ETSI TS 129 523 V19.5.0 (2026-07)

TECHNICAL SPECIFICATION

5G;
5G System;
Policy Control Event Exposure Service;
Stage 3
(3GPP TS 29.523 version 19.5.0 Release 19)

Reference
RTS/TSGC-0329523vj50

Keywords
5G

ETSI

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

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

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

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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

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

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

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 document specifies the stage 3 protocol and data model for the Policy Control Event Exposure Service of the 5G System. It provides stage 3 protocol definitions, message flows and specifies the API for the Npcf Event Exposure service.

The 5G System stage 2 architecture and the procedures are specified in 3GPP TS 23.501 [2], 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 [8].

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 Control Event Exposure Service is provided by the Policy Control Function (PCF). This service exposes policy control events observed at the PCF.

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

[8] 3GPP TS 29.513: "5G System; Policy and Charging Control signalling flows and QoS parameter mapping; Stage 3".

[9] 3GPP TS 29.512: "5G System; Session Management Policy Control Service; Stage 3".

[10] 3GPP TS 29.507: "5G System; Access and Mobility Policy Control Service; Stage 3".

[11] 3GPP TS 29.525: "5G System; UE Policy Control Service; Stage 3".

[12] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[13] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[14] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[15] 3GPP TS 29.508: "5G System; Session Management Event Exposure Service; Stage 3".

[16] IETF RFC 9113: "HTTP/2".

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

[18] IETF RFC 9457: "Problem Details for HTTP APIs".

[19] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

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

[21] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

[22] 3GPP TR 21.900: "Technical Specification Group working methods".

[23] 3GPP TS 29.534: "5G System; Access and Mobility Policy Authorization Service; Stage 3".

[24] 3GPP TS 29.519: "5G System; Usage of the Unified Data Repository service for Policy Data, Application Data and Structured Data for Exposure; Stage 3".

[25] 3GPP TS 29.522: "5G System; Network Exposure Function Northbound APIs; Stage 3".

[26] 3GPP TS 29.122: "T8 reference point for Northbound APIs".

3 Definitions, symbols 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].

example: text used to clarify abstract rules by applying them literally.

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
AMF	Access and Mobility Management Function
API	Application Programming Interface
ATSSS	Access Traffic Steering, Switching and Splitting
DNN	Data Network Name
ePDG	evolved Packet Data Gateway
GEO	Geosynchronous Orbit
GPSI	Generic Public Subscription Identifier
HTTP	Hypertext Transfer Protocol
LEO	Low Earth Orbit
MA	Multi-Access
MEO	Medium Earth Orbit
NEF	Network Exposure Function
NID	Network Identifier
NF	Network Function
NRF	Network Repository Function
NWDAF	Network Data Analytics Function
OAM	Operation And Maintenance
PCF	Policy Control Function
RFSP	RAT Frequency Selection Priority
SAC	Service Area Coverage
S-NSSAI	Single Network Slice Selection Assistance Information
SMF	Session Management Function

SNPN	Stand-alone Non-Public Network
SUPI	Subscription Permanent Identifier
UDM	Unified Data Management
UDR	Unified Data Repository
UPF	User Plane Function
URSP	UE Route Selection Policy

4 Npcf_EventExposure Service

4.1 Service Description

4.1.1 Overview

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

This service:

- allows NF service consumers to subscribe to, modify and unsubscribe from policy control events; and
- notifies NF service consumers with a corresponding subscription about observed events on the PCF.

The types of observed events include:

- PLMN identifier notification;

NOTE 1: Within the PLMN identifier notification event the PLMN Identifier or SNPN Identifier where the UE is currently located is provided. The SNPN Identifier consists of the PLMN Identifier and the NID.

NOTE 2: Mobility between non-equivalent SNPNs, and between SNPN and PLMN is not supported. When the UE is operating in SNPN access mode, the trigger reports changes of equivalent SNPNs.

- access type change;
- satellite backhaul category change;
- service area coverage change;
- successful or unsuccessful outcome of the UE Policy Delivery;
- unsuccessful PCF service parameter authorization;
- application traffic detection events;
- rate limitation information event notification;
- signalling information events; and
- AF requested Network Slice Replacement outcome.

The target of the event reporting may include a group of UE(s) or any UE (i.e. all UEs). When an event occurs, to which the NF service consumer has subscribed, the PCF reports the requested information to the NF service consumer based on the event reporting information definition requested by the NF service consumer (see 3GPP TS 23.502 [3], clause 4.15.1).

4.1.2 Service Architecture

The 5G System Architecture is defined in 3GPP TS 23.501 [2]. The Policy and Charging related 5G architecture and signalling flows are also described in 3GPP TS 29.513 [8].

The Policy Event Exposure Service (Npcf_EventExposure) is part of the Npcf service-based interface exhibited by the Policy Control Function (PCF).

The known NF service consumers of the Npcf_EventExposure service are the Network Exposure Function (NEF), the Application Function (AF), the Network Data Analytics Function (NWDAF), and the Data Collection Coordination Function (DCCF).

The Npcf_EventExposure service is provided by the PCF and consumed by NF service consumers, as shown in figure 4.1.2-1 for the SBI representation model and in figure 4.1.2-2 for reference point representation model.

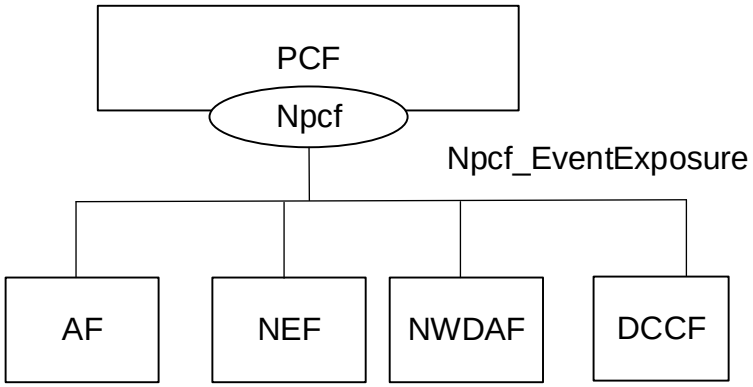

Figure 4.1.2-1: Npcf_EventExposure service Architecture, SBI representation

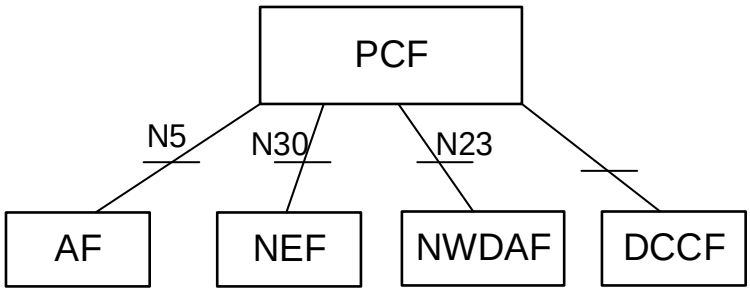

Figure 4.1.2-2: Npcf_EventExposure service Architecture, reference point representation

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 as defined in 3GPP TS 29.512 [9], access and mobility policy decisions for the control of the UE Service Area Restrictions and RAT/RFSP control as defined in 3GPP TS 29.507 [10] and UE Policy decisions for the control of Access network discovery and selection policy and UE Route Selection Policy (URSP) as defined in 3GPP TS 29.525 [11].

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 offers these capabilities to the NF service consumers (e.g. the AF and NEF) as defined in 3GPP TS 29.514 [12] and 3GPP TS 29.214 [13].

The PCF also offers the access and mobility policy control to the NF service consumers as defined in 3GPP TS 29.534 [23].

The Policy Event Exposure Service enables the PCF to report policy control events observed in one or more PCF services to NF service consumers.

4.1.3.2 NF Service Consumers

As indicated in clause 4.1.2 above, the known NF service consumer of the Npcf_EventExposure service are the Network Exposure Function (NEF), the Application Function (AF), the Network Data Analytics Function (NWDAF), and the Data Collection Coordination Function (DCCF).

The Network Exposure Function (NEF) is a functional element that supports the following functionalities:

- The NEF securely exposes network capabilities and events provided by 3GPP NFs to AF.
- The NEF provides a means for the AF to securely provide information to 3GPP network and can authenticate, authorize and assist in throttling the AF.
- The NEF translates the information received from the AF to the one sent to internal 3GPP NFs, and vice versa.
- The NEF supports exposing information (collected from other 3GPP NFs) to the AF.

The Application Function (AF) is a functional element offering control to applications that require the policy and charging control of traffic plane resources; specific user plane paths for the requested traffic, the monitoring of the required service QoS, and/or specific QoS and alternative QoS profiles. The AF uses the Npcf_EventExposure service to receive exposed information from the 5GC network.

The Network Data Analytics Function (NWDAF) is a network function which computes and exposes different types of analytics information.

The Data Collection Coordination Function (DCCF) is a network function which coordinates the data collection for the purpose of analytics computation.

4.2 Service Operations

4.2.1 Introduction

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

Table 4.2.1-1: Npcf_EventExposure Service Operations

Service Operation Name	Description	Initiated by
Npcf_EventExposure_Subscribe	This service operation is used by an NF service consumer to subscribe for event notifications on a specified policy control event for a group of UE(s) or any UE, or to modify a subscription.	NF service consumer (e.g. NEF)
Npcf_EventExposure_Unsubscribe	This service operation is used by an NF service consumer to unsubscribe from event notifications.	NF service consumer (e.g. NEF)
Npcf_EventExposure_Notify	This service operation is used by the PCF to report UE related policy control event(s) to the NF service consumer which has subscribed to the event report service.	PCF

4.2.2 Npcf_EventExposure_Subscribe service operation

4.2.2.1 General

This service operation is used by an NF service consumer to explicitly subscribe for policy events notifications on a specified context for a group of UE(s) or any UE, or to modify an existing subscription.

The following are the types of events for which a subscription can be made:

- PLMN identifier notification;

NOTE 1: Within the PLMN identifier notification event the PLMN Identifier or SNPN Identifier where the UE is currently located is provided. The SNPN Identifier consists of the PLMN Identifier and the NID.

NOTE 2: Mobility between non-equivalent SNPNs, and between SNPN and PLMN is not supported. When the UE is operating in SNPN access mode, the trigger reports changes of equivalent SNPNs.

- change of Access Type;
- when the feature "AMPoliciesEvents" is supported, change of Service Area Coverage;

- when the feature "SatelliteBackhaul" is supported, satellite backhaul category change;
- when the feature "DeliveryOutcome" is supported, UE Policy delivery outcome;
- when the feature "PCFSerParAuth" is supported, unsuccessful PCF service parameter authorization;
- when the feature "AppDetection" is supported, application traffic detection (Start/Stop) event notification;
- when the feature "RateLimitReport" is supported, Rate Limitation information event notification;
- when the feature "SignallingInfo" is supported, signalling information events; and
- when the "AfNetSliceRepl" feature is supported, the AF requested Network Slice Replacement outcome.

The following procedures using the Npcf_EventExposure_Subscribe service operation are supported:

- creating a new subscription;
- modifying an existing subscription.

NOTE 3: It is also possible to implicitly subscribe for policy events notifications for a single UE, for a group of UE(s) or any UE. Implicit subscription information is obtained from the UDR for application data. In this case, the PCF will use the callback URI provided by the AF to the UDR, see 3GPP TS 29.519 [24] for the details.

4.2.2.2 Creating a new subscription

Figure 4.2.2.2-1 illustrates the creation of a subscription.

