ETSI TS 129 512 V15.2.0 (2019-04)

TECHNICAL SPECIFICATION

5G;
5G System;
Session Management Policy Control Service;
Stage 3
(3GPP TS 29.512 version 15.2.0 Release 15)

Reference
RTS/TSGC-0329512vf20

Keywords
5G

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

ETSI

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document provides the stage 3 specification of the Session Management Policy Control Service of 5G system. The stage 2 definition and related procedures of the Session Management Policy Control Service are contained in 3GPP TS 23.502 [3] and 3GPP TS 23.503 [6]. The 5G System Architecture is defined in 3GPP TS 23.501 [2].

Stage 3 call flows are provided in 3GPP TS 29.513 [7].

The Technical Realization of the Service Based Architecture and the Principles and Guidelines for Services Definition of the 5G System are specified in 3GPP TS 29.500 [4] and 3GPP TS 29.501 [5].

The Policy Control Function with session related policies provides the Session Management Policy Control Service to the NF consumers (i.e. Session Management Function).

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

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

[6]   3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

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

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

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

[10]   OpenAPI: "OpenAPI 3.0.0 Specification", https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md.

[11]   3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[12]   3GPP TS 29.508: "5G System; Session Management Event Exposure Service; Stage 3".

[13]   3GPP TS 29.244: "Interface between the Control Plane and the User Plane of EPC Nodes".

[14]   3GPP TS 23.003: "Numbering, addressing and identification".

[15]   3GPP TS 29.519: "5G System; Usage of the Unified Data Repository service for Policy Control Data, Application Data and Structured Data for Exposure; Stage 3".

[16]   3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[17]   3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[18]   3GPP TS 29.214: "Policy and Charging Control over Rx reference point 5".

[19]   3GPP TS 32.291: "5G System; Charging service; Stage 3".

[20]   3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[21]   3GPP TS 23.380: "IMS Restoration Procedures".

[22]   3GPP TS 29.502: "5G System; Session Management Services; Stage 3".

[23]   3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[24]   3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[25]   3GPP TS 29.507: "5G System; Access and Mobility Policy Control Service; Stage 3".

[26]   3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[27]   3GPP TS 33.501: "Security architecture and procedures for 5G system".

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

[29]   3GPP TS 29.510: "Network Function Repository Services; Stage 3".

[30]   3GPP TS 32.290: "5G system; Services, operations and procedures of charging using Service Based Interface (SBI)".

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

[32]   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].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [2], subclause 3.1 apply:

5G QoS Identifier

PCC rule

PDU Session

Service Data Flow

Service Data Flow Filter

Service Data Flow Template

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
API	Application Programming Interface
CHF	Charging Function
DNN	Data Network Name
GFBR	Guaranteed Flow Bit Rate
HTTP	Hypertext Transfer Protocol
NEF	Network Exposure Function
NF	Network Function
PCC	Policy and Charging Control
PCF	Policy Control Function
PSAP	Public Safety Answering Point
QoS	Quality of Service
SDF	Service Data Flow
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
UDR	Unified Data Repository
UE	User Equipment

4 Npcf_SMPolicyControl Service

4.1 Service Description

4.1.1 Overview

The Session Management Policy Control Service performs provisioning, update and removal of session related policies and PCC rules by the Policy Control Function (PCF) to the NF service consumer (i.e. SMF). The Session Management Policy Control Service can be used for charging control, policy control and/or application detection and control. Session Management Policy Control Service applies to the cases where the SMF interacts with the PCF in the non-roaming scenario, the V-SMF interacts with the V-PCF in the local breakout roaming scenario and the H-SMF interacts with the H-PCF in the home-routed scenario.

4.1.2 Service Architecture

The Session Management Policy Control Service is provided by the PCF to the consumer and shown in the SBI representation model in figure 4.1.2-1 and in the reference point representation model in figure 4.1.2.2. The overall Policy and Charging Control related 5G architecture is depicted in 3GPP TS 29.513 [7].

The only known NF Service Consumer is the SMF.
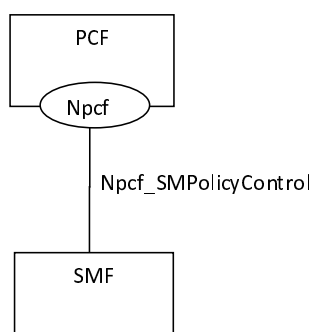
Figure 4.1.2-1: Reference Architecture for the Npcf_SMPolicyControl Service; SBI representation
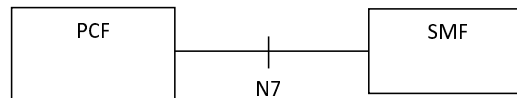
Figure 4.1.2-2: Reference Architecture for the Npcf_SMPolicyControl Service; reference point representation

NOTE: The SMF represents the V-SMF and the PCF represents the V-PCF in the local breakout scenario. The SMF represents the H-SMF and the PCF represents the H-PCF in the home routed scenario.

4.1.3 Network Functions

4.1.3.1 Policy Control Function (PCF)

The PCF is responsible for policy control decisions and flow based charging control functionalities. The PCF provides the following:

- policies for application and service data flow detection, gating, QoS, flow based charging, traffic steering control, usage monitoring control, access network information report and RAN support information to the SMF.

The policy decisions made by the PCF may be based on one or more of the following:

- Information obtained from the AF, e.g. the session, media and subscriber related information;

- Information obtained from the UDR;

- Information obtained from the AMF, e.g. UE related and access related information;

- Information obtained from the SMF;

- Information obtained from the NWDAF;

- Information obtained from the NEF;

- Information obtained from another PCF in the roaming scenario;

- information from CHF; and

- PCF pre-configured policy context.

4.1.3.2 NF Service Consumers

The SMF is responsible for the enforcement of session management related policy decisions from the PCF, related to service flow detection, QoS, charging, gating, traffic usage reporting and traffic steering

The SMF shall support:

- sending the PDU session related attributes to the PCF;

- requesting and receiving the PCC rule(s) from the PCF;

- binding of service data flows to QoS flow as defined in 3GPP TS 29.513 [7];

- deriving rule(s) from the PCC rule(s) and then providing those rules to the user plane function or remove the rule(s) from the user plane as defined in 3GPP TS 29.244 [13];

- deriving the QoS rules towards the UE;

- deriving the QoS profile towards the access network;

- handling the policy control request trigger; and

- handling the PDU session related policy information.

 NOTE: SMF functionality related to event exposure is defined in 3GPP TS 29.508 [12].

4.1.4 Rules

4.1.4.1 General

A rule is a set of policy information elements associated with a PDU session, or with service data flows (i.e., with a PCC rule).

Two types of rules are defined:

- Session rule; and

- PCC rule.

Both Session rules and PCC rules are composed of embedded information elements as well as information elements that are part of the referenced objects (e.g. condition data, or usage monitoring policy data type) by the rule.

PCC rule is defined in subclause 4.1.4.2. Session rule is defined in subclause 4.1.4.3.

4.1.4.2 PCC rules

4.1.4.2.1 PCC rules definition

A PCC rule is a set of information elements enabling the detection of a service data flow and providing parameters for policy control and/or charging control.There are two different types of PCC rules as defined in 3GPP TS 23.503 [6]:

- Dynamic PCC rules. PCC rules that are dynamically provisioned by the PCF to the SMF. These PCC rules may be either predefined or dynamically generated in the PCF. Dynamic PCC rules can be installed, modified and removed at any time.

- Predefined PCC rules. PCC rules that are preconfigured in the SMF. Predefined PCC rules can be activated or deactivated by the PCF at any time. Predefined PCC rules within the PCF may be grouped allowing the PCF to dynamically activate a set of PCC rules.

 NOTE: Additionally, predefined PCC rules can be grouped within the SMF as predefined PCC rule bases which allow the PCF to dynamically activate these sets of rules. In this case, the PCC rule identifier is used to hold the predefined PCC rule base identifier.

A PCC rule consists of:

Table 4.1.4.2.1-1: PCC rule information elements

Information name	Description	Category
Rule identifier	Uniquely identifies the PCC rule, within a PDU Session. It is used between PCF and SMF for referencing PCC rules.	Mandatory
Service data flow detection		
Precedence	Determines the order, in which the service data flow templates are applied at service data flow detection, enforcement and charging.	Mandatory
Service Data Flow Template	For IP PDU traffic: Either a list of service data flow filters or an application identifier that references the corresponding application detection filter for the detection of the service data flow. For Ethernet PDU traffic: Combination of traffic patterns of the Ethernet PDU traffic.	Mandatory
Mute for notification	Defines whether application's start or stop notification is to be muted.	Optional
Charging		
Charging key	The charging system (CHF) uses the charging key to determine the tariff to apply to the service data flow.	Optional
Service identifier	The identity of the service or service component the service data flow in a rule relates to.	Optional
Sponsor Identifier	An identifier, provided from the AF, which identifies the Sponsor, used for sponsored flows to correlate measurements from different users for accounting purposes.	Optional
Application Service Provider Identifier	An identifier, provided from the AF, which identifies the Application Service Provider, used for sponsored flows to correlate measurements from different users for accounting purposes.	Optional
Charging method	Indicates the required charging method for the PCC rule. Values: online, offline or neither.	Optional
Measurement method	Indicates whether the service data flow data volume, duration, combined volume/duration or event shall be measured. This is applicable to reporting, if the charging method is online or offline. Note: Event based charging is only applicable to predefined PCC rules and PCC rules used for application detection filter (i.e. with an application identifier).	Optional
Application Function Record Information	An identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports.	Optional
Service identifier level reporting	Indicates that separate usage reports shall be generated for this Service identifier. Values: mandated or not required.	Optional
Policy control		
5QI	Identifier for the authorized QoS parameters for the service data flow.	Mandatory
ARP	The Allocation and Retention Priority for the service data flow consisting of the priority level, the pre-emption capability and the pre-emption vulnerability	Mandatory
Gate status	The gate status indicates whether the service data flow, detected by the service data flow template, may pass (Gate is open) or shall be discarded (Gate is closed).	Optional
QoS Notification Control (QNC)	Indicates whether notifications are requested from 3GPP NG-RAN when the GFBR can no longer (or again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow.	Optional
Reflective QoS Control	Indicates to apply reflective QoS for the SDF.	Optional
MBR (UL/DL)	The uplink/downlink maximum bitrate authorized for the service data flow.	Optional
GBR (UL/DL)	The uplink/downlink guaranteed bitrate authorized for the service data flow.	Optional
UL sharing indication	Indicates resource sharing in uplink direction with service data flows having the same value in their PCC rule.	Optional
DL sharing indication	Indicates resource sharing in downlink direction with service data flows having the same value in their PCC rule.	Optional
Redirect	Redirect state of the service data flow (enabled/disabled).	Optional
Redirect Destination	Controlled Address to which the service data flow is redirected when redirect is enabled.	Optional

Bind to default QoS Flow	Indicates that the dynamic PCC rule shall always have its binding with the default QoS Flow.	Optional
Priority Level	Indicates a priority in scheduling resources among QoS Flows.	Optional
Averaging Window	Represents the duration over which the guaranteed and maximum bitrate shall be calculated.	Optional
Maximum Data Burst Volume	Denotes the largest amount of data that is required to be transferred within a period of 5G-AN PDB.	Optional
Access Network Information Reporting		
User Location Required	The serving cell of the UE is to be reported. When the corresponding QoS flow is deactivated, and if available, information on when the UE was last known to be in that location is also to be reported.	Optional
UE Timezone Required	The time zone of the UE is to be reported.	Optional
Usage Monitoring Control		
Monitoring key	The PCF uses the monitoring key to group services that share a common allowed usage.	Optional
Indication of exclusion from session level monitoring	Indicates that the service data flow shall be excluded from PDU Session usage monitoring.	Optional
Traffic Steering Enforcement Control		
Traffic steering policy identifier(s)	Reference to a pre-configured traffic steering policy at the SMF.	Optional
Data Network Access Identifier	Identifier of the target Data Network Access.	Optional
Information on AF subscription to UP path changes events	Indicates whether a notification in case of UP path change is requested, as well as the destination(s) for where to provide the notification.	Optional
RAN support information		
UL Maximum Packet Loss Rate	The maximum rate for lost packets that can be tolerated in the uplink direction for the service data flow.	Optional
DL Maximum Packet Loss Rate	The maximum rate for lost packets that can be tolerated in the downlink direction for the service data flow.	Optional

The above information is organized into a set of decision data objects as defined in subclause 4.1.4.4. The exact encoding of PCC rules is defined in subclause 5.6.2.6.

4.1.4.2.2   PCC rules operation

For dynamic PCC rules, the following applies:

- Installation: to provision the PCC rules.

- Modification: to modify the PCC rules.

- Removal: to remove the PCC rules.

For predefined PCC rules, the following operations are available:

- Activation: to activate the PCC rules.

- Deactivation: to deactivate the PCC rules.

4.1.4.3   Session rule

4.1.4.3.1   Session rules definition

A session rule consists of policy information elements associated with PDU session. The encoding of the SessionRule data type is defined in subclause 5.6.2.7.

A session rule may include:

- Session Rule ID;

- Authorized Session AMBR;

- Authorized Default QoS;

- Reference to Usage Monitoring Data; and

- Reference to Condition Data.

4.1.4.3.2 Session rules operation

For Session rules, the following applies:

- Installation: to provision the session rules.

- Modification: to modify the session rules.

- Removal: to remove the session rules.

4.1.4.4 Policy Decision types

4.1.4.4.1 General

A policy decision is a grouping of cohesive information elements describing a specific type of decision, e.g. QoS, Charging data, etc. A policy decision can be linked to one or more PCC rules or one or more Session rules. A PCC rule or session rule can at most refer to one instance of the policy decision for each type.

The following types of policy decision are defined:

- Traffic control data;

- QoS data;

- Charging data; and

- Usage Monitoring data.

4.1.4.4.2 Traffic control data definition

Traffic control data defines how traffic data flows associated with a rule are treated (e.g. blocked, redirected). The traffic control data encoding table is defined in subclause 5.6.2.10.

Traffic control data shall include:

- Traffic Control Data ID.

Traffic control data may include:

- Flow status;

- Redirect Information;

- Mute Notification;

- Traffic Routing Location;

- Traffic Steering Policy ID UL; - Traffic Steering Policy ID DL;

- Routing requirements; and

- UP path change event subscription from the AF.

4.1.4.4.3 QoS data definition

QoS data defines QoS parameters (e.g. bitrates) associated with a rule. The QoS data encoding table is defined in subclause 5.6.2.8.

QoS data shall include:

- QoS Data ID;

- 5QI;

- ARP;

QoS data may include:

- QNC;

- Packet Loss Rate UL;

- Packet Loss Rate DL;

- Maximum Bit Rate UL;

- Maximum Bit Rate DL;

- Guaranteed Bit Rate UL;

- Guaranteed Bit Rate DL;

- 5QI Priority Level;

- Averaging window;

- Maximum Data Burst Volume;

- Bound to default QoS flow indication;

- Resource Sharing Key UL;

- Resource Sharing Key DL; and

- Reflective QoS attribute.

4.1.4.4.4 Charging data definition

Charging data defines charging related parameters (e.g. rating group) associated with a rule. The charging data encoding table is defined in subclause 5.6.2.11.

Charging data shall include:

- Charging Data ID;

- Rating Group.

Charging data may include:

- Metering Method;

- Charging Method;

- Reporting Level;

- Service ID;

- Sponsor ID;

- Application Service Provider ID; and

- AF Charging ID.

4.1.4.4.5 UsageMonitoring data definition

UsageMonitoring data defines usage monitoring information associated with a rule. The UsageMonitoring data encoding table is defined in subclause 5.6.2.12.

Usage Monitoring Data shall include:

- Usage Monitoring ID;

Usage Monitoring Data may include:

- Volume Threshold;

-   Volume Threshold UL;

-   Volume Threshold DL;

-   Time Threshold;

-   Monitoring Time;

-   Next Volume Threshold;

-   Next Volume Threshold UL;

-   Next Volume Threshold DL;

-   Next Time Threshold; and

-   Inactivity Time.

-   PCC rule identifier(s) corresponding to the service data flow(s) which needs to be excluded from PDU session level usage monitoring.

4.1.5 Policy control request trigger

Policy control request trigger is a condition when the SMF shall interact again with PCF for further policy decision of a PDU session.

The policy control request trigger is designed as an Enumeration type defined in the subclause 5.6.3.6.

The PCF can provide an array of policy control request triggers in policy decision to subscribe the triggers in SMF.

When SMF interacts with PCF due to the triggering of the policy control request triggers, the SMF shall send the related attributes that have changed together with the corresponding triggers.

4.1.6 Requested rule data

Requested rule data consists of requested information by the PCF associated with one or more PCC rules.

The requested rule data is designed as a subresource of the policy decision within an attribute called "lastReqRuleData". The PCF only records the last requested rule data.

When requesting rule data, the PCF shall include the types of data requested for the rules within the "reqData" array of the "lastReqRuleData" and shall also provide the corresponding policy control request triggers if the triggers are not yet set.

The encoding of the requested rule data is further specified in subclause 5.6.2.23.

When the SMF receives the requested rule data, the SMF shall report the corresponding information to the PCF for the associated PCC rule(s). The requested rule data shall not be valid for the PCC rule(s) after the reporting.

4.1.7 Requested usage data

Requested Usage data consists of requested usage reports by the PCF for one or more instances of Usage Monitoring data decision.

The requested usage data is designed as a sub resource of the policy decision within an attribute called "lastReqUsageCtlData". The PCF only records the last requested usage data.

The encoding of the requested usage data is further specified in subclause 5.6.2.24.

When the SMF receives the requested usage data, the SMF shall report the corresponding accumulated usage to the PCF for the corresponding Usage Monitoring data decision(s). The requested usage data shall not be valid for the Usage Monitoring data decision(s) after the reporting.

4.1.8 Condition data

Condition data defines the condition(s) where the PCC rules or session rules are applicable and/or not applicable. The condition data encoding is defined in subclause 5.6.2.9.

Condition data shall include:

- Condition Data ID.

Condition data may include:

- Activation Time; and

- Deactivation Time.

4.2 Service Operations

4.2.1 Introduction

The service operations defined for Npcf_SMPolicyControl are shown in table 4.2.1-1.

Table 4.2.1-1: Npcf_SMPolicyControl Operations

Service Operation Name	Description	Initiated by
Npcf_SMPolicyControl_Create	Request to create an SM Policy Association with the PCF to receive the policy for a PDU session.	NF consumer (SMF)
Npcf_SMPolicyControl_Update	Request to update the SM Policy association with the PCF to receive the updated policy when Policy Control Request Trigger condition is met.	NF consumer (SMF)
Npcf_SMPolicyControl_UpdateNotify	Update and/or delete the PCC rule(s) PDU session related policy context at the SMF and Policy Control Request Trigger information.	PCF
Npcf_SMPolicyControl_Delete	Request to delete the SM Policy Association and the associated resources.	NF consumer (SMF)

4.2.2 Npcf_SMPolicyControl_Create Service Operation

4.2.2.1 General

The Npcf_SMPolicyControl_Create service operation provides means for the SMF to request the creation of a corresponding SM Policy Association with PCF.

The Session Management procedures of the SMF and related to policies are defined in 3GPP TS 23.501 [2], 3GPP TS 23.502 [3] and 3GPP TS 23.503 [6].

The following procedures using the Npcf_SMPolicyControl_Create service operation are supported:

- Request of creation of a corresponding SM Policy Association with PCF.

- Provisioning of PCC rules.

- Provisioning of policy control request triggers.

- Provisioning of charging related information for PDU session.

- Provisioning of revalidation time.

- Policy provisioning and enforcement of authorized AMBR per PDU session.

- Policy provisioning and enforcement of authorized default QoS.

- Provisioning of PCC rule for Application Detection and Control.

- 3GPP PS Data Off Support.

- IMS Emergency Session Support.

- Request Usage Monitoring Control.

- Access Network Charging Identifier report.

- Request for the successful resource allocation notification.

- Provisioning of IP Index Information.

- Negotiation of the QoS flow for IMS signalling.

4.2.2.2 SM Policy Association establishment
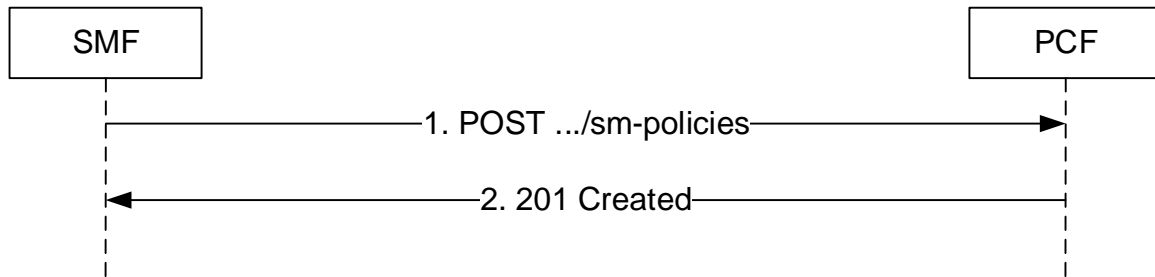
Figure 4.2.2.2-1: SM Policy Association establishment

When the SMF receives the Nsmf_PDUSession_CreateSMContext Request as defined in subclause 5.2.2.2 of 3GPP TS 29.502 [22], if the SMF is being requested via Nsmf_PDUSession_CreateSMContext Request not to interact with the PCF, the SMF shall not interact with the PCF; otherwise, the SMF shall send the POST method as step 1of the figure 4.2.2.2-1 to request to create an "Individual SM Policy".

NOTE 1: The decision to not interact with PCF applies for the life time of the PDU session.

NOTE 2: The indicator to not interact with PCF is configured in the UDR. It is delivered to the SMF within the Charging Characteristics. The indicator is operator specific, therefore it can only be used in non-roaming and home routed roaming cases.

The SMF shall include SmPolicyContextData data structure in the payload body of the HTTP POST to request a creation of representation of the "Individual SM Policy" resource. The "Individual SM Policy" resource is created as described below.

The SMF shall include (if available) in SmPolicyContextData data structure:

- SUPI of the user within the "supi" attribute;

- PDU Session Id within the "pduSessionId" attribute;

- DNN within the "dnn" attribute;

- URL identifying the recipient of SM policies update notification within the "notificationUri" attribute;

- PDU Session Type within the "pduSessionType" attribute;

- PEI within the "pei" attribute;

- Internal Group Id(s) within the "InterGrpIds" attribute;

- type of access within the "accessType" attribute;

- type of the radio access technology within the "ratType" attribute;

- the UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "ipv6AddressPrefix" attribute;

- the UE time zone information within "ueTimeZone" attribute;

- subscribed Session-AMBR within "subsSessAmbr" attribute;

- subscribed Default QoS Information within "subsDefQos" attribute;

- the number of supported packet filters for signalled QoS rules within the "numOfPackFilter";

- the charging characteristics within "chargingCharacteristics" attribute;

- access network charging identifier within the " accNetChId" attribute;

- the address of the network entity performing charging within the "chargEntityAddr" attribute;

- 3GPP PS data off status within the "3gppPsDataOffStatus" attribute;

- indication of UE supporting reflective QoS within the "refQosIndication" attribute;

- user location information within the "userLocationInfo" attribute;

- the S-NSSAI corresponding to the network slice the PDU session is allocated within the "sliceInfo" attribute.

- the QoS flow usage required of the default QoS flow within the "qosFlowUsage" attribute;

- identifier of the serving network within the "servingNetwork" attribute; and

- trace control and configuration parameters information encoded as "traceReq" attribute.

The SMF may include in "SmPolicyContextData" data structure the IPv4 address domain identity within the "ipDomain" attribute.

NOTE 3: The "ipDomain" attribute is helpful when within a network slice instance, there are several separate IP address domains, with SMF/UPF(s) that allocate Ipv4 IP addresses out of the same private address range to UE PDU Sessions. The same IP address can thus be allocated to UE PDU sessions served by SMF/UPFs in different IPv4 address domains. If one PCF controls several SMF/UPFs in different IP address domains, the UE IP address is thus not sufficient for the AF session binding procedure, as described in 3GPP TS 29.514 [17]. The SMF assits the PCF in the session binding supplying an "ipDomain" attribute denoting the IPv4 address domain identity of the allocated UE IPv4 address.

When the PCF receives the HTTP POST request from the SMF, the PCF shall make an authorization based on the information received from the SMF and, if available, AMF, CHF, AF, UDR, NWDAF and operator policy pre-configured at the PCF. If the authorization is successful, the PCF shall create a new resource, which represents "Individual SM Policy", addressed by a URI as defined in subclause 5.3.3.2 and contains a PCF created resource identifier. The PCF shall respond to the SMF with a 201 Created message, including:

- Location header field containing the URI for the created resource; and

- a response body providing session management related policies, e.g. provisioning of PCC rules as defined in subclause 4.2.6.2, provisioning of policy control request triggers as defined in subclause 4.2.6.4.1.

The SMF shall use the URI received in the Location header in subsequent requests to the PCF to refer to the "Individual SM Policy".

It the PCF received a "traceReq" attribute, it shall perform trace procedures as defined in 3GPP TS 32.422 [24].

If errors occur when processing the HTTP POST request, the PCF shall apply error handling procedures as specified in subclause 5.7.

If the user information received within the "supi" attribute is unknown, the PCF shall reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "USER_UNKNOWN".

If the PCF is, due to incomplete, erroneous or missing information (e.g. QoS, RAT type, subscriber information) not able to provision a policy decision as response to the request for PCC rules by the SMF, the PCF may reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR_INITIAL_PARAMETERS".

If the PCF, based on local configuration and/or operator policies, denies the creation of the Individual SM Policy resource, the PCF may reject the request and include in an HTTP "403 Forbidden" response message the "cause"

attribute of the ProblemDetails data structure set to "POLICY_CONTEXT_DENIED". Based on configured failure action, the SMF at reception of this error code may reject the PDU session establishment or allow the PDU session establishment applying local policies.

