of Supported features used as described in subclause 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.	Influence on Traffic Routing
aspId	AspId	O	0..1	Application service provider identity.	Sponsored Connectivity
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.	
medComponents	map(MediaComponentRm)	O	1..N	Media Component information.	
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.	
sponId	SponId	O	0..1	Sponsor identity.	Sponsored Connectivity
sponStatus	SponsoringStatus	O	0..1	Indication of whether sponsored connectivity is enabled or disabled/not enabled.	Sponsored Connectivity

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.	
usgThres	UsageThreshold	O	0..1	Includes the volume and/or time thresholds for sponsored data connectivity.	Sponsored Connectivity

ETSI

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.	Influence on Traffic Routing
contVer	ContentVersion	O	0..1	Represents the content version of a media component.	Media Component Versioning
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 IP 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.	
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 IP flows is enabled, or disabled.	
resPrio	ReservPriority	O	0..1	Indicates the reservation priority.	
codecs	array(CodecData)	O	1..2	Indicates the codec data.	

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] subclause 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
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	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
accessType	AccessType	C	0..1	Includes the access type. It shall be present when the notified event is "ACCESS_TYPE_CHG".	
anGwAddr	AnGwAddress	O	0..1	Access network Gateway Address. It shall be present, if applicable, when the notified event is "ACCESS_TYPE_CHG".	
evSubsUri	Uri	M	1	The Events Subscription URI. Identifies the Events Subscription sub-resource that triggered the notification.	
evNotifs	array(AfEventNotification)	M	1..N	Notifications about individual events.	
failedResourcAllocReports	array(ResourcesAllocationInfo)	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".	
plmnId	PlmnId	C	0..1	PLMN Identifier. It shall be present when the notified event is "PLMN_CHG".	
qncReports	array(QosNotificationControlInfo)	C	1..N	QoS notification control information. It shall be present when the notified event is "QOS_NOTIF_CONTROL".	
ratType	RatType	O	0..1	RAT type. It shall be present, if applicable, when the notified event is "ACCESS_TYPE_CHG".	
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".	Sponsored Connectivity

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.	

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.	

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.	Influence on traffic routing
routeToLocs	array(RouteToLocation)	O	1..N	A list of traffic routes to applications locations.	Influence on traffic routing
spVal	SpatialValidity	O	0..1	Indicates where the traffic routing requirements apply. The absence of this attribute indicates no spatial restrictions.	Influence on traffic routing
tempVals	array(TemporalValidity)	O	1..N	Indicates the time interval(s) during which the AF request is to be applied.	Influence on traffic routing
upPathChgSub	UpPathChgEvent	O	0..1	Subscription to UP path management events.	Influence on traffic routing

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	M	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. It shall be included if Media Component Versioning feature is supported. When Media Component Versioning feature is not supported, if no flows are provided, the status in the "mcResourcStatus" applies for all flows within the AF session.	

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	0..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 Media Component Versioning feature is supported. When Media Component Versioning feature is not supported, if no flows are provided, the notification in the "notifType" applies for all flows within the AF session.	

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 AF. The "presenceState" attribute within the "PresenceInfo" data type shall not be supplied.	Influence on Traffic Routing

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. 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.	
fDir	FlowDirection	O	0..1	Contains the packet filter direction.	
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]. 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 4 most significant bits of the VID or PCF/DEI field shall appear first in the string, and the character representing the 4 least significant bits of the VID or PCF/DEI field shall appear last in the string.	
NOTE: The EthFlowDescription data type allows any combination of the defined properties.					

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 Media Component Versioning feature is supported, the content version shall be included if it was included when the corresponding media component was provided or modified.	Media Component Versioning
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
startime	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.	Influence on traffic 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.	Influence on traffic 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; and

- the removable attribute "spVal" is defined with the data type "SpatialValidityRm", and the removable attribute "tempVals" is 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.	Influence on traffic routing
routeToLocs	array(RouteToLocation)	O	1..N	A list of traffic routes to applications locations.	Influence on traffic routing
spVal	SpatialValidityRm	O	0..1	Indicates where the traffic routing requirements apply.	Influence on traffic routing
tempVals	array(TemporalValidity)	O	1..N	Indicates the time interval(s) during which the AF request is to be applied.	Influence on traffic routing
upPathChgSub	UpPathChgEvent	O	0..1	Subscription to UP path management events.	Influence on traffic routing

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".

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.	
usgThres	UsageThresholdRm	O	0..1	Includes the volume and/or time thresholds for sponsored data connectivity.	Sponsored Connectivity

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", "medSubComps", and "marBwDl", "marBwUl", "mirBwDl" and "mirBwUl" are defined with the removable data types "AfRoutingRequirementRm", "MediaSubComponentRm", and "BitRateRm".