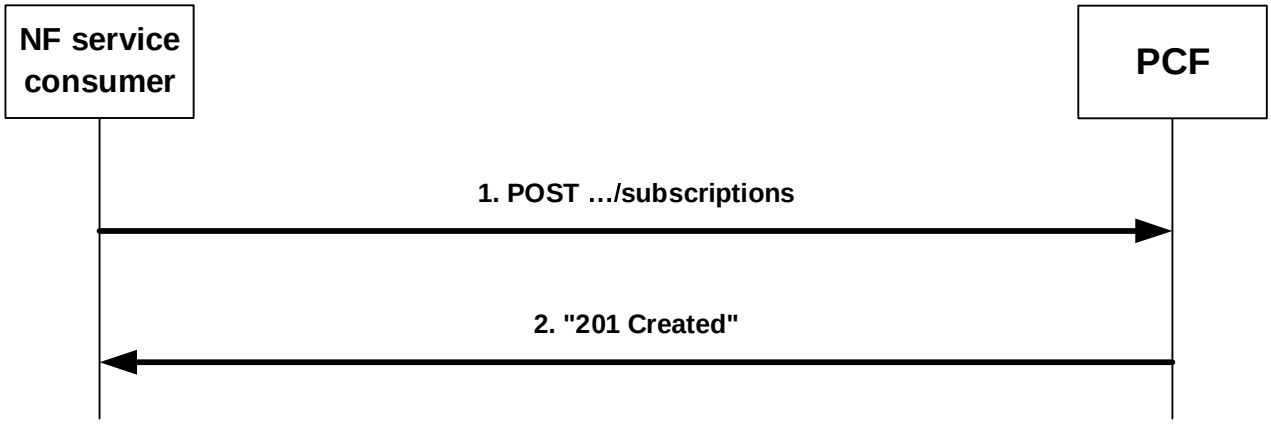

Figure 4.2.2.2-1: Creation of a subscription

To subscribe to event notifications, the NF service consumer shall send an HTTP POST request with: "{apiRoot}/npcf-eventexposure/v1/subscriptions" as request URI as shown in figure 4.2.2.2-1, step 1, and the "PcEventExposureSubsc" data structure as request body.

The "PcEventExposureSubsc" data structure shall include:

- identification of the policy events to subscribe as "eventSubs" attribute;
- indication of the UEs to which the subscription applies via:
  a) identification of a group of UE(s) via a "groupId" attribute; or
  b) identification of any UE by omitting the "groupId" attribute;
- a URI where to receive the requested notifications as "notifUri" attribute;
- a Notification Correlation Identifier assigned by the NF service consumer for the requested notifications as "notifId" attribute; and

- when the feature "AppDetection" is supported, to indicate the specific application(s) for which the application detection policy event report shall occur, the application identifier(s) in the "appIds" attribute and the concerned S-NSSAI and DNN within the "snssaiDnns" attribute.

NOTE: The subscription to "APPLICATION_START" and/or "APPLICATION_STOP" application detection policy event(s) for one or more application identifiers can impact the SMF/UPF performance. The restriction to a specific combination of S-NSSAI and DNN avoids excessive signalling load.

The "PcEventExposureSubsc" data structure may also include:

- description of the event reporting information as "eventsRepInfo", which may include:

  a) event notification method (periodic, one time, on event detection) as "notifMethod" attribute;

  b) Maximum Number of Reports as "maxReportNbr" attribute;

  c) Monitoring Duration as "monDur" attribute;

  d) repetition period for periodic reporting as "repPeriod" attribute;

  e) immediate reporting indication as "immRep" attribute;

  f) sampling ratio as "sampRatio" attribute;

  g) group reporting guard time as "grpRepTime" attribute;

  h) partitioning criteria for partitioning the UEs before performing sampling as "partitionCriteria" attribute if the EneNA feature is supported; and/or

  i) a notification flag as "notifFlag" attribute if the EneNA feature is supported;

- if the supported feature "ExtendedSessionInformation" is supported, to filter the AF sessions for which the policy event report shall occur, the identification of the services one or more AF sessions may belong to as "filterServices" attribute, which may include per service identification:

  a) a list of ethernet flows in the "servEthFlows" attribute; or

  b) a list of IP flows in the "servIpFlows" attribute; and/or

  c) an AF application identifier in the "afAppId" attribute;

- to filter the DNNs for which the policy event report shall occur, the identification of the DNNs in the "filterDnns" attribute;

- to filter the S-NSSAIs for which the policy event report shall occur, the identification of the S-NSSAIs in the "filterSnssais" attribute;

- when the feature "EneNA" is supported, to filter the specific DNN and S-NSSAI combination list for which the policy event report shall occur, the identification of each combination within the "snssaiDnns" attribute; and

- when the feature "SignallingInfo" is supported, the time windows for which signalling information shall be reported within the "tws" attribute.

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

Upon successful reception of the HTTP POST request with "{apiRoot}/npcf-eventexposure/v1/subscriptions" as request URI and "PcEventExposureSubsc" data structure as request body, the PCF shall create a new "Individual Policy Events Subscription" resource, store the subscription and send a HTTP "201 Created" response 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 "PcEventExposureSubsc" data type in the content.

The Location header field shall contain the URI of the created individual application session context resource i.e. "{apiRoot}/npcf-eventexposure/v1/subscriptions/{subscriptionId}".

The "PcEventExposureSubsc" data type in the response content shall contain the representation of the created "Individual Policy Events Subscription".

When the "monDur" attribute is included in the response, it represents a server selected expiry time that is equal or less than a possible expiry time in the request.

When the "immRep" attribute set to true is included in the subscription and the subscribed policy control events are available:

- if the feature "ERIR" is not supported, the PCF shall immediately notify the NF service consumer with the current available value(s) for the subscribed event(s) using the Npcf_EventExposure_Notify service operation, as described in clause 4.2.4.2.
- if the feature "ERIR" is supported, the PCF shall immediately notify the NF service consumer with the current available value(s) for the subscribed event(s) within the HTTP "201 Created" response as shown in figure 4.2.2.2-1, step 2. The "PcEventExposureSubsc" data type shall include the corresponding event(s) notification within the "eventNotifs" attribute, as described in clause 4.2.4.2.

When the sampling ratio as the "sampRatio" attribute is included in the subscription without a "partitionCriteria" attribute, the PCF shall select a random subset of UEs among the target UEs according to the sampling ratio and only report the event(s) related to the selected subset of UEs. If the "partitionCriteria" attribute is additionally included, then the PCF shall first partition the UEs according to the value of the "partitionCriteria" attribute and then select a random subset of UEs from each partition according to the sampling ratio and only report the event(s) related to the selected subsets of UEs.

When the group reporting guard time as the "grpRepTime" attribute is included in the subscription, the PCF shall accumulate all the event reports for the target UEs until the group reporting guard time expires. Then the PCF shall notify the NF service consumer using the Npcf_EventExposure_Notify service operation, as described in clause 4.2.4.2.

When the "notifFlag" attribute is included and set to "DEACTIVATE" in the request, the PCF shall mute the event notification and store the available events until the NF service consumer requests to retrieve them by setting the "notifFlag" attribute to "RETRIEVAL" or until a muting exception occurs (e.g. full buffer).

When the feature "AppDetection" is supported, and the "APPLICATION_START" and/or "APPLICATION_STOP" policy event(s) are included in the request, the PCF shall trigger the provisioning of the PCC rule(s) for application detection and control for the application identifier(s) included in the "appIds" attribute as specified in 3GPP TS 29.512 [9], clause 4.2.6.2.11, if not previously provisioned, and for every PDU session of the DNN and S-NSSAI included in the "snssaiDnns" attribute.

When the feature "RateLimitReport" is supported, and the "RATE_LIMIT_INFO_REPO" event is included in the request, the PCF shall determine the Authorized Session AMBR as the rate limitation for the PDU session and report to the NF service consumer in the "rateLimitRepo" attribute in the response.

4.2.2.3 Modifying an existing subscription

Figure 4.2.2.3-1 illustrates the modification of an existing subscription.

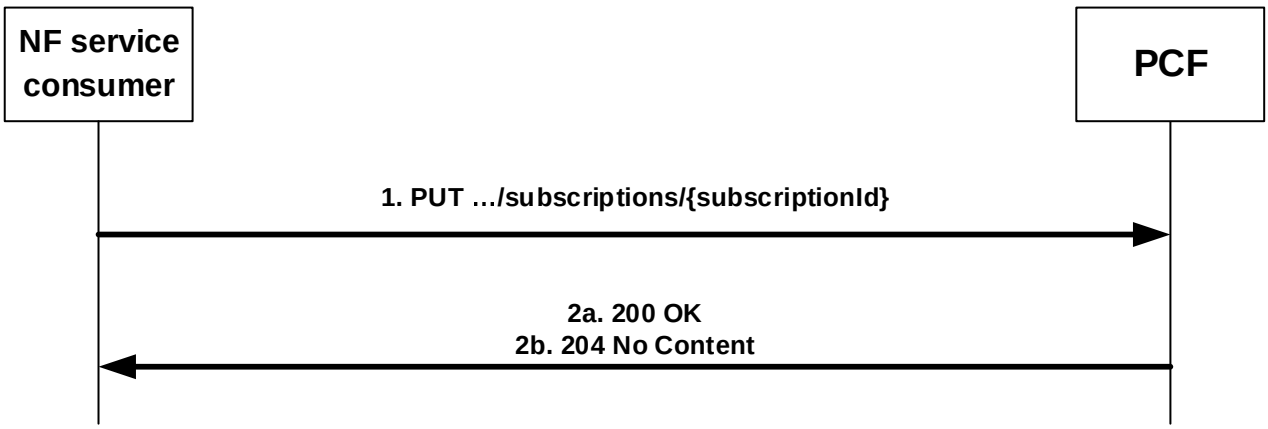

Figure 4.2.2.3-1: Modification of an existing subscription

To modify an existing subscription to event notifications, the NF service consumer shall send an HTTP PUT request with: "{apiRoot}/npcf-eventexposure/v1/subscriptions/{subscriptionId}" as request URI, as shown in figure 4.2.2.3-1, step 1, where "{subscriptionId}" is the subscription correlation ID of the existing subscription. The "PcEventExposureSubsc" data structure is included as request body as described in clause 4.2.2.2.

NOTE 1: An alternate NF service consumer than the one that requested the generation of the subscription resource can send the PUT.

NOTE 2: The "notifUri" attribute within the PcEventExposureSubsc data structure can be modified to request that subsequent notifications are sent to a new NF service consumer.

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

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

Upon successful reception of an HTTP PUT request with: "{apiRoot}/npcf-eventexposure/v1/subscriptions/{subscriptionId}" as request URI and "PcEventExposureSubsc" data structure as request body, the PCF shall store the subscription and send an HTTP "200 OK" response with the "PcEventExposureSubsc" data structure as response body or an HTTP "204 No Content" response, as shown in figure 4.2.2.3-1, step 2.

The "PcEventExposureSubsc" data structure in the response content shall contain the representation of the modified "Individual Policy Events Subscription".

When the "monDur" attribute is included in the response, it represents a NF service producer selected expiry time that is equal or less than a possible expiry time received in the request.

When the "immRep" attribute set to true is included in the updated subscription and the subscribed policy control events are available:

- if the feature "ERIR" is not supported, the PCF shall immediately notify the NF service consumer with the current available value(s) for the subscribed event(s) using the Npcf_EventExposure_Notify service operation, as described in clause 4.2.4.2.
- if the feature "ERIR" is supported, the PCF shall immediately notify the NF service consumer with the current available value(s) for the subscribed event(s) within the HTTP "200 OK" response as shown in figure 4.2.2.3-1, step 2a. The "PcEventExposureSubsc" data type shall include the corresponding event(s) notification within the "eventNotifs" attribute, as described in clause 4.2.4.2.

When the sampling ratio as the "sampRatio" attribute is included in the subscription without a "partitionCriteria" attribute, the PCF shall select a random subset of UEs among the target UEs according to the sampling ratio and only report the event(s) related to the selected subset of UEs. If the "partitionCriteria" attribute is additionally included, then the PCF shall first partition the UEs according to the value of the "partitionCriteria" attribute and then select a random subset of UEs from each partition according to the sampling ratio and only report the event(s) related to the selected subsets of UEs.

When the group reporting guard time as the "grpRepTime" attribute is included in the subscription, the PCF shall accumulate all the event reports for the target UEs until the group reporting guard time expires. Then the PCF shall notify the NF service consumer using the Npcf_EventExposure_Notify service operation, as described in clause 4.2.4.2.

When the "notifFlag" attribute is included, and set to "DEACTIVATE" in the request, the PCF shall mute the event notification and store the available events until the NF service consumer requests to retrieve them by setting the "notifFlag" attribute to "RETRIEVAL" or until a muting exception occurs (e.g. full buffer); if the "notifFlag" attribute is set to "RETRIEVAL" in the request, the PCF shall send the stored events to the NF service consumer, mute the event notification again and store available events; if the "notifFlag" attribute is set to "ACTIVATE" and the event notifications are muted (due to a previously received "DECATIVATE" value), the PCF shall unmute the event notification, i.e. start sending again notifications for available events.