If the SMF receives HTTP response with these codes, the SMF shall reject the PDU session establishment that initiated the HTTP POST Request.

4.2.2.3 Provisioning of charging related information for PDU session

4.2.2.3.1 Provisioning of Charging Addresses

The PCF may provide the CHF address(es) to the SMF during the initial interaction with the SMF defining the charging function respectively based on the operator policy. In this case, the PCF may retrieve the CHF address(es) as follows:

- receives it from the UDR as part of the Policy Data Subscription information as defined in subclause 5.2.10 of 3GPP TS 29.519 [15].

- locally configured in the PCF based on operator policies.

- discovers using NRF as described in subclause 6.1 of 3GPP TS 32.290 [30].

In order to provision the CHF address(s) to the SMF, the PCF shall include the "chargingInfo" attribute containing the charging address within the SmPolicyDecision data structure. Within the ChargingInformation data structure, both primary CHF address within a "primaryChfAddress" attribute and secondary CHF address within a "secondaryChfAddress" attribute shall be provided simultaneously. These shall overwrite any predefined addresses at the SMF. Provisioning CHF addresses without PCC rules for charged service data flows shall not be considered as an error since such PCC rules may be provided later. If the PCF has provided the CHF address, it shall not modify the CHF address in subsequent interactions.

If no CHF address is available at the SMF (i.e. no predefined CHF addresses, and no CHF addresses supplied by the PCF and/or by the Charging Characteristics), the SMF shall use the SUPI (MNC and MCC values of the IMSI) of the user to construct the CHF Home network domain name as specified in 3GPP TS 23.003 [14], clause 25.

4.2.2.3.2 Provisioning of Default Charging Method

The default charging method indicates what charging method shall be used for every PCC rule where the charging method is omitted within the PCC rule. The SMF may have a pre-configured default charging method.

Upon the initial interaction with the PCF, the SMF shall provide the pre-configured default charging method, if available, within the "offline" attribute and/or "online" attribute embedded directly within the SmPolicyContextData data structure of HTTP POST message to the PCF.

The PCF may provide the default charging method which applies to the PDU session. In order to do so, if offline charging applies, the PCF shall include the "offline" attribute set to "true" within the SmPolicyDecision data structure, and/or if online charging applies, the PCF shall include the "online" attribute set to "true" within the SmPolicyDecision data structure in the response of HTTP POST message. The default charging method provided by the PCF shall overwrite any predefined default charging method at the SMF. If the PCF has provided the default charging method, it shall not modify the default charing method in subsequent interactions.

4.2.2.4 Provisioning of revalidation time

The PCF may within the SmPolicyDecision data structure provide the revalidation time within the "revalidationTime" attribute and the RE_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute to instruct the SMF to trigger a PCF interaction to request PCC rule from the PCF.

The SMF shall start the timer based on the revalidation time and shall send the PCC rule request before the indicated revalidation time.

4.2.2.5 Policy provisioning and enforcement of authorized AMBR per PDU session

The SMF may include the subscribed AMBR per PDU session with the "subsSessAmbr" attribute within the SmPolicyContextData data structure as defined in subclause 4.2.2.2. The PCF shall authorize the session AMBR based on the operator's policy and provision the authorized session AMBR to the SMF in the response of the message as defined in subclause 4.2.6.3.1 and 4.2.6.3.2.

Upon receiving the authorized session AMBR, the SMF shall apply the corresponding procedures towards the access network, the UE and the UPF for the enforcement of the AMBR per PDU session.

4.2.2.6 Policy provisioning and enforcement of authorized default QoS

During the PDU session establishment as defined in subclause 4.2.2.2, the SMF may include the subscribed default QoS with the "subsDefQos" attribute. The PCF shall provision the authorized default QoS to the SMF in the response of the message as defined in subclause 4.2.6.3.1 and 4.2.6.3.2.

Upon receiving the authorized default QoS, the SMF enforces it which may lead to the change of the subscribed default QoS. The SMF shall apply the corresponding procedures towards the access network, the UE and the UPF for the enforcement of the authorized default QoS.

> NOTE 1: If dynamic PCC is not deployed, the SMF can have a DNN based configuration to enable the establishment of a GBR resource type default QoS flow. This configuration contains a standardized GBR 5QI as well as GFBR and MFBR for UL and DL.

> NOTE 2: GBR resource type is not applicable to the default QoS flow of the PDU session which is interworking with EPS.

4.2.2.7 Provisioning of PCC rule for Application Detection and Control

If the ADC feature is supported, and the user subscription indicates that the application detection and control is required, the PCF may provision PCC rule for application detection and control as defined in subclause 4.2.6.2.11 in the response message.

If the SMF receives the PCC rule for application detection and control, the SMF shall instruct the UPF as defined in 3GPP TS 29.244 [13] to detect the application traffic.

4.2.2.8 3GPP PS Data Off Support

When the 3GPP-PS-Data-Off feature as defined in subclause 5.8 is supported, and if the SMF is informed that the 3GPP PS Data Off status of the UE is set to active during the PDU session establishment, it shall include the "3gppPsDataOffStatus" attribute set to true within the SmPolicyContextData data structure in the HTTP POST message as defined in subclause 4.2.2.2.

If the PCF receives that HTTP POST message with a "3gppPsDataOffStatus" set to true as above and the access type of the PDU session indicated as "3GPP_ACCESS", the PCF shall configure the SMF to block any downlink and optionally uplink IP flows not relating to a service within the list of 3GPP PS Data Off Exempt Services, for instance by not installing any related dynamic PCC rule(s) or by not activating related predefined PCC rule(s) such as PCC rule(s) with wild-carded service data flow filters. The PCRF may also, subject to its normal policies, provide the PCC rule for service(s) from the list of 3GPP PS Data Off Exempt Service as defined in subclause 4.2.6.2.1.

> NOTE 1: The PCF can be configured with a list of 3GPP PS Data Off Exempt Services per DNN. The list of 3GPP PS Data Off Exempt Services for an DNN can also be empty, or can allow for any service within that DNN, according to operator policy.

> NOTE 2: For the PDU session used for IMS services, the 3GPP Data Off Exempt Services are enforced in the IMS domain as specified 3GPP TS 23.228 [16]. Policies configured in the PCF need to ensure that IMS services are allowed when the 3GPP Data Off status of the UE is set to activated, e.g. by treating any service within a well-known IMS DNN as 3GPP PS Data Off Exempt Services.

4.2.2.9 IMS Emergency Session Support

A SMF that requests PCC Rules at PDU Session Establishment shall send an HTTP POST message as defined in subclause 4.2.2.2 and the "dnn" attribute including the Emergency DNN. The SMF may include the SUPI within the "supi" attribute and if the SUPI is not available, the SMF shall include the PEI within the "pei". The SMF may include the rest of the attributes described in subclause 4.2.2.2. The SMF may also include the GPSI if available within the "gpsi" attribute.

The PCF shall detect that a PDU session is restricted to IMS Emergency services when the HTTP POST message is received and the "dnn" attribute includes a data network identifier that matches one of the Emergency DNs from the configurable list. The PCF:

- shall provision PCC Rules restricting the access to Emergency Services (e.g. P-CSCF(s), DHCP(s) and DNS (s) and SUPL(s) addresses) as required by local operator policies in a response message according to the procedures described in clause 4.2.6.

- may provision the authorized QoS that applies to the default QoS flow within the "authDefQos" attribute of a session rule according to the procedures described in subclause 4.2.8.4 except for obtaining the authorized QoS upon interaction with the UDR. The value for the "priorityLevel" attribute shall be assigned as required by local operator policies (e.g. if an IMS Emergency session is prioritized the "priorityLevel" attribute may contain a value that is reserved for an operator domain use of IMS Emergency sessions). If the "accessType" attribute is assigned to "3GPP_ACCESS" the values for "preemptCap" attribute and the "preemptVuln" attribute shall be assigned as required by local operator policies.

- may provision the authorized session AMBR in the response message according to the procedures described in clause 4.2.8.3.

When the SMF detects that the provisioning of PCC Rules failed, the PCC rule error handling procedure shall be performed.

4.2.2.10   Request Usage Monitoring Control

If the UMC as defined in subclause 5.8 is support, the PCF may provision the usage monitoring control policy to the SMF as defined in subclause 4.2.6.5.3.

4.2.2.11   Access Network Charging Identifier report

During the PDU session establishment, the SMF may provide the access network charging identifier information within the "accNetChId" attribute. Within the AccNetChId data structure, the SMF shall include the "accNetChaIdValue" containing the Access Network Charging Identifier for the default QoS flow and the "sessionChScope" attribute set to true if the Access Network Charging Identifier is applied to the whole PDU session. The SMF may provide the address of the network entity performing charging within the "chargEntityAddr" attribute.

NOTE: During the PDU Session Establishment no "refPccRuleIds" attribute is provided regardless if the charging identifier applies to the entire PDU session or to the default QoS flow since the PCC Rules are not yet authorized at this stage.

4.2.2.12   Request for the successful resource allocation notification

The PCF may request the SMF to confirm that the resources associated to a PCC rule are successfully allocated as defined in subclause 4.2.6.5.5.

4.2.2.13   Request of Presence Reporting Area Change Report

If the PRA feature as defined in subclause 5.8 is supported, the PCF may provision the Presence Reporting Area Information to the SMF as defined in subclause 4.2.6.5.6.

4.2.2.14   Provisioning of IP Index Information

If the PDU session type received within the "pduSessiontype" attribute is "IPv4" or "IPv6" or "IPv4v6", and no corresponding IP address/prefix is received, the PCF may within the SmPolicyDecision data structure include the IP index information within the "ipv4Index" attribute for IPv4 address allocation and/or "ipv6Index" attribute for IPv6 address allocation.

The SMF may use this to assist in selecting how the IP address is to be allocated when multiple allocation methods, or multiple instances of the same method are supported.

4.2.2.x   Negotiation of the QoS flow for IMS signalling

If the SMF includes the "qosFlowUsage" attribute required for the default QoS flow within the SmPolicyContextData data structure during the PDU session establishment procedure, the PCF shall provide the "qosFlowUsage" attribute back in the response with the authorized usage.

If during PDU session establishment procedure, the SMF includes the "IMS_SIG" value within the "qosFlowUsage" attribute and the PCF accepts that default QoS flow is dedicated to IMS signalling, the PCF shall within the SmPolicyDecision data structure include the "IMS_SIG" value within the "qosFlowUsage" attribute. In this case, the

PCF shall restrict the QoS flow to only be used for IMS signalling as specified in 3GPP TS 23.228 [16] by applying the applicable 5QI for IMS signalling.

If the SMF include the "IMS_SIG" value within the "qosFlowUsage" attribute of the SmPolicyContextData data structure, but the PCF does not include the "IMS_SIG" within the"qosFlowUsage" attribute of SmPolicyDecision data structure, the PCC Rules provided by the PCF shall have a 5QI value different from the 5QI value for the IMS signalling.

4.2.3 Npcf_SMPolicyControl_UpdateNotify Service Operation

4.2.3.1 General

The UpdateNotify service operation provides updated Session Management related policies to the NF service consumer (SMF) or triggers the deletion of the context of SM related policies. The POST method is used for both, update and delete operations.

The following procedures using the Npcf_SMPolicyControl_UpdateNotify service operation are supported:

- PCF initiated update of the policies associated with the PDU session.

- PCF initiated deletion of SM Policy Association of a PDU session.

- Provisioning of PCC rules.

- Provisioning of policy control request triggers.

- Provisioning of revalidation time.

- Policy provisioning and enforcement of authorized AMBR per PDU session.

- Policy provisioning and enforcement of authorized default QoS.

- Provisioning of PCC rule for Application Detection and Control.

- 3GPP PS Data Off Support.

- IMS Emergency Session Support.

- Request Access Network Information.

- Request Usage Monitoring Control.

- Request for the result of PCC rule removal.

- Access Network Charging Identifier request.

- Request for the successful resource allocation notification.

- IMS Restoration Support.

- P-CSCF Restoration Enhancement Support.

4.2.3.2 SM Policy Association Update request
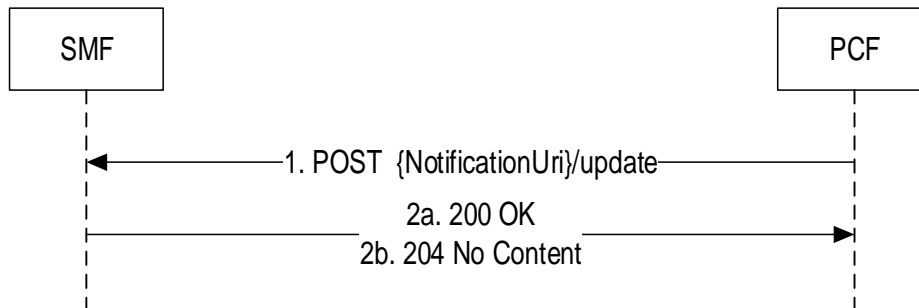
Figure 4.2.3.2-1: SM Policy Association Update request

The PCF may decide to provision policies without obtaining a request from the SMF, e.g. in response to information provided to the PCF via the Rx or N5 reference point, or in response to an internal trigger within the PCF. The PCF shall send a POST request to the NF Service Consumer (SMF) (../{NotificationUri}/update). The payload body of the message shall contain an SmPolicyNotification data structure that contains the representation of the updated policies within the "smPolicyDecision" attribute and the resource URI of individual SM Policy related to the notification within the "resourceUri" attribute. Detailed procedures related to the provisioning and enforcement of the policy decisions within the SmPolicyDecision data structure are contained in subclause 4.2.6.

In case of a successful update of SM policies:

- if the PCF provisioned the policy control request triggers related to access type change, RAT change or location change, a "200 OK" response code and a response body with the corresponding available information in the "UeCampingRep" data structure shall be returned in the response;

- otherwise, a "204 No Content" response code shall be returned in the response.

If errors occur when processing the HTTP POST request, the SMF shall apply error handling procedures as specified in subclause 5.7.

If the SMF received one or more PCC rules from the PCF but the validation of all the PCC Rules were unsuccessful, the SMF shall reject the request and include in an HTTP "400 Bad Request" response message the ErrorReport data sturcutre. Within the ErrorReport data structure, SMF shall include the "error" attribute containing the "cause" attribute of the ProblemDetails data structure set to "PCC_RULE_EVENT" or "PCC_QOS_FLOW_EVENT" and the "ruleReports" attribute to report the PCC rule status of affected PCC rules as defined in subclause 4.2.3.16.

If the SMF received one or more PCC rules from the PCF but the validation of some of them were unsuccessful, the SMF shall include an HTTP "200 OK" status code together with the one or more RuleReport data structure(s) to report the PCC rule status of affected PCC rules as defined in subclause 4.2.3.16 in the "PartialSuccessReport" data structure included in the response message. The "failureCause" attribute of the "PartialSuccessReport" shall be set to "PCC_RULE_EVENT" or "PCC_QOS_FLOW_EVENT". If the PCF provisioned policy control request triggers, the SMF may include in the "PartialSuccessReport" data structure the "ueCampingRep" attribute with the corresponding available information. When it is required to report multiple instances of the "PartialSuccessReport" data structure due to different "failureCause" values, the SMF shall use only one instance of the "PartialSuccessReport" data structure to include the ueCampingRep" attribute with the corresponding available information.

4.2.3.3 SM Policy Association termination request
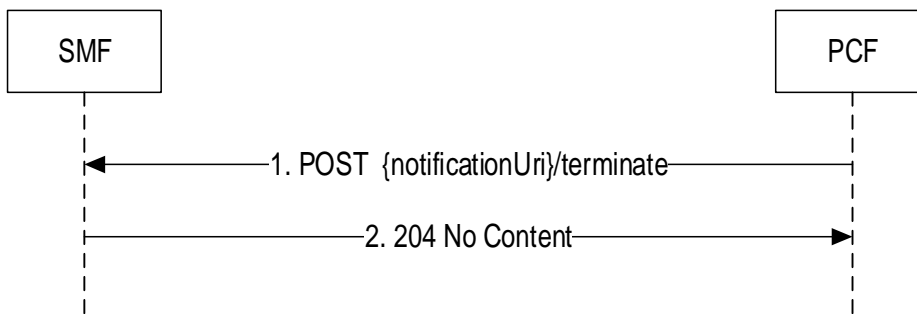
Figure 4.2.3.3-1: SM Policy Association termination request

The PCF may request the PDU session termination in the following instances:

- If the PCF decides to terminate a PDU session due to an internal trigger or trigger from the UDR.

- The PCF may also decide to terminate an PDU session upon receiving POST message from the SMF (e.g. when usage quota reached).

The PCF shall send a POST request to the NF Service Consumer (SMF) (../{NotificationUri}/terminate) and include the TerminationNotification data structure in the body of the HTTP POST request. Within the TerminationNotification data structure, the PCF shall include the resource URI of the individual SM policy related to the notification within the "resourceUri" attribute and the cause why the PCF requests the termination of the policy association encoded as "cause" attribute.

If the SMF accepted received POST request the SMF shall send "204 No Content" response.

After the succesfull processing of the HTTP POST request, the SMF shall invoke the Npcf_SMPolicyControl_Delete Service Operation defined in subclause 4.2.5 to terminate the policy association and initiate the procedure to terminate the PDU session as defined in 3GPP TS 29.502 [22].

If errors occur when processing the HTTP POST request, the SMF shall apply error handling procedures as specified in subclause 5.7.

4.2.3.4 Provisioning of revalidation time

During the lifetime of the PDU session, within the SmPolicyDecision data structure, the PCF may provide the revalidation time within the "revalidationTime" attribute and the RE_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute to instruct the SMF to trigger a PCF interaction to request PCC rule from the PCF if not provided yet. The PCF may also update the revalidation time by including the new value within the "revalidationTime" attribute. The PCF may disable the revalidation function by removing RE_TIMEOUT policy control request trigger if it has been provided.

If the SMF receives revalidation time or new revalidation time, the SMF shall store the received value and start the timer based on it. Then the SMF shall send the PCC rule request before the indicated revalidation time.

If the RE_TIMEOUT policy control request trigger is removed, SMF shall stop the timer for revalidation.

4.2.3.5 Policy provisioning and enforcement of authorized AMBR per PDU session

The PCF may modify the authorized session AMBR at any time during the lifetime of the PDU session and provision it to the SMF by invoking the procedure as defined in subclause 4.2.3.2. The PCF shall provision the new authorized session AMBR to the SMF in the response of the message as defined in subclause 4.2.6.2.1 and 4.2.6.2.2.

Upon receiving the authorized session AMBR, the SMF shall apply the corresponding procedures towards the access network, the UE and the UPF for the enforcement of the AMBR per PDU session.

For UL Classifier or Multi-homing PDU Session, the SMF will provision the policies of session-AMBR for downlink and uplink direction to the UL Classifier/Branching Point functionality and in addition provision the policies of session-AMBR in the downlink direction to all the PDU session anchors as defined in subclause 5.4.4 of 3GPP TS 29.244 [13].

4.2.3.6 Policy provisioning and enforcement of authorized default QoS

The PCF may modify the authorized default QoS during the lifetime of the PDU session and provision it to the SMF by invoking the procedure as defined in subclause 4.2.3.2. The PCF shall provision the authorized default QoS to the SMF in the response of the message as defined in subclause 4.2.6.3.1 and 4.2.6.3.2.

Upon receiving the authorized default QoS, the SMF enforces it which may lead to the change of the subscribed default QoS. The SMF shall apply the corresponding procedures towards the access network, the UE and the UPF for the enforcement of the authorized default QoS.

4.2.3.7 Provisioning of PCC rule for Application Detection and Control

If the ADC feature is supported, and the user subscription indicates that the application detection and control is required, the PCF may provision PCC rule for application detection and control as defined in subclause 4.2.6.2.11 in the HTTP POST request.

If the SMF receives the PCC rule for application detection and control, the SMF shall instruct the UPF as defined in 3GPP TS 29.244 [13] to detect the application traffic.

4.2.3.8 3GPP PS Data Off Support

When the PCF receives service information from the AF while the 3GPP PS Data Off handling functionality is active, the PCF shall check whether the corresponding service is a 3GPP PS Data Off Exempt Service and permissible according to the user´s subscription and the policies of the PCF. If so, the PCF shall install, modify or delete corresponding PCC rules. Otherwise, the PCF shall reject the service information from the AF.

If the PCF determines that the 3GPP PS Data Off handling functionality becomes inactive, the PCF shall perform policy control decision and provision the PCC rules to make sure that services are allowed according to the user's subscription and operator policy (irrespective of whether they belong to the list of 3GPP PS Data Off Exempt Services).

> NOTE: The PCF can then open gates via the "flowStatus" attribute for active PCC associated to services not within the list 3GPP PS Data Off Exempt Services. The PCF can also install PCC rules or activate predefined PCC rules for some services not belonging to the list 3GPP PS Data Off Exempt Services. If the PCF activates or installs a PCC rule with wildcarded filters, it can remove or de-activate PCC rules for 3GPP PS Data Off Exempt Services that are made redundant by this PCC rule.

4.2.3.9 IMS Emergency Session Support

4.2.3.9.1 Provisioning of PCC rule

When the PCF receives IMS service information from the AF for an Emergency service and derives authorized PCC Rules from the service information, the "priorityLevel" attribute, the "preemptCap" attribute and the "preemptVuln" attribute in the ARP within the QoS data decision which the PCC Rule refers to shall be assigned a priority and pre-emption as required by local operator policies (e.g. if an IMS Emergency session is prioritized the "priorityLevel" attribute may contain a value that is reserved for an operator domain use of IMS Emergency session).

The PCF shall immediately initiate the procedure as described in clause 4.2.6.2.1 to provision PCC Rules and the procedures described in clause 4.2.6.2.3 to provision the authorized QoS per service data flow.

The provisioning of PCC Rules at the SMF that require the establishment of a dedicated QoS flow for emergency services shall cancel the inactivity timer in the SMF, if it started running as defined in the subclause 4.2.3.9.2.

Any SMF-initiated request for PCC Rules for an IMS Emergency servicewith the "repPolicyCtrlReqTriggers" attribute containing the "RES_MO_RE" value (i.e. UE-initiated resource reservation) shall be rejected by the PCF with an appropriate status code.

The SMF shall execute the procedures to ensure that a new QoS flow is established for the Emergency service.

When the SMF detects that the provisioning of PCC Rules failed, the PCC rule error handling procedure shall be performed.

4.2.3.9.2 Removal of PCC Rules for Emergency Services

The reception of a request to terminate an AF session for an IMS Emergency service by the PCF triggers the removal of PCC Rules assigned to the terminated IMS Emergency Service from the SMF by using the procedure as defined in subclause 4.2.6.2.1 to removed PCC Rules.

At reception of an HTTP POST message that removes one or several PCC Rules from an PDU Session restricted to emergency services the SMF shall:

- when all PCC Rules bound to a QoS flow are removed, initiate a QoS flow termination procedure.

- when not all PCC Rule bound a QoS flow are removed, initiate an QoS flow modification procedure.

In addition, the SMF shall initiate an inactivity timer if all PCC Rules with a 5QI other than the 5QI of the default QoS flow or the 5QI used for IMS signalling were removed from the PDU session restricted to Emergency Services (e.g., to enable PSAP Callback session). When the inactivity timer expires, the SMF shall initiate a PDU session termination procedure as defined in clause 4.2.3.3.

4.2.3.10 Request of Access Network Information

If the NeLoc as defined in subclause 5.8 is supported, the PCF may request the SMF to report the access network information as defined in subclause 4.2.6.5.4.

4.2.3.11 Request Usage Monitoring Control

If the UMC as defined in subclause 5.8 is supported, the PCF may provision the usage monitoring control policy to the SMF as defined in subclause 4.2.6.5.3 to request the usage monitoring control.

4.2.3.12 Ipv6 Multi-homing support

During the lifetime of the Multi-homing PDU session, the PCF shall provision the PCC rules and session rules to SMF. The SMF shall derive the appropriate policies based on the policies provisioned by the PCF and provision them to the appropriate UPF if applicable, access network, if applicable, and UE if applicable.

4.2.3.13 Request for the result of PCC rule removal

If the RAN-NAS-Cause feature is supported, the PCF may request the SMF to inform it of the result of the PCC rule removal when the PCF removes the PCC rule as defined in subclause 4.2.6.5.2.

When the SMF receives the request, the SMF shall maintain locally the removed PCC rules until it receives of the resource release outcome from the network.

4.2.3.14 Access Network Charging Identifier request

The PCF may request the SMF to provide the Access Network Charging Identifier associated to the dynamic PCC rules as defined in subclause 4.2.6.4.1.

4.2.3.15 Request for the successful resource allocation notification

The PCF may request the SMF to confirm that the resources associated to a PCC rule are successfully allocated as defined in subclause 4.2.6.5.5.

4.2.3.16 PCC Rule Error Report

If the SMF receives one or more PCC rules as defined in subclause 4.2.3.1 but the validation of all the PCC Rule was unsuccessful, the SMF shall reject the request and include an HTTP "400 Bad Request" status code and the "ruleReports" attribute for the affected PCC rules to report the failure within the ErrorReport data structure; otherwise if the validation of some of PCC rules was unsuccessful, the SMF shall include an HTTP "200 OK" status code and one or more RuleReport data structure(s) for the affected PCC rules to report the failure within the PartialSuccessReport data structure in the response message. Within each RuleReport instance, the SMF shall identify the failed PCC rule(s) by including the affected PCC rules within the "pccRuleIds" attribute(s), identify the failed reason code by including a "failureCode" attribute, and shall include rule status within the "ruleStatus" attribute with the value as described below.

If the installation/activation of one or more new PCC rules (i.e. rules which were not previously successfully installed) fails, the SMF shall set the "ruleStatus" to INACTIVE.

If the modification of a currently active PCC rule fails, the SMF shall retain the existing PCC rule as active without any modification unless the reason for the failure has an impact also on the existing PCC rule.