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.	Influence on Traffic Routing
contVer	ContentVersion	O	0..1	Represents the content version of a media component.	Media Component Versioning
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 IP 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.	
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 IP flows is enabled, or disabled.	
resPrio	ReservPriority	O	0..1	Indicates the reservation priority.	
codecs	array(CodecData)	O	1..2	Indicates the codec data.	

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; and

- the removable attributes "marBwDl", "marBwUl", defined with the removable data type "BitRateRm".

Table 5.6.2.27-1: Definition of type MediaSubComponentRm

Attribute name	Data type	P	Cardinality	Description	Applicability
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.

5.6.3 Simple data types and enumerations

5.6.3.1 Introduction

This subclause defines simple data types and enumerations that can be referenced from data structures defined in the previous subclauses.

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.	Sponsored Connectivity
CodecData	string	Contains codec related information. Refer to subclause 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)	Media Component Versioning
FlowDescription	string	Defines a packet filter for an IP flow. Refer to subclause 5.3.8 of 3GPP TS 29.214 [20] for encoding.	
SponId	string	Contains an identity of a sponsor.	Sponsored Connectivity
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.	
TosTrafficClassRm	string	This data type is defined in the same way as the "TosTrafficClass" data type, but with the OpenAPI "nullable: true" property.	
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 AF.

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.	

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.	Sponsored Connectivity
SPONSOR_ENABLED	Sponsored data connectivity is enabled.	Sponsored Connectivity

5.6.3.7 Enumeration: AfEvent

The enumeration "AfEvent" represents the traffic events the PCF can notify to the AF.

Table 5.6.3.7-1: Enumeration AfEvent

Enumeration value	Description	Applicability
ACCESS_TYPE_CHG	Access type change.	
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.	
PLMN_CHG	This trigger indicates PLMN change.	
QOS_NOTIF	The GBR QoS targets of a SDF are not fulfilled or are fulfilled again.	
SUCCESSFUL_RESOURCES_ALLOCATION	Indicates that the resources requested for particular service information have been successfully allocated.	
USAGE_REPORT	Volume and/or time usage for sponsored data connectivity.	Sponsored Connectivity

5.6.3.8   Enumeration: AfNotifMethod

The enumeration "AfNotifMethod" represents the notification methods that can be subscribed by an AF.

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.	

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 AF 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.	
PDU_SESSION_TERMINATION	The PDU session is terminated.	

5.6.3.11   Void

5.6.3.12   Enumeration: FlowStatus

The enumeration "FlowStatus" represents whether the IP 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 IP flow(s) and to disable associated downlink IP flow(s).	
ENABLED-DOWNLINK	Indicates to enable associated downlink IP flow(s) and to disable associated uplink IP flow(s).	
ENABLED	Indicates to enable all associated IP flow(s) in both directions.	
DISABLED	Indicates to disable all associated IP flow(s) in both directions.	
REMOVED	Indicates to remove all associated IP flow(s). The IP Filters for the associated IP flow(s) shall be removed. The associated IP 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.	

NOTE: An AF can choose not to identify RTCP flows, e.g. in order to avoid that RTCP flows are always enabled by the server.

5.7 Error handling

5.7.1 General

HTTP error handling shall be supported as specified in subclause 5.2.4 of 3GPP TS 29.500 [5].

For the Npcf_PolicyAuthorization API, HTTP error responses shall be supported as specified in subclause 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 subclauses 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. The PCF shall include in the HTTP status code a "ProblemDetails" data structure with the "cause" attribute indicating the application error as listed in table 5.7.3-1.

Table 5.7.3-1: Application errors

Application Error	HTTP status code	Description
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)
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 subclauses 4.2.2.2 and 4.2.2.5) and to the PATCH request (see subclauses 4.2.3.2 and 4.2.3.5).		
NOTE 2: This application error is included in the response to the POST request (see subclause 4.2.2.2) and to the PATCH request (see subclause 4.2.3.2).		
NOTE 3: This application error is included in the response to the POST request (see subclause 4.2.2.5) and to the PATCH request (see subclause 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.		
NOTE 5: This application error is included in the response to the POST request (see subclauses 4.2.2.2).		

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 subclause 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 subclause 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	Influence on Traffic Routing	Indicates support of Application Function influence on traffic routing. If the PCF supports this feature, the AF may influence SMF routing to applications or subscribe to notifications of UP path management for the traffic flows of an active PDU session.
2	Sponsored Connectivity	Indicates support of sponsored data connectivity. If the PCF supports this feature, the AF may provide sponsored data connectivity to the SUPI.
3	Media Component Versioning	Indicates the support of the media component versioning.

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], subclause 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.