When the feature "AppDetection" is supported, and the "APPLICATION_START" and/or "APPLICATION_STOP" policy event(s) are included in the request, the PCF shall trigger the provisioning of the PCC rule(s) for application detection and control for the application identifiers indicated within the "appIds" attribute, (if not previously provisioned) and/or the removal application detection and control for the PCC rule(s) (if application detection and

control is not required for other use cases) for the removed application identifier(s) as specified in 3GPP TS 29.512 [9], clause 4.2.6.2.11, and for every PDU session of the DNN and S-NSSAI included in the "snssaiDnns" attribute. If the APPLICATION_START" and/or "APPLICATION_STOP" policy event(s) are removed from the subscription, the PCF shall trigger the removal/update of application detection and control for the PCC rule(s) (if application detection and control is not required for other use cases) for the previously subscribed application identifier(s) as specified in 3GPP TS 29.512 [9], clause 4.2.6.2.11, and for every PDU session of the previously subscribed DNN and S-NSSAI.

When the feature "RateLimitReport" is supported, and the "RATE_LIMIT_INFO_REPO" event is included in the request, the PCF shall determine the Authorized Session AMBR as the rate limitation for the PDU session and report to the NF service consumer in the "rateLimitRepo" attribute in the response.

4.2.3 Npcf_EventExposure_UnSubscribe service operation

4.2.3.1 General

This service operation is used by an NF service consumer to unsubscribe from event notifications.

The following procedure using the Npcf_EventExposure_UnSubscribe service operation is supported:

- unsubscription from event notifications.

4.2.3.2 Unsubscription from event notifications

Figure 4.2.3.2-1 illustrates the unsubscription from event notifications.

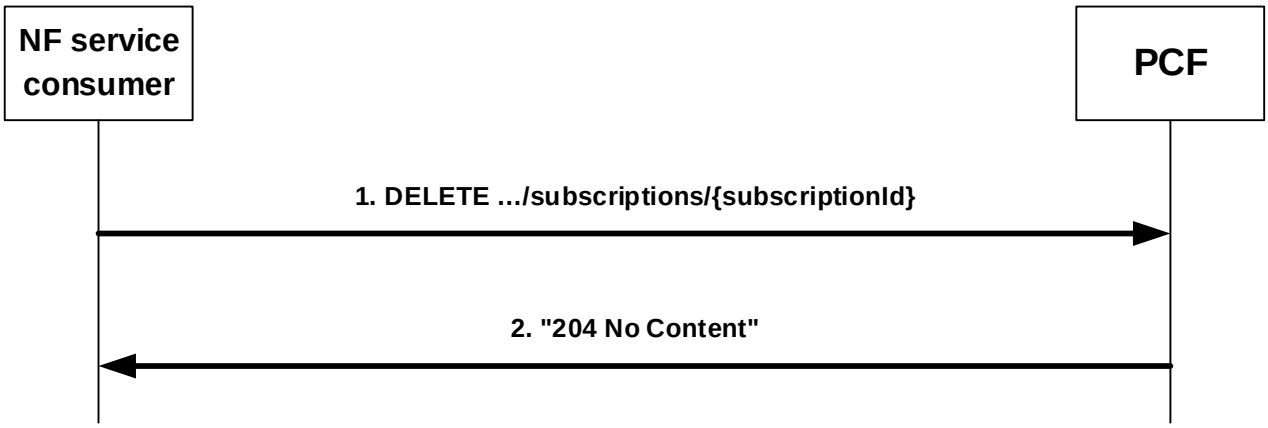

Figure 4.2.3.2-1: Unsubscription from event notifications

To unsubscribe from event notifications, the NF service consumer shall send an HTTP DELETE request with: "{apiRoot}/npcf-eventexposure/v1/subscriptions/{subscriptionId}" as request URI, as shown in figure 4.2.3.2-1, step 1, where "{subscriptionId}" is the subscription correlation identifier of the existing resource subscription that is to be deleted.

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

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

Upon successful reception of the HTTP DELETE request with: "{apiRoot}/npcf-eventexposure/v1/subscriptions/{subscriptionId}" as request URI, the PCF shall remove the corresponding subscription and send an HTTP "204 No Content" response as shown in figure 4.2.3.2-1, step 2.

4.2.4 Npcf_EventExposure_Notify service operation

4.2.4.1 General

The Npcf_EventExposure_Notify service operation enables the PCF to notify the NF service consumers that the previously (explicitly or implicitly) subscribed policy control event occurred.

The following procedure using the Npcf_EventExposure_Notify service operation is supported:

- notification about subscribed events.

4.2.4.2 Notification about subscribed events

Figure 4.2.4.2-1 illustrates the notification about subscribed events.

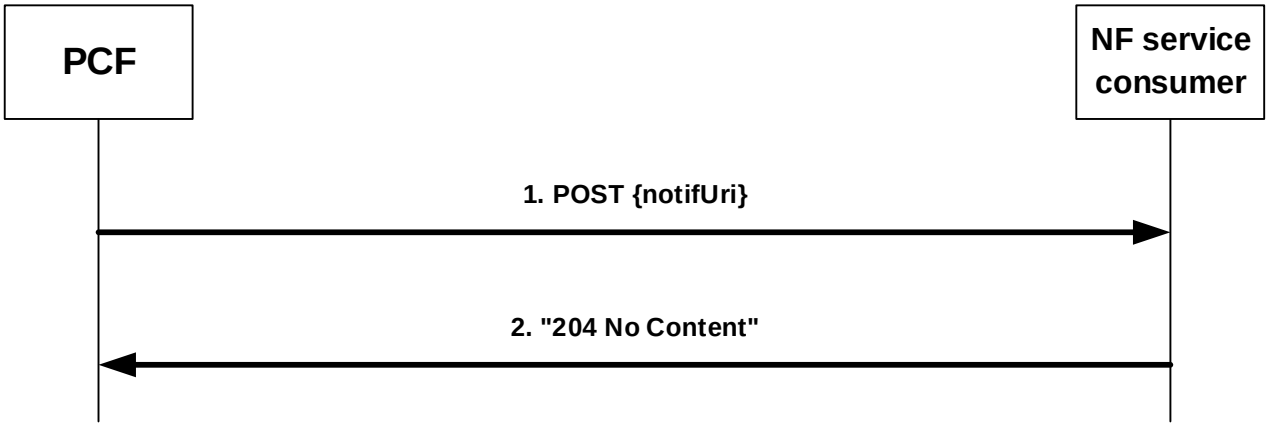

Figure 4.2.4.2-1: Notification about subscribed events

If the PCF observes policy control related event(s) for which an NF service consumer has subscribed explicitly as defined in clause 4.2.2 or implicitly when the subscription information is obtained from the UDR for application data, the PCF shall send an HTTP POST request as shown in figure 4.2.4.2-1, step 1, with the "{notifUri}" as request URI containing the value previously provided by the NF service consumer within the corresponding subscription or containing the callback URI provided by the AF to the UDR, and the "PcEventExposureNotif" data structure.

The "PcEventExposureNotif" data structure shall include:

- The notification correlation ID provided by the NF service consumer during the subscription as "notifId" attribute or obtained from the UDR as specified in 3GPP TS 29.519 [24]; and
- information about the observed event(s) within the "eventNotifs" attribute that shall contain for each observed event an "PcEventNotification" data structure that shall include:
  1. the Policy Control event as "event" attribute;
  2. for an access type change:
     a) new access type as "accType" attribute;
     b) the new RAT type as "ratType" attribute, if applicable for the notified access type;
     c) if the "ATSSS" feature is supported:
        i. if it is the first access type report for a PDU session, and both, 3GPP and non-3GPP access information is available, the "addAccessInfo" attribute. The "addAccessInfo" attribute contains the additional access type information, where the access type is encoded in the "accessType" attribute, and the RAT type is encoded in the "ratType" attribute when applicable for the notified access type;
        ii. if it is a subsequent access type change report:

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

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

NOTE 1: For a MA PDU session, if the "ATSSS" feature is not supported by the AF, the PCF includes the "accessType" attribute and the "ratType" attribute with a currently active combination of access type and RAT type (if applicable for the notified access type). When both 3GPP and non-3GPP accesses are available, the PCF includes the information corresponding to the 3GPP access.

and

d) for EPC interworking scenarios, the ePDG address as "anGwAddr" attribute, if applicable for the notified access type;

3. for a PLMN change:

a) new network identity containing the PLMN Identifier or the SNPN Identifier in the "plmnId" attribute;

NOTE 2: The SNPN Identifier consists of the PLMN Identifier and the NID.

NOTE 3: Mobility between non-equivalent SNPNs, and between SNPN and PLMN is not supported. When the UE is operating in SNPN access mode, the trigger reports changes of equivalent SNPNs.

4. when the feature "AMPoliciesEvents" is supported, for a service area coverage change, the new service area coverage in the "appliedCov" attribute, encoded as specified in 3GPP TS 29.534 [23], clause 4.2.7.4;

NOTE 4: The service area coverage change event is met and the notification is triggered when the PCF determines the tracking areas where the service is allowed in relation to the NF consumer requested service area coverage. The actual service area coverage for the UE might be larger than the one reported with the service area coverage change event.

5. for a satellite backhaul category change:

a) when the "SatelliteBackhaul" feature is supported:

i) the satellite backhaul category (i.e., "GEO", "MEO", "LEO", or "OTHER_SAT") or the indication of non-satellite backhaul category (i.e., "NON_SATELLITE") in the "satBackhaulCategory" attribute;

or

b) when dynamic satellite backhaul is used by the NG-RAN and the feature "EnSatBackhaulCatChg" is supported:

i) the dynamic satellite backhaul category (i.e., "DYNAMIC_GEO", "DYNAMIC_MEO", "DYNAMIC_LEO", or "DYNAMIC_OTHER_SAT") in the "satBackhaulCategory" attribute;

6. when the feature "DeliveryOutcome" is supported, to report the unsuccessful outcome of the UE Policy Delivery related to the invocation of AF provisioned service parameters, the reason of failure within the "delivFailure" attribute. If the feature "ExtDeliveryOutcome" is also supported, when the PCF, based on the received "uePolDelResult" attribute from the AMF indicating the UE Policy Delivery result as defined in 3GPP TS 29.525 [11], may determine and include the unsuccessfully executed UE policy detailed information related to the invocation of AF provisioned service parameters within the "uePolEventInfos" attribute;

7. the identity of the affected UE in the "supi" attribute and, if available, in the "gpsi" attribute;

8. the time at which the event was observed encoded as "timeStamp" attribute;

9. if available, and if the feature "ExtendedSessionInformation" is supported, information about the PDU session involved in the reported event in the "pduSessionInfo" attribute, that shall include:

a) the S-NSSAI of the PDU session in the "snssai" attribute;

b) the DNN of the PDU session in the "dnn" attribute;

c) the IPv4 address in the "ueIpv4" attribute and/or the IPv6 prefix in the "ueIpv6" attribute, or the Ethernet MAC address in the "ueMac" attribute; and

d) if the IPv4 address is included in the "ueIpv4" attribute, may include the IP domain in the "ipDomain" attribute;

10. if available, and if the feature "ExtendedSessionInformation" is supported, information about the services involved in the reported event in the indicated PDU session in the "repServices" attribute, which may include per identified service:

a) a list of Ethernet flows in the "servEthFlows" attribute which contains an impacted Ethernet flow number within the "flowNumber" attribute in each EthernetFlowInfo data structure; or

b) a list of IP flows in the "servIpFlows" attribute which contains an impacted IP flow number within the "flowNumber" attribute in each IpFlowInfo data structure; and/or

c) an AF application identifier in the "afAppId" attribute;

11. for an application detection event and if the feature "AppDetection" is supported:

a) optionally, information about the PDU session involved in the reported event in the "pduSessionInfo" attribute; and

NOTE 5: In the case of subscriptions targeting any UE, the served UE IP address (an Ipv4Addr or Ipv6Prefix or both if available) can be necessary to be provided in the "pduSessionInfo" attribute for the AF to function properly.

b) the application identifier for which the notification applies in the "appId" attribute;

12. for an rate limitation information event and if the feature "RateLimitReport" is supported, the authorized session AMBR information for the PDU session in the "rateLimitRepo" attribute.