The removal of a PCC rule shall not fail, even if the PDU session procedures with the UE fail. The SMF shall retain information on the removal and conduct the necessary PDU session procedures with the UE when it is possible.

Depending on the value of the "failureCode" attribute, the PCF may decide whether retaining of the old PCC rule, re-installation, modification, removal of the PCC rule or any other action applies.

If the "RuleVersioning" feature is supported and the PCF included the "contVer" attribute for a specific PCC rule instance in the "pccRules" attribute, then if the resource allocation for the corresponding PCC rule was unsuccessful, the SMF shall include the "contVers" attribute for the corresponding RuleReport instance included in the "ruleReports" attribute. Depending on the value of the "failureCode" attribute, and when applicable, depending also on the value of the "contVer" attribute, the PCF may decide whether retaining of the old PCC rule, re-installation, modification, removal of the PCC rule or any other action applies.

4.2.3.17 IMS Restoration Support

In order to support IMS Restoration procedures (refer to 3GPP TS 23.380 [21]), PCF needs to convey the AF address to the SMF. In order to do so, in case AF provisions information about the AF signalling flows between the UE and the AF, as defined in 3GPP TS 29.214 [18] subclause 4.4.5a, the PCF shall install the corresponding dynamic PCC rules (if not installed before) as defined in subclause 4.2.6.2.1. The PCF shall within the PccRule instance include the signalling flows between UE and the AF within the "flowInfos" attribute and the "afSigProtocol" attribute set to the value corresponding to the signalling protocol used between the UE and the AF.

The SMF shall respond with "204 no content" to the PCF and initiate the corresponding QoS flow procedure if required. The SMF shall extract the AF address from the PCC rules and use it for the monitoring procedure as defined for the different access types.

   NOTE 1: The SMF can use the extracted AF address from the PCC rule to check if, the monitoring procedure has to be started for the corresponding AF.

In case AF de-provisions information about the AF signalling flows between the UE and the AF, as defined in 3GPP TS 29.214 [18] subclause4.4.5a, the PCF shall remove the corresponding dynamic PCC rules by triggering an HTTP POST message. The PCF shall apply the procedure as defined in subclause 4.2.6.2.1.

The SMF shall send a HTTP response message to the PCF.

NOTE 2: The SMF can use the AF address associated with the removed rule to check if it can stop monitoring the corresponding AF.

4.2.3.18 P-CSCF Restoration Enhancement Support

This subclause is applicable when the PCF-based P-CSCF Restoration Enhancement, as defined in 3GPP TS 23.380 [21], is supported by both PCF and SMF.

If the PCF receives a request for P-CSCF restoration from the P-CSCF as defined in subclause 4.4.7 of 3GPP TS 29.214 [18], the PCF shall send an HTTP POST meessage including the "pcscfRestIndication" attribute set to true to the SMF for the corresponding PDU session.

The SMF shall acknowledge to the PCF and shall initiate the corresponding QoS flow procedure for the IMS PDU connection as defined in 3GPP TS 23.380 [21].

4.2.3.19 Request of Presence Reporting Area Change Report

If the PRA feature as defined in subclause 5.8 is supported, the PCF may provision the Presence Reporting Area Information to the SMF as defined in subclause 4.2.6.5.6.

4.2.4 Npcf_SMPolicyControl_Update Service Operation

4.2.4.1 General

The Npcf_SMPolicyControl_Update service operation provides means for the NF service consumer to inform the PCF that a policy control request trigger condition has been met and for the PCF to inform the NF service consumer of any resulting update of the Session Management related policies.

The following procedures using the Npcf_SMPolicyControl_Update service operation are supported:

- Provisioning of PCC rules.

- Provisioning of policy control request triggers.

- Request the policy based on revalidation time.

- Policy provisioning and enforcement of authorized AMBR per PDU session.

- Policy provisioning and enforcement of authorized default QoS.

- Application detection information reporting.

- Indication of QoS Flow Termination Implications.

- 3GPP PS Data Off Support.

- Requst and report Access Network Information.

- Request Usage Monitoring Control and report Accumulated Usage.

- Ipv6 Multi-homing support.

- Request and report the result of PCC rule removal.

- Access Network Charging Identifier Request and report.

- Request and report the successful resource allocation notification.

- Negotiation of the QoS flow for IMS signalling.

- Notification about Service Data Flow QoS target enforcement.

4.2.4.2 Requesting the update of the Session Management related policies
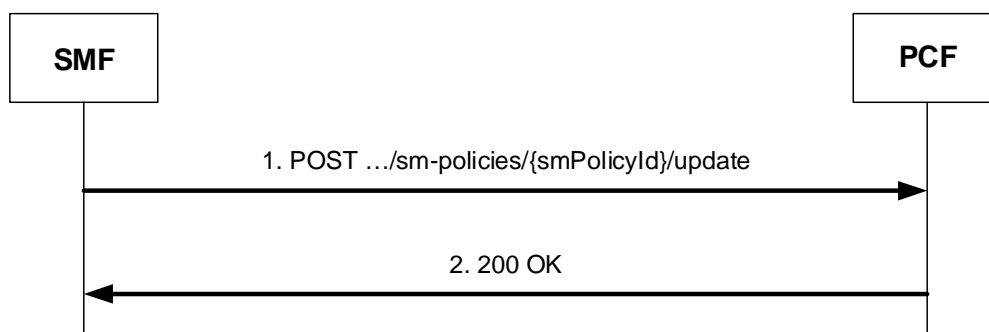
Figure 4.2.4.2-1: Requesting the update of the Session Management related policies

When the SMF detects that one or more policy control request triggers are met, the SMF shall send a POST request to the PCF to update an Individual SM Policy resource. The {smPolicyId} in the URI identifies the Individual SM Policy resource to be updated. The SMF include SmPolicyUpdateContextData data structure in the payload body of the HTTP POST to request a update of representation of the "Individual SM Policy" resource. The SMF shall include the met policy control request trigger(s) within the "repPolicyCtrlReqTriggers" attribute and applicable updated value(s) in the corresponding attribute(s).

The SMF shall include (if available) in SmPolicyUpdateContextData data structure:

- type of access within the "accessType" attribute;

- type of the radio access technology within the "ratType" attribute;

- the new allocated UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "ipv6AddressPrefix" attribute;

- the released UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "relIpv6AddressPrefix" attribute;

- the UE MAC address within the "ueMac" attribute;

- the released UE MAC address within the "relUeMac" attribute;

- the indication of UE supporting reflective QoS within the "refQosIndication" attribute;

- access network charging identifier within the " accNetChIds" attribute;

- 3GPP PS data off status within the "3gppPsDataOffStatus" attribute;

- the UE time zone information within the "ueTimeZone" attribute;

- subscribed Session-AMBR within the "subsSessAmbr" attribute;

- subscribed Default QoS Information within the "subsDefQos" attribute;

- detected application information within the "appDetectionInfos" attribute;

- accumulated usage reports within the "accuUsageReports" attribute;

- reported presence reporting area information within the "praInfos" attribute;

- the QoS flow usage required of the default QoS flow within the "qosFlowUsage" attribute;

- indication whether the QoS targets of one or more SDFs are not guaranteed or guaranteed again with the "qncReports" attribute;

- user location information within the "userLocationInfo" attribute; and

- identifier of the serving network within the "servingNetwork" attribute.

In case of a successful update, "200 OK" response shall be returned. The PCF shall include in the "200 OK" response the representation of the updated policies within the SmPolicyDecision data structure. Detailed procedures related to the provisioning and enforcement of the policy decisions within the SmPolicyDecision data structure are contained in subclause 4.2.6.

If errors occur when processing the HTTP POST request, the PCF shall apply error handling procedures as specified in subclause 5.7.

If the PCF is, due to incomplete, erroneous or missing information (e.g. QoS, RAT type, subscriber information) not able to provision a policy decision as response to the request for PCC rules by the SMF, the PCF may reject the request and include in an HTTP "400 Bad Request " response message the "cause" attribute of the ProblemDetails data structure set to "INITIAL_PARAMETERS".

If the PCF receives the set of session information which is sent in the message originated due to a trigger being met is incoherent with the previous set of session information for the same session (E.g. trigger met was RAT changed, and the RAT notified is the same as before), the PCF may reject the request and include in an HTTP "400 Bad Request" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR_TRIGGER_EVENT".

If the PCF detects that the packet filters in the request for new PCC rules received from the SMF is covered by the packet filters of outstanding PCC rules that the PCF is provisioning to the SMF, the PCF may reject the request and include in an HTTP "403 Forbidden" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR_CONFLICTING_REQUEST".

If the PCF does not accept one or more of the traffic mapping filters provided by the SMF in an HTTP POST request (e.g. because the PCF does not allow the UE to request enhanced QoS for services not known to the PCF), the PCF shall reject the request and include in an HTTP "403 Forbidden" response message the "cause" attribute of the ProblemDetails data structure set to "ERROR_TRAFFIC_MAPPING_INFO_REJECTED".

If the SMF receives HTTP response with these codes, the SMF shall reject the PDU session modification that initiated the HTTP Request.

The PCF shall not combine a rejection with provisioning of PCC rule operations in the same HTTP response message.

4.2.4.3 Request the policy based on revalidation time

If the timer for the policy revalidation is started, the SMF shall send the PCC rule request before the indicated revalidation time. The SMF shall within the SmPolicyUpdateContextData data structure include RE_TIMEOUT within the "repPolicyCtrlReqTriggers" attribute. The SMF shall stop the timer once the SMF sends the request.

NOTE 1: The PCF is expected to be prepared to provide a new policy, as desired for the revalidation time, during a preconfigured period before the revalidation time. The preconfigured periods in the SMF and PCF need to be aligned.

The PCF may provide a new value of revalidation time by including "revalidationTime" attribute within the SmPolicyDecision in the response. The PCF may disable the revalidation function by removing the RE_TIMEOUT policy control request trigger in the response.

When the SMF receives the response message, the SMF shall start the timer for revalidation based on the new value or existing value of revalidation time if the revalidation function is not disabled; otherwise, the SMF shall not start the timer for revalidation.

NOTE 2: By removing the RE_TIMEOUT the revalidation time value previously provided to the SMF is not applicable anymore.

4.2.4.4 Policy provisioning and enforcement of authorized AMBR per PDU session

When the SMF detects that the subscribed session AMBR change, the SMF shall notify of the PCF by invoking the procedure as defined in subclause 4.2.4.2, include the new subscribed session AMBR within the "subsSessAmbr" attribute and the SE_AMBR_CH policy control request trigger within the "repPolicyCtrlReqTriggers". Upon receiving the change of session AMBR, the PCF shall provision the new authorized session AMBR to the SMF in the response as defined in subclause 4.2.6.2.1 and 4.2.6.2.2.

Upon receiving the authorized session AMBR, the SMF shall apply the corresponding procedures towards the access network, the UE and the UPF for the enforcement of the AMBR per PDU session.

For UL Classifier or Multi-homing PDU Session, the SMF will provision the policies of session-AMBR for downlink and uplink direction to the UL Classifier/Branching Point functionality and in addition provision the policies of session-AMBR in the downlink direction to all the PDU session anchors as defined in subclause 5.4.4 of 3GPP TS 29.244 [13].

4.2.4.5 Policy provisioning and enforcement of authorized default QoS

When the SMF detects that the subscribed default QoS change, the SMF shall notify of the PCF by invoking the procedure as defined in subclause 4.2.4.2, include the new subscribed default QoS within the "subsDefQos" attribute and "repPolicyCtrlReqTriggers" set to DEF_QOS_CH. Upon receiving the change of default QoS, the PCF shall provision the authorized default QoS to the SMF in the response of the message The PCF shall provision the authorized default QoS to the SMF in the response of the message as defined in subclause 4.2.6.3.1 and 4.2.6.3.2.

Upon receiving the authorized default QoS, the SMF enforces it which may lead to the change of the subscribed default QoS. The SMF shall apply the corresponding procedures towards the access network, the UE and the UPF for the enforcement of the authorized default QoS.

4.2.4.6 Application detection information reporting

If the ADC feature is supported and if the SMF receives the PCC rule for application detection and control, the SMF shall instruct the UPF as defined in 3GPP TS 29.244 [13] to detect the application traffic. When the start of the application`s traffic, identified by an application identifier, is received from the UPF, if PCF has previously provisioned the APP_STA/APP_STO policy control request trigger, unless a request to mute such a notification (i.e. the "muteNotif" attribute set to true within the Traffic Control Data decision which the PCC rule refers to), the SMF shall report the start of the application to the PCF. In order to do so, the SMF shall perform the procedure as defined in subclause 4.2.4.1 by including the information regarding the detected application`s traffic within the "appDetectionInfo" attribute and the "APP_STA" within the "repPolicyCtrlReqTriggers" attribute even if the application traffic is discarded due to enforcement actions of the PCC rule. In this case, within the "appDetectionInfo" attribute, the SMF shall include the corresponding application identifier within the "appId" attribute, may include the detected service data flow description within the "sdfDescriptions" attribute and application instance identifier within the "instanceId" if deducible. The "sdfDescriptions" attribute, if present, shall contain the "flowDescription" attribute and "flowDirection" attribute. The application instance identifier, which is dynamically assigned by the SMF in order to allow correlation of APP_STA and APP_STO policy control request trigger to the specific service data flow descriptions.

When the stop of the application's traffic, identified by an application identifier is received from the UPF and the SMF has reported the start of the application to the PCF, the SMF shall report the stop of the application to the PCF. In order to do so, the SMF shall perform the procedure as defined in subclause 4.2.4.1 by including the including the information regarding the detected application`s traffic within the "appDetectionInfo" attribute and the "APP_STO" within the "repPolicyConReqTriggers" attribute. For "appDetectionInfo" attribute, the PCF shall include the corresponding application identifier within the "appId" attribute and application instance identifier within the "instanceId" if it is provided along with the APP_STA.

The PCF then may make policy decisions based on the information received and send the corresponding updated PCC rules to the SMF.

4.2.4.7 Indication of QoS Flow Termination Implications

When the SMF detects that a dedicated QoS flow could not be activated or has been terminated it shall remove the affected PCC rules and send an HTTP POST request to the PCF with an SmPolicyUpdateContextData data structure, including the "ruleReports" attribute containing the RuleReport data instance which specifies the affected PCC rules within the "pccRuleIds" attribute(s), "INACTIVE" as the value within the "ruleStatus" attribute and the "RES_ALLO_FAIL" as the value of the "failureCode" attribute.

If the RAN-NAS-Cause feature is supported, the SMF shall provide the available access network information within the "userLocationInfo" attribute (if available), "userLocationInfoTime" attribute (if available) and "ueTimezone" attribute (if available). Additionally, if the SMF receives from the access network the RAN cause and/or the NAS cause due to QoS flow termination the SMF shall provide the received cause(s) in the "ranNasRelCauses" attribute included in RuleReport data instance.

This shall be done whenever one of these conditions applies:

- The SMF is requested by the RAN to initiate the deactivation of a QoS flow,

- PCC rule(s) are removed/deactivated by the SMF without PCF request (e.g. due to unsuccessful reservation of resources to satisfy the QoS flow binding).

NOTE: The SMF will not initiate the deactivation of the QoS flow upon reception of the UE-initiated resource modification procedure indicating packet filter deletion. If all the PCC rules associated to a QoS flow have been deleted as a consequence of the PCF interaction, the SMF will initiate the QoS flow termination procedure towards the RAN.

Signalling flows for the QoS flow termination and details of the binding mechanism are presented in 3GPP TS 29.513 [7].

4.2.4.8 3GPP PS Data Off Support

If the SMF is informed that the 3GPP PS Data Off status of the UE changes, the SMF shall provide the PS_DA_OFF value within the "repPolicyCtrlReqTriggers" attribute and the "3gppPsDataOffStatus" attribute set to the value indicated by the UE within "SmPolicyUpdateContextData" and send the HTTP POST message as defined in subclause 4.2.4.2 to the PCF.

Upon receipt of an HTTP POST message with the "repPolicyCtrlReqTriggers" attribute with the value PS_DA_OFF or the AC_TY_CH the PCF shall determine whether the 3GPP PS Data Off handling functionality (as described below) becomes active or inactive. The 3GPP PS Data Off handling functionality is active if, and only if,

- the latest received "3gppPsDataOffStatus" attribute is set to true, and

NOTE 1: If the 3GPP_PS_DATA_OFF_CH policy control request trigger is received, the latest received value is the one received in the HTTP POST message. Otherwise, it corresponds to the stored value.

- the UE uses an access with "accessType set to "3GPP_ACCESS ".

If the PCF determines that the 3GPP PS Data Off handling functionality becomes active, the PCRF shall configure the SMF in such a way that:

- only packets for services belonging to the list of 3GPP PS Data Off Exempt Services are forwarded; and

- all other downlink packets and optionally uplink packets are discarded by modifying or removing any related dynamic PCC rule(s) or by deactivating any related predefined PCC rule(s).

NOTE 2: In order for the UPF to prevent the services that do not belong to the list of 3GPP PS Data Off Exempted Services, if such services are controlled by dynamic PCC rules, PCF can either close gates for the downlink and optionally the uplink direction via the "flowStatus" attribute in related dynamic PCC rules or remove those dynamic PCC rules. If the services are controlled by predefined PCC rules, PCF needs to deactivate those PCC rules. PCC rule(s) with wild-carded service data flow filters can be among the PCC rules that are modified, Removed or disabled in that manner. It can then be necessary that the PCF at the same time installs or activates PCC rules for data-off exempt services. The network configuration can ensure that at least one PCC Rule is bound to the default QoS flow when Data Off is activated in order to avoid a deletion of an existing PDU session or in order to not fail a PDU session establishment.

4.2.4.9 Request and Report of Access Network Information

If the NeLoc as defined in subclause 5.8 is supported, the PCF may request the SMF to report the access network information as defined in subclause 4.2.6.5.4.

If the AN_INFO policy control request rigger is set, upon receiving the "lastReqRuleData" attribute with the "reqData" attribute with the value(s) MS_TIME_ZONE and/or USER_LOC_INFO together with installation, modification and removal of any PCC rule(s), the SMF shall apply appropriate procedures to obtain this information. When the SMF then receives access network information through those procedures, the SMF shall provide the required access network information to the PCF by as defined in subclause 4.2.4.1 and set the corresponding attributes as follows:

- If the user location information was requested by the PCF and was provided to the SMF, the SMF shall provide the user location information within the "userLocationInfo" attribute and the time when it was last known within "userLocationInfoTime" attribute (if available).

- If the user location information was requested by the PCF and was not provided to the SMF, the SMF shall provide the serving PLMN identifier within the "servingNetwork" attribute.

- If the time zone was requested by the PCF, the SMF shall provide it within the "ueTimeZone" attribute.

In addition, the SMF shall provide the AN_INFO policy control request trigger within the "repPolicyCtrlReqTriggers" attribute.

During QoS flow deactivation, when the NetLoc feature is supported, the SMF shall provide the access network information to the PCF by including the user location information within the "userLocationInfo" attribute (if requested by the PCF and if provided to the SMF), the information on when the UE was last known to be in that location within "userLocationInfoTime" attribute (if user location information was requested by the PCF and if the corresponding information was provided to the SMF), the PLMN identifier within the "servingNetwork" attribute (if the user location information was requested by the PCF but it is not provided to the SMF) and the timezone information within the "ueTimeZone" attribute (if requested by the PCF and available).

During PDU session termination procedure, the SMF shall, if AC_INFO policy control request trigger is set, provide the access network information to the PCF by including the user location information within the "userLocationInfo" attribute (if it was provided to the SMF), the information on when the UE was last known to be in that location within "userLocationInfoTime" attribute (if it was provided to the SMF), the PLMN identifier within the "servingNetwork" attribute (if the user location information was not provided to the SMF) and the timezone information within the "ueTimeZone" attribute (if available).

The SMF shall not report any subsequent access network information updates received from the RAN without any further provisioning or removal of related PCC rules unless the associated QoS flow bearer or PDU session has been released.

4.2.4.10 Request Usage Monitoring Control and Reporting Accumulated Usage

If the UMC as defined in subclause 5.8 is supported, the PCF may provision the usage monitoring control policy to the SMF as defined in subclause 4.2.6.5.3 to request the usage monitoring control.

When the SMF receives the accumulated usage report from the UPF as defined in subclause 7.5.5.2, 7.5.7.2 or 7.5.8.3 of 3GPP TS 29.244 [13], the SMF shall send an HTTP POST message as defined in subclause 4.2.4.2 by including one or more accumulate usage reports within the "accuUsageReports" attribute(s).

When the PCF receives the accumulated usage in the HTTP POST message, the PCF shall indicate to the SMF if usage monitoring shall continue for usage monitoring control instance as follows:

- If monitoring shall continue for specific level(s), the PCF shall provide the new thresholds for the level(s) in the response of HTTP POST message using the same attribute as before (i.e. "volumeThreshold attribute", "volumeThresholdUplink" attribute or "volumeThresholdDownlink" attribute; "nextVolThreshold attribute", "nextVolThresholdUplink", "nextVolThresholdDownlink", or "nextTimeThreshold" if monitoring time is provided within an entry of the "umDecs" attribute);

- otherwise, if the PCF wishes to stop monitoring for specific level(s) the PCF shall not include an updated threshold in the response of HTTP POST message for the stopped level(s) i.e. the corresponding "volumeThreshold" attribute, "volumeThresholdUplink" attribute or "volumeThresholdDownlink" attribute shall not be included within an entry of the "umDecs" attribute.

If both volume and time thresholds were provided and the threshold for one of the measurements is reached, the SMF shall report this event to the PCF and the accumulated usage since last report shall be reported for both measurements.

The PCF shall process the usage reports and shall perform the actions as appropriate for each report.

4.2.4.11   Ipv6 Multi-homing support

The SMF may insert an additional PDU Session Anchor to an existing PDU session by using Ipv6 multi-homing mechanism. In this case, the SMF shall inform the PCF when a new Ipv6 prefix is allocated to the new PDU Session Anchor as defined in subclause 4.2.4.2. The SMF shall, within the SmPolicyUpdateContextData data structure, include the "UE_ IP_CH" within the "repPolicyCtrlReqTrigger" attribute and include the new Ipv6 prefix within the "ipv6AddressPrefix" attribute.

When the PCF receives the request from the SMF indicating the addition of a new Ipv6 prefix, the PCF shall determine the impacted PCC rules and/or session rules associated with the new Ipv6 prefix and provision them to the SMF as defined in subclause 5.6.2.6 and 5.6.2.7. The SMF shall derive the appropriate policies based on the policies provisioned by the PCF and provision them to the appropriate UPF, if applicable, access network, if applicable, and UE, if applicable.

When the SMF removes a PDU Session anchor from the Multi-homing PDU session, the SMF shall inform the PCF of the released Ipv6 prefix related to the PDU Session anchor as defined in subclause 4.2.5.2. The SMF shall, within the SmPolicyUpdateContextData data structure, include the "UE_ IP_CH" within the "repPolicyConReqTrigger" attribute and include the released Ipv6 prefix within the "relIpv6AddressPrefix" attribute.

4.2.4.12   Request and report for the result of PCC rule removal

If the RAN-NAS-Cause feature is supported, the PCF may request the SMF to inform it of the result of the PCC rule removal when the PCF removes the PCC rule as defined in subclause 4.2.6.5.2.

When the SMF receives the request, the SMF shall maintain locally the removed PCC rules until it receives of the resource release outcome from the network.

The SMF shall notify the PCF by include the "RES_RELEASE" within the "repPolicyCtrlReqTrigger" attribute and the affected rules indicated within one instance of the "ruleReports" attribute with the "ruleStatus" attribute set to the value INACTIVE.

If the the QoS flow is terminated as a consequence of the removal of one or more PCC rules, the SMF shall inform the PCF about the completion of the QoS flow procedure related to the removal of PCC rules that indicated resource release notification by including the RequestedRuleData instance containing the "reqData" attribute with the RES_RELEASE referring to the PCC rule. If the SMF received from the access network some RAN/NAS release cause(s), the SMF shall also provide the received cause(s) in the "ruleReports" attribute. The SMF shall also provide the available access network information within the "userLocationInfo" attribute (if available), "userLocationInfoTime" attribute (if available) and "ueTimezone" attribute (if available).

4.2.4.13   Access Network Charging Identifier request and report

If the "PolicyCtrlReqTriggers" attribute with the value "AN_CH_COR" has been provided to the SMF, the SMF shall notify of the PCF the Access Network Charging Identifier(s) that the SMF has assigned for the dynamic PCC Rules which referred from the RequestedRuleData data structure containing the CH_ID within the "reqData" attribute by including an "accNetChIds" attribute within the SmPolicyUpdateContextData data structure in the HTTP POST message. If the SMF assigns a Access Network Charging Identifier to the whole PDU session, the SMF shall include one AccNetChId instance within the "accNetChIds" attribute and include the Access Network Charging Identifier within the "accNetChaIdValue" attribute and the "sessionChScope" attribute set to true; otherwise, within each

AccNetChId instance, the PCF shall include Access Network Charging Identifier within the "accNetChaIdValue" attribute and all the PCC rule identifier(s) associated to the provided Access Network Charging Identifier within the "refPccRuleIds" attribute.

The PCF may request the SMF to provide the Access Network Charging Identifier associated to the new dynamic PCC rules as defined in subclause 4.2.6.4.1 in the response message.

4.2.4.14 Request and report for the successful resource allocation notification

The PCF may request the SMF to confirm that the resources associated to a PCC rule are successfully allocated as defined in subclause 4.2.6.5.5.