In case of conflicts between the main body of the present document and the present Annex, the information in the main body shall be applicable.

A.2　Npcf_PolicyAuthorization API

```
openapi: 3.0.0
info:
  title: "Npcf_PolicyAuthorization Service API"
  version: "1.0.0"
  description: "This is the Policy Authorization Service"

externalDocs:
  description: 3GPP TS 29.514 V15.2.0; 5G System; Policy Authorization Service;Stage 3.
  url: 'http://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 subclause 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. The HTTP response shall contain a Location header field set to
the URI of the existing individual Application Session Context resource
        '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:
                  $ref: 'TS29571_CommonData.yaml#/components/responses/default'
          callbacks:
            terminationRequest:
              '{$request.body#/notifUri}/terminate':
                post:
                  requestBody:
                    description: Request of the termination of the Individual Application Session
Context
                    content:
                      application/json:
                        schema:
                          $ref: '#/components/schemas/TerminationInfo'
                  responses:
                    '204':
                      description: The receipt of the notification is acknowledged.
                    '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#/evSubsc/notifUri}/notify':
                post:
                  requestBody:
                    description: Notification of an event occurrence in the PCF.
                    content:
                      application/json:
                        schema:
                          $ref: '#/components/schemas/EventsNotification'
                  responses:
                    '204':
                      description: The receipt of the notification is acknowledged
                    '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'
        '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/AppSessionContextUpdateData'
      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
            '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#/evSubsc/notifUri}/notify':
                post:
                  requestBody:
                    description: Notification of an event occurrence in the PCF.
                    content:
                      application/json:
                        schema:
                          $ref: '#/components/schemas/EventsNotification'
                  responses:
                    '204':
                      description: The receipt of the notification is acknowledged
                    '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.
        '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:
                anyOf:
                  - $ref: '#/components/schemas/EventsSubscReqData'
                  - $ref: '#/components/schemas/EventsNotification'
          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 of the Events Subscription resource is confirmed its
representation is returned.
          content:
            application/json:
```

```
                        schema:
                          anyOf:
                          - $ref: '#/components/schemas/EventsSubscReqData'
                          - $ref: '#/components/schemas/EventsNotification'
              '204':
                description: The modification of the Events Subscription subresource is confirmed without
returning additional data.
              '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.
                  content:
                    application/json:
                      schema:
                        $ref: '#/components/schemas/EventsNotification'
                responses:
                  '204':
                    description: The receipt of the notification is acknowledged.
                  '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.
                    '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'
        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'
        medComponents:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MediaComponent'
          minProperties: 1
        ipDomain:
          type: string
        mpsId:
          description: indication of MPS service request
          type: string
        notifUri:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Uri'
        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'
        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'
    AppSessionContextRespData:
      description: Describes the authorization data of an Individual Application Session Context
created by the PCF.
      type: object
      properties:
        servAuthInfo:
          $ref: '#/components/schemas/ServAuthInfo'
        suppFeat:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
    AppSessionContextUpdateData:
      description: Identifies the modifications to an Individual Application Session Context and 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'
        medComponents:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MediaComponentRm'
          minProperties: 1
        mpsId:
          description: indication of MPS service request
          type: string
        sponId:
          $ref: '#/components/schemas/SponId'
        sponStatus:
          $ref: '#/components/schemas/SponsoringStatus'
    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: 'TS29122_CommonData.yaml#/components/schemas/Uri'
        usgThres:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/UsageThreshold'
    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: 'TS29122_CommonData.yaml#/components/schemas/Uri'
        usgThres:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/UsageThresholdRm'
```

```
        nullable: true
    MediaComponent:
      description: Identifies a media component.
      type: object
      required:
        - medCompN
      properties:
        afAppId:
          $ref: '#/components/schemas/AfAppId'
        afRoutReq:
          $ref: '#/components/schemas/AfRoutingRequirement'
        contVer:
          $ref: '#/components/schemas/ContentVersion'
        codecs:
          type: array
          items:
            $ref: '#/components/schemas/CodecData'
          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'
        medCompN:
          type: integer
        medSubComps:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MediaSubComponent'
          minProperties: 1
        medType:
          $ref: '#/components/schemas/MediaType'
        mirBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        mirBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        resPrio:
          $ref: '#/components/schemas/ReservPriority'
    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'
        contVer:
          $ref: '#/components/schemas/ContentVersion'
        codecs:
          type: array
          items:
            $ref: '#/components/schemas/CodecData'
          minItems: 1
          maxItems: 2
        fStatus:
          $ref: '#/components/schemas/FlowStatus'
        marBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        marBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        medCompN:
          type: integer
        medSubComps:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/MediaSubComponentRm'
          minProperties: 1
        medType:
          $ref: '#/components/schemas/MediaType'
        mirBwDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
        mirBwUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
```

```
            resPrio:
              $ref: '#/components/schemas/ReservPriority'
          nullable: true
    MediaSubComponent:
      description: Identifies a media subcomponent
      type: object
      required:
        - fNum
      properties:
        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 marBwDland marBwUl are defined
with the corresponding removable data type.
      type: object
      required:
        - fNum
      properties:
        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:
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        anGwAddr:
```

```
                  $ref: '#/components/schemas/AnGwAddress'
              evSubsUri:
                $ref: 'TS29122_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
              plmnId:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnId'
              qncReports:
                type: array
                items:
                  $ref: '#/components/schemas/QosNotificationControlInfo'
                minItems: 1
              ratType:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
              usgRep:
                $ref: 'TS29122_CommonData.yaml#/components/schemas/AccumulatedUsage'
      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'
      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: 'TS29122_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'
      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
      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
        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'
        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


    ResourcesAllocationInfo:
      description: describes the status of the PCC rule(s) related to certain media components.
      type: object
      required:
        - mcResourcStatus
      properties:
        mcResourcStatus:
          $ref: '#/components/schemas/MediaComponentResourcesStatus'
        flows:
          type: array
          items:
            $ref: '#/components/schemas/Flows'
          minItems: 1
    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
#
# 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
      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
#
# ENUMERATIONS DATA TYPES
#
      MediaType:
        anyOf:
        - type: string
          enum:
            - AUDIO
            - VIDEO
            - DATA
            - APPLICATION
            - CONTROL
            - TEXT
            - MESSAGE
            - OTHER
        - type: string
#
      ReservPriority:
        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:
        anyOf:
        - type: string
          enum:
            - TP_NOT_KNOWN
            - TP_EXPIRED
            - TP_NOT_YET_OCURRED
        - type: string
#
      SponsoringStatus:
        anyOf:
        - type: string
          enum:
            - SPONSOR_DISABLED
            - SPONSOR_ENABLED
        - type: string
#
      AfEvent:
        anyOf:
        - type: string
          enum:
            - ACCESS_TYPE_CHANGE
            - FAILED_RESOURCES_ALLOCATION
            - PLMN_CHG
            - QOS_NOTIF
```

```
                - SUCCESSFUL_RESOURCES_ALLOCATION
                - USAGE_REPORT
          - type: string
#
      AfNotifMethod:
        anyOf:
        - type: string
          enum:
              - EVENT_DETECTION
              - ONE_TIME
        - type: string
#
      QosNotifType:
        anyOf:
        - type: string
          enum:
              - GUARANTEED
              - NOT_GUARANTEED
        - type: string
#
      TerminationCause:
        anyOf:
        - type: string
          enum:
              - ALL_SDF_DEACTIVATION
              - PDU_SESSION_TERMINATION
        - type: string
#
      MediaComponentResourcesStatus:
        anyOf:
        - type: string
          enum:
              - ACTIVE
              - INACTIVE
        - type: string
#
#
      FlowUsage:
        anyOf:
        - type: string
          enum:
              - NO_INFO
              - RTCP
        - type: string


      FlowStatus:
        anyOf:
        - type: string
          enum:
              - ENABLED-UPLINK
              - ENABLED-DOWNLINK
              - ENABLED
              - DISABLED
              - REMOVED
        - type: string
```