13. for a signalling information event, if the feature "SignallingInfo" is supported:

a) the signalling information within the "sigInfos" attribute;

14. when the feature "PCFSerParAuth" is supported, to report the unsuccessful PCF authorization related to the invocation of AF provisioned service parameters, the reason of failure within the "delivFailure" attribute. In addition, if the feature "ExtDeliveryOutcome" is also supported, the PCF may include the not successfully authorized UE policy detailed information related to the invocation of AF provisioned service parameters within the "uePolEventInfos" attribute; and

15. when the "AfNetSliceRepl" feature is supported, to report the AF requested Network Slice Replacement outcome, the notification of the outcome of either the AF requested Network Slice Replacement initiation or the AF requested Network Slice Replacement termination within the "afSliceReplOut" attribute.

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

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

Upon successful reception of the HTTP POST request with "{notifUri}" as request URI and a "PcEventExposureNotif" data structure as request body, the NF service consumer shall send a "204 No Content" HTTP response, as shown in figure 4.2.4.2-1, step 2, for a successful processing.

5 Npcf_EventExposure Service API

5.1 Introduction

The Npcf_EventExposure Service shall use the Npcf_EventExposure API.

The API URI of the Npcf_EventExposure API shall be:

{apiRoot}/<apiName>/<apiVersion>

The request URIs used in HTTP requests from the NF service consumer towards the PCF shall have the Resource URI structure defined in clause 4.4.1 of 3GPP TS 29.501 [6], i.e.:

{apiRoot}/<apiName>/<apiVersion>/<apiSpecificResourceUriPart>

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [6].
- The <apiName> shall be "npcf-eventexposure".
- The <apiVersion> shall be "v1".
- The <apiSpecificResourceUriPart> shall be set as described in clause 5.3.

5.2 Usage of HTTP

5.2.1 General

HTTP/2, IETF RFC 9113 [16], shall be used as specified in clause 5.2 of 3GPP TS 29.500 [5].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [5].

The OpenAPI [7] specification of HTTP messages and content bodies for the Npcf_EventExposure is contained in Annex A.

5.2.2 HTTP standard headers

5.2.2.1 General

See clause 5.2.2 of 3GPP TS 29.500 [5] for the usage of HTTP standard headers.

5.2.2.2 Content type

JSON, IETF RFC 8259 [17], shall be used as content type of the HTTP bodies specified in the present specification as specified in clause 5.4 of 3GPP TS 29.500 [5]. The use of the JSON format shall be signalled by the content type "application/json".

"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 9457 [18].

5.2.3 HTTP custom headers

5.2.3.1 General

The mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [5] shall be supported, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [5] may be supported.

In this Release of the specification, no specific custom headers are defined for the Npcf_EventExposure API.

5.3 Resources

5.3.1 Resource Structure

This clause describes the structure for the Resource URIs and the resources and methods used for the service.

Figure 5.3.1-1 depicts the resource URIs structure for the Npcf_EventExposure API.

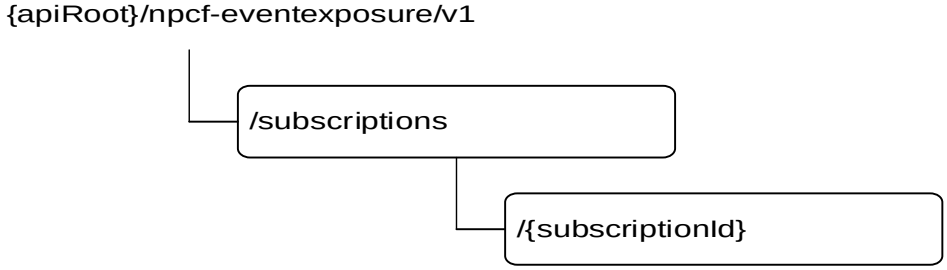

Figure 5.3.1-1: Resource URI structure of the Npcf_EventExposure API

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
Policy Control Events Subscriptions	/subscriptions	POST	Subscription to the notification of policy control events and creation of an Individual Policy Control Events Subscription resource.
Individual Policy Control Events Subscription	/subscriptions/{subscriptionId}	GET	Reads an Individual Policy Control Events Subscription resource.
		PUT	Modifies an Individual Policy Control Events Subscription.
		DELETE	Cancels an individual subscription to notifications of policy control events.

5.3.2 Resource: Policy Control Events Subscriptions (Collection)

5.3.2.1 Description

The Policy Control Events Subscriptions resource represents all subscriptions of the Npcf_EventExposure service at a given PCF.

5.3.2.2 Resource definition

Resource URI: **{apiRoot}/npcf-eventexposure/v1/subscriptions**

This resource shall support the resource URI variables defined in table 5.3.2.2-1.

Table 5.3.2.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 5.1

5.3.2.3 Resource Standard Methods

5.3.2.3.1 POST

This method shall support the URI query parameters specified in table 5.3.2.3.1-1.

Table 5.3.2.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 5.3.2.3.1-2 and the response data structures and response codes specified in table 5.3.2.3.1-3.

Table 5.3.2.3.1-2: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
PcEventExposure Subsc	M	1	Contains the information required for the creation of a new individual policy control events subscription.

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
PcEventExposure Subsc	M	1	201 Created	Contains the representation of the Individual Policy Control Events Subscription resource.
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply.				

Table 5.3.2.3.1-4: Headers supported by the 201 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains the URI of the newly created resource, according to the structure: {apiRoot}/npcf-eventexposure/v1/subscriptions/{subscriptionId}

5.3.2.4 Resource Custom Operations

None.

5.3.3 Resource: Individual Policy Control Events Subscription (Document)

5.3.3.1 Description

The Individual Policy Control Events Subscription resource represents a single subscription of the Npcf_EventExposure service at a given PCF.

5.3.3.2 Resource definition

Resource URI: **{apiRoot}/npcf-eventexposure/v1/subscriptions/{subscriptionId}**

This resource shall support the resource URI variables defined in table 5.3.3.2-1.

Table 5.3.3.2-1: Resource URI variables for this resource

Name	Data type	Definition
apiRoot	string	See clause 5.1
subscriptionId	string	Identifies a subscription to the PCF event exposure service.

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
PcEventExposureSubsc	M	1	200 OK	A representation of the Individual Policy Control Events Subscription is returned.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during subscription retrieval. Applicable if the feature "ES3XX" is supported. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during subscription retrieval. Applicable if the feature "ES3XX" is supported. (NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the GET method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply. NOTE 2: The RedirectResponse data structure may be provided by an SCP (see clause 6.10.9.1 of 3GPP TS 29.500 [5]).				

Table 5.3.3.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative PCF (service) instance towards which the request is redirected. For the case where the request is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target PCF (service) instance towards which the request is redirected.

Table 5.3.3.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative PCF (service) instance towards which the request is redirected. For the case where the request is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target PCF (service) instance towards which the request is redirected.

5.3.3.3.2 PUT

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 PUT method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 5.3.3.3.2-2 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 PUT Request Body on this resource

Data type	P	Cardinality	Description
PcEventExposureSubsc	M	1	Modifies the existing Individual Policy Control Events Subscription resource.

Table 5.3.3.3.2-3: Data structures supported by the PUT Response Body on this resource

Data type	P	Cardinality	Response codes	Description
PcEventExposureSubsc	M	1	200 OK	Successful case: The Individual Policy Control Events Subscription was modified and a representation is returned.
n/a			204 No Content	Successful case: The Individual Policy Control Events Subscription was modified.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during subscription modification. Applicable if the feature "ES3XX" is supported. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during subscription modification. Applicable if the feature "ES3XX" is supported. (NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the PUT method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply. NOTE 2: The RedirectResponse data structure may be provided by an SCP (see clause 6.10.9.1 of 3GPP TS 29.500 [5]).				

Table 5.3.3.3.2-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative PCF (service) instance towards which the request is redirected. For the case where the request is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target PCF (service) instance towards which the request is redirected

Table 5.3.3.3.2-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative PCF (service) instance towards which the request is redirected. For the case where the request is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target PCF (service) instance towards which the request is redirected

5.3.3.3.3 DELETE

This method shall support the URI query parameters specified in table 5.3.3.3.3-1.

Table 5.3.3.3.3-1: 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 5.3.3.3.3-2 and the response data structures and response codes specified in table 5.3.3.3.3-3.

Table 5.3.3.3.3-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

Table 5.3.3.3.3-3: 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 Individual Policy Control Events Subscription resource matching the subscriptionId was deleted.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during subscription termination. Applicable if the feature "ES3XX" is supported. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during subscription termination. Applicable if the feature "ES3XX" is supported. (NOTE 2)
NOTE 1: The mandatory HTTP error status code for the DELETE method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [5] also apply. NOTE 2: The RedirectResponse data structure may be provided by an SCP (see clause 6.10.9.1 of 3GPP TS 29.500 [5]).				

Table 5.3.3.3.3-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative PCF (service) instance towards which the request is redirected. For the case where the request is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target PCF (service) instance towards which the request is redirected.

Table 5.3.3.3.3-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	Contains an alternative URI of the resource located in an alternative PCF (service) instance towards which the request is redirected. For the case where the request is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target PCF (service) instance towards which the request is redirected.

5.3.3.4 Resource Custom Operations

None.

5.4 Custom Operations without associated resources

None.

5.5 Notifications

5.5.1 General

Notifications shall comply with clause 6.2 of 3GPP TS 29.500 [5] and clause 4.6.2.3 of 3GPP TS 29.501 [6].

Table 5.5.1-1: Notifications overview

Notification	Callback URI	HTTP method or custom operation	Description (service operation)
Policy Control Event Notification	{notifUri}	POST	Notification of policy control event reporting.

5.5.2 Policy Control Event Notification

5.5.2.1 Description

The Policy Control Event Notification is used by the PCF to report one or several observed policy control events to the NF service consumer that has subscribed to such notifications.

NOTE 1: The "callback" clause of the OpenAPI specification found in Annex A.2 associated to the POST method of the "Policy Control Events Subscriptions" resource is used as the notification request for both explicit and implicit subscriptions.

NOTE 2: For implicit subscriptions, the NEF can have previously stored in the UDR the notification URI to be used in the notifications initiated by the PCF. See 3GPP TS 29.519 [24] for the details.

5.5.2.2 Target URI

The Callback URI **"{notifUri}"** shall be used with the callback URI variables defined in table 5.5.2.2-1.

Table 5.5.2.2-1: Callback URI variables

Name	Data type	Definition
notifUri	Uri	The Notification Uri as assigned by the NF service consumer either during the explicit subscription service operation and described within the PcEventExposureSubsc data type (see table 5.6.2.2-1) or during the implicit subscription via the provisioning of the corresponding application data in UDR (see 3GPP TS 29.519 [24]. (NOTE).
NOTE: When obtained from the UDR, it corresponds to the notification URI previously stored by the NEF.		

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
PcEventExposureNotif	M	1	Provides Information about observed policy control events

Table 5.5.2.3.1-3: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The receipt of the Notification is acknowledged.
RedirectResponse	O	0..1	307 Temporary Redirect	Temporary redirection, during event notification. Applicable if the feature "ES3XX" is supported. (NOTE 2)
RedirectResponse	O	0..1	308 Permanent Redirect	Permanent redirection, during event notification. Applicable if the feature "ES3XX" is supported. (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: The RedirectResponse data structure may be provided by an SCP (see clause 6.10.9.1 of 3GPP TS 29.500 [5]).				

Table 5.5.2.3.1-4: Headers supported by the 307 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification is redirected. For the case where the notification is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the notification request is redirected.

Table 5.5.2.3.1-5: Headers supported by the 308 Response Code on this resource

Name	Data type	P	Cardinality	Description
Location	string	M	1	An alternative URI representing the end point of an alternative NF consumer (service) instance towards which the notification is redirected. For the case where the notification is redirected to the same target via a different SCP, refer to clause 6.10.9.1 of 3GPP TS 29.500 [5].
3gpp-Sbi-Target-Nf-Id	string	O	0..1	Identifier of the target NF (service) instance ID towards which the notification request is redirected.

5.6 Data Model

5.6.1 General

This clause specifies the application data model supported by the API.

Table 5.6.1-1 specifies the data types defined for the Npcf_EventExposure service based interface protocol.