If the "PolicyCtrlReqTriggers" attribute with the value "SUCC_RES_ALLO" has been provided to the SMF, the SMF shall notify of the PCF the resources associated to the PCC rules which referred from the RequestedRuleData data structure containing the "SUCC_RES_ALLO" within the "reqData" attribute are successfully allocated. When the SMF received successful resource allocation response from the access network, the SMF shall within the SmPolicyUpdateContextData data structure include the "SUCC_RES_ALLO" within the "repPolicyCtrlReqTriggers" attribute and "ruleReports" attribute. Within the RuleReport instance, the SMF shall include the corresponding PCC rule identifier(s) within the "pccRuleIds" attribute and the "ruleStatus" attribute set to value "ACTIVE".

If the "RuleVersioning" feature is supported and the PCF included the "contVer" attribute for a specific PCC rule instance, and the resource allocation was successful for this PCC rule, the SMF shall include the rule content version within the "contVers" attribute in the corresponding RuleReport instance.

4.2.4.15 PCC Rule Error Report

If the installation/activation of one or more PCC rules fails using the procedure as defined in subclause 4.2.2.1 or 4.2.4.1 or the PCF installed, activated or modified one or more PCC rules as defined in subclause 4.2.3.1 but resource allocation for the PCC Rule was unsuccessful, the SMF shall include the "ruleReports" attribute for the affected PCC rules to report the failure within the SmPolicyUpdateContextData data structure. Within each RuleReport instance, the SMF shall identify the failed PCC rule(s) by including the affected PCC rules within the "pccRuleIds" attribute(s), identify the failed reason code by including a "failureCode" attribute, and shall include rule status within the "ruleStatus" attribute with the value as described below.

If the installation/activation of one or more new PCC rules (i.e., rules which were not previously successfully installed) fails, the SMF shall set the "ruleStatus" to INACTIVE.

The removal of a PCC rule shall not fail, even if the PDU session procedures with the UE fail. The SMF shall retain information on the removal and conduct the necessary PDU session procedures with the UE when it is possible.

If the modification of a currently active PCC rule, the SMF shall retain the existing PCC rule as active without any modification unless the reason for the failure has an impact also on the existing PCC rule. The SMF shall report the modification failure to the PCF.

If a PCC rule was successfully installed/activated, but can no longer be enforced by the SMF, the SMF shall set the "ruleStatus" attribute to INACTIVE.

NOTE: When the PCF receives "ruleStatus" set to INACTIVE, the PCF does not need request the SMF to remove the inactive PCC rule.

Depending on the value of the "failureCode" attribute, the PCF may decide whether retaining of the old PCC rule, re-installation, modification, removal of the PCC rule or any other action applies.

If the RAN-NAS-Cause feature is supported and as part of any of the procedures described in this subclause the SMF receives from the access network some RAN/NAS release cause(s) or untrusted WLAN release cause(s), the SMF shall also provide the received cause(s) in the RuleReport instance. If RAN-NAS-Cause feature is supported the SMF shall provide the available access network information within the "userLocationInfo" attribute (if available), "userLocationInfoTime" attribute (if available) and "ueTimezone" attribute (if available).

If the "RuleVersioning" feature is supported and the PCF included the "contVer" attribute for a specific PCC rule instance, and the resource allocation was unsuccessful as for any of the procedures described in this subclause the SMF shall include the rule content version within the "contVers" attribute for the corresponding RuleReport instance.

4.2.4.16 Presence Reporting Area Information Report

If the PRA feature as defined in subclause 5.8 is support and when the SMF receives the presence reporting area information from the serving node as defined in 3GPP TS 29.502 [22] indicating that the UE is inside or outside of one or more presence reporting areas or any of the presence reporting areas is set to inactive, the SMF shall check if the reported presence reported area identifier corresponds to a presence reporting area that is relevant for the PCF. In that case, the SMF shall within the SmPolicyUpdateContextData data structure include the "PRA_CH" within the "repPolicyCtrlReqTriggers" attribute and one or more Presence Reporting Area Information Report within the "repPraInfos" attribute. For each PresenceInfo data structure, the SMF shall also include the presence reporting area status within the "presenceState" attribute and the presence reporting area identifier within the "praId" attribute for each of the presence reporting areas reported by the serving node.

If the SMF receives additional presence reporting area information together with the PRA Identifier as described in 3GPP TS 29.502 [22], the SMF shall only provide the PCF with the presence reporting area information corresponding to the additional PRA information.

NOTE 1: The SMF will receive additional presence reporting area information when the UE enters or leaves one or more presence reporting areas related to a PRA set. In that case, the additional presence reporting area information corresponds to the actual individual presence reporting area. The received presence reporting area identifier corresponds to the PRA set id and is used to identify the requester (PCF or CHF) of the notification information.

NOTE 2: The PCF can acquire the necessary data for presence reporting from the UDR.

NOTE 3: Homogeneous support of Presence Area reporting in a network is assumed.

NOTE 4: The serving node can activate the reporting for the PRAs which are inactive as described in the 3GPP TS 23.501 [2].

4.2.4.17 UE initiates a resource modification support

In the case that the UE initiates a resource modification procedure, the SMF shall within the SmPolicyUpdateContextData data structure include the "RES_MO_RE" within the "repPolicyCtrlReqTriggers" attribute and shall include the UE request of specific QoS handling for selected SDF within the "ueInitResReq" attribute. Within the UeInitiatedResourceRequest data structure, the SMF shall included the "packFiltOp" attribute, "packetFilterInfo" attribute and "reqQos" attribute if applicable as follows:

- When the UE requests to add filters, the SMF shall include the "packFiltOp" attribute set to "ADDITION", the "packFiltInfo" attribute and "reqQos" attribute containing the requested QoS for the new packet filters. Each PacketFilterInfo instance shall contain one packet filters requested for addition;

- When the UE requests to modify existing packet filter the SMF shall include the "packFiltOp" attribute set to "MODIFICATION" and the "packFiltInfo" attribute. Each PacketFilterInfo instance shall contain one packet filters requested for modification and correspdong packet filter identifier assigned by the PCF during the procedure for addition within the "packFiltId" attribute. If the UE request includes modified QoS information the SMF shall also include the "reqQos" attribute to indicate the updated QoS for the affected PCC rule(s).

- When the UE requests to modify the QoS associated with existing packet filter(s), without modifying the filter(s), the SMF shall include "packFiltOp" attribute to "MODIFICATION", the "packFiltInfo" attribute and the updated QoS for the affected PCC rules(s) within the "reqQos" attribute. Each PacketFilterInfo shall include the affected packet filter identifier assigned by the PCF during the procedure for addition within the "packFiltId" attribute.

- When the UE requests to delete existing packet filter the SMF shall include the "packFiltOp" attribute set to "DELETION", the "packFiltInfo" attribute and the updated QoS for the affected PCC rules(s) within the "reqQos" attribute. Each PacketFilterInfo shall include the removed packet fitler identifier assigned by the PCF during the procedure for addition within the "packFiltId" attribute.

The SMF shall calculate the requested GBR, for a GBR 5QI, as the sum of the previously authorized GBR for the set of affected PCC rules, containing one or more affected packet filter, adjusted with the difference between the requested GBR for the QoS flow and previously negotiated GBR for the QoS flow. For the UE request to add filters, the GBR as requested by the UE for those filters shall be used.

If the request covers all the PCC rules with a QoS flow binding to the same QoS flow, then the SMF may request a change to the 5QI for existing packet filters.

For the purpose of adding or modifying a packet filter, within each PacketFilterInfo instance, the SMF shall include the packet filter precedence information within the "precedence" attribute and the "packFiltCont" attribute, "tosTrafficClass" attribute, "spi" attribute, "flowLabel" attribute and "flowDirection" attribute set to the value(s) describing the packet filter provided by the UE.

> NOTE: The UE signalling with the network is governed by the applicable NAS signalling TS. The NAS 3GPP TS for a specific access may restrict the UE possibilities to make requests compared to what is stated above.

If the PCF authorizes the request from the UE, the PCF shall construct a PCC rule(s) based on the UeInitiatedResourceRequest data structure. For the request to add the filter(s), the PCF shall within the FlowInformation data structure include the assigned packet filter identifier within the "packFiltId" attribute.

If the PCF detects that the packet filters in the request for new PCC rules received from the SMF is covered by the packet filters of outstanding PCC rules that the PCF is provisioning to the SMF, the PCF may reject the request and indicate the casue for the rejection including the "cause" attribute of the ProblemDetails data structure set to "ERROR_CONFLICTING_REQUEST" in an HTTP "403 Forbidden" response message. If the SMF receives a response message with this code, the SMF shall reject the PDU session modification that initiated the HTTP request.

If the PCF does not accept one or more of the traffic mapping filters provided by the SMF in an HTTP Request (e.g. because the PCF does not allow the UE to request enhanced QoS for services not known to the PCF), the PCF shall reject the request and indicate the cause for the rejection including the "cause" attribute of the ProblemDetails data structure set to "ERROR_TRAFFIC_MAPPING_INFO_REJECTED" in an HTTP "403 Forbidden" response message. If the SMF receives an HTTP response with this code, the SMF shall reject the PDU session modification that initiated the HTTP request.

The PCF shall not combine a rejection with provisioning of PCC rule operations in the same HTTP response.

4.2.4.18   Trace Control

When there is the requirement to activate tracing the SMF may provide trace control parameters to the PCF via the Npcf_SMPolicyControl_Update service operation. The update service operation may also indicate the deactivation of the trace session to the PCF.

4.2.4.19   Negotiation of the QoS flow for IMS signalling

When UE initiates a resource modification request, if the SMF includes the "qosFlowUsage" attribute containing "IMS_SIG" within SmPolicyUpdateContextData data structure and the PCF accepts that a QoS flow dedicated to IMS signalling shall be used, the PCF shall return the "qosFlowUsage" containing "IMS_SIG" value within the SmPolicyDecision data structure. The provided PCC rules shall have the 5QI applicable for IMS signalling.

4.2.4.20   Notification about Service Data Flow QoS target enforcement

When the SMF gets the knowledge that for one or more QoS Flows:

-   the GBR QoS targets cannot be guaranteed; or

-   the GBR QoS targets can be guaranteed again;

the SMF shall inform the PCF that the GBR QoS targets cannot be guaranteed or guaranteed again for the PCC rules bound to the QoS flows. The SMF shall send an HTTP POST request to the PCF with an SmPolicyUpdateContextData data structure, including the "QOS_NOTIF" within "repPolicyCtrlReqTriggers" attribute and the "qncReports" attribute. In each QosNotifcationControlInfo data structure, the PCF shall include the indication that the GBR QoS targets cannot be guaranteed or the GBR QoS targets can be guaranteed again within the "notifType" attribute and affected PCC rule identifiers within the "refPccRuleIds" attribute.

If the affected PCC rule was provisioned with a content version, the SMF shall include the "contVers" attribute defined in the QosNotifcationControlInfo data structure for those corresponding PCC rules. The SMF may include more than one content version in the "contVers" attribute for the same PCC rule within the corresponding QosNotifcationControlInfo instance included in the "qncReports" attribute (e.g. the SMF has combined multiple PCC rule versions enforcement into one QoS flow operation).

When the PCF receives the HTTP POST request, it shall acknowledge the request by sending a "204 No Content" response to the SMF and then notify the AF as defined in 3GPP TS 29.514 [17], subclause 4.2.5.4

4.2.5 Npcf_SMPolicyControl_Delete Service Operation

4.2.5.1 General

The delete service operation provides means for the NF service consumer to delete the context of PDU Session related information.

The following procedures using the Npcf_SMPolicyControl_Delete service operation are supported:

- Deletion of the policy context associated with a PDU session.

- Report Accumulated Usage.

- Report Access Network Information.

4.2.5.2 SM Policy Association termination
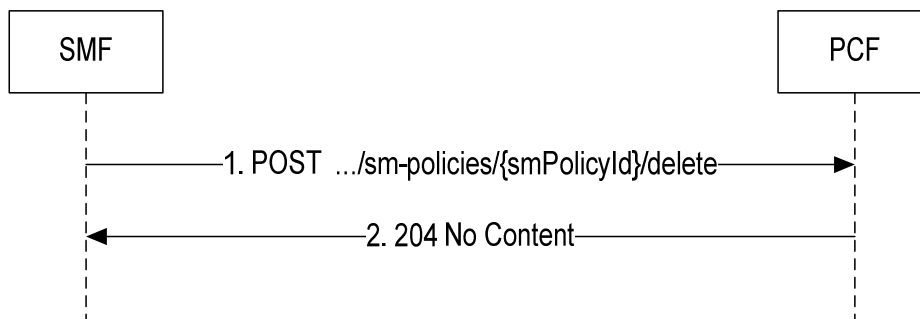
Figure 4.2.5.2-1: SM Policy Association termination

When an individual resource of the SM Policy Association shall be deleted the SMF shall invoke the Npcf_SMPolicyContext_DELETE service operation to the PCF using an HTTP POST request, as shown in figure 4.2.5.2-1, step 1.

The SMF shall set the request URI to "{apiRoot}/npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}/delete". The {smPolicyId} in the URI identifies the "Individual SM Policy" to be deleted.

The SMF delete request shall (if available) contain SM Policy Association related information within the SmPolicyDeleteData data structure in the body:

- accumulated usage within the "accuUsageReport" attribute ;

- the user location information within the "userLocationInfo" attribute, the information on when the UE was last known to be in that location within the "userLocationInfoTime" attribute, the PLMN identifier within the "servingNetwork" attribute;

- the timezone information within the "ueTimeZone" attribute ;

- RAN cause and/or the NAS cause within the "ranNasRelCauses" attribute.

When the PCF receives the HTTP POST request from the SMF, the PCF shall acknowledge the request by sending an HTTP response message with the corresponding status code. The PCF acknowledged the delete request by sending a "204 No Content" response to the SMF, as shown in figure 4.2.5.2-1, step 2. Further, the PCF shall remove the individual resources linked to the delete request.

4.2.5.3 Report Accumulated Usage

If the UMC feature is supported, when the SMF receives the accumulated usage report from the UPF as defined in subclause 7.5.7.2 of 3GPP TS 29.244 [13], within the SmPolicyDeleteData data structure the SMF shall include one or more accumulated usage reports within the "accuUsageReports" attribute.

If all PDU sessions of a user to the same DNN are terminated, the PCF may store the remaining allowed usage, i.e. the information about the remaining overall amount of resources, in the UDR as defined in 3GPP TS 29.519 [15].

4.2.5.4 Report Access Network Information

If the RAN-NAS-Cause feature is supported, within the SmPolicyDeleteData data structure the SMF shall provide the available access network information within the "userLocationInfo" attribute (if available), "userLocationInfoTime" attribute (if available), "ueTimezone" attribute (if available). Additional, if the SMF received from the access network the RAN cause and/or the NAS cause due to PDU session termination, the SMF shall provide the received cause(s) in the "ranNasRelCauses" attribute.

4.2.6 Provisioning and Enforcement of Policy Decisions

4.2.6.1 General

Policy Decisions are provided from the PCF to the NF service consumer (SMF) as part of the following service operations:

- The Npcf_SMPolicyControl_Create Service Operation described in subclause 4.2.2;

- The SM Policy Association Notification request as part of the Npcf_SMPolicyControl_UpdateNotify Service Operation as described in subclause 4.2.3.2; and

- the Npcf_SMPolicyControl_Update service operation as described in subclause 4.2.4

Policy decisions shall be encoded within the SmPolicyDecision data structure defined in subclause 5.6.2.4

Policy decisions may include:

- Session Rules as described in subclause 4.1.4.3 encoded within the "sessRules" attribute;

- PCC Rules as described in subclause 4.1.4.2 encoded within the "pccRules" attribute;

- QoS decisions as described in subclause 4.1.4.4.3 that can be referenced from PCC rules and session rules encoded within the "qosDescs" attribute;

- charging decisions as described in subclause 4.1.4.4.4 that can be referenced from PCC rules encoded within the "ChgDescs" attribute;

- Traffic control decisions as described in subclause 4.1.4.4.2 that can be referenced from PCC rules encoded within the "traffContDescs" attribute;

- Usage monitoring control decisions as described in subclause 4.1.4.4.5 that can be referenced from PCC rules and session rules encoded within the "umDescs" attribute;

- Conditions that can be referenced from PCC rules and session rules encoded within the "conds" attribute;

- A reflective QoS timer;

- Policy control request triggers and applicable additional information, e.g., Revalidation Time, PRA information;

- Last requested rule data;

- Last requested usage data;

- Default charging method of the PDU session;

- Charging information;

- P-CSCF Restoration Support Indication;

- IP index information;

- Usage of QoS flow.

For the Npcf_SMPolicyControl_Create Service Operation, the SmPolicyDecision data structure shall contain a full description of all of policies decisions provided by the PCF for the policy association.

For the Npcf_SMPolicyControl_UpdateNotify service operation for the SM Policy Association Notification request and for the Npcf_SMPolicyControl_Update service operation, the SmPolicyDecision data structure shall contain a description of changes of the policies decisions with respect to the last provided previous policy decision for the corresponding policy association. The default charging method of the PDU session, charging information, Reflective QoS Timer, P-CSCF Restoration Support Indication and IP index information shall not been updated by the PCF.

If no other rules are defined for specific data types within the SmPolicyDecision data structure, the encoding of changes of the policies decisions in the SmPolicyDecision data structure shall follow the following principles:

1) To modify an attribute with a value of type map (e.g. the "sessRules" attribute, the "pccRules" attribute, the "qosDescs" attribute, the "traffContDescs" attribute, the "umDescs" attribute, and the "conds" attribute) the attribute shall be provided with a value containing a map with entries according to the following principles:

   - A new entry shall be added by supplying a new identifier (e.g. rule / decision identifier) as key and the corresponding structured data type instance (e.g. PCC rule) with complete contents as value as an entry within the map.

   - An existing entry shall be modified by supplying the existing identifier as key and the corresponding structured data type instance with the same existing identifier (e.g. set the "qosId" to the same existing QoS data decision identifier), which shall describe the modifications following bullets 1 to 6, as value as an entry within the map.

   - An existing entry shall be deleted by supplying the existing identifier as key and "NULL" as value as an entry within the map.

   - For an unmodified entry, no entry needs to be provided within the map.

2) To modify an attribute with a structured data type instance as value, the attribute shall be provided with a value containing a structured data type instance with entries according to bullets 1 to 6.

3) To modify an attribute with another type than map or structured data type as value, the attribute shall be provided with a complete representation of its value that shall replace the previous value.

4) To create an attribute of any type, the attribute shall be provided with a complete representation of its value.

5) To delete an attribute of any type, the attribute shall be provided with NULL as value.

NOTE 1: Attributes that are allowed to be deleted need to be marked as "nullable" within the OpenAPI file in Annex A.

6) Attributes that are not added, modified, or deleted do not need to be provided.

NOTE 2: In related data structures no attribute can be marked as mandatory except the attribute for the identifier (e.g. rule / decision identifier).

The PCF shall not remove a provisioned policy decision data or condition data from the SMF when the reference(s) from the PCC rule(s) or session rule(s) are still valid. The PCF may keep a policy decision data or condition data valid when the PCF removes all the PCC(s) or session rule(s) referring to the policy decision data or condition data.

4.2.6.2   PCC Rules

4.2.6.2.1   Overview

The PCF may perform an operation on a single PCC rule or a group of PCC rules. The impacted rules shall be included in the "pccRules" map attribute within the SMPolicyDecision data structure with the "pccRuleId" as a key. For activating the pre-defined PCC rule, or installing or modifying a dynamic PCF-provisioned PCC rule, the corresponding PccRule data instance shall be provided as the map entry value. For deactivating or removing a PCC rule, the map entry value shall be set to NULL.

NOTE 1: When deactivating a predefined PCC rule that is activated in more than one QoS flow, the predefined PCC rule is deactivated simultaneously in all the QoS flow where it was previously activated.

In order to activate a pre-defined PCC rule, the PCF shall within the PccRule instance include the pre-defined PCC rule identifier within the "pccRuleId" attribute and the "refCondData" attribute if applicable, i.e. the PccRule instance is empty except for the "pccRuleId" attribute and the "refCondData" if applicable. If the "refCondData" attribute is

applicable, a "conds" attributes containing the corresponding Condition Data referred by the PCC rule shall be included in the SmPolicyDecision data structure if it has not been provided.

In order to install a new dynamic PCF-provisioned PCC rule, the PCF shall further set other attributes within the PccRule data structure as follows:

- it may include the precedence within the "precedence" attribute;

- it shall include either the flow information within the "flowInfos" attribute(s) or the application identifier within the "appId" attribute;

- it shall include one reference to the QoSData data structure within the "refQosData" attribute. In this case, a "qosDecs" attributes containing the corresponding QoS data policy decisions shall be included in the SmPolicyDecision data structure if it has not been provided;

- it shall include one reference to the TrafficControlData data structure within the "refTcData" attribute. In this case, a "traffContDecs" attribute containing the corresponding Traffic Control data policy decision shall be included in the SmPolicyDecision data structure if it has not been provided;

- it may include one reference to the ChargingData data structure within the "refChgData" attribute. In this case, a "chgDecs" attribute containing the corresponding Charging Data policy decisions shall be included in SmPolicyDecision data structure if it has not been provided;

- it may include one reference to the UsageMonitoringData data boolean within the "refUmData" attribute. In this case, a "umDecs" attribute containing the corresponding Usage Monitoring data policy decision shall be included in the SmPolicyDecision data structure if it has not been provided; and

- it may include one reference to the ConditionData data type within the "refCondData" attribute. In this case, a "conds" attributes containing the corresponding Condition Data shall be included in the SmPolicyDecision data structure if it has not been provided;

In order to modify an existing dynamic PCF-provisioned PCC rule, the PCF shall further set other attributes within the PccRule data structure as follows:

- If the PCF needs to modify the attribute(s) within a PCC rule, the PCF shall include the modified attributes(s) with the new value(s) within the PccRule data instance. Previously supplied attributes not supplied in the modified PCC rule instance shall remain valid.

- If the PCF only needs to modify the content of referenced policy decision data (e.g. QoSData, ChargingData, etc.) and/or condition data for one or more PCC rules, the PCF shall, within the SmPolicyDecision data structure, include the corresponding policy decision data and/or condition data within the corresponding map attributes (e.g. include the QoS data decision within the"qosDecs" attribute).

In order to modify the content of referenced condition data for one or more existing pre-defined PCC rules, the PCF shall, within the SmPolicyDecision data structure, include the corresponding condition data within the "conds" attribute.

The PCF may combine multiple of the above PCC rule operations in a single message.

   NOTE x: The network configuration can ensure that at least one PCC Rule is activated for the PDU Session.

4.2.6.2.2   Gate function

The Gate Function represents a user plane function enabling or disabling the forwarding of data packets belonging to a service data flow. A gate is described within a PCC rule. If the PCC rule contains the "flowInfos" attribute(s) applicable for uplink service data flows, it shall describe a gate for the corresponding uplink service data flows. If the PCC rule contains the "flowInfos" attribute(s) applicable for downlink service data flows, it shall describe a gate for the corresponding downlink service data flows. If the PCC rule contains the "appId" attribute, it shall describe a gate for the corresponding detected application traffic. The "flowStatus" attribute within a TrafficControlData data structure which the PCC rule refers to shall describe if the possible uplink and possible downlink gate is opened or closed.

The commands to open or close the gate shall lead to the enabling or disabling of the passage for corresponding data packets. If the gate is closed all packets of the related service data flows shall be dropped. If the gate is opened the packets of the related service data flows are allowed to be forwarded.

4.2.6.2.3 Policy enforcement for authorized QoS per PCC Rule

The PCF can provide the authorized QoS for a PCC rule to the SMF. The Provisioning of authorized QoS per PCC Rule shall be performed using the PCC rule provisioning procedure as defined in subclause 4.2.6.2.1. For a PCF-provided PCC rule, the authorized QoS shall be encoded using a QosData data structure. The PCF shall include the reference to the QosData data structure within the "refQosData" attribute of the PCC rule and a "qosDecs" attribute containing this QoS data decision within the SmPolicyDecision data structure.

If the authorized QoS is provided for a PCC rule, the SMF shall derive the QoS profile towards the access network if applicable, the QoS rule towards the UE if applicable, and the QoS information with the PDR(s) towards the UPF.

4.2.6.2.4 Redirect function

The PCF may provide the redirect instruction for one or several dynamic PCC rule to the SMF. The Provisioning shall be performed using the policy provisioning procedure as defined in subclause 4.2.6.1.

The"traffContDescs" attribute within the SmPolicyDecision is used to provide traffic control decisions. The redirect instruction shall be encoded using a "redirectInfo" attribute within the corresponding TrafficControlData data structure. That attribute provides a RedirectInformation data structure with the following components:

- The "redirectEnabled" attribute indicates whether redirect is enabled. It shall be included and set to true when the redirect instruction is initially provisioned and may be included in subsequent updates of the RedirectInformation to enable or disable the redirect instruction.

- The redirect address may be provided using the "redirectAddressType" and "redirectServerAddress" attributes or may be preconfigured in the SMF/UPF. A redirect destination provided within the "redirectServerAddress" attribute for a dynamic PCC Rule shall override the redirect destination preconfigured in the SMF/UPF.

NOTE: The SMF/UPF uses the preconfigured redirection address only if it can be applied to the application traffic being detected, e.g. the redirection destination address could be preconfigured on a per application identifier basis.

If redirect needs to be applied to a dynamic PCC rule, that PCC rule shall reference a traffic control decision with such redirect instructions.

If "redirectInfo" attribute is provided for a dynamic PCC rule, the SMF shall instruct the UPF to perform the redirection as defined in 3GPP TS 29.244 [13].

To disable the redirect function for one or more already installed PCC Rule, the PCF shall:

- update the PCC rule to modify the reference to a new Traffic Control Data decision which does not have the "redirectInfo"; or

- update the Traffic Control Data decision which the PCC rule refers to with the "redirectEnabled" attribute set to false if the PCF disables the redirect function for all the PCC rules which refer to this Traffic Control Data decision.

4.2.6.2.5 Usage Monitoring Control

Usage monitoring may be performed for service data flows associated with one or more PCC rules.