Annex B (informative): Change history

						Change history	
Date	**TSG #**	**TSG Doc.**	**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: C3-180036, C3-180038, C3-180212, C3-180213, C3-180214, C3-180217, C3-180218, C3-180243, C3-180313, C3-180314, C3-180315, C3-180316.	0.2.0
2018-03	CT3#95					Inclusion of documents agreed in CT3#95: 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: C3-182057, C3-182333, C3-182235, C3-182334, C3-182474, C3-182336, C3-182337, C3-182338, C3-182339, C3-182245, C3-182475, C3-182247, C3-182248, C3-182249, C3-182250, C3-182251	0.4.0
2018-06	CT3#97					Inclusion of documents agreed in CT3#97: C3-183220, C3-183222, C3-183230, C3-183233, C3-183234, C3-183239, C3-183281, C3-183300, C3-183301, C3-183517, C3-183518, C3-183520, C3-183521, C3-183522, C3-183523, C3-183524, C3-183525, C3-183526, C3-183577, C3-183579, C3-183580, C3-183581, C3-183582, C3-183583, C3-183584, C3-183585, C3-183586, C3-183587, C3-183588, C3-183589, C3-183590, C3-183591, C3-183592, C3-183820, C3-183821, C3-183822, 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

History

Document history		
V15.0.0	July 2018	Publication
V15.1.0	October 2018	Publication
V15.2.0	April 2019	Publication