Table 5.6.1-1: Npcf_EventExposure specific Data Types

Data type	Section defined	Description	Applicability
EthernetFlowInfo	5.6.2.6	Identification of an UL/DL ethernet flow.	ExtendedSession Information
IpFlowInfo	5.6.2.7	Identification of an UL/DL IP flow.	ExtendedSession Information
PcEvent	5.6.3.3	Policy Control Events.	
PcEventExposureNotif	5.6.2.3	Describes notifications about Policy Control events that occurred in an Individual Policy Events Subscription resource.	
PcEventExposureSubsc	5.6.2.2	Represents an Individual Policy Events Subscription resource.	
PcEventNotification	5.6.2.8	Represents the information reported for a Policy Control event.	
PduSessionInformation	5.6.2.9	Represents PDU session identification information.	ExtendedSession Information AppDetection
ReportingInformation	5.6.2.4	Represents the type of reporting the subscription requires.	
ServiceIdentification	5.6.2.5	Identification of the service to which the subscription applies.	ExtendedSession Information
SnssaiDnnCombination	5.6.2.10	Represents a combination of S-NSSAI and DNN(s).	EneNA AppDetection

Table 5.6.1-2 specifies data types re-used by the Npcf_EventExposure 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_EventExposure service based interface.

Table 5.6.1-2: Npcf_EventExposure re-used Data Types

Data type	Reference	Comments	Applicability
AccessType	3GPP TS 29.571 [14]	Access Type.	
AdditionalAccessInfo	3GPP TS 29.512 [9]	Indicates the combination of additional Access Type and RAT Type for MA PDU session.	ATSSS
AfAppId	3GPP TS 29.514 [12]	AF application Identifier.	ExtendedSession Information
Ambr	3GPP TS 29.571 [14]	Contains AMBR.	RateLimitReport
AnGwAddress	3GPP TS 29.514 [12]	Carries the control plane address of the EPC untrusted non-3GPP access network gateway. (NOTE 1)	
ApplicationId	3GPP TS 29.571 [14]	Application Identifier.	AppDetection
DateTime	3GPP TS 29.571 [14]	Time stamp.	
Dnn	3GPP TS 29.571 [14]	Identifies a DNN.	
DurationSec	3GPP TS 29.571 [14]	Seconds of duration.	
EthFlowDescription	3GPP TS 29.514 [12]	Identifies an ethernet flow description. (NOTE 2)	ExtendedSession Information
Failure	3GPP TS 29.522 [25]	Indicates the failure reason for an unsuccessful outcome of the UE Policy Delivery or service parameter authorization.	DeliveryOutcome PCFSerParAuth
FlowDescription	3GPP TS 29.514 [12]	Identifies an IP flow description.	ExtendedSession Information
Gpsi	3GPP TS 29.571 [14]	Generic Public Subscription Identifier.	
GroupId	3GPP TS 29.571 [14]	Identifies a group of UEs.	
Ipv4Addr	3GPP TS 29.571 [14]	Represents an Ipv4 address.	ExtendedSession Information AppDetection
Ipv6Prefix	3GPP TS 29.571 [14]	Represents an Ipv6 prefix.	ExtendedSession Information AppDetection
MacAddr48	3GPP TS 29.571 [14]	Mac Address of the UE.	ExtendedSession Information
MutingExceptionInstructions	3GPP TS 29.571 [14]	Contains instructions to be executed upon the occurrence of an event muting exception (e.g. full buffer).	
MutingNotificationsSettings	3GPP TS 29.571 [14]	Contains setting related to the muting of notifications.	
NfSignallingInfo	3GPP TS 29.571 [14]	Contains NF signalling information.	SignallingInfo
NotificationFlag	3GPP TS 29.571 [14]	Notification flag.	EneNA
NotificationMethod	3GPP TS 29.508 [15]	Represents the Notification Method.	
PartitioningCriteria	3GPP TS 29.571 [14]	Used to partition UEs before applying sampling.	EneNA
PlmnIdNid	3GPP TS 29.571 [14]	Identifies the network: the PLMN Identifier or the SNPN Identifier. (NOTE 3)	
RatType	3GPP TS 29.571 [14]	RAT Type.	
RedirectResponse	3GPP TS 29.571 [14]	Contains redirection related information.	ES3XX
SamplingRatio	3GPP TS 29.571 [14]	Sampling Ratio.	
SatelliteBackhaulCategory	3GPP TS 29.571 [14]	Indicates the satellite or non-satellite backhaul category.	SatelliteBackhaul
ServiceAreaCoverageInfo	3GPP TS 29.534 [23]	Service area coverage in terms of tracking area codes and serving network.	AMPoliciesEvents
SliceReplOutcomeInfo	3GPP TS 29.534 [23]	Represents the AF requested Network Slice Replacement outcome related information.	AfNetSliceRepl
Snssai	3GPP TS 29.571 [14]	Identifies a S-NSSAI.	
Supi	3GPP TS 29.571 [14]	Identifies the SUPI of the UE.	
SupportedFeatures	3GPP TS 29.571 [14]	Used to negotiate the applicability of the optional features defined in clause 5.8.	
TimeWindow	3GPP TS 29.122 [26]	Represents a Time Window.	SignallingInfo
UePolEventInfo	3GPP TS 29.522 [25]	Event information about the outcome of Service Parameter provisioning requests for the UE policy delivery.	ExtDeliveryOutcome
Uinteger	3GPP TS 29.571 [14]	Represents an unsigned integer.	
Uri	3GPP TS 29.571 [14]	Represents a URI.	

NOTE 1: "AnGwAddress" data structure is only used to encode the ePDG address and is only applicable to the 5GS and EPC/E-UTRAN interworking scenario as defined in 3GPP TS 29.512 [9], Annex B.
NOTE 2: In order to support a set of MAC addresses with a specific range in the traffic filter, feature MacAddressRange as specified in clause 5.8 shall be supported.
NOTE 3: The SNPN Identifier consists of the PLMN Identifier and the NID.

5.6.2 Structured data types

5.6.2.1 Introduction

This clause defines the structures to be used in resource representations.

5.6.2.2 Type PcEventExposureSubsc

Table 5.6.2.2-1: Definition of type PcEventExposureSubsc

Attribute name	Data type	P	Cardinality	Description	Applicability
eventSubs	array(PcEvent)	M	1..N	Subscribed Policy Control events.	
eventsRepInfo	ReportingInformation	O	0..1	Represents the reporting requirements of the subscription.	
groupId	GroupId	C	0..1	Represents an internal group identifier and identifies a group of UEs. It shall be present when the subscription is targeting a Group of UE(s).	
filterDnns	array(Dnn)	O	1..N	Represents the DNNs for which the policy event report shall apply. Each DNN is a full DNN with both the Network Identifier and Operator Identifier, or a DNN with the Network Identifier only. If omitted it represents any DNN.	
filterSnssais	array(Snssai)	O	1..N	Represents the S-NSSAIs for which the policy event report shall apply. If omitted it represents any S-NSSAI.	
snssaiDnns	array(SnssaiDnnCombination)	C	1..N	Represents the combination list of S-NSSAI and DNN for which the policy event report shall apply. If omitted, it represents any combination. When the feature "AppDetection" is supported, one combination of S-NSSAI and DNN shall be provided for event "APPLICATION_START" or "APPLICATION_STOP".	EneNA, AppDetection
filterServices	array(ServiceIdentification)	O	1..N	Represents the services for which the policy event report shall apply. If omitted, the policy event report shall apply for all the active services.	ExtendedSessionInformation
appIds	array(ApplicationId)	C	1..N	Represents the applications for which the policy event report shall apply. It shall be provided for event "APPLICATION_START" or "APPLICATION_STOP".	AppDetection
tws	array(TimeWindow)	O	1..N	Contains the time windows for which the NF service consumer is requesting to receive signalling information. It may only be provided if the SIGNALLING_INFO event is subscribed. If omitted, the PCF determines the time windows for which the signalling information is reported based on local configuration.	SignallingInfo
notifUri	Uri	M	1	Notification URI for Policy Control event reporting.	
notifId	string	M	1	Notification Correlation ID assigned by the NF service consumer.	
eventNotifs	array(PcEventNotification)	C	1..N	Represents the Policy Control Events to be reported in the Npcf_EvenExposure_Subscribe response. It shall be present in the resource creation/update response when the "eventsRepInfo" attribute includes the "immRep" attribute set to true. Otherwise, it shall be omitted.	ERIR

suppFeat	SupportedFeatures	C	0..1	Contains the list of supported features among the ones defined in clause 5.8. Shall be present only when feature negotiation needs to take place. (NOTE)	
NOTE: In the HTTP request, it represents the set of features supported by the NF service consumer. In the HTTP response, it represents the set of features supported by both the NF service consumer and the PCF.					

5.6.2.3 Type PcEventExposureNotif

Table 5.6.2.3-1: Definition of type PcEventExposureNotif

Attribute name	Data type	P	Cardinality	Description	Applicability
notifId	string	M	1	Notification Correlation ID assigned by the NF service consumer.	
eventNotifs	array(PcEventNotification)	M	1..N	Represents the Policy Control Events to be reported according to the subscription corresponding to the Notification Correlation ID.	

5.6.2.4 Type ReportingInformation

Table 5.6.2.4-1: Definition of type ReportingInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
immRep	boolean	O	0..1	Indication of immediate reporting. If included, when it is set to true it indicates immediate reporting of the subscribed events, if available. Otherwise, reporting will occur when the event is met.	
notifMethod	NotificationMethod	O	0..1	Represents the notification method (periodic, one time, on event detection). If "notifMethod" attribute is not supplied, the default value "ON_EVENT_DETECTION" applies.	
maxReportNbr	Uinteger	O	0..1	Represents the maximum number of reports, after which the subscription ceases to exist (i.e., the reporting ends). It may be present for the "PERIODIC" and on "ON_EVENT_DETECTION" notification methods. If omitted, there is no limit.	
monDur	DateTime	C	0..1	Represents the time at which the subscription ceases to exist (i.e. the subscription becomes invalid and the reporting ends). If omitted, there is no time limit. If present in the subscription request, it shall be present in the subscription response.	
repPeriod	DurationSec	O	0..1	Indicates the time interval between successive event notifications. It is supplied for notification method "PERIODIC".	
sampRatio	SamplingRatio	O	0..1	Indicates the ratio of the random subset to target UEs, event reports only relates to the subset.	
partitionCriteria	array(PartitioningCriteria)	O	1..N	Defines criteria for partitioning the UEs in order to apply the sampling ratio for each partition. It may only be included in event subscription requests when the "sampRatio" attribute is also provided. (NOTE 1)	EneNA
grpRepTime	DurationSec	O	0..1	Indicates the time during which the event reports detected for the concerned UEs are aggregated in a group, in order to be reported together to the NF service consumer.	
notifFlag	NotificationFlag	O	0..1	Indicates the notification flag, which is used to mute/unmute notifications and to retrieve events stored during a period of muted notifications. Default: "ACTIVATE".	EneNA
notifFlagInstruct	MutingExceptionInstructions	O	0..1	Contains instructions to be executed upon the occurrence of an event muting exception (e.g. full buffer). It may only be provided if the "notifFlag" is provided and set to "DEACTIVATE".(NOTE 2)	

mutingSetting	MutingNotificationsSettings	O	0..1	Contains settings related to the muting of notifications. It may only be provided in the NF service producer response and only if the muting instructions provided in the "notifFlag" and/or the "notifFlagInstruct" attributes are accepted.(NOTE 2)	
NOTE 1: For a given type of partitioning criteria, the UE shall belong to only one single partition as long as it is served by the NF service producer. NOTE 2: This attribute is not used in this API and is applicable only in APIs that re-use this data type for the purpose of data collection for analytics.					

5.6.2.5 Type ServiceIdentification

Table 5.6.2.5-1: Definition of type ServiceIdentification

Attribute name	Data type	P	Cardinality	Description	Applicability
servEthFlows	array(EthernetFlowInfo)	C	1..N	Ethernet flows of a service.	
servIpFlows	array(IpFlowInfo)	C	1..N	IP flows of a service.	
afAppId	AfAppId	O	0..1	Contains an AF application identifier.	
NOTE: At least one of the "servEthFlows", "servIpFlows" or "afAppId" attributes shall be present. The "servEthFlows" attribute and the "servIpFlows" attribute shall not be both present at the same time.					

5.6.2.6 Type EthernetFlowInfo

Table 5.6.2.6-1: Definition of type EthernetFlowInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
ethFlows	array(EthFlowDescription)	C	1..2	Contains the flow description for the Uplink and/or Downlink Ethernet flows. It shall be present in the subscription request.	
flowNumber	integer	M	1	Identifies the ordinal number of the Ethernet flow.	