The provisioning of usage monitoring control per PCC rule shall be performed using the PCC rule provisioning procedure as defined in subclause 4.2.6.2.1. The reference to the UsageMonitoringData data structure of the usage monitoring control instance, which is related with the PCC rule, shall be included within the "refUmData" attribute of the PccRule data structure of the PCC rule(s). Usage monitoring shall be activated for both service data flows associated with predefined PCC rules and dynamic PCC rules, including rules with deferred activation and/or deactivation times while those rules are active.

4.2.6.2.6 Traffic Steering Control support

If the TSC feature is supported, the PCF may instruct the SMF to apply a traffic steering control for the purpose of steering the subscriber's traffic to appropriate operator or 3rd party service functions (e.g. NAT, antimalware, parental control, DdoS protection) in the N6-LAN or enabling the routing of the user traffic to a local Data Network identified by the DNAI per AF request.

4.2.6.2.6.1 Steering the traffic in the N6-LAN

For the purpose of steering the subscriber's traffic to appropriate operator or 3rd party service functions in the N6-LAN, the PCF shall include the reference to a Traffic Control Data decision within the PccRule data instance and set other attribute as follows:

- either include the application to be detected is identified by the "appId" attribute or the service data flow to be detected is identified by the "flowInfos" attribute(s) within the PccRule data structure, and

- include a "traffContDecs" contain the corresponding Traffic Control Data decision within the SmPolicyDecssion if it has not been provided yet. In this case, the PCF shall include the traffic steering policy identifier(s) for downlink and/or uplink identified by the "trafficSteeringPolIdDl" attribute and/or "trafficSteeringPolIdUl" attribute within the Traffic Control Data data decision.

The PCF may also provision the traffic steering control information by activating the pre-defined PCC rule(s) in the SMF.

4.2.6.2.6.2 Steering the traffic to a local access of the data network

The PCF shall determine if the ongoing PDU Session is impacted by the routing of traffic to a local access to a data network as follows.

- If the AF request includes individual IP address/ prefix allocated or user identifier to an UE, the PCF shall store the received traffic routing information and shall perform the session binding as defined in subclause 6.2 of 3GPP TS 29.513 [7] to determine the impacted PDU session;

- Otherwise, the PCF fetches the traffic routing data information from the UDR as defined in 3GPP TS 29.519 [15] applicable for any UE or Internal Group Id if received in the SMF request.

Then the PCF authorizes the request for influencing SMF routing decisions. For impacted PDU Session that corresponds to the AF request, the PCF shall determine the PCC rules that are generated based on the AF request as follows:

- When the request is for influencing SMF routing decisions, based on the traffic routing information, operator's policy, etc. and determines the traffic steering policy. The traffic steering policy indicates the list of suitable traffic steering policy IDs configured in SMF and if the N6 routing information associated to the application is explicitly provided by the AF, the N6 routing information. The traffic steering policy IDs are related to the mechanism enabling traffic steering to the DN. The PCF shall within the PccRule data instance(s) include the information to identify the traffic within the "flowInfos" attribute or "appId" attribute, and within the Traffic Control Data data decision which the PCC rule refers to include a list of locations which the traffic shall be routed to in the "routeToLocs" attribute. Within each RouteToLocation instance, the PCF shall include a DNAI in the "dnai" attribute to indicate the location of the application towards which the traffic routing is applied and either a traffic steering policy identifier in the "routeProfId" attribute, or the explicit routing information in the "routeInfo" attribute.

- When the request is for subscribing the UP path change event of the PDU session , the PCF shall include the information on AF subscription to UP path change event within the PCC rule(s) to request the notification from the SMF for the AF. In order to do so, the PCF shall within the PccRule data instance(s) include the information to identify the traffic either within the "flowInfos" attribute or "appId" attribute, and/or within the Traffic Control Data data decision which the PCC rule refers to include the information on AF subscription to the events within the "upPathChgEvent" attribute. Within the "upPathChgEvent" attribute, the PCF shall include the "dnaiChgType" attribute to indicate the type of notification (i.e. early notification, late notification or both), the notification address within the "notificationUri" attribute and the notification correlation Id within the "notifCorreId" attribute. In order to enable the AF to identify the AF request which the notification corresponds to when the AF receives the notification from the SMF as defined in subclause 4.2.2.2 of 3GPP TS 29.508 [12], the PCF shall set the values of "notificationUri" attribute and "notifCorreId" attribute respectively as follows:

  - If the PCF fetches the traffic routing data information from the UDR, the PCF shall set the value of "notificationUri" to the value of the "upPathChgNotifUri" attribute of the TrafficInfluData data structure and set the value of "NotifCorreId" attribute to value of "upPathChgCorreId "attribute of the TrafficInfluData data structure as defined in 3GPP TS 29.519 [15].

- If the PCF receives the traffic routing data information from the AF via N5 interface, the PCF shall set the values of "notificationUri" attribute and "NotifCorreId" attribute according to the "upPathChgSub" attribute within the AfRoutingRequirement data structure as defined in 3GPP TS 29.514 [17].

- If the AF request includes an indication indicating that application relocation is not possible, the PCF shall within the PccRule data instance(s) include the information to identify the traffic either within the "flowInfos" attribute or "appId" attribute and the "appReloc" attribute set to true.

The PCF shall provide the PCC rule(s) as defined in subclause 4.2.6.2.1.

If the temporal validity condition is received, the PCF shall evaluate the temporal validity condition of the AF request and informs the SMF to install or remove the corresponding PCC rules according to the evaluation result. When policies specific to the PDU Session and policies general to multiple PDU Sessions exist, the PCF gives precedence to the PDU Session specific policies over the general policies.

If the spatial validity condition is received, the PCF considers the latest known UE location to determine the PCC rules provided to the SMF. In order to do that, the PCF shall request the SMF to report the notifications about change of UE location in an area of interest (i.e. Presence Reporting Area) as defined in subclause 4.2.2.13 or 4.2.3.19. The subscribed area of interest may be the same as spatial validity condition, or may be a subset of the spatial validity condition (e.g. a list of TAs) based on the latest known UE location. When the SMF detects that UE entered the area of interest subscribed by the PCF, the SMF notifies the PCF and the PCF provides to the SMF the PCC rules described above. When the SMF becomes aware that the UE left the area subscribed by the PCF, the SMF notifies the PCF and the PCF may remove or provide updated PCC rules to the SMF.

When the PCC rules are installed, the SMF may, based on local policies, take the information in the PCC rules into account to:

- (re)select UPF(s) for PDU Sessions.

- activate mechanisms for traffic multi-homing or enforcement of an UL Classifier (UL CL).

- Inform the AF of the (re)selection of the UP path (change of DNAI).

4.2.6.2.7 Conditioned PCC rule

The PCF may control at what time the status of a PCC rule changes. In order to provision a PCC rule with conditional data, the PCF shall provision a PCC rule as defined in subclause 4.2.6.2.1and include within its "refCondData" attribute the corresponding ConditionData's "condId" attribute value. The PCF shall also ensure that the referenced ConditionData instance is included in the "conds" map within the SmPolicyDecision data structure following the procedures defined in subclause 4.2.6.1. Within the ConditionData instance, the PCF shall include the activation time within the "activationTime" attribute and/or deactivation time within the "deactivationTime" attribute.

When the SMF receives the PCC rule, the SMF shall act as follows:

1) If "activationTime" attribute is specified only and the time specified in "activationTime" attribute is in the future, then the SMF shall set the PCC rule inactive and make it active at that time. If time specified in the "activationTime" attribute is in the past, then the SMF shall immediately set the PCC rule active.

2) If "deactivationTime" attribute is specified only and the time specified in "activationTime" attribute is in the future, then the SMF shall set the PCC rule active and make it inactive at that time. If the time specified in the "deactivationTime" is in the past, then the SMF shall immediately set the PCC rule inactive.

3) If both "activationTime" attribute and "deactivationTime" attribute are specified, and the time specified in the "activationTime" occurs before the time specified in the "deactivationTime" attribute, and also when the PCC rule is provided before or at the time specified in the "deactivationTime", the SMF shall handle the rule as defined in 1) and then as defined in 2).

4) If both "activationTime" attribute and "deactivationTime" attribute are specified, and the time specified in the "deactivationTime" attribute occurs before the time specified in the "activationTime", and also when the PCC rule is provided before or at the time specified in the "activationTime" attribute, the SMF shall handle the rule as defined in 2) and then as defined in 1).

5) If both the "activationTime" attribute and the "deactivationTime" attribute are specified but time has already occurred for both, and the time specified in the "activationTime" occurs before the time specified in the "deactivationTime" attribute, then the SMF shall immediately set the PCC rule inactive.

6) If both the "activationTime" attribute and the "deactivationTime" attribute are specified but time has passed for both, and the time specified in "deactivationTime" attribute occurs before the "activationTime" attribute, then the SMF shall immediately set the PCC rule active.

The PCF may modify a currently installed/activated PCC rule, including setting, modifying or deleting its deferred activation and/or deactivation time as follows:

1) When modifying a PCC rule by setting the deferred activation time and/or deactivation time, the PCF shall update the PCC rule by including the corresponding ConditionData's "condId" attribute value within the "refCondData" attribute and within the SmPolicyDecision data structure include the ConditionData instance within the "conds" attribute if not provisioned yet.

2) When modifying a PCC rule by modifying the deferred activation time and/or deactivation time,

    -   the PCF may update the PCC rule by replacing the existing ConditionData instance's "condId" attribute value within the "refCondData" attribute with a new one and within the SmPolicyDecision data structure include the new ConditionData instance within the "conds" attribute if not provisioned yet; or

    -   the PCF may update the condition data decision which the PCC rule refers to by updating the corresponding ConditionData instance as defined in subclause 4.2.6.1. The PCF may add an activation time or an deactivation time, update the values of the existing activation time and/or the existing deactivation time, or delete either the exiting activation time or the existing deactivation time.

3) When modifying a PCC rule by deleting the deferred activation time and deactivation time,

    -   the PCF shall delete the reference to the ConditionData instance within the PCC rule by updating PCC rule with the "refCondData" attribute set to NULL; and

    -   the PCF may delete the condition data decision which the PCC rule refers to as defined in subclause 4.2.6.1 if no other PCC rules are referring to the condition data decision.

To delete a conditioned PCC rule, the PCF shall perform the deletion of PCC rule as defined in subclause 4.2.6.2.1.

The UE timezone information, if available, may be used by the PCF to derive the values of "activationTime" attribute and the "deactivationTime" attribute.

If the PCC rule(s) including the reference to the Condition Data decision which includes the "activationTime" attribute are bound to a QoS flow that will require traffic mapping information to be sent to the UE, the SMF shall report the failure to the PCF by including the "ruleReports" attribute with the "failureCode" attribute set the value "NO_QOS_FLOW_BOUND" for the affected PCC rule(s).

NOTE 3: This limitation prevents dependencies on the signalling of changed traffic mapping information towards the UE.

The PCC rule(s) including the reference to the Condition Data decision which includes the "activationTime" attribute and the "deactivationTime" attribute shall not be applied for changes of the QoS or service data flow filter information.

4.2.6.2.8 PCC rule for resource sharing

If the ResShare feature is supported by both the SMF and PCF as described in subclause 5.8, the PCF may indicate that the SMF should commonly reserve resources for a set of PCC rules. The SMF shall then, for PCC rules bound to the same QoS flow and the same sharing key value , use the highest GBR value among those PCC rules as input for calculating the common GBR value when reserving QoS flow resources. The GBR value for each direction shall be considered separately, so that the uplink and downlink GBR values may originate from different PCC rules.

The SMF may based on internal logic use the highest MBR value among the provided PCC rules indicated to share resources, when determining the MBR for the QoS flow. Each individual PCC rule is still subject to data rate policing based on its own MBR values.

The PCF shall provide the "sharingKeyDl" attribute and/or "sharingKeyUl" attribute within the QosData data structure which the PCC rules refers to in order to indicate that the related PCC rule may share resources with other PCC rules bound to the same QoS flow.

The SMF shall apply resource sharing if at least two PCC rules bound to the same QoS flow share the same value in the "sharingKeyDl" attribute and/or "sharingKeyUl" attribute.

When modifying the value of "sharingKeyDl" attribute and/or "sharingKeyUl" attribute of the QosData data structure, which a PCC rule refers to for the PCC rule that is subject to resource sharing the SMF may adjust the resource sharing of the remaining PCC rules.

NOTE 1: A PCC rule that is deleted is also removed from the resource sharing, while the remaining PCC rules continue their sharing relationship.

NOTE 2: The state of resource sharing ends when less than two of the PCC rules in the set remains.

4.2.6.2.9 Resource reservation for services sharing priority

When the PCF derives PCC Rules corresponding to a service related to an AF that has indicated that priority sharing is allowed for that service over Rx interface, it derives the corresponding PCC Rules according to current procedures as described in 3GPP TS 29.513 [7], subclause 7.3. The PCF may additionally take the suggested pre-emption capability and vulnerability values into account if the AF provided them when the PCF determines the ARP pre-emption capability and vulnerability. The ARP derived at this point and the priority sharing indicator provided over Rx reference point (see 3GPP TS 29.214 [18] for further information) related to these derived PCC Rules are stored for later use.

For PCC Rules related to the same PDU session with the same assigned 5QI and with the priority sharing indicator enabled (see 3GPP TS 29.214 [18], subclause 4.4.8), the PCF shall rederive the ARP into a shared ARP for these PCC Rules as follows:

- The Priority Level shall be set to the lowest value (i.e. highest priority) among the Priority Level values derived for the PCC rules that include the priority sharing indicator;

- The Pre-emption Capability shall be set to true if any of the original derived PCC Rules have the Pre-emption-Capability value set to true.

- The Pre-emption Vulnerability shall be set to true if all the original derived PCC Rules have the Pre-emption Vulnerability value set to true.

NOTE 1: Having the same setting for the ARP parameter in the PCC Rules with the priority sharing indicator set enables the usage of the same bearer. Furthermore, a combined modification of the ARP parameter in the PCC rules ensures that a bearer modification is triggered when a media flow with higher service priority starts.

If the 5QI and/or ARP related to any of the PCC Rules that share priority is changed (e.g. based on local policies), the PCF shall rederive the ARP for the impacted PCC Rules following the same procedure as defined in this subclause.

The PCF shall provision the PCC Rules according to the rederived ARP information as described in subclause 4.2.6.2.1.

If the PCF receives a report that a PCC rule provisioning or modification failed due to the resource reservation failure as defined in subclause 4.2.x (PCC Rule Error Handling) and if the PCF supports the MCPTT-Preemption feature as defined in subclause 5.4.1 of 3GPP TS 29.214 [18], the PCF shall check if pre-emption control based on the pre-emption control information provided by the AF as defined in subclause 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18] applies.

NOTE 2: The PCF determines that pre-emption control applies based on the presence of the preEemptionControlInfo attribute received over Rx/N5 reference point as defined in 3GPP TS 29.214 [18] and operator policies.

If pre-emption control applies, the PCF shall check the corresponding derived PCC Rules (before applying priority sharing procedures). If the Pre-emption Capability of the derived PCC Rule is disabled the PCF shall notify that resource allocation has failed for this PCC rule to the AF as defined in subclause 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18]. Otherwise, if the Pre-emption Capability of the derived PCC Rule is enabled, the PCF shall perform the pre-emption control as follows:

- For all the active PCC rule(s) that applied priority sharing mechanism, the PCF shall identify the PCC Rules that have the Pre-emption Vulnerability enabled. For those selected PCC Rule(s), the PCF shall check the Priority Level value.

- If there is only one PCC Rule with the Priority Level value higher (i.e. lower priority) than the derived Priority Level value of new or modified PCC Rule, the PCF shall remove this PCC rule. The PCF shall retry the PCC rule provisioning or modification procedure for the PCC rule that failed.

- Otherwise, if there are more than one PCC Rule with the Priority Level value higher (i.e. lower priority) than the derived Priority Level value of new or modified PCC Rule, the PCF shall remove the PCC Rule with the highest Priority Level from the SMF. The PCF shall retry the PCC rule provisioning or modification procedure for the PCC rule that failed; If more than one PCC Rule have the same highest Priority Level, the PCF shall check the Pre-Emption-Control-Info AVP received over Rx interface as defined in 3GPP TS 29.214 [18] and remove the PCC Rule that matches the condition.

- Otherwise, if there is at least one PCC Rule with the same Priority Level value than the derived Priority Level value of new or modified PCC Rule, the PCF shall check the Pre-emption-Control-Info AVP received over Rx interface as defined in 3GPP TS 29.214 [18] for these PCC Rules and remove the PCC Rule that matches the condition.

- Otherwise, the PCF shall notify that resource allocation has failed for this PCC rule to the AF as defined in subclause 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18].

If there is no active PCC Rule with the Pre-emption Vulnerability enabled, the PCF shall notify that resource allocation has failed for this PCC rule to the AF as defined in subclause 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18].

NOTE 3: If the PCF receives a report that a PCC rule provisioning or modification failed due to the resource reservation failure and the PCF does not support the MCPTT-Preemption feature as defined in subclause 5.4.1 of 3GPP TS 29.214 [18], the PCF can apply pre-emption and remove active PCC rules from the SMF and then retry the PCC rule provisioning or modification procedure. Otherwise, the PCF will notify it to the AF as defined in subclause 4.4.1 or 4.4.2 of 3GPP TS 29.214 [18]. How the PCF applies the pre-emption depends on the implementation.

4.2.6.2.10 PCC rule bound to the default QoS flow

The PCF may indicate to the SMF that a PCC rule shall be bound to the default QoS flow and shall remain on the default QoS flow. The SMF shall then, for the indicated PCC rule bind it to the default QoS flow until the PCC rule is removed or until the PCF modifies the PCC rule to set the "defQosFlowIndication" attribute to false. The SMF this second case shall evaluate the full QoS information within the QosData data structure which the PCC rule refers and follow normal policy enforcement procedures for authorized QoS per service data flow as descibed in subclause 4.2.8.2.

NOTE: 5QI, ARP, QNC (if available), Priority Level (if available), Averaging Window (if available) and Maximum Data Burst Volume (if available) within QoS Data decision referred by the PCC rule are only used by the SMF for QoS flow binding purposes when the "defQoSFlowIndication" attribute is not included in "qoSData" attribute or it is set to false.

The PCF shall provide the "defQoSFlowIndication" attribute set to true in order to indicate that the related PCC rule shall be bound to the default QoS flow.

If the "defQoSFlowIndication" attribute set to true within the QosData data structure which the PCC rule refers to is received in the SMF, the SMF shall bind the related PCC rule to the default QoS flow. This remains valid until the PCC rule is removed or if the PCF indicates to the SMF that the binding to the default QoS flow no longer applies. The SMF shall ignore other values including 5QI, ARP, QNC (if available), Priority Level (if available), Averaging Window (if available) and Maximum Data Burst Volume (if available) within the QosData data structure if the "defQoSFlowIndication" attribute set to true. If the PCF has previously indicated to the SMF that a PCC rule shall be bound to the default QoS flow, to indicate that the binding to the default QoS flow no longer applies the PCF shall update the PCC rule by including the "defQosFlowIndication" attribute set to false. The SMF in this case shall evaluate the full QoS information within the QosData data structure which the PCC rule refers to and follow normal policy enforcement procedures for authorized QoS per service data flow.

If the PCF has not previously indicated to the SMF that a PCC rule shall be bound to the default QoS flow (i.e. it may be bound to another QoS flow) in order to indicate that the binding to the default QoS flow applies, the PCF shall update the PCC rule by including the "defQoSFlowIndication" set to true. The SMF in this case shall follow the procedures described in this subclause.

4.2.6.2.11 PCC rule for Application Detection and Control

If the ADC feature is supported and the user subscription indicates that the application detection and control is required, the PCF may instruct the SMF to detect application (s) by installing or activating a PCC rule. Within the PCC rule, the PCF shall provide an "appId" attribute set to the value of an application identifier. If the PCF requires to be reported about when the application start/stop is detected, it shall also provide the APP_STA and APP_STO policy control request trigger to the SMF as defined in subclause 4.2.6.4. The PCF may also mute such a notification about a specific

detected application by including a "traffContDecs" attribute to contain a Traffic Control Data decision which includes the "muteNotif" attribute set to true and including a "refTcData" attribute referring to the Traffic Control Data decision within the PCC rule.

4.2.6.2.12 Provisioning of PCC Rules for Multimedia Priority Services

4.2.6.2.12.1 General

The provision of PCC Rules corresponding to both MPS and non-MPS service shall be performed as described in subclause 4.2.6.2.1 "Provisioning of PCC rules".

When the PCF derives PCC Rules corresponding to MPS service, the ARP and 5QI shall be set as appropriate for the prioritized service, e.g. an IMS Multimedia Priority Service. The PCF may authorize a standardized 5QI or a standardized 5QI with a specific 5QI priority level as defined in subclause 4.2.6.6.2. The PCF may also authorize a non-standardized 5QI with explicitly signalled QoS characteristics as defined in subclause 4.2.6.6.3.

When the PCF derives PCC Rules corresponding to non-MPS service, the PCF shall generate the PCC Rules as per normal procedures. At the time the Priority PDU connectivity services is invoked (i.e. Indication for support of priority PDU connectivity service and MPS Priority Level are set), the PCF shall upgrade the ARP and/or change 5QI for the PCC Rules to appropriate values as needed for MPS. The PCF shall change the ARP and/or 5QI (also associated QoS characteristics if applicable) modified for the priority PDU connectivity service to an appropriate value according to PCF decision.

When the PCF receives an HTTP POST message as defined in subclause 4.2.2.1, the PCF shall check whether any of these parameters is stored in the UDR: indication for support of priority PDU connectivity service, MPS Priority Level and/or indication of IMS priority service support. The PCF shall derive the applicable PCC rules and default QoS flow QoS based on that information. If the indication of IMS priority service support is set and the "dnn" attribute corresponds to a DNN dedicated for IMS, the PCF shall assign an ARP corresponding to MPS for the default QoS flow and for the PCC Rules corresponding to the IMS signalling QoS flow. If the "dnn" does not correspond to a DNN dedicated for IMS, the ARP shall be derived without considering IMS Signalling Priority.

> NOTE 1: Subscription data for MPS is provided to PCF through the Nudr service.

Once the PCF receives a notification of a change in Priority PDU connectivity services support, MPS Priority Level and/or IMS priority service support from the UDR, the PCF shall make the corresponding policy decisions (i.e. ARP and/or 5QI (also associated QoS characteristics if applicable) change) and, if applicable, shall initiate an HTTP POST message as defined in subclause 4.2.3.2 to provision the modified data.

> NOTE 2: The details associated with the UDR service are specified in 3GPP TS 29.519 [15].

> NOTE 3: The MPS Priority Level is one among other input data such as operator policy for the PCF to set the ARP.

Whenever one or more AF sessions of an MPS service are active within the same PDU session, the PCF shall ensure that the ARP priority level of the default QoS flow is at least as high as the highest ARP priority level used by any authorized PCC rules belonging to an MPS service. If the ARP pre-emption capability is enabled for any of the authorized PCC rules belonging to an MPS service, the PCF shall also enable the ARP pre-emption capability for the default QoS Flow.

> NOTE 4: This ensures that services using dedicated QoS flows are not terminated because of a default QoS flow with a lower ARP priority level or disabled ARP pre-emption capability being dropped during mobility events.

> NOTE 5: This PCF capability does not cover interactions with services other than MPS services.

4.2.6.2.12.2 Invocation/Revocation of Priority PDU connectivity services

When a Priority PDU connectivity services is invoked, the PCF shall

- Derive the corresponding PCC Rules with the ARP and 5QI (also associated QoS characteristics if applicable) set as appropriate for a prioritized service.

- Set the ARP of the default QoS flow as appropriate for a Priority PDU connectivity services under consideration of the requirement described in subclause 4.2.6.2.12.1.

- Set the 5QI (also associated QoS characteristics if applicable) of the default QoS flow as appropriate for the Priority PDU connectivity services.

- Set the ARP of PCC Rules installed before the activation of the Priority PDU connectivity services to the ARP as appropriate for the Priority PDU connectivity services under the consideration of the requirements described in subclause 4.2.6.2.12.1.

- Set the 5QI of the PCC Rules installed before the activation of the Priority PDU connectivity services to the 5QI (also associated QoS characteristics if applicable) as appropriate for the Priority PDU connectivity services if modification of the 5QI of the PCC Rules is required.

When a Priority PDU connectivity services is revoked, the PCF shall

- Delete the PCC Rules corresponding to the Priority PDU connectivity services if they were previously provided.

- Set the ARP of the default QoS flow to the normal ARP under the consideration of the requirements described in subclause 4.2.6.2.12.1.

- Set the 5QI of the default QoS flow as appropriate for PCF decision.

- Set the ARP of all active PCC Rules as appropriate for the PCF under the consideration of the requirements described in subclause 4.2.6.2.12.1.

- Set the 5QI to an appropriate value according to PCF decision if modification of the 5QI of PCC Rules is required.

   NOTE: Priority PDU connectivity services can be explicitly invoked/revoked via UDR MPS user profile (Indication of Priority PDU connectivity services, MPS Priority Level). An AF for MPS Priority Service can also be used to provide Priority PDU connectivity services using network-initiated resource allocation procedures (via interaction with PCC) for originating accesses.

The PCF shall provision the SMF with the applicable PCC Rules upon Priority PDU connectivity services activation and deactivation as described above. The provision of the QoS information applicable for the PCC Rules shall be performed as described in clause 4.5.6.2. The provision of QoS information for the default QoS flow shall be performed as described in clause 4.2.6.3.

4.2.6.2.12.3   Invocation/Revocation of IMS Multimedia Priority Services

If the PCF receives service information including an MPS session indication and the service priority level from the P-CSCF or at reception of the indication that IMS priority service is active for the PDU session, the PCF shall under consideration of the requirements described in subclause 4.2.6.2.12.1:

- if required, set the ARP and 5QI (also associated QoS characteristics if applicable) of the default QoS flow as appropriate for the prioritized service;

- if required, set the ARP and 5QI (also associated QoS characteristics if applicable) of all PCC rules assigned to the IMS signalling QoS flow as appropriate for IMS Multimedia Priority Services;

- derive the PCC Rules corresponding to the IMS Multimedia Priority Service and set the ARP and 5QI (also associated QoS characteristics if applicable) of these PCC Rules based on the information received over N5/Rx.