5.6.2.7 Type IpFlowInfo

Table 5.6.2.7-1: Definition of type IpFlowInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
ipFlows	array(FlowDescription)	C	1..2	Contains the flow description for the Uplink and/or Downlink IP flows. It shall be present in the subscription request.	
flowNumber	integer	M	1	Identifies the ordinal number of the IP flow.	

5.6.2.8 Type PcEventNotification

Table 5.6.2.8-1: Definition of type PcEventNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
event	PcEvent	M	1	Reported Policy Control event.	
accType	AccessType	C	0..1	Access Type. It shall be included when the reported PcEvent is "AC_TY_CH".	
addAccessInfo	AdditionalAccessInfo	O	0..1	Indicates the additional combination of Access Type and RAT Type available for MA PDU session. It may be present when the notified event is "AC_TY_CH" and the PDU session is a Multi-Access PDU session.	ATSSS
relAccessInfo	AdditionalAccessInfo	O	0..1	Indicates the release of a combination of Access Type and RAT Type available for MA PDU session. It may be present when the notified event is "AC_TY_CH" and the PDU session is a Multi-Access PDU session.	ATSSS
anGwAddr	AnGwAddress	O	0..1	ePDG address. It shall be included if applicable when the reported PcEvent is "AC_TY_CH".	
ratType	RatType	O	0..1	RAT Type. It shall be included if applicable when the reported PcEvent is "AC_TY_CH".	
plmnId	PlmnIdNid	C	0..1	PLMN Identifier or the SNPN Identifier. It shall be included when the reported PcEvent is "PLMN_CH". (NOTE 1)	
appliedCov	ServiceAreaCoverageInfo	C	0..1	The list of applied allowed Tracking Areas for the serving network where the UE is camping. It shall be included when the reported PcEvent is "SAC_CH".	AMPoliciesEvents
supi	Supi	C	0..1	SUPI of the UE. It shall be present if available.	
gpsi	Gpsi	O	0..1	Gpsi shall contain either an External Id or an MSISDN.	
timeStamp	DateTime	M	1	Time at which the event is observed.	
pduSessionInfo	PduSessionInformation	O	0..1	Represents PDU session information related to the observed event.	ExtendedSessionInformation, AppDetection
appId	ApplicationId	O	0..1	Represents the detected application.	AppDetection
repServices	ServiceIdentification	O	0..1	Represents service information related to the observed event.	ExtendedSessionInformation
satBackhaulCategory	SatelliteBackhaulCategory	C	0..1	Indicates the satellite or non-satellite backhaul category of the PDU session. It shall be included when the reported PcEvent is "SAT_CATEGORY_CH". If the "EnSatBackhaulCatChg" feature is supported, the different dynamic satellite backhaul categories may also be provided.	SatelliteBackhaul

delivFailure	Failure	C	0..1	Indicates the failure reason for an unsuccessful outcome of the UE Policy Delivery or service parameter authorization in the PCF. It shall be included when the reported PcEvent is "UNSUCCESS_UE_POL_DEL_SP" or "UNSUCCESS_PCF_SERVICE_AUTHORIZATION". (NOTE 2).	DeliveryOutcome PCFSerParAuth
uePolEventInfos	array(UePolEventInfo)	O	1..N	Contains the UE policy event information. It may be included when the reported PcEvent is "PARTLY_UNSUCC_UE_POL_DEL_SP".	ExtDeliveryOutcome
rateLimitRepo	Ambr	C	0..1	Rate limitation information for a PDU session. It shall be included when the reported PcEvent is "RATE_LIMIT_INFO_REPO".	RateLimitReport
sigInfos	array(NfSignallingInfo)	C	1..N	Contains signalling information. It shall be included when the reported event is "SIGNALLING_INFO".	SignallingInfo
afSliceReplOut	SliceReplOutcomeInfo	C	0..1	Contains the notification of the outcome of either the AF requested Network Slice Replacement initiation or the AF requested Network Slice Replacement termination. This attribute shall be present only when the reported event within the "event" attribute is "SLICE_REPLACE_OUTCOME".	AfNetSliceRepl
NOTE 1: The SNPN Identifier consists of the PLMN Identifier and the NID. NOTE 2: The values "DNN_NOT_ALLOWED" and "SNSSAI_NOT_ALLOWED" are only applicable if the feature "PCFSerParAuth" is supported.					

5.6.2.9 Type PduSessionInformation

Table 5.6.2.9-1: Definition of type PduSessionInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
snssai	Snssai	M	1	S-NSSAI of the PDU session.	
dnn	Dnn	M	1	Dnn of the PDU session, a full DNN with both the Network Identifier and Operator Identifier, or a DNN with the Network Identifier only.	
ueIpv4	Ipv4Addr	C	0..1	The IPv4 address of the served UE. (NOTE 1)	
ueIpv6	Ipv6Prefix	C	0..1	The IPv6 prefix of the served UE. (NOTE 1)	
ipDomain	string	O	0..1	Identifies the IP domain. (NOTE 2)	
ueMac	MacAddr48	C	0..1	UE MAC address. (NOTE 1)	
NOTE 1: Either the served UE IP address (an Ipv4Addr or Ipv6Prefix or both if available) or UE MAC address shall be present. NOTE 2: An "ipDomain" attribute, may be provided in combination with a "ueIpv4" attribute.					

5.6.2.10 Type SnssaiDnnCombination

Table 5.6.2.10-1: Definition of type SnssaiDnnCombination

Attribute name	Data type	P	Cardinality	Description	Applicability
snssai	Snssai	M	1	S-NSSAI	
dnns	array(Dnn)	M	1..N	Dnn	

5.6.3 Simple data types and enumerations

5.6.3.1 Introduction

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

5.6.3.2 Simple data types

The simple data types defined in table 5.6.3.2-1 shall be supported.

Table 5.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability

5.6.3.3 Enumeration: PcEvent

The enumeration PcEvent represents the policy control events that can be subscribed. It shall comply with the provisions defined in table 5.6.3.3-1.

Table 5.6.3.3-1: Enumeration PcEvent

Enumeration value	Description	Applicability
AC_TY_CH	Access Type Change	
PLMN_CH	PLMN Change	
SAC_CH	Service Area Coverage change	AMPoliciesEvents
SAT_CATEGORY_CH	Indicates that a change between different satellite backhaul category, or non-satellite backhaul, has been detected.	SatelliteBackhaul
SUCCESS_UE_POL_DEL_SP	Indicates about the successful UE Policy delivery related to the invocation of AF provisioned service parameters.	DeliveryOutcome
UNSUCCESS_UE_POL_DEL_SP	Indicates about the unsuccessful UE Policy delivery related to the invocation of AF provisioned service parameters.	DeliveryOutcome
PARTLY_UNSUCC_UE_POL_DEL_SP	Partially unsuccessful UE Policy Delivery related to the invocation of AF provisioned Service Parameters.	ExtDeliveryOutcome
UNSUCCESS_PCF_SERVICE_AUTHORIZATION	Unsuccessful authorization in the PCF to the invocation of AF provisioned Service Parameters.	PCFSerParAuth
APPLICATION_START	The start of application traffic has been detected. (NOTE)	AppDetection
APPLICATION_STOP	The stop of application traffic has been detected. (NOTE)	AppDetection
RATE_LIMIT_INFO_REPO	Indicates reporting of the Rate Limitation Information for the PDU session.	RateLimitReport
SIGNALLING_INFO	Information related to signalling is being reported.	SignallingInfo
SLICE_REPLACE_OUTCOME	This event indicates the notification of the outcome of either the AF requested Network Slice Replacement initiation or the AF requested Network Slice Replacement termination.	AfNetSliceRepl
NOTE: The subscription to the "APPLICATION_START" and/or "APPLICATION_STOP" event(s) shall trigger the provisioning of the PCC rule(s) for application detection and control in the SMF as specified in clauses 4.2.2.2, 4.2.2.3 and 4.2.3.2.		

5.7 Error handling

5.7.1 General

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

For the Npcf_EventExposure API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [6].

Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [5] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in table 5.2.7.1-1 of 3GPP TS 29.500 [5].

In addition, the requirements in the following clauses are applicable for the Npcf_EventExposure API.

5.7.2 Protocol Errors

In this Release of the specification, there are no service specific protocol errors applicable for the Npcf_EventExposure API.

5.7.3 Application Errors

The application errors defined for the Npcf_EventExposure service are listed in table 5.7.3-1.

Table 5.7.3-1: Application errors

Application Error	HTTP status code	Description

5.8 Feature negotiation

The optional features in table 5.8-1 are defined for the Npcf_EventExposure API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [5].

Table 5.8-1: Supported Features

Feature number	Feature Name	Description
1	ExtendedSessionInformation	Indicates the support of additional session information in the subscription and report of policy control event.
2	MacAddressRange	Indicates the support of a set of MAC addresses with a specific range in the traffic filter.
3	ATSSS	Indicates the support of the report of the multiple access types of a MA PDU session.
4	ES3XX	Extended Support for 3xx redirections. This feature indicates the support of redirection for any service operation, according to Stateless NF procedures as specified in clauses 6.5.3.2 and 6.5.3.3 of 3GPP TS 29.500 [5] and according to HTTP redirection principles for indirect communication, as specified in clause 6.10.9 of 3GPP TS 29.500 [5].
5	AMPoliciesEvents	Indicates the support of the report of changes of service area coverage for a UE.
6	EneNA	This feature indicates support for the enhancements of network data analytics requirements.
7	SatelliteBackhaul	Indicates the support of the report of the satellite or non-satellite backhaul category of the PDU session.
8	DeliveryOutcome	Indicates the support of notifications about the outcome of the UE Policy delivery related to the invocation of AF provisioned service parameters.
9	ERIR	Indicates the support of immediate report within the subscription response.
10	EnSatBackhaulCatChg	This feature indicates the support of the report of the dynamic satellite backhaul category of the PDU session. This feature requires the support of SatelliteBackhaul feature.
11	AppDetection	Indicates the support of Application Traffic Detection Event Exposure.
12	RateLimitReport	This feature indicates the support of the report of the Authorized Session AMBR as the Rate Limitation Information for the PDU session.
13	SignallingInfo	This feature indicates the support of signalling information events.
14	PCFSerParAuth	Indicates the support of notifications about the unsuccessful authorization related to the invocation of AF provisioned service parameters.
15	AfNetSliceRepl	This feature indicates the support of the AF requested Network Slice Replacement services. The following functionalities are supported: - Support the reporting of the AF requested Network Slice Replacement outcome related event(s).
16	ExtDeliveryOutcome	Indicates the support of notifications about the unsuccessfully executed UE policy outcome together with the partially unsuccessful UE policy delivery event related to the invocation of AF provisioned service parameters. This feature requires the support of DeliveryOutcome feature and PCFSerParAuth feature.

5.9 Security

As indicated in 3GPP TS 33.501 [19] and 3GPP TS 29.500 [5], the access to the Npcf_EventExposure API, based on local configuration, may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [20]), using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [21]) plays the role of the authorization server.

If OAuth2 authorization is used, an NF Service Consumer, prior to consuming services offered by the Nnrf_NFManagement API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [21], clause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF where the NF Service Consumer invoked the discovery of the Npcf_EventExposure service.

The Npcf_EventExposure API defines a single scope "npcf-eventexposure" for the entire service, 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 [7] specification of HTTP messages and content bodies used by the Npcf_EventExposure API.

This Annex shall take precedence when being discrepant to other parts of the specification with respect to the encoding of information elements and methods within the API.

NOTE: The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

Informative copies of the OpenAPI specification file contained in this 3GPP Technical Specification are available on a Git-based repository that uses the GitLab software version control system (see clause 5B of the 3GPP TR 21.900 [22] and clause 5.3.1 of the 3GPP TS 29.501 [6] for further information).

A.2 Npcf_EventExposure API

```
openapi: 3.0.0
info:
  version: 1.4.2
  title: Npcf_EventExposure
  description: |
    PCF Event Exposure Service.
    © 2026, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).
    All rights reserved.

externalDocs:
  description: 3GPP TS 29.523 V19.5.0; 5G System; Policy Control Event Exposure Service; Stage 3.
  url: https://www.3gpp.org/ftp/Specs/archive/29_series/29.523/

servers:
  - url: '{apiRoot}/npcf-eventexposure/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501

security:
  - {}
  - oAuth2ClientCredentials:
    - npcf-eventexposure

paths:
  /subscriptions:
    post:
      summary: Creates a new Individual Policy Control Events Subscription resource
      operationId: PostPcEventExposureSubsc
      tags:
        - Policy Control Events Subscription (Collection)
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/PcEventExposureSubsc'
      responses:
        '201':
          description: Success
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/PcEventExposureSubsc'
          headers:
```

```
          Location:
            description: >
              Contains the URI of the created individual policy control events subscription
              resource, according to the structure
              {apiRoot}/npcf-eventexposure/v1/subscriptions/{subscriptionId}
            required: true
            schema:
              type: string
      '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'
      '502':
        $ref: 'TS29571_CommonData.yaml#/components/responses/502'
      '503':
        $ref: 'TS29571_CommonData.yaml#/components/responses/503'
      default:
        $ref: 'TS29571_CommonData.yaml#/components/responses/default'
    callbacks:
      PcEventNotification:
        '{$request.body#/notifUri}':
          post:
            requestBody:
              required: true
              content:
                application/json:
                  schema:
                    $ref: '#/components/schemas/PcEventExposureNotif'
            responses:
              '204':
                description: No Content, Notification was succesfull.
              '307':
                $ref: 'TS29571_CommonData.yaml#/components/responses/307'
              '308':
                $ref: 'TS29571_CommonData.yaml#/components/responses/308'
              '400':
                $ref: 'TS29571_CommonData.yaml#/components/responses/400'
              '401':
                $ref: 'TS29571_CommonData.yaml#/components/responses/401'
              '403':
                $ref: 'TS29571_CommonData.yaml#/components/responses/403'
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '411':
                $ref: 'TS29571_CommonData.yaml#/components/responses/411'
              '413':
                $ref: 'TS29571_CommonData.yaml#/components/responses/413'
              '415':
                $ref: 'TS29571_CommonData.yaml#/components/responses/415'
              '429':
                $ref: 'TS29571_CommonData.yaml#/components/responses/429'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              '502':
                $ref: 'TS29571_CommonData.yaml#/components/responses/502'
              '503':
                $ref: 'TS29571_CommonData.yaml#/components/responses/503'
              default:
                $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  /subscriptions/{subscriptionId}:
    get:
      summary: "Reads an existing Individual Policy Control Events Subscription"
      operationId: GetPcEventExposureSubsc
      tags:
```

```
    - Individual Policy Control Events Subscription (Document)
  parameters:
    - name: subscriptionId
      in: path
      description: Policy Control Event Subscription ID.
      required: true
      schema:
        type: string
  responses:
    '200':
      description: OK. Resource representation is returned.
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/PcEventExposureSubsc'
    '307':
      $ref: 'TS29571_CommonData.yaml#/components/responses/307'
    '308':
      $ref: 'TS29571_CommonData.yaml#/components/responses/308'
    '400':
      $ref: 'TS29571_CommonData.yaml#/components/responses/400'
    '401':
      $ref: 'TS29571_CommonData.yaml#/components/responses/401'
    '403':
      $ref: 'TS29571_CommonData.yaml#/components/responses/403'
    '404':
      $ref: 'TS29571_CommonData.yaml#/components/responses/404'
    '406':
      $ref: 'TS29571_CommonData.yaml#/components/responses/406'
    '429':
      $ref: 'TS29571_CommonData.yaml#/components/responses/429'
    '500':
      $ref: 'TS29571_CommonData.yaml#/components/responses/500'
    '502':
      $ref: 'TS29571_CommonData.yaml#/components/responses/502'
    '503':
      $ref: 'TS29571_CommonData.yaml#/components/responses/503'
    default:
      $ref: 'TS29571_CommonData.yaml#/components/responses/default'
put:
  summary: "Modifies an existing Individual Policy Control Events Subscription "
  operationId: PutPcEventExposureSubsc
  tags:
    - Individual Policy Control Events Subscription (Document)
  requestBody:
    required: true
    content:
      application/json:
        schema:
          $ref: '#/components/schemas/PcEventExposureSubsc'
  parameters:
    - name: subscriptionId
      in: path
      description: Policy Control Event Subscription ID.
      required: true
      schema:
        type: string
  responses:
    '200':
      description: OK. Resource was succesfully modified and representation is returned.
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/PcEventExposureSubsc'
    '204':
      description: No Content. Resource was succesfully modified.
    '307':
      $ref: 'TS29571_CommonData.yaml#/components/responses/307'
    '308':
      $ref: 'TS29571_CommonData.yaml#/components/responses/308'
    '400':
      $ref: 'TS29571_CommonData.yaml#/components/responses/400'
    '401':
      $ref: 'TS29571_CommonData.yaml#/components/responses/401'
    '403':
      $ref: 'TS29571_CommonData.yaml#/components/responses/403'
    '404':
      $ref: 'TS29571_CommonData.yaml#/components/responses/404'
```

```
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '502':
          $ref: 'TS29571_CommonData.yaml#/components/responses/502'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
    delete:
      summary: "Cancels an existing Individual Policy Control Events Subscription "
      operationId: DeletePcEventExposureSubsc
      tags:
        - Individual Policy Control Events Subscription (Document)
      parameters:
        - name: subscriptionId
          in: path
          description: Policy Control Event Subscription ID.
          required: true
          schema:
            type: string
      responses:
        '204':
          description: No Content. Resource was succesfully deleted.
        '307':
          $ref: 'TS29571_CommonData.yaml#/components/responses/307'
        '308':
          $ref: 'TS29571_CommonData.yaml#/components/responses/308'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '502':
          $ref: 'TS29571_CommonData.yaml#/components/responses/502'
        '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-eventexposure: Access to the Npcf_EventExposure API.

  schemas:
    PcEventExposureNotif:
      description: >
        Represents notifications about Policy Control events related to an Individual
        Policy Events Subscription resource.
      type: object
      properties:
        notifId:
          type: string
        eventNotifs:
          type: array
          items:
            $ref: '#/components/schemas/PcEventNotification'
```

```
        minItems: 1
    required:
      - notifId
      - eventNotifs

  PcEventExposureSubsc:
    description: Represents an Individual Policy Events Subscription resource.
    type: object
    properties:
      eventSubs:
        type: array
        items:
          $ref: '#/components/schemas/PcEvent'
        minItems: 1
      eventsRepInfo:
        $ref: '#/components/schemas/ReportingInformation'
      groupId:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/GroupId'
      filterDnns:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        minItems: 1
      filterSnssais:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        minItems: 1
      snssaiDnns:
        type: array
        items:
          $ref: '#/components/schemas/SnssaiDnnCombination'
        minItems: 1
      filterServices:
        type: array
        items:
          $ref: '#/components/schemas/ServiceIdentification'
        minItems: 1
      appIds:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ApplicationId'
        minItems: 1
      tws:
        type: array
        items:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/TimeWindow'
        minItems: 1
      notifUri:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
      notifId:
        type: string
      eventNotifs:
        type: array
        items:
          $ref: '#/components/schemas/PcEventNotification'
        minItems: 1
      suppFeat:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
    required:
      - eventSubs
      - notifId
      - notifUri

  ReportingInformation:
    description: Represents the type of reporting that the subscription requires.
    type: object
    properties:
      immRep:
        type: boolean
      notifMethod:
        $ref: 'TS29508_Nsmf_EventExposure.yaml#/components/schemas/NotificationMethod'
      maxReportNbr:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
      monDur:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
      repPeriod:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
```

```
        sampRatio:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SamplingRatio'
        partitionCriteria:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PartitioningCriteria'
          minItems: 1
          description: Criteria for partitioning the UEs before applying the sampling ratio.
        grpRepTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        notifFlag:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NotificationFlag'
        notifFlagInstruct:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MutingExceptionInstructions'
        mutingSetting:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MutingNotificationsSettings'

    ServiceIdentification:
      description: Identifies the service to which the subscription applies.
      type: object
      properties:
        servEthFlows:
          type: array
          items:
            $ref: '#/components/schemas/EthernetFlowInfo'
          minItems: 1
        servIpFlows:
          type: array
          items:
            $ref: '#/components/schemas/IpFlowInfo'
          minItems: 1
        afAppId:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/AfAppId'
      # All conditions in allOf must be met
      allOf:
        # First condition is that servEthFlows and servIpFlows are mutually exclusive
        - not:
            required: [servEthFlows, servIpFlows]
        # Second condition is that at least one the servEthFlows, servIpFlows and afAppId shall be
present
        - anyOf:
          - required: [servEthFlows]
          - required: [servIpFlows]
          - required: [afAppId]

    EthernetFlowInfo:
      description: Identifies an UL/DL ethernet flow.
      type: object
      properties:
        ethFlows:
          type: array
          items:
            $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/EthFlowDescription'
          minItems: 1
          maxItems: 2
        flowNumber:
          type: integer
      required:
        - flowNumber

    IpFlowInfo:
      description: Identifies an UL/DL IP flow.
      type: object
      properties:
        ipFlows:
          type: array
          items:
            $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/FlowDescription'
          minItems: 1
          maxItems: 2
        flowNumber:
          type: integer
      required:
        - flowNumber

    PcEventNotification:
      description: Represents the information reported for a Policy Control event.
      type: object
```

```
      properties:
        event:
          $ref: '#/components/schemas/PcEvent'
        accType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        addAccessInfo:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/AdditionalAccessInfo'
        relAccessInfo:
          $ref: 'TS29512_Npcf_SMPolicyControl.yaml#/components/schemas/AdditionalAccessInfo'
        anGwAddr:
          $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/AnGwAddress'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
        plmnId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PlmnIdNid'
        satBackhaulCategory:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SatelliteBackhaulCategory'
        appliedCov:
          $ref:
'TS29534_Npcf_AMPolicyAuthorization.yaml#/components/schemas/ServiceAreaCoverageInfo'
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
        timeStamp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        pduSessionInfo:
          $ref: '#/components/schemas/PduSessionInformation'
        appId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ApplicationId'
        repServices:
          $ref: '#/components/schemas/ServiceIdentification'
        delivFailure:
          $ref: 'TS29522_ServiceParameter.yaml#/components/schemas/Failure'
        rateLimitRepo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        uePolEventInfos:
          type: array
          items:
            $ref: 'TS29522_ServiceParameter.yaml#/components/schemas/UePolEventInfo'
          minItems: 1
        sigInfos:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/NfSignallingInfo'
          minItems: 1
        afSliceReplOut:
          $ref: 'TS29534_Npcf_AMPolicyAuthorization.yaml#/components/schemas/SliceReplOutcomeInfo'
      required:
        - event
        - timeStamp

    PduSessionInformation:
      description: Represents PDU session identification information.
      type: object
      properties:
        snssai:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        dnn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        ueIpv4:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ueIpv6:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        ipDomain:
          type: string
        ueMac:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
      required:
        - snssai
        - dnn
      oneOf:
        - required: [ueMac]
        - anyOf:
          - required: [ueIpv4]
          - required: [ueIpv6]

    SnssaiDnnCombination:
```

```
      description: Represents a combination of S-NSSAI and DNN(s).
      type: object
      properties:
        snssai:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
        dnns:
          type: array
          items:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
          minItems: 1

# Simple data types and Enumerations

    PcEvent:
      description: Represents the policy control events that can be subscribed.
      anyOf:
      - type: string
        enum:
          - AC_TY_CH
          - PLMN_CH
          - SAC_CH
          - SAT_CATEGORY_CH
          - SUCCESS_UE_POL_DEL_SP
          - UNSUCCESS_UE_POL_DEL_SP
          - UNSUCCESS_PCF_SERVICE_AUTHORIZATION
          - APPLICATION_START
          - APPLICATION_STOP
          - RATE_LIMIT_INFO_REPO
          - SIGNALLING_INFO
          - SLICE_REPLACE_OUTCOME
          - PARTLY_UNSUCC_UE_POL_DEL_SP
      - type: string
        description: >
          This string provides forward-compatibility with future extensions to the enumeration
          and is not used to encode content defined in the present version of this API.
```