If the PCF detects that the P-CSCF released all the MPS session and the IMS priority service has been deactivated for the PDU session the PCF shall under consideration of the requirements described in clause 4.2.6.2.12.1:

- delete the PCC Rules corresponding to the IMS Multimedia Priority Service;

- if required, set the ARP and 5QI of the default QoS flow as appropriate for the IMS Multimedia Priority set to inactive;

- replace the ARP and 5QI of all PCC Rules assigned to the IMS signalling QoS flow as appropriate when the IMS Multimedia Priority is inactive.

4.2.6.2.13   Sponsored Data Connectivity

Sponsored data connectivity may be performed for service data flows associated with one or more PCC rules if the information about the sponsor, the application service provider and optionally the threshold values are provided by the

AF and if the AF has not indicated to disable/not enable sponsored data connectivity as described in
3GPP TS 29.214 [18] subclauses 4.4.1 and 4.4.2 or 3GPP TS 29.514 [17] subclauses 4.2.2.5 and 4.2.3.5.

The provisioning of sponsored data connectivity per PCC rule shall be performed using the PCC rule provisioning
procedure as defined in subclause 4.2.6.2.1. The sponsor identity shall be set using the "sponsorId" attribute within the
ChargingData data type which the PCC rule refers to. The application service provider identity shall be set using the
"appSvcProvId" attribute within the ChargingData data type which the PCC rule refers to. The "sponsorId" attribute and
"appSvcProvId" shall be set if the "reportingLevel" attribute within the ChargingData data type which the PCC rule
refers to is set to the value "SPON_CON_LEVEL".

When receiving the usage thresholds from the AF, the PCF shall use the sponsor identity to generate a value of "umId"
attribute of the UsageMonitoringData data type which the PCC rule refers to and request usage monitoring control for
the sponsored data connectivity by following the procedures specified in subclauses 4.2.6.4.3.

When the AF disables sponsoring a service (See 3GPP TS 29.214 [18] subclause 4.4.2 or 3GPP TS 29.514 [17]
subclause 4.2.3.5), the PCF

- may modify the PCC rules in order to set the "reportingLevel" attribute to "SER_ID_LEVEL" or
  "RAT_GR_LEVEL" within the ChargingData data type which the PCC rule refers to and not include the
  "sponsorId" attribute and "appSvcProvId" attribute if they were included previously.

- may modify the PCC rules to update the charging key by setting the new value of the "ratingGroup" attribute
  within the ChargingData data type which the PCC rule refers to.

NOTE: A specific charging key can be applied to the sponsored data connectivity for online charging.

- shall disable the usage monitoring for the sponsored data connectivity according to subclause 4.2.6.4.3 if it was
  enabled previously. As a result, PCF gets the accumulated usage of the sponsored data connectivity.

4.2.6.2.14   Support for PCC rule versioning

The support of PCC rule versioning is optional. When the "RuleVersioning" feature is supported, the SMF and the PCF
shall comply with the procedures specified in this subclause.

If required by operator policies, the PCF shall assign a content version for each generated PCC rule and shall include
the assigned version in the "contVer" attribute included within the PccRule data structure. Upon each PCC rule
modification, if the content version was previously assigned to a PCC rule, the PCF shall assign a new content version.
In this case, all the content related to that PCC rule shall be included. The content version is unique for the lifetime of
the PCC rule.

NOTE 1: The PCF will include all the content of the PCC rule in each modification of the PCC rule in order to
         ensure that the rule is installed with the proper information regardless of the outcome of the QoS flow
         procedure related to previous rule provisioning versions that are not reported yet.

NOTE 2: The operation policies can take into account whether the AF provides the related content version
         information over Rx reference point (see subclause 4.4.9 in 3GPP TS 29.214 [18]), or over
         Npcf_PolicyAuthorization service (see subclauses 4.2.2.13 and 4.2.3.13 in 3GPP TS 29.514 [17]).

Whenever the SMF provides a PCC rule report for rules that were provisioned with a content version, the SMF shall
include the "contVers" attribute defined in the RuleReport data structure for those corresponding PCC rules. In case it is
required to report the content version of multiple PCC rules, the SMF shall use one instance of RuleReport data
structure per PCC rule, and shall include in the "pccRuleIds" attribute only the identifier of the corresponding PCC rule.
The SMF may include more than one content version in the "contVers" attribute for the same PCC rule within the
corresponding RuleReport instance included in the "ruleReports" attribute (e.g. the SMF has combined multiple PCC
rule versions enforcement into one QoS flow operation). In this case, the "ruleStatus" attribute shall indicate the final
status of the PCC rule.

NOTE 3: The PCF will use the content version to identify the PCC rule version that failed or succeeded when
         multiple provisions of the same PCC rule occur in a short period of time. If required by the AF, the PCF
         will inform the AF according to 3GPP TS 29.214 [18], subclause 4.4.9, or according to
         3GPP TS 29.514 [17], subclause 4.2.5.8 about the failure or success for the media component version
         associated to the PCC rule version.

4.2.6.2.15 Background data transfer support

If the PCF receives Reference Id within the service information from the AF as defined in 3GPP TS 29.514 [17] or 3GPP TS 29.214 [18], the PCF shall retrieve the corresponding transfer policy from the UDR based on the Reference Id as defined in 3GPP TS 29.519 [15], then the PCF shall take the transfer policy as input for policy decisions (e.g. setting the charging key equal to the charging key of the transfer policy, rule activation/deactivation time according to the time window).

4.2.6.2.16 Number of supported packet filter for signalled QoS rule limitation support

If the PCF includes the flow information within the "flowInfos" attribute(s) and if the number of supported packet filter for signalled QoS rules within the "numOfPackFilter" attribute is received from the SMF during the PDU session establishment, the PCF may ensure that for all PCC rules of a PDU session, the number of packet filters contained within the "flowDescription" attribute or the "ethFlowDescripiont" attribute with the "packetFilterUsage" set to true does not exceed the value of the "numOfPackFilter" attribute.

4.2.6.3 Session Rules

4.2.6.3.1 Overview

The PCF may perform operations on session rules. The impacted rules shall be included in the "SessRules" map attribute within the SMPolicyDecision data structure with the "sessRuleId" as a key. For installing or modifying a session rule, the corresponding SessionRule data instance shall be provided as the map entry value. For removing a session rule, the map entry value shall be set to NULL.

In order to install a new session rule, the PCF shall further set other attributes within the SessionRule data structure as follows:

- it may include the authorized session AMBR within the "authSessAmbr" attribute;

- it may include the authorized default QoS within the "authDefQoS" attribute using the procedure as defined in subclause 4.2.6.3.3;

- it may include one reference to the UsageMonitoringData data structure within the "refUmData" attribute. In this case, a "umDecs" attribute containing the corresponding Usage Monitoring data policy decisions shall be included in SmPolicyDecision data structure if it has been provided; and

- it may include one reference to the ConditionData data structure within the "refCondData" attribute. In this case, a "conds" attribute containing the corresponding Condition Data decision shall be included in SmPolicyDecision data structure if it has been provided;

In order to modify an existing session rule, the PCF shall further set other attributes within the SessionRule data structure as follows:

- If the PCF needs to modify the attribute(s) within a session rule, the PCF shall include the modified attributes(s) with the new value(s) within the SessionRule data instance. Previously supplied attributes not supplied in the modified PCC rule instance shall remain valid.

- If the PCF only needs to modify the content of referenced policy decision data (e.g. UsageMonitoringData, etc.) and/or condition data for one or more session rules, the PCF shall, within the SmPolicyDecision data structure, include the corresponding policy decision data and/or condition data within the corresponding map attributes (e.g. include the usage monitoring data decision within the"umDecs" attribute).

The PCF may combine multiple of the above session rule operations in a single message, but the PCF shall make sure that these is only one session rule active.

4.2.6.3.2 Conditioned Session rule

4.2.6.3.2.1 General

Up to four conditioned session rules (i.e. authorized session AMBR and/or authorized default QoS) may be provisioned by the PCF. In order to provision a session rule with conditional data, the PCF shall provision a session rule as defined in subclause 4.2.6.3.1 and include within its "refCondData" attribute the corresponding ConditionData's "condId" attribute value. The PCF shall also ensure that the referenced ConditionData instance is included in the "conds" map

within the SmPolicyDecision data structure following the procedures defined in subclause 4.2.6.1. Within the ConditionData instance, the PCF shall include the activation time within the "activationTime" attribute.

NOTE 1: The same instance of session rule can convey information related to the authorized session-AMBR and authorized default QoS when the same time condition applies to both.

NOTE 2: The SMF retains remaining time conditioned authorized QoS that have an execution time in the future.

If the SMF receives the conditioned session rule, at the time indicated in the "activationTime" attribute, the SMF shall perform the requested change without interaction with the PCF.

If time conditioned session rule(s) to change the non-conditioned session rule are received by the SMF and the earliest Activation Time is in the past, then the SMF shall immediately enforce the most recent time conditioned instance that is not in the future.

The PCF may modify a currently installed session rule, including setting, modifying or deleting its deferred activation time as follows:

1)   When modifying a session rule by setting the deferred activation time, the PCF shall update the session rule by including the corresponding ConditionData's "condId" attribute value within the "refCondData" attribute and within the SmPolicyDecision data structure include the ConditionData instance within the "conds" attribute if not provisioned yet.

2)   When modifying a session rule by modifying the deferred activation time,

   -   the PCF may update the session rule by replacing the existing ConditionData instance's "condId" attribute value within the "refCondData" attribute with a new one and within the SmPolicyDecision data structure include the new ConditionData instance within the "conds" attribute if not provisioned yet; or

   -   the PCF may update the condition data decision which the session rule refers to by updating the corresponding ConditionData instance as defined in subclause 4.2.6.1. The PCF may update the value of the existing deferred activation time.

3)   When modifying a session rule by deleting the deferred activation time,

   -   the PCF shall delete the reference to the ConditionData instance within the session rule by updating session rule with the "refCondData" attribute set to NULL; and

   -   the PCF may delete the condition data decision which the session rule refers to as defined in subclause 4.2.6.1 if no other session rules are referring to the condition data decision.

To delete a time conditioned session rule, the PCF shall perform the deletion of session rule as defined in subclause 4.2.6.3.1.

NOTE 3: Time conditioned session AMBR and default QoS change helps reducing the signaling load over N7. However, the session AMBR and default QoS change needs to be communicated to the UE. Consequently a simultaneous change of the session AMBR and default QoS for many UE(s) may introduce a signaling storm in the 5GC (e.g. over N1/N2/N4/N11). The PCF can avoid this simultaneous change of the session AMBR and default QoS (e.g. spread the time conditioned change over time for many UEs).

4.2.6.3.2.2   Time conditioned authorized session AMBR

The procedures in subclause 4.2.6.2.2.1 apply with clarifications in the present subclause.

Each instance of the session rule shall include authorized session AMBR within the "authSessAmbr" attribute.

The SMF shall, after applying a time conditioned instruction to change the authorized AMBR, apply the corresponding procedures towards to the access network, the UE and the UPF for the enforcement of the AMBR per PDU session.

4.2.6.3.2.3   Time conditioned authorized default QoS

The procedures in subclause 4.2.6.3.2.1 apply with clarifications in the present subclause.

Each instance of the session rule shall include authorized default QoS within the "authDefQos" attribute.

The SMF shall, after applying a time conditioned instruction to change the authorized default QoS, apply the corresponding procedures towards to the access network, the UE and the UPF for the enforcement of the authorized default QoS. All PCC rule(s) with the "defQosFlowIndication" attribute set to true shall remain bound to the default QoS flow. For any other PCC rule previously bound to the default QoS flow, SMF shall then perform the QoS flow binding according to clause 6.4 in 3GPP TS 29.513 [7].

4.2.6.3.3 Provisioning of authorized default QoS Characteristics

The PCF can provide the authorized default QoS for a session rule to the SMF. The provisioning of authorized default QoS for a session rule shall be performed using the session rule provisioning procedure as defined in subclause 4.2.6.3.1. The authorized default QoS shall be encoded using a AuthorizedDefaultQos data structure.

In order to provision authorized default QoS for a new session rule, the PCF shall include the assigned 5QI value within the "5qi" attribute and the assigned ARP value within the "arp" attribute in the AuthorizedDefaultQos data structure. The PCF may include "priorityLevel", "averWindow" and/or "maxDataBurstVol" attributes in the AuthorizedDefaultQos data structure to authorize particular QoS characteristics that override the default values for a standardized or pre-configured 5QI. The PCF may include a "QosCharacteristics" entry in the "qosChars" attribute map to provide explicitly signalled QoS characteristics associated with a 5QI that is neither standardized nor pre-configured. When the authorized default QoS applies to explicitly signalled QoS Characteristics, it shall be provisioned as defined in subclause 4.2.6.6.3.

In order to modify authorized default QoS for an existing session rule, the PCF shall include the modified attributes(s) with the new value(s) within the AuthorizedDefaultQos data structure. Previously supplied attributes not supplied in the AuthorizedDefaultQos data structure shall remain valid.

4.2.6.4 Policy control request triggers

The PCF may provide one or several policy control request trigger(s) to the SMF. In order to do so, the PCF shall include one or several policy control request trigger(s) within the "policyCtrlReqTriggers" attribute(s) within the SmPolicyDecision data structure.

During the lifetime of the PDU session, the PCF may update or remove the policy control request triggers. In order to update the policy control request trigger, the PCF shall provide the new complete list of applicable policy control request triggers by including one or several policy control request trigger(s) within the "policyCtrlReqTriggers" attribute within the SmPolicyDecision data structure.

The PCF may remove all previously provided policy control request triggers by providing a "policyCtrlReqTriggers" attribute set to the value NULL. Upon reception of a policy control request trigger with this value, the SMF shall not inform PCF of any trigger except for those triggers that are always reported and do not require provisioning from the PCF.

Whenever the PCF provisions one or serveral policy control request trigger(s) by using an HTTP POST message as defined in subclause 4.2.3.2, unless otherwise specified in a policy control request trigger's value definition, the SMF shall send the corresponding currently applicable values (e.g. access type, RAT type, user location information, etc.) to the PCF within the UeCampingRep data structure in the response of the HTTP POST message, and in this case, the "repPolicyCtrlReqTriggers" attribute shall not be included.

4.2.6.5 Encoding of the request of information reporting

4.2.6.5.1 Request of Access Network Charging Identifier

When the Access Network Charging Identifier is unknown for an AF session to the PCF, the PCF may request the SMF to provide the Access Network Charging Identifier associated to the dynamic PCC rules. To do so, the PCF shall within SmPolicyDecision data structure provide the "policyCtrlReqTriggers" attribute with the value "AN_CH_COR" if the policy control request trigger is not previously set and the "lastReqRuleData" attribute. For the RequestedRuleData instance, the PCF shall include the CH_ID within the "reqData" attribute and reference of the PCC rule wthin the "refPccRuleIds" attribute.

The PCF shall interpret that the Access Network Charging Identifier is known when the PCF receives an "accNetChId" attribute with the "sessionChScope" attribute included and set to true.

4.2.6.5.2 RAN NAS Cause Support

When RAN-NAS-Cause feature is supported, the PCF may request the SMF to inform it of the result of the PCC rule removal when the PCF removes the PCC rule. In order to do so, the PCF shall additionally include the "policyCtrlReqTriggers" attribute with RES_RELEASE if the policy control request trigger is not previously set and the "lastReqRuleData" attribute. For the RequestedRuleData instance, the PCF shall inlcude the RES_RELEASE within the "reqData" attribute and reference of the removed PCC rule wthin the "refPccRuleIds" attribute.

> NOTE: This is done to allow the PCF to notify the AF when there is an abnormal termination of the QoS flow. The PCF does not have to retry the removal of these PCC Rules.

4.2.6.5.3 Provisioning of the Usage Monitoring Control Policy

The PCF may indicate the need to apply monitoring control for the accumulated usage of network resources on a PDU session basis. Usage is defined as volume or time of user plane traffic. Monitoring for traffic volume and traffic time can be performed in parallel. The data collection for usage monitoring control shall be performed per monitoring key, which may apply for a single service data flow, a set of service data flows or for all the traffic in a PDU session. If the usage monitoring of a PDU session level is enabled, the PCF may request the SMF to exclude a single service data flow or a set of service data flows from the usage monitoring of PDU session level.

During the PDU session establishment, the PCF may receive information about total allowed usage per DNN and UE from the UDR, i.e. the overall amount of allowed traffic volume and/or time of usage that are to be monitored per DNN and UE and/or total allowed usage for Monitoring key(s) per DNN and UE.

> NOTE: It depends on the implementation of UDR to provide the total allowed usage per DNN and UE to different PCFs if the different PCFs are serving the PDU sessions with same value of DNN and UE.

If the SMF supports the UMC feature, the PCF may request usage monitoring control for the PDU session. If at this time, the PCF has not provided "US_RE" policy control request trigger to the SMF, the PCF shall include the "policyCtrlReqTriggers" attribute with the value "US_RE" and provide it to the SMF as defined in subclause 4.2.6.4. The PCF shall not remove the "US_RE" policy control request trigger while usage monitoring is still active in the SMF.

At PDU session establishment and modification, the PCF may provide the applicable thresholds, volume threshold, time threshold or both volume threshold and time threshold, for each usage monitoring control instance to the SMF. To provide the initial threshold for each usage monitoring control instance, the PCF shall include the threshold(s) within the "umDecs" attribute within the SmPolicyDecision data structure.

Threshold levels, monitoring time if applicable and inactive time if application for each usage monitoring control instance may be provisioned within an entry of the "umDecs" attribute as follows:

- the total volume threshold within the "volumeThreshold" attribute if applicable;

- the uplink volume threshold within the "volumeThresholdUplink" attribute if applicable;

- the downlink volume threshold within the "volumeThresholdDownlink" attribute if applicable;

- the time threshold whithin the "timeThreshold" attribute if applicable;

. the total volume threshold after the monitoring time within the "nextVolThreshold" attribute if applicable;

- the uplink volume threshold after the monitoring time whithin the "nextVolThresholdUplink" attribute if applicable;

- the downlink volume threshold after the monitoring time whithin the "nextVolThresholdDownlink" attribute if applicable;

- the time threshold after the monitoring time whithin the "nextTimeThreshold" attribute if applicable;

- the monitoring time within the "monitoringTime" attribute if applicable;

- the inactive time within the "inactivityTime" attribute if applicable.

If the usage monitoring control instance applies to the PDU session level, the PCF shall include the reference to the Usage Monitoring Data decision within the "refUmData" attribute of a session rule.

If the usage monitoring control instance applies to a service data flow or a group of service data flows, the PCF shall include the reference to the Usage Monitoring Data decision within the "refUmData" attribute of one or more PCC rule.

The PCF may provide one usage monitoring control instance applicable at PDU session level and one or more usage monitoring instances applicable at PCC Rule level.

If the PDU session level usage monitoring is enabled and if the service data flow(s) need to be excluded from PDU session level usage monitoring, the PCF shall include the corresponding PCC rule identifier(s) within the "exUsagePccRuleIds" attribute of the UsageMonitoringData instance of PDU session level usage monitoring. If the exclusion is enabled, the PCF may disable the exclusion again for the service data flow(s) by removing the corresponding PCC rule identifier from "exUsagePccRuleIds" attribute.

If the PCF wishes to remove the threshold level for one or more monitoring keys, the PCF shall provide the corresponding attribute with NULL value to the corresponding usage monitoring control instance.

When the SMF receives the usage monitoring control request above from the PCF, the SMF shall initiate the PFCP Session Establishment Request as defined in subclause 7.5.2 or PFCP Session Modification Request as defined in subclause 7.5.4 of 3GPP TS 29.244 [13] to request the UPF to perform the usage monitoring control.

When usage monitoring is enabled, the PCF may request the SMF to report accumulated usage for one or more enabled usage monitoring control instance regardless if a usage threshold has been reached. In order do so, the PCF shall include the "lastReqUsageData" attribute to contain one more reference(s) to usage monitoring data decision(s) within the "refUmIds" attribute or contain the "allUmIds" set to true.

4.2.6.5.4 Request for Access Network Information

When the NetLoc feature is supported, if the AF requests the PCF to report the access network information as described in subclause 4.2.2, 4.2.3 or 4.2.4 of 3GPP TS 29.514 [17] or in subclause 4.1 and 4.2 of 3GPP TS 29.214 [18], the PCF shall perform the PCC rule provisioning procedure as defined in subclause 4.2.6.2.1 and additionally provide the requested access network information indication (e.g. user location and/or user timezone information) to the SMF as follows:

- it shall include the "lastReqRuleData" attribute to contain the "reqData" attribute with the value(s) MS_TIME_ZONE and/or USER_LOC_INFO and the "refPccRuleIds" attribute to contain the related installed/modified/removed PCC rule identifier(s).

- it shall provide the AN_INFO policy control request rigger within the "policyCtrlReqTriggers" attribute (if not yet set).

For those PCC Rule(s) based on preliminary service information as described in 3GPP TS 29.514 [17] or in 3GPP TS 29.514 [17], the PCF may assign the 5QI and ARP of the default QoS flow to avoid signalling to the UE. These PCC Rules shall not include the "packetFilterUsage" attribute set to true within the "flowInfos" attribute.

4.2.6.5.5 Request for the successful resource allocation notification

The PCF may request the SMF to confirm that the resources associated to a PCC rule are successfully allocated. To do so the PCF shall within the SmPolicyDecision data structure provide the "policyCtrlReqTriggers" attribute with the value "SUCC_RES_ALLO " if the policy control request trigger is not previously set and the "lastReqRuleData" attribute. For the RequestedRuleData instance, the PCF shall include the "SUCC_RES_ALLO" within the "reqData" attribute and the reference of the PCC rule within the "refPccRuleIds" attribute.

4.2.6.5.6 Provisioning of Presence Reporting Area Information

When PRA feature is supported, the PCF may determine during the lifetime of the IP-CAN session whether reports for change of UE presence in Presence Reporting Area(s) are desired for the PDU session based on the subscriber's profile configuration. If the reporting is desired for the PDU session, the PCF shall provide the "praInfos" attribute within the SmPolicyDecision data structure. Within each PresenceInfo data structure, the PCF shall include the Presence Reporting Area Identifier within the "praId" attribute, and, for a UE-dedicated Presence Reporting Area, the list of elements composing the presence reporting area within the "trackingAreaList" attribute, "ecgiList" attribute, "ncgiList" attribute, and/or "globalRanNodeIdList" attribute. If PCF is configured with a Presence Reporting Area identifier referring to the list of Presence Reporting Area Identifier(s) within a Set of Core Network predefined Presence Reporting Areas as defined in 3GPP TS 23.501 [2], the PCF shall include the identifier of the Presence Reporting Area set within the "praId" attribute.The PCF shall activate the reporting changes of UE presence in Presence Reporting Area(s) by provisioning the "PRA_CH" policy control request trigger to the SMF.

NOTE 1: If this feature is not supported, the PCF can instead activate location change reporting that reports actual location. Due to the potential increase in signalling load, careful consideration of the network load is necessary for such reporting, e.g. limiting the number of subscribers subject to such reporting.

NOTE 2: The Presence Reporting Area Identifier can correspond to a list of Presence Reporting Area Identifier(s) within a set of Core Network predefined Presence Reporting Areas (PRA set identifier) as defined in 3GPP TS 23.501 [2] if the PCF is configured.

The PCF may modify the list of PRA Identifier(s) by providing the new Presence Reporting Area or by removing existing Presence Reporting Area(s) or modify the list(s) of Presence Reporting Area elements by providing the updated Presence Reporting Area. In order to do that, the PCF shall follows the general procedure as defined in subclause 4.2.6.1 and supply the Presence Reporting Area identifier(s) as the key(s) of the map.

The PCF may remove the policy control request trigger of change of UE presence in Presence Reporting Area as defined in subclause 4.2.6.4, if previously activated.

If the "PRA_CH" policy control request trigger is provisioned, when the PCF provides a list of presence reporting areas as described above, the PCF shall ensure that the maximum number of provisioned Presence Reporting Area Identifiers is not exceeded. The maximum number of PRAs may be configured in the PCF. The PCF may have independent configuration of the maximum number for Core Network pre-configured PRAs and UE-dedicated PRAs.

NOTE 3: For all the Presence Reporting Area(s) provided by the PCF, the SMF can store the Presence Reporting Area Identifier(s) together with an indication that states that it relates to PCF requested PRA status changes.

NOTE 4: This information is needed so that if both PCF and CHF request the reports of PRA status changes, the SMF is able to differentiate whether the reported PRA changes are relevant to PCF or CHF.

The SMF shall initiate the appropriate PDU session specific procedure according to 3GPP TS 29.502 [22].

The PCF may be notified during the lifetime of an PDU session that the UE is located in an access network where local configuration indicates that the reporting change of UE presence in Presence Reporting Area is not supported. The PCF may remove the policy control request trigger of the change of UE presence in Presence Reporting Area, if previously activated. In this case, the PCF shall also remove the provisioned presence reporting areas by including the "praInfos" attribute set to NULL within the SmPolicyDecision data structure.

The SMF shall de-activate the relevant PDU session specific procedure for reporting Change of UE presence in Presence Reporting Area, when the PCF and CHF remove the request trigger of change of UE presence in Presence Reporting Area.

4.2.6.5.7　　　Policy provisioning and enforcement of reflective QoS

If the PCF receives the "refQosIndication" attribute set to true as defined in subclause 4.2.2.2 or 4.2.4.2, and if the PCF determines that Reflective QoS Control will be enabled for the PDU session based on the operator's policy and user subscriptions, the PCF may provision the Reflective QoS Timer by including the "reflectiveQoSTimer" attribute within the SmPolicyDecision data structure in the response message. The PCF may within a QoS data decision which a PCC rule refer to include the "reflectiveQos" attribute set to true to enable the Reflective QoS control to a service data flow when the PCF authorizes the QoS for the service data flow as defined in subclause 4.2.6.5.2. The PCF shall activate the reporting changes of reflective QoS indication by provisioning the "REF_QOS_IND_CH" policy control request trigger to the SMF.

NOTE: While the UE applies a standardized value for the precedence of all UE derived QoS rules, PCC rules require different precedence values and PCF configuration has to ensure that there is a large enough value range for the precedence of PCC rules corresponding to UE derived QoS rules. To avoid that the precedence of network provided QoS rules need to be changed when Reflective QoS is activated and filters are overlapping, the PCF will take the standardized value for the precedence of UE derived QoS rules into account when setting the precedence value of PCC rules subject to Reflective QoS.

The PCF shall not include the "reflectiveQos" attribute set to true within the QoS data decision which the PCC rule with match-all SDF template refers to. If a PCC rule with match-all SDF template has been provisioned to the SMF, the PCF shall not include the "reflectiveQos" attribute within the QoS data decision which contains the "defQosFlowIndication" attribute, either.

If the PCF receives the "refQosIndication" attribute set to false as defined in subclause 4.2.4.2, the PCF shall disable the reflective QoS Control for the PDU session. In order to do so, the PCF shall within the QoS data decision which

affected PCC rule refer to include the "reflectiveQos" attribute set to false and may update other QoS parameters within the QoS data decision and/or update the flow information of PCC rule by including the "packetFilterUsage" attribute set to true.

4.2.6.6   Authorized QoS

4.2.6.6.1   General

The PCF shall provision the authorized QoS. The authorized QoS may apply to a PCC rule or to a PDU session.

- When the authorized QoS applies to a PCC rule, it shall be provisioned within the corresponding PCC rule as defined in subclause 4.2.6.6.2.

- When the authorized QoS for a PCC rule with a GBR QCI is candidate for resource sharing an instruction on the allowed sharing may be provisioned as defined in subclause 4.2.6.2.8.

- When the authorized QoS applies to a PDU session, it shall be provisioned as defined in subclause 4.2.6.3.1.

- When the authorized QoS applies to the default QoS flow, it shall be provisioned as defined in subclause 4.2.6.3.1.

- When the authorized QoS applies to an explicitly signalled QoS Characteristics, it shall be provisionedas defined in subclause 4.2.6.6.3.

- When the authorized QoS applies to the Reflective QoS, it shall be provisioned as defined in subclause 4.2.6.5.7.

The authorized QoS provides appropriate values for the resources to be enforced. The authorized QoS for a PCC rule is a request for allocating the corresponding resources. The Provisioning of authorized QoS per PCC rule is a part of PCC rule provisioning procedure.

If the SMF cannot allocate any of the resources as authorized by the PCF, the SMF informs the PCF and acts as described in subclause 4.2.3.16 and 4.2.4.15.

The SMF shall interact with the (R)AN, UPF and UE for enforcing the policy based authorization.

QoS authorization information may be dynamically provisioned by the PCF or it may be a pre-defined PCC rule in the SMF. Moreover, all the parameters of the authorized QoS may be changed.

NOTE 1:   A change of 5QIs cannot be described as an upgrade or downgrade and also no 5QI can be referred to as the higher or lower. Whether the 5QI is permitted to be changed or not is subject to both operator policies and normal restrictions on changing from a non-GBR 5QI value to GBR 5QI value on an IP flow.

NOTE 2:   All attributes of the ARP QoS parameter can be changed but only the ARP priority level represents an ordered range of values. The ARP priority level attribute represents the actual priority for the service/user with the value 1 as the highest and can thus be upgraded and downgraded.

If the PCF is unable to make a decision for the response to the HTTP POST message by the SMF, the PCF may reject the request as described in subclause 5.7.

4.2.6.6.2   Policy provisioning and enforcement of authorized QoS per service data flow

The Provisioning of authorized QoS per service data flow is a part of PCC rule provisioning procedure, as described in subclause 4.2.6.2.1.

The authorized QoS per service data flow shall be provisioned within a QosData data structure. The PCF shall includea "qosDecs" attribute containing the corresponding QoS data decision within the SmPolicyDecision data structure and include the reference to this QoS data decision within the "refQosData" attribute of the PccRule data instance.

Within the QoS data decision, for 5QI of GBR type or delay critical GBR type, the PCF shall include the authorized GBR 5QI or delay critical GBR 5QI respectively within the "5qi" attribute, the ARP within the "arp" attribute, max bandwidth in uplink within the "maxbrUl" attribute, max bandwidth in downlink within the "maxbrDl" attribute, the guaranteed bandwidth in uplink within the "gbrUl" attribute and the guaranteed bandwidth in downlink within the "gbrDl" attribute. If the PCF determines that the application traffic can be adapted to the change in the QoS based on the configuration (e.g. if the AF is capable to trigger rate adaptation), the PCF may request a notification when authorized GBR or delay critical GBR cannot be guaranteed or can be guaranteed again by including the "qnc" attribute set to true;

for 5QI of non-GBR type, the PCF shall include the authorized non-GBR 5QI within the "5qi" attribute, and may include the ARP within the "arp" attribute.

When the PCF authorizes a standardized 5QI but a Priority Level, an Averaging Window and/or a Maximum Data Burst Volume which are different from the standardized value in the table 5.7.4-1 of 3GPP TS 23.501 [2] are required, the PCF shall include the Priority Level within the "priorityLevel" attribute, the Averaging Window within the "averWindow" attribute and/or the Maximum Data Burst Volume within the "maxDataBurstVol" attribute.

NOTE 1: If no ARP is included, a default ARP applies for the service data flow template.

NOTE 2: For the non-standardized or non-configured 5QI, the PCF needs to authorize explicitly signalled QoS Characteristics associated with the 5QI if the PCF has not provisioned it.

If the configured policy allows at reception of the service information from the AF and the application of the rules of the QoS mapping procedures defined in 3GPP TS 29.513 [7] subclause 7.3.2 for the received service information result in a 5QI of 1 associated with the corresponding flows, and the RAN-Support-Info feature as defined subclause 5.8 is supported, the PCF shall determine the Maximum Packet Loss Rate for UL and DL for those flows associated within 5QI of 1. In this case, the PCF shall include the value of Maximum Packet Loss Rate for UL within the "maxPacketLossRateUl" attribute and/or the value of Maximum Packet Loss Rate for DL within the "maxPacketLossRateDl" attribute.

NOTE 3: Based on local configuration, the PCF sets the downlink and uplink maximum packet loss rates corresponding to either the most robust codec mode or the least robust codec mode of the negotiated set in each direction.

If the PCF wants to ensure that a PCC Rule is always bound to the default QoS flow, the policy provisioning for the related authorized QoS shall be done as described in subclause 4.2.6.2.10.

The SMF shall perform a QoS flow binding based on the QoS information within the Qos data decision as defined in subclause 6.4 of 3GPP TS 29.513 [7] after the SMF installs or activates the PCC rules.

The SMF shall reserve the resources necessary for the guaranteed bitrate for the PCC rule upon receipt of a PCC rule provisioning including QoS information. For GBR QoS flows the SMF should set the QoS flow's GBR to the sum of the GBRs of all PCC rules that are active/installed and bound to that GBR QoS flow. For GBR QoS flow the SMF should set the QoS flow's MBR to the sum of the MBRs of all PCC rules that are active/installed and bound to that GBR QoS flow.

NOTE 4: Since the PCF controls the GBR value in the PCC rule, the PCF can prevent that uplink GBR resources are reserved by providing an uplink GBR value of zero for that PCC rule This may be useful e.g. for a PCC rule with application identifier as the uplink traffic can be received in other QoS flow than the one the PCC rule is bound to.

The SMF shall assign a QFI if a new QoS flow needs to be established and shall derive, if applicable, the QoS profile required towards the Access Network, the QoS rule required towards the UE and the QoS information with PDRs towards to the UPF. If multiple PCC rules with the Maximum Packet Loss Rate for UL and DL are bound to the same QoS flow, the SMF shall choose the lowest value per direction related to the PCC rules within the QoS profile towards to the access network.

If one or more of the 5QI, ARP, QNC, Priority level, Averaging Window and Maximum Data Burst Volume attributes of a PCC rule are modified to the same updated values for all the PCC rules bound to the same QoS flow, then the SMF should modify the corresponding attributes for that impacted QoS flow.

Upon deactivation or removal of a PCC rule, the SMF shall free the resources reserved for that PCC rule, and initiate the corresponding procedure with access network, UE and UPF to remove the resources.

4.2.6.6.3 Policy provisioning and enforcement of authorized explicitly signalled QoS Characteristics

The PCF may provision a dynamically assigned 5QI value (from the non-standardized value range) and non-preconfigured and the associated 5G QoS characteristics to the SMF. In order to do so, the PCF shall include the "qosChars" attribute to contain one more authorized signalled QoS Characteristics instances. For each QoS Characteristics instance, the PCF shall include assigned 5QI value within the "5qi" attribute, resource type value within the "resourceType" attribute, the 5QI Priority Level value within the "priorityLevel" attribute, the Packet Delay Budget value within the "packetDelBudget" attribute, Packet Error Rate value within the "packetErrorRate" attribute, the

Averaging Window value within the "averagingWindow" attribute if applicable and the Maximum Data Burst Volume value within the "maxDataBurstVol" attribute if applicable. If the PCF has provisioned an authorized signalled QoS Characteristics instance to the SMF, the PCF shall not update nor remove it during the lifetime of the policy association.

Upon receiving the authorized explicitly signalled QoS characteristics, the SMF shall derive the QoS profile towards the access network and provide it to the access network by invoking corresponding procedure.

5 Npcf_SMPolicyControl Service API

5.1 Introduction

The request URI used in HTTP request from the NF service consumer towards the PCF shall have the structure defined in subclause 4.4.1 of 3GPP TS 29.501 [5], i.e.:

All resource URIs of this API shall have the following root:

{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [5].

- The {apiName} shall be "npcf-smpolicycontrol".

- The {apiVersion} shall be "v1".

- The {apiSpecificResourceUriPart} shall be set as described in subclause 5.3.

5.2 Usage of HTTP

5.2.1 General

HTTP/2, IETF RFC 7540 [8], shall be used as specified in clause 5 of 3GPP TS 29.500 [4].

HTTP/2, shall be transported as specified in subclause 5.3 of 3GPP TS 29.500 [4].

An OpenAPI [10] specification of HTTP messages and content bodies for the Npcf_SMPolicyControl is contained in Annex A.

5.2.2 HTTP standard headers

5.2.2.1 General

See subclause 5.2.2 of 3GPP TS 29.500 [4] for the usage of HTTP standard headers.

5.2.2.2 Content type

JSON, IETF RFC 8259 [9], shall be used as content type of the HTTP bodies specified in the present specification as specified in subclause 5.4 of 3GPP TS 29.500 [4]. 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 7807 [31].

5.2.3 HTTP custom headers

5.2.3.1 General

The mandatory HTTP custom header fields specified in subclause 5.2.3.2 of 3GPP TS 29.500 [4] shall be applicable.

5.3   Resources

5.3.1   Resource Structure
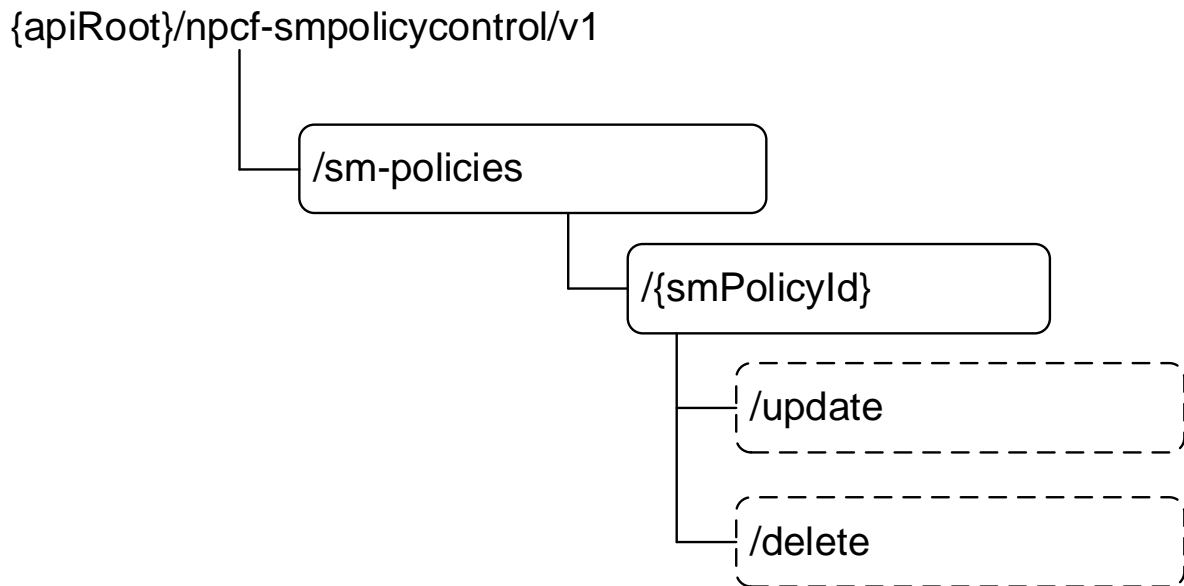
Figure 5.3.1-1: Resource URI structure of the Npcf_SMPolicyControl API

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
SM Policies	{apiRoot}/ npcf-smpolicycontrol/ v1/sm-policies	POST	Create a new Individual SM Policies resource for an SUPI or for a PEI and PDU Session ID and PDU Session ID supplied by the SMF.
Individual SM Policy	{apiRoot}/ npcf-smpolicycontrol/ v1/sm-policies/{smPolicyId}	GET	Read the Individual SM Policies resource.
	{apiRoot}/ npcf-smpolicycontrol/v1/ sm-policies/{smPolicyId}/delete	delete (POST)	Delete the Individual SM Policies resource.
	{apiRoot}/ npcf-smpolicycontrol/v1/ sm-policies/{smPolicyId}/update	update (POST)	Update the Individual SM Policies resource when a policy control request event is met or an error of policy enforcement occurs.

5.3.2   Resource: SM Policies

5.3.2.1   Description

This resource represents the collection of the individual SM Policies created in the PCF.

5.3.2.2   Resource definition

Resource URI: **{apiRoot}/npcf-smpolicycontrol/v1/sm-policies**

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

Table 5.3.2.2-1: Resource URI variables for this resource

Name	Definition
apiRoot	See subclause 5.1

5.3.2.3   Resource Standard Methods

5.3.2.3.1   POST

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

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

Name	Data type	P	Cardinality	Description
n/a				

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

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

Data type	P	Cardinality	Description
SmPolicyContextData	M	1	Parameters to create an individual SM policies resources.

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
SMPolicyDecision	M	1	201 Created	An individual SM Policy resources for the SUPI and PDU session id are created successfully.
ProblemDetails	M	1	400 Bad Request	(NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply.				
NOTE 2: Failure cases are described in subclause 5.7.				

5.3.2.4   Resource Custom Operations

None.

5.3.3   Resource: Individual SM Policy

5.3.3.1   Description

The individual SM Policy resource represents an individual SM Policy created in the PCF and associated with the SUPI and PDU session ID.

5.3.3.2   Resource definition

Resource URI: **{apiRoot}/npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}**

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	Definition
apiRoot	See subclause 5.1
smPolicyId	Unique identifier of the individual SM Policy resource.

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
SmPolicyControl	M	1	200 OK	An individual SM Policy resources for the SUPI and PDU session id are returned successfully.
NOTE: The mandatory HTTP error status codes for the GET method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply.				

5.3.3.4 Resource Custom Operations

5.3.3.4.1 Overview

Table 5.3.3.4.1-1: Custom operations

Custom operation URI	Mapped HTTP method	Description
{apiRoot}/ npcf-smpolicycontrol/ v1/sm-policies/{smPolicyId}/delete	POST	Delete an individual SM Policy resource.
{apiRoot}/ npcf-smpolicycontrol/ v1/sm-policies/{smPolicyId}/update	POST	Update an individual SM Policy resource.

5.3.3.4.2 Operation: delete

5.3.3.4.2.1 Description

5.3.3.4.2.2 Operation Definition

This custom operation deletes an individual SM Policy resource in the PCF.

This operation shall support the request data structures specified in table 5.3.3.4.2.2-1 and the response data structure and response codes specified in table 5.3.3.4.2.2-2.

Table 5.3.3.4.2.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
SmPolicyDeleteData	O	0..1	Parameters to be sent by the SMF when the individual SM policy is deleted.

Table 5.3.3.4.2.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	This case represents a successful deletion of the individual SM policy 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 [4] shall also apply.				

5.3.3.4.3 Operation: update

5.3.3.4.3.1 Description

5.3.3.4.3.2 Operation Definition

This custom operation updates an individual SM Policy resource in the PCF.

This operation shall support the request data structures specified in table 5.3.3.4.3.2-1 and the response data structure and response codes specified in table 5.3.3.4.3.2-2.

Table 5.3.3.4.3.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
SmPolicyUpdateContextData	M	1	Parameters to be sent by the SMF when the individual SM policy is updated. It indicates the occurred changes.

Table 5.3.3.4.3.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
SmPolicyDecision	M	1	200 OK	An individual SM Policy resources is updated successfully. Response body includes the policy decision changes.
ProblemDetails	M	1	400 Bad Request	(NOTE 2)
ProblemDetails	M	1	403 Forbidden	(NOTE 2)
NOTE 1: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply.				
NOTE 2: Failure cases are described in subclause 5.7.				

5.4 Custom Operations without associated resources

None.

5.5 Notifications

5.5.1 General

Table 5.5.1-1: Notifications

Custom operation URI	Mapped HTTP method	Description
{Notification URI}/update	POST	Policy Update Notification.
{Notification URI}/terminate	POST	Request for termination of the policy association.

5.5.2 Policy Update Notification

5.5.2.1 Description

This notification is used by the PCF to update the policy.

5.5.2.2 Operation Definition

This operation shall support the request data structures specified in table 5.5.2.2-1 and the response data structure and response codes specified in table 5.5.2.2-2.

Table 5.5.2.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
SmPolicyNotification	M	1	Update the SM policies provided by the PCF

Table 5.5.2.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The SM policies are updated successfully.
UeCampingRep	O	0..1	200 OK	The current applicable values corresponding to the policy control request trigger is reported.
array(PartialSuccessReport)	O	1..N	200 OK	Some of the PCC rules provisioned by the PCF are not installed/activated successfully.
ErrorReport	M	1	400 Bad Request	The SM policies including all the PCC rules provisioned by the PCF are not installed/activated successfully.
NOTE 1: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply.				
NOTE 2: Failure cases are described in subclause 5.7.				

5.5.3 Request for termination of the policy association

5.5.3.1 Description

This notification is used by the PCF to request the termination of a policy association.

5.5.3.2 Operation Definition

This operation shall support the request data structures specified in table 5.5.3.2-1 and the response data structure and response codes specified in table 5.5.3.2-2.

Table 5.5.3.2-1: Data structures supported by the POST Request Body on this resource

Data type	P	Cardinality	Description
TerminationNotification	M	1	Request to terminate the policy association.

Table 5.5.3.2-2: Data structures supported by the POST Response Body on this resource

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The request for policy association termination was received.
NOTE: The mandatory HTTP error status codes for the POST method listed in table 5.2.7.1-1 of 3GPP TS 29.500 [4] shall also apply.				

5.6 Data Model

5.6.1 General

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

The Npcf_SMPolicyControl API allows the SMF to retrieve the session management related policy from the PCF as defined in 3GPP TS 23.503 [6].

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

Table 5.6.1-1: Npcf_SMPolicyControl specific Data Types

Table 5.6.1-1: Npcf_SMPolicyControl specific Data Types

Data type	Section defined	Description	Applicability
5GSmCause	5.6.3.2	Indicates the 5GSM cause code value.	RAN-NAS-Cause
AccNetChargingAddress	5.6.2.35	Identifies the address of the network node performing charging and used for charging applications.	
AccNetChId	5.6.2.23	Contains the access network charging identifier for the PCC rule(s) or whole PDU session.	
AccuUsageReport	5.6.2.18	Contains the accumulated usage report information.	UMC
AfSigProtocol	5.6.3.10	Indicates the protocol used for signalling between the UE and the AF	ProvAFsignalFlow
AuthorizedDefaultQos	5.6.2.34	Authorized Default QoS	
ChargingData	5.6.2.11	Contains charging related parameters.	
ChargingInformation	5.6.2.17	Contains the addresses of the charging functions.	
ConditionData	5.6.2.9	Contains conditions for applicability of a rule.	
ErrorReport	5.6.2.36	Contains the rule reports.	
FailureCause	5.6.3.14	Indicates the cause of the failure in a Partial Success Report.	
FailureCode	5.6.3.9	Indicates the reason of the failure.	
FlowDirection	5.6.3.3	Indicates the direction of the service data flow.	
FlowDirectionRm	5.6.3.15	This data type is defined in the same way as the "FlowDirection" data type, but with the OpenAPI "nullable: true" property.	
FlowInformation	5.6.2.14	Contains the flow information.	
MeteringMethod	5.6.3.5	Indicates the metering method.	
PacketFilterInfo	5.6.2.30	Contains the information from a single packet filter sent from the SMF to the PCF.	
PacketFilterOperation	5.6.3.11	Indicates a UE initiated resource operation that causes a request for PCC rules.	
PartialSuccessReport	5.6.2.33	Includes the information reported by the SMF when some of the PCC rules are not successfully installed/activated.	
PccRule	5.6.2.6	Contains the PCC rule information.	
PolicyControlRequestTrigger	5.6.3.6	Contains the policy control request trigger(s).	
QosCharacteristics	5.6.2.16	Contains QoS characteristics for a non-standardized or non-configured 5QI.	
QosData	5.6.2.8	Contains the QoS parameters.	
QosNotificationControlInfo	5.6.2.32	Contains the QoS Notification Control Information.	
RanNasRelCause	5.6.2.28	Contains the RAN/NAS release cause.	RAN-NAS-Cause
RedirectAddressType	5.6.3.12	Indicates the redirect address type.	
RedirectInformation	5.6.2.13	Contains the redirect information.	
ReportingLevel	5.6.3.4	Indicates the reporting level.	
RequestedQos	5.6.2.31	Contains the QoS information requested by the UE	
RequestedRuleData	5.6.2.24	Contains rule data requested by the PCF to receive information associated with PCC rules.	
RequestedRuleDataType	5.6.3.7	Contains the type of rule data requested by the PCF.	
RequestedUsageData	5.6.2.25	Contains usage data requested by the PCF requesting usage reports for the corresponding usage monitoring data instances.	
RuleReport	5.6.2.27	Reports the status of PCC or session rule.	
RuleStatus	5.6.3.8	Indicates the status of PCC or session rule.	
SessionRule	5.6.2.7	Contains session level policy information.	
SmPolicyControl	5.6.2.2	Contains the parameters to request the SM policies and the SM policies authorized by the PCF.	
SmPolicyContextData	5.6.2.3	Contains the parameters to create individual SM policy resource.	
SmPolicyDecision	5.6.2.4	Contains the SM policies authorized by the PCF.	
SmPolicyNotification	5.6.2.5	Contains the update of the SM policies	
SmPolicyDeleteData	5.6.2.15	Contains the parameters to be sent to the PCF when the individual SM policy is deleted.	

SmPolicyUpdateContextData	5.6.2.19	Contains the met policy control request trigger(s) and corresponding new value(s) or the error report of the policy enforcement.	
TerminationNotification	5.6.2.21	Termination Notification	
TrafficControlData	5.6.2.10	Contains parameters determining how flows associated with a PCCRule are treated (blocked, redirected, etc).	
UeCampingRep	5.6.2.26	Contains the current applicable values corresponding to the policy control request triggers.	
UeInitiatedResourceRequest	5.6.2.29	Indicates a UE requests specific QoS handling for selected SDF.	
UpPathChgEvent	5.6.2.20	Contains the UP path change event subscription from the AF	TSC
UsageMonitoringData	5.6.2.12	Contains usage monitoring related control information.	UMC
Volume	3GPP TS 29.122 [32]	Unsigned integer identifying a volume in units of bytes	
VolumeRm	3GPP TS 29.122 [32]	This data type is defined in the same way as the "VolumeRm" data type, but with the OpenAPI "nullable: true" property.	

Table 5.6.1-2 specifies data types re-used by the Npcf_SMPolicyControl 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_SMPolicyControl service based interface.