Annex B (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2018-11						TS skeleton of Policy Event Exposure Service specification	0.0.0
2018-11	CT3#99	C3-187718				API Introduction and Usage of HTTP for new PCF TS	1.0.0
2018-11	CT3#99	C3-187416				Npcf_EventExposure Resources Definition and Error handling	1.0.0
2018-11	CT3#99	C3-187419				Npcf_EventExposure, Policy Control Event Notification	1.0.0
2018-11	CT3#99	C3-187675				Npcf_EventExposure Service Description	1.0.0
2018-11	CT3#99	C3-187717				Npcf_EventExposure Service Operations and Data Structures	1.0.0
2018-11	CT3#99	C3-187734				Npcf_EventExposure, OpenAPI	1.0.0
2018-11	CT3#99	C3-187677				Npcf_EventExposure, Security	1.0.0
2018-12	CT#82	CP-183131				TS sent to plenary for information and approval	1.0.0
2018-12	CT#82	CP-183166				Npcf_EventExposure, OpenAPI	1.1.0
2018-12	CT#82	CP-183251				TS number assigned in the plenary for approval	1.1.0
2018-12	CT#82	CP-183253				TS approved by plenary	15.0.0
2019-03	CP#83	CP-190112	0001	1	F	Handling of IPdomain and UE addresses in Npcf_EventExposure service	15.1.0
2019-03	CT#83	CP-190160	0002	3	F	Correction on Presence conditions for ServiceIdentification data type	15.1.0
2019-03	CT#83	CP-190112	0003	1	F	Handling of UE identities in Npcf_EventExposure service	15.1.0
2019-03	CP#83	CP-190112	0004		F	Correction on the handling of access type change	15.1.0
2019-03	CT#83	CP-190112	0005		F	Correction of OpenAPI errors	15.1.0
2019-03	CP#83	CP-190161	0006	1	F	OpenAPI Version number updates	15.1.0
2019-06	CT#84	CP-191081	0007	1	F	Report ePDG address	15.2.0
2019-06	CT#84	CP-191081	0008		F	Storage of OpenAPI specification file	15.2.0
2019-06	CT#84	CP-191081	0009	2	F	Correction to the notification procedure	15.2.0
2019-06	CT#84	CP-191081	0010		F	Correction on PCF event exposure service	15.2.0
2019-06	CT#84	CP-191081	0011	2	F	Precedence of OpenAPI file	15.2.0
2019-06	CT#84	CP-191182	0012	2	F	Copyright note in YAML file	15.2.0
2019-06	CT#84	CP-191081	0013	1	F	OpenAPI Version number update	15.2.0
2019-09	CT#85	CP-192156	0014	1	B	Support of a set of MAC addresses in traffic filter	16.0.0
2019-09	CT#85	CP-192157	0015	1	B	Enhancement of event reporting information	16.0.0
2019-09	CT#85	CP-192173	0016		F	OpenAPI version update	16.0.0
2020-03	CT#87e	CP-200207	0018		B	DNN Clarification	16.1.0
2020-06	CT#88e	CP-201252	0019		B	Adding support of NID	16.2.0
2020-06	CT#88e	CP-201229	0020	3	B	Access Type Report for a MA PDU session	16.2.0
2020-06	CT#88e	CP-201244	0021	1	F	Storage of YAML files in ETSI Forge	16.2.0
2020-06	CT#88e	CP-201256	0022	1	F	URI of the Npcf_EventExposure service	16.2.0
2020-06	CT#88e	CP-201223	0024	1	A	suppFeat within PcEventExposureSubsc	16.2.0
2020-06	CT#88e	CP-201244	0025	1	F	Supported headers, Resource Data type	16.2.0
2020-06	CT#88e	CP-201255	0027		F	Update of OpenAPI version and TS version in externalDocs Field	16.2.0
2020-09	CT#89e	CP-202055	0031	1	A	Resource URI for individual subscription	16.3.0
2020-09	CT#89e	CP-202073	0028		B	Successful status code	17.0.0
2020-12	CT#90e	CP-203076	0033	2	A	TS 29.523 Essential Corrections and alignments	17.1.0
2020-12	CT#90e	CP-203139	0035	1	A	Storage of YAML files in ETSI Forge	17.1.0
2020-12	CT#90e	CP-203144	0037	1	F	Combination of DNN and S-NSSAI	17.1.0
2020-12	CT#90e	CP-203110	0039	1	A	Correction to support Stateless NFs	17.1.0
2020-12	CT#90e	CP-203153	0041		F	Update of OpenAPI version and TS version in externalDocs field	17.1.0
2021-03	CT#91e	CP-210218	0042		F	OpenAPI reference	17.2.0
2021-03	CT#91e	CP-210219	0043		F	Adding some missing description fields to data type definitions in OpenAPI specification files	17.2.0
2021-03	CT#91e	CP-210227	0044		F	Missing data type in the Npcf_EventExposure specific Data Types table	17.2.0
2021-03	CT#91e	CP-210240	0045		F	Update of OpenAPI version and TS version in externalDocs field	17.2.0
2021-06	CT#92e	CP-211257	0046	1	B	Support of notifications of SAR changes	17.3.0
2021-06	CT#92e	CP-211221	0047	2	B	Partitioning criteria for applying sampling in specific UE partitions in PCF exposure	17.3.0
2021-06	CT#92e	CP-211234	0048		F	Support of optional HTTP custom header fields	17.3.0
2021-06	CT#92e	CP-211221	0049	1	B	Support of Mute reporting	17.3.0
2021-06	CT#92e	CP-211200	0051	1	A	Redirect responses with "application/json" media type	17.3.0
2021-06	CT#92e	CP-211213	0052	1	B	Satellite backhaul change event in PCF exposure	17.3.0
2021-06	CT#92e	CP-211211	0053		F	Correction to subscription filters	17.3.0
2021-06	CT#92e	CP-211265	0055		F	Update of OpenAPI version and TS version in externalDocs field	17.3.0
2021-09	CT#93e	CP-212205	0056		B	Definition of PLMN identifier notification event	17.4.0
2021-09	CT#93e	CP-212220	0057	1	F	URI representing Policy Control Events Subscriptions resource	17.4.0
2021-12	CT#94e	CP-213222	0058	1	B	Notification on the outcome of UE Policies delivery due to service specific parameter provisioning	17.5.0
2021-12	CT#94e	CP-213194	0059	1	F	Updates in subscription to service area coverage changes	17.5.0
2021-12	CT#94e	CP-213226	0060	1	A	Corrections in PCF event exposure NF service consumers	17.5.0
2021-12	CT#94e	CP-213244	0061	1	B	Event report in the subscription response	17.5.0
2021-12	CT#94e	CP-213246	0063		F	Update of OpenAPI version and TS version in externalDocs field	17.5.0

2022-03	CT#95e	CP-220179	0064		F	Completion of the information related to satellite backhaul change event	17.6.0
2022-03	CT#95e	CP-220185	0065		F	Completion of the information related to UE Policy Delivery outcome event	17.6.0
2022-03	CT#95e	CP-220197	0066	1	B	Clarification of the report of the requested service area coverage change	17.6.0
2022-03	CT#95e	CP-220197	0067		B	Definition of Service Area Coverage	17.6.0
2022-03	CT#95e	CP-220179	0068		F	Changing reference for the SatelliteBackhaulCategory data type	17.6.0
2022-03	CT#95e	CP-220201	0069	1	F	Update of description fields	17.6.0
2022-03	CT#95e	CP-220194	0070		F	Update of info and externalDocs fields	17.6.0
2022-06	CT#96	CP-221157	0071		F	Inaccurate condition for immediate reporting	17.7.0
2022-06	CT#96	CP-221154	0072		F	Alignment with the SBI template	17.7.0
2022-06	CT#96	CP-221151	0073		F	Update of info and externalDocs fields	17.7.0
2022-09	CT#97e	CP-222099	0074	1	F	Correction to notification of outcome of the UE Policy Delivery	17.8.0
2022-12	CT#98e	CP-223191	0075		F	Adding the mandatory error code 502 Bad Gateway	18.0.0
2022-12	CT#98e	CP-223192	0077	1	F	PcEvent enumeration definition in the OpenAPI file	18.0.0
2022-12	CT#98e	CP-223200	0080	2	F	Correction to Data Type PduSessionInformation	18.0.0
2022-12	CT#98e	CP-223178	0081		B	SNPN mobility	18.0.0
2022-12	CT#98e	CP-223189	0085		F	Update of info and externalDocs fields	18.0.0
2023-03	CT#99	CP-230167	0086	1	D	Removing wrong feature indication	18.1.0
2023-03	CT#99	CP-230162	0087		F	Update of info and externalDocs fields	18.1.0
2023-06	CT#100	CP-231125	0088	1	B	Event muting enhancements for PCF event exposure	18.2.0
2023-06	CT#100	CP-231250	0089	2	B	Support of application detection event exposure	18.2.0
2023-06	CT#100	CP-231131	0091	1	F	Corrections to the redirection mechanism description	18.2.0
2023-06	CT#100	CP-231141	0092		F	Update of info and externalDocs fields	18.2.0
2023-12	CT#102	CP-233247	0096	1	F	Correcting the cardinality of event	18.3.0
2023-12	CT#102	CP-233253	0097	1	B	Support of Dynamic Satellite Backhaul	18.3.0
2023-12	CT#102	CP-233257	0098	1	F	Completion of Application Detection	18.3.0
2023-12	CT#102	CP-233228	0099	1	F	Reference update: IETF RFC 9113	18.3.0
2023-12	CT#102	CP-233228	0100		F	ProblemDetails RFC 7807 obsoleted by RFC 9457	18.3.0
2023-12	CT#102	CP-233226	0101	1	F	Applicability of muting exception instructions	18.3.0
2023-12	CT#102	CP-233253	0102	1	B	Support of dynamic satellite backhaul category changes	18.3.0
2024-03	CT#103	CP-240185	0103	1	F	Updates on application detection event exposure	18.4.0
2024-03	CT#103	CP-240185	0104	1	B	AF/NEF subscription to application detection and PCF provisioning of PCC rule(s).	18.4.0
2024-06	CT#104	CP-241077	0105		F	Muting resolution	18.5.0
2024-06	CT#104	CP-241085	0106		F	Update of info and externalDocs fields	18.5.0
2025-03	CT#107	CP-250082	0107	1	B	Support of AF request rate limitation information reporting over PCF event exposure	19.0.0
2025-03	CT#107	CP-250083	0108	1	B	Signalling storm information exposure	19.0.0
2025-03	CT#107	CP-250102	0109	1	F	Service parameter authorization in the PCF	19.0.0
2025-03	CT#107	CP-250129	0111		F	Update of info and externalDocs fields	19.0.0
2025-06	CT#108	CP-251094	0112	1	B	Updates and corrections to the new AF-requested Network Slice Replacement functionality	19.1.0
2025-06	CT#108	CP-251241	0115	2	A	Corrections on data type PcEventExposureSubsc	19.1.0
2025-06	CT#108	CP-251228	0116	2	B	UE policy delivery outcome handling	19.1.0
2025-06	CT#108	CP-251231	0117		F	Update of info and externalDocs fields	19.1.0
2025-09	CT#109	CP-252073	0118		F	Missing applicable feature for SnssaiDnnCombination data type	19.2.0
2025-09	CT#109	CP-252090	0119		F	Corrections related to PCFSerParAuth feature	19.2.0
2025-09	CT#109	CP-252085	0124		A	Corrections to PcEventNotification data type	19.2.0
2025-09	CT#109	CP-252080	0125	1	F	Corrections to the AF requested Network Slice Replacement functionality	19.2.0
2025-09	CT#109	CP-252070	0126		B	Remove the editor note for the data rate limit report	19.2.0
2025-09	CT#109	CP-252113	0127		F	Update of info and externalDocs fields	19.2.0
2025-12	CT#110	CP-253029	0128		F	Correction to Supported Features	19.3.0
2025-12	CT#110	CP-253058	0129		F	Corrections to PcEvent in OpenAPI	19.3.0
2025-12	CT#110	CP-253049	0130	1	F	Corrections to AF requested slice replacement outcome event	19.3.0
2025-12	CT#110	CP-253030	0131	1	F	Correction of re-used Data Types table	19.3.0
2025-12	CT#110	CP-253064	0132		F	Update of info and externalDocs fields	19.3.0
2026-03	CT#111	CP-260081	0133		F	Update of info and externalDocs fields	19.4.0
2026-06	CT#112	CP-261249	0135		F	Update of info and externalDocs fields	19.5.0

History

Version	Date	Status
V19.2.0	January 2026	Publication
V19.3.0	February 2026	Publication
V19.4.0	March 2026	Publication
V19.5.0	July 2026	Publication