Table 5.6.1-2: Npcf_SMPolicyControl re-used Data Types

Data type	Reference	Comments	Applicability
5GMmCause	3GPP TS 29.571 [11]	Contains the cause value of 5GMM protocol.	RAN-NAS-Cause
5Qi	3GPP TS 29.571 [11]	Unsigned integer representing a 5G QoS Identifier (see subclause 5.7.2.1 of 3GPP TS 23.501 [2]), within the range 0 to 255.	
5QiPriorityLevel	3GPP TS 29.571 [11]	Unsigned integer indicating the 5QI Priority Level (see subclauses 5.7.3.3 and 5.7.4 of 3GPP TS 23.501 [2]), within the range 1 to 127. Values are ordered in decreasing order of priority, i.e. with 1 as the highest priority and 127 as the lowest priority.	
5QiPriorityLevelRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "5QiPriorityLevel" data type, but with the OpenAPI "nullable: true" property.	
AccessType	3GPP TS 29.571 [11]	The identification of the type of access network.	
Ambr	3GPP TS 29.571 [11]	Session AMBR	
Arp	3GPP TS 29.571 [11]	ARP	
AverWindow	3GPP TS 29.571 [11]	Averaging Window	
AverWindowRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "AverWindow" data type, but with the OpenAPI "nullable: true" property.	
BitRate	3GPP TS 29.571 [11]	String representing a bit rate that shall be formatted as follows: pattern: "^\d+(\.\d+)?(bps|Kbps|Mbps|Gbps|Tbps)$" Examples: "125 Mbps", "0.125 Gbps", "125000 Kbps"	
BitRateRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "BitRate" data type, but with the OpenAPI "nullable: true" property.	
ChargingId	3GPP TS 29.571 [11]	Charging identifier allowing correlation of charging information	
ContentVersion	3GPP TS 29.514 [17]	Indicates the content version of a PCC rule. It uniquely identifies a version of the PCC rule as defined in subclause 4.2.6.7.	RuleVersioning
DateTime	3GPP TS 29.571 [11]	String with format "date-time" as defined in OpenAPI Specification [10].	
DateTimeRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "DateTime" data type, but with the OpenAPI "nullable: true" property.	
DnaiChangeType	3GPP TS 29.571 [11]	Describes the types of DNAI change.	
Dnn	3GPP TS 29.571 [11]	The DNN the user is connected to.	
DurationSec	3GPP TS 29.571 [11]	Identifies a period of time in units of seconds.	
DurationSecRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "DurationSec" data type, but with the OpenAPI "nullable: true" property.	
EthFlowDescription	3GPP TS 29.514 [17]	Defines a packet filter for an Ethernet flow.	
FinalUnitAction	3GPP TS 32.291 [19]	Indicates the action to be taken when the user's account cannot cover the service cost.	
FlowStatus	3GPP TS 29.514 [17]	Describes whether the IP flow(s) are enabled or disabled. The value "REMOVED" is not applicable to Npcf_SMPolicyControl service.	
Gpsi	3GPP TS 29.571 [11]	Identifies a GPSI.	
GroupId	3GPP TS 29.571 [11]	Identifies a group of internal globally unique ID.	
IpIndex	3GPP TS 29.519 [15]	Information that identifies which IP pool or external server is used to allocate the IP address.	
Ipv4Addr	3GPP TS 29.571 [11]	Identifies an Ipv4 address.	

Ipv6Addr	3GPP TS 29.571 [11]	Identifies an IPv6 address.	
Ipv6Prefix	3GPP TS 29.571 [11]	The Ipv6 prefix allocated for the user.	
MacAddr48	3GPP TS 29.571 [11]	MAC Address.	
MaxDataBurstVol	3GPP TS 29.571 [11]	Maximum Data Burst Volume	
MaxDataBurstVolRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "MaxDataBurstVol" data type, but with the OpenAPI "nullable: true" property.	
NetworkId	3GPP TS 29.571 [11]	The identification of the Network.	
NgApCause	3GPP TS 29.571 [11]	Contains the cause value of NgAP protocol.	RAN-NAS-Cause
PacketDelBudget	3GPP TS 29.571 [11]	Packet Delay Budget	
PacketErrRate	3GPP TS 29.571 [11]	Packet Error Rate	
PacketLossRateRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "PacketLossRate" data type, but with the OpenAPI "nullable: true" property.	
PduSessionId	3GPP TS 29.571 [11]	The identification of the PDU session.	
PduSessionType	3GPP TS 29.571 [11]	Indicate the type of a PDU session	
Pei	3GPP TS 29.571 [11]	The Identification of a Permanent Equipment.	
PolicyAssociationReleaseCause	3GPP TS 29.507 [25]	The cause why the PCF requests the termination of the policy association	
PresenceInfo	3GPP TS 29.571 [11]	Contains the information which describes a Presence Reporting Area.	PRA
PresenceInfoRm	3GPP TS 29.571 [11]	This data type is defined in the same way as the "PresenceInfo" data type, but with the OpenAPI "nullable: true" property.	
QosNotifType	3GPP TS 29.514 [17]	Indicates whether the GBR targets for the indicated SDFs are "NOT_GUARANTEED" or "GUARANTEED" again.	
QosResourceType	3GPP TS 29.571 [11]	Indicates whether the resource type is GBR, delay critical GBR, or non-GBR.	
RatingGroup	3GPP TS 29.571 [11]	Identifier of a rating group	
RatType	3GPP TS 29.571 [11]	The identification of the RAT type.	
RouteToLocation	3GPP TS 29.571 [11]	A traffic routes to applications location.	TSC
ServiceId	3GPP TS 29.571 [11]	Identifier of a service	
Snssai	3GPP TS 29.571 [11]	Identifies the S-NSSAI.	
SubscribedDefaultQos	3GPP TS 29.571 [11]	Subscribed Default QoS.	
Supi	3GPP TS 29.571 [11]	The identification of the user (i.e. IMSI, NAI).	
SupportedFeatures	3GPP TS 29.571 [11]	Used to negotiate the applicability of the optional features defined in table 5.8-1.	
TraceData	3GPP TS 29.571 [11]		
TimeZone	3GPP TS 29.571 [11]	Contains the user time zone information.	
Uri	3GPP TS 29.571 [11]	URI.	
UserLocation	3GPP TS 29.571 [11]	Contains the user location	

5.6.2 Structured data types

5.6.2.1 Introduction

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

5.6.2.2 Type SmPolicyControl

Table 5.6.2.2-1: Definition of type SmPolicyControl

Attribute name	Data type	P	Cardinality	Description	Applicability
context	SmPolicyContextData	M	1	Includes the parameters to request the SM policies by the SMF.	
policy	SmPolicyDecision	M	1	Includes the SM policies authorized by the PCF.	

5.6.2.3 Type SmPolicyContextData

Table 5.6.2.3-1: Definition of type SmPolicyContextData

Attribute name	Data type	P	Cardinality	Description	Applicability
accNetChId	AccNetChId	O	0..1	Indicates the access network charging identifier for default QoS flow or whole PDU session.	
chargEntityAddr	AccNetChargingAddress	O	0..1	Address of the network entity performing charging.	
gpsi	Gpsi	O	0..1	Gpsi shall contain either an External Id or an MSISDN.	
supi	Supi	C	0..1	Subscription Permanent Identifier. It can be omitted for the emergency session.	
pduSessionId	PduSessionId	M	1	PDU session Id	
dnn	Dnn	M	1	The DNN of the PDU session.	
InterGrpIds	array(GroupId)	O	1..N	The internal Group Id(s).	
notificationUri	Uri	M	1	Identifies the recipient of SM policies update notifications sent by the PCF.	
pduSessionType	PduSessionType	M	1	Indicates the type of a PDU session	
accessType	AccessType	O	0..1	The Access Type where the served UE is camping.	
ratType	RatType	O	0..1	The RAT Type where the served UE is camping.	
servingNetwork	NetworkId	O	0..1	The serving network where the served UE is camping.	
userLocationInfo	UserLocation	O	0..1	The location of the served UE is camping.	
ueTimeZone	TimeZone	O	0..1	The time zone where the served UE is camping.	
pei	Pei	O	0..1	The Permanent Equipment Identifier of the served UE.	
ipv4Address	Ipv4Addr	O	0..1	The IPv4 Address of the served UE.	
ipv6AddressPrefix	Ipv6Prefix	O	0..1	The Ipv6 Address Prefix of the served UE.	
ipDomain	string	O	0..1	IPv4 address domain identifier. (NOTE)	
subsSessAmbr	Ambr	O	0..1	Subscribed Session-AMBR.	
subsDefQos	SubscribedDefaultQos	O	0..1	Subscribed Default QoS Information.	
numOfPackFilter	integer	O	0..1	Contains the number of supported packet filter for signalled QoS rules.	
online	boolean	O	0..1	If it is included and set to true, the online charging is applied to the PDU session.	
offline	boolean	O	0..1	If it is included and set to true, the offline charging is applied to the PDU session.	
chargingCharacteristics	string	O	0..1	Contains the Charging Characteristics applied to the PDU session	
3gppPsDataOffStatus	boolean	O	0..1	If it is included and set to true, the 3GPP PS Data Off is activated by the UE.	
refQosIndication	boolean	O	0..1	If it is included and set to true, the reflective QoS is supported by the UE.	
sliceInfo	Snssai	M	1	Identifies the S-NSSAI.	
qosFlowUsage	QosFlowUsage	O	0..1	Indicates the required usage for default QoS flow	
suppFeat	SupportedFeatures	C	0..1	Indicates the list of Supported features used as described in subclause 5.8. This parameter shall be supplied by the NF service consumer in the POST request that requested the creation of an individual SM policy resource.	

traceReq	TraceData	O	0..1	Trace control and configuration parameters information defined in 3GPP TS 32.422 [24].	
NOTE: The value provided in this attribute is implementation specific. The only constraint is that the SMF shall supply a different identifier for each overlapping address domain (e.g. the SMF NF instance identifier).					

5.6.2.4 Type SmPolicyDecision

Table 5.6.2.4-1: Definition of type SmPolicyDecision

Attribute name	Data type	P	Cardinality	Description	Applicability
sessRules	map(SessionRule)	O	1..N	A map of Sessionrules with the content being the SessionRule as described in subclause 5.6.2.7. The key used in this map for each entry is the sessRuleId attribute of the corresponding SessionRule. (NOTE 2)	
pccRules	map(PccRule)	O	1..N	A map of PCC rules with the content being the PCCRule as described in subclause 5.6.2.6. The key used in this map for each entry is the pccRuleId attribute of the corresponding PccRule.	
qosDecs	map(QoSData)	O	1..N	Map of QoS data policy decisions. The key used in this map for each entry is the qosId attribute of the corresponding QoSData. (NOTE 2)	
chgDecs	map(ChargingData)	O	1..N	Map of Charging data policy decisions. The key used in this map for each entry is the chgId attribute of the corresponding ChargingData. (NOTE 2)	
chargingInfo	ChargingInformation	C	1	Contains the CHF addresses of the PDU session. (NOTE 3)	
traffContDecs	map(TrafficControlData)	O	1..N	Map of Traffic Control data policy decisions. The key used in this map for each entry is the tcId attribute of the corresponding TrafficControlData. (NOTE 2)	
umDecs	map(UsageMonitoring Data)	O	1..N	Map of Usage Monitoring data policy decisions. The key used in this map for each entry is the umId attribute of the corresponding UsageMonitoringData.	
qosChars	map(QosCharacteristics)	O	1..N	Map of QoS characteristics for non standard 5QIs and non-preconfigured 5QIs. This map uses the 5QI values as keys. (NOTE 2)	
reflectiveQoSTimer	DurationSec	O	0..1	Defines the lifetime of a UE derived QoS rule belonging to the PDU Session for reflective QoS. (NOTE 2)	
offline	boolean	C	0..1	Indicates the offline charging is applicable to the PDU session or PCC rule. (NOTE 3) (NOTE 4)	
online	boolean	C	0..1	Indicates the online charging is applicable to the PDU session or PCC rule. (NOTE 3) (NOTE 4)	
conds	map(ConditionData)	O	1..N	A map of condition data with the content being as described in subclause 5.6.2.9. The key used in this map for each entry is the condId attribute of the corresponding ConditionData.	
revalidationTime	DateTime	O	0..1	Defines the time before which the SMF shall have to re-request PCC rules.	
pcscfRestIndication	boolean	O	0..1	If this attribute is included and set to true, it indicates that the P-CSCF Restoration is requested. The default value "FALSE" applies, if the attribute is not present and has not been supplied previously.	PCSCF-Restoration-Enhancement
policyCtrlReqTriggers	array(PolicyControlRequestTrigger)	O	1..N	Defines the policy control request triggers subscribed by the PCF.	
lastReqRuleData	array(RequestedRuleData)	O	1..N	Defines the last list of rule control data requested by the PCF.	

lastReqUsageData	RequestedUsageData	O	0..1	Defines the last requested usage data by the PCF.	
praInfos	map(PresenceInfoRm)	O	1..N	Defines the PRA information provisioned by the PCF. The "praId" attribute within the PresenceInfo data type shall also be the key of the map. The "presenceState" attribute within the PresenceInfo data type shall not be supplied.	PRA
ipv4Index	IpIndex	C	0..1	Information that identifies the IP address allocation method for IPv4 address allocation. (NOTE 3)	
ipv6Index	IpIndex	C	0..1	Information that identifies the IP address allocation method for IPv6 address allocation. (NOTE 3)	
qosFlowUsage	QosFlowUsage	O	0..1	Indicates the required usage for default QoS flow	
suppFeat	SupportedFeatures	C	0..1	Indicates the list of negotiated supported features. This parameter shall be supplied by the PCF in the response to the POST request that requested the creation of an individual SM policy resource.	
NOTE 1: For IPv4v6 PDU session, both the "ipv4Index" attribute and "ipv6Index" attribute may be provisioned by the PCF.						
NOTE 2: This attribute shall not be removed if it was provisioned.						
NOTE 3: This attribute may only be supplied by the PCF in the response to the POST request that requested the creation of an individual SM policy resource.						
NOTE 4: If neither "offline" attribute nor "online" attribute is supplied by the PCF, the default charging method pre-cofigured at the SMF shall be applied to the PDU session.						
NOTE 5: If the "chargingInfo" attribute is not supplied by the PCF, the charging information configured at the SMF shall be applied to the PDU session.						

5.6.2.5 Type SmPolicyNotification

Table 5.6.2.5-1: Definition of type SmPolicyNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
resourceUri	Uri	M	1	The resource URI of the individual SM policy related to the notification.	
smPolicyDecision	SmPolicyDecision	M	1	Session management policy (see subclause 5.6.2.4).	

5.6.2.6 Type PccRule

Table 5.6.2.6-1: Definition of type PccRule

Attribute name	Data type	P	Cardinality	Descriptio
flowInfos	array(FlowInformation)	C	1..N	An array of IP flow pac information. (NOTE 3)
appId	string	C	0..1	A reference to the app detection filter configu UPF. (NOTE 3)
contVer	ContentVersion	O	0..1	Indicates the content v the PCC rule.
pccRuleId	string	M	1	Univocally identifies th within a PDU session.
precedence	integer	O	0..1	Determines the order i PCC rule is applied rel other PCC rules within PDU session. It shall b if the "flowInfos" attribu included or may be inc "appId" attribute is incl the PCF initially provis PCC rule. (NOTE 2)
afSigProtocol	AfSigProtocol	O	0..1	Indicates the protocol signalling between the AF. The default value "NO_INFORMATION" if the attribute is not pr has not been supplied
appReloc	boolean	O	0..1	Indication of applicatio possibility. The default "NO_INFORMATION" if the attribute is not pr has not been supplied
refQosData	array(string)	O	1..N	A reference to the QoS type decision type. It is described in subclause (NOTE 1)
refTcData	array(string)	O	1..N	A reference to the TrafficControlData poli type. It is the tcId desc subclause 5.6.2.10. (NOTE 1)
refChgData	array(string)	O	1..N	A reference to the Cha policy decision type. It described in subclause (NOTE 1)
refUmData	array(string)	O	1..N	A reference to UsageMonitoringData decision type. It is the described in subclause (NOTE 1)
refCondData	string	O	0..1	A reference to the con It is the condId describ subclause 5.6.2.9.

roduced for future compatibility. In this release of the specification the maximum number of
ay is 1.
h the "appId" attribute, the precedence can be preconfigured in SMF or provided in the
F. The precedence provided by the PCF shall take precedence.
os" attribute or "appId" attribute shall be supplied by the PCF when the PCC rule is initially
"appId" attribute is supplied, the PCF shall not modify the application identifier supplied
attribute later.

5.6.2.7 Type SessionRule

Table 5.6.2.7-1: Definition of type SessionRule

Attribute name	Data type	P	Cardinality	Description	Applicability
authSessAmbr	Ambr	O	0..1	Authorized Session-AMBR	
authDefQos	AuthorizedDefaultQos	O	0..1	Authorized default QoS information.	
sessRuleId	string	M	1	Univocally identifies the session rule within a PDU session.	
refUmData	string	O	0..1	A reference to UsageMonitoringData policy decision type. It is the umId described in subclause 5.6.2.12.	
refCondData	string	O	0..1	A reference to the condition data. It is the condId described in subclause 5.6.2.9.	

5.6.2.8 Type QosData

Table 5.6.2.8-1: Definition of type QosData

Attribute name	Data type	P	Cardinality	Description	Applicability
qosId	string	M	1	Univocally identifies the QoS control policy data within a PDU session.	
5qi	5Qi	C	0..1	Identifier for the authorized QoS parameters for the service data flow. It shall be included when the QoS data decision is initially provisioned and "defQosFlowIndication" is not included or is included and set to false.	
maxbrUl	BitRateRm	O	0..1	Indicates the max bandwidth in uplink.	
maxbrDl	BitRateRm	O	0..1	Indicates the max bandwidth in downlink.	
gbrUl	BitRateRm	O	0..1	Indicates the guaranteed bandwidth in uplink.	
gbrDl	BitRateRm	O	0..1	Indicates the max guaranteed in downlink.	
arp	Arp	M	1	Indicates the allocation and retention priority.	
qnc	boolean	O	0..1	Indicates whether notifications are requested from 3GPP NG-RAN when the GFBR can no longer (or again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow. Default value "FALSE" is used, if not present and has not been supplied previously.	
reflectiveQos	boolean	O	0..1	Indicates whether the QoS information is reflective for the corresponding service data flow. Default value "FALSE" is used, if not present and has not been supplied previously.	
sharingKeyDl	string	O	0..1	Indicates, by containing the same value, what PCC rules may share resource in downlink direction.	
sharingKeyUl	string	O	0..1	Indicates, by containing the same value, what PCC rules may share resource in uplink direction.	
priorityLevel	5QiPriorityLevelRm	O	0..1	Indicates a priority in scheduling resources among QoS Flows (NOTE).	
averWindow	AverWindowRm	O	0..1	Represents the duration over which the guaranteed and maximum bitrate shall be calculated (NOTE).	
maxDataBurstVol	MaxDataBurstVolRm	O	0..1	Denotes the largest amount of data that is required to be transferred within a period of 5G-AN PDB (NOTE).	
maxPacketLossRateDl	PacketLossRateRm	O	0..1	Indicates the downlink maximum rate for lost packets that can be tolerated for the service data flow.	RAN-Support-Info
maxPacketLossRateUl	PacketLossRateRm	O	0..1	Indicates the uplink maximum rate for lost packets that can be tolerated for the service data flow.	RAN-Support-Info
defQosFlowIndication	boolean	O	0..1	Indicates that the dynamic PCC rule shall always have its binding with the QoS Flow associated with the default QoS rule. Default value "FALSE" is used, if not present and has not been supplied previously.	
NOTE: Applicable only when a value different from the standardized value for this 5QI in table 5.7.4-1 3GPP TS 23.501 [2] is required.					

5.6.2.9 Type ConditionData

Table 5.6.2.9-1: Definition of type ConditionData

Attribute name	Data type	P	Cardinality	Description	Applicability
condId	string	M	1	Uniquely identifies the condition data within a PDU session.	
activationTime	DateTimeRm	O	0..1	The time when the decision data shall be activated.	
deactivationTime	DateTimeRm	O	0..1	The time when the decision data shall be deactivated.	

5.6.2.10 Type TrafficControlData

Table 5.6.2.10-1: Definition of type TrafficControlData

Attribute name	Data type	P	Cardinality	Description	Applicability
tcId	string	M	1	Univocally identifies the traffic control policy data within a PDU session.	
flowStatus	FlowStatus	O	0..1	Enum determining what action to perform on traffic. Possible values are: [enable, disable, enable_uplink, enable_downlink] . The default value "ENABLED" shall apply, if the attribute is not present and has not been supplied previously.	
redirectInfo	RedirectInformation	O	0..1	It indicates whether the detected application traffic should be redirected to another controlled address	ADC
muteNotif	boolean	O	0..1	Indicates whether applicat'on's start or stop notification is to be muted. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously.	ADC
trafficSteeringPolIdDl	string	O	0..1	Reference to a pre-configured traffic steering policy for downlink traffic at the SMF.	TSC
trafficSteeringPolIdUl	string	O	0..1	Reference to a pre-configured traffic steering policy for uplink traffic at the SMF.	TSC
routeToLocs	array(RouteToLocation)	O	1..N	A list of location which the traffic shall be routed to for the AF request	TSC
upPathChgEvent	UpPathChgEvent	O	0..1	Contains the information about the AF subscriptions of the UP path change.	TSC

5.6.2.11 Type ChargingData

Table 5.6.2.11-1: Definition of type ChargingData

Attribute name	Data type	P	Cardinality	Description	Applicability
chgId	string	M	1	Univocally identifies the charging control policy data within a PDU session.	
meteringMethod	MeteringMethod	O	0..1	Defines what parameters shall be metered for offline charging. If the attribute is not present but it has been supplied previously, the previous information remains valid. If the attribute is not present and it has not been supplied previously or the attribute has been supplied previously but the attribute is set to NULL, the metering method pre-configured at the SMF is applicable as default metering method.	
offline	boolean	O	0..1	Indicates the offline charging is applicable to the PDU session or PCC rule. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously. (NOTE)	
online	boolean	O	0..1	Indicates the online charging is applicable to the PDU session or PCC rule. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously. (NOTE)	
ratingGroup	RatingGroup	O	0..1	The charging key for the PCC rule used for rating purposes.	
reportingLevel	ReportingLevel	O	0..1	Defines on what level the SMF reports the usage for the related PCC rule. If the attribute is not present but it has been supplied previously, the previous information remains valid. If the attribute is not present and it has not been supplied previously or the attribute has been supplied previously but it is set to NULL, the reporting level pre-configured at the SMF is applicable as default reporting level.	
serviceId	ServiceId	O	0..1	Indicates the identifier of the service or service component the service data flow in a PCC rule relates to.	
sponsorId	string	O	0..1	Indicates the sponsor identity.	Sponsored-Connectivity
appSvcProvId	string	O	0..1	Indicates the application service provider identity.	Sponsored-Connectivity
afChargingIdentifier	ChargingId	O	0..1	An identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports.	
NOTE:	If neither the "offline" attribute nor "online" attribute has been supplied previously or both the "offline" attribute and "online" attribute are set to FALSE, the default charging method of the PDU session is applicable to the PCC rule referring to the Charging Data decision.				

5.6.2.12 Type UsageMonitoringData

Table 5.6.2. 12-1: Definition of type UsageMonitoringData

Attribute name	Data type	P	Cardinality	Description	Applicability
umId	string	M	1	Univocally identifies the usage monitoring policy data within a PDU session.	
volumeThreshold	VolumeRm	O	0..1	Indicates the total volume threshold.	
volumeThresholdUplink	VolumeRm	O	0..1	Indicates a volume threshold in uplink.	
volumeThresholdDownlink	VolumeRm	O	0..1	Indicates a volume threshold in downlink.	
timeThreshold	DurationSecRm	O	0..1	Indicates a time threshold.	
monitoringTime	DateTimeRm	O	0..1	Indicates the time at which the UP function is expected to reapply the next thresholds (e.g. nextVolThreshold)	
nextVolThreshold	VolumeRm	C	0..1	Indicates a volume threshold after the Monitoring Time.	
nextVolThresholdUplink	VolumeRm	O	0..1	Indicates a volume threshold in uplink after the Monitoring Time.	
nextVolThresholdDownlink	VolumeRm	O	0..1	Indicates al volume threshold in downlink after the Monitoring Time.	
nextTimeThreshold	DurationSecRm	C	0..1	Indicates a time threshold after the Monitoring.	
inactivityTime	DurationSecRm	O	0..1	Defines the period of time after which the time measurement shall stop, if no packets are received.	
exUsagePccRuleIds	array(string)	C	1..N	Contains the PCC rule identifier(s) which corresponding service data flow(s) shall be excluded from PDU Session usage monitoring. It is only included in the UsageMonitoringData instance for session level usage monitoring.	

5.6.2.13 Type RedirectInformation

Table 5.6.2.13-1: Definition of type RedirectInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
redirectEnabled	boolean	C	0..1	This attribute indicates whether the redirect instruction is enable. It shall be included and set to true when the redirect instruction is provisioned initially and may be included subsequently to disable or re-enable the redirect instruction. If the attribute omitted, the previous value shall apply.	
redirectAddressType	RedirectAddressType	O	0..1	Indicates the type of redirect address.	
redirectServerAddress	string	O	0..1	Indicates the address of the redirect server.	

5.6.2.14 Type FlowInformation

Table 5.6.2.14-1: Definition of type FlowInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
flowDescription	FlowDescription	O	0..1	Contains the packet filters of the IP flow(s).	
ethFlowDescription	EthFlowDescription	O	0..1	Defines a packet filter for an Ethernet flow. "fDir" attribute is not applicable.	
packFiltId	string	O	0..1	An identifier of packet filter.	
packetFilterUsage	boolean	O	0..1	The packet shall be sent to the UE. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously.	
tosTrafficClass	string	O	0..1	Contains the Ipv4 Type-of-Service and mask field or the Ipv6 Traffic-Class field and mask field.	
spi	string	O	0..1	The security parameter index of the IPSec packet.	
flowLabel	string	O	0..1	The Ipv6 flow label header field.	
flowDirection	FlowDirectionRm	O	0..1	Indicates the direction/directions that a filter is applicable, downlink only, uplink only or both down- and uplink (bidirectional).	

5.6.2.15 Type SmPolicyDeleteData

Table 5.6.2.15-1: Definition of type SmPolicyDeleteData

Attribute name	Data type	P	Cardinality	Description	Applicability
userLocationInfo	UserLocation	O	0..1	The location of the served UE is camping.	RAN-NAS-Cause, NetLoc
ueTimeZone	TimeZone	O	0..1	The time zone where the served UE is camping.	RAN-NAS-Cause, NetLoc
userLocationInfoTime	DateTime	O	0..1	Contains the NTP time at which the UE was last known to be in the location.	RAN-NAS-Cause, NetLoc
servingNetwork	NetworkId	O	0..1	The serving network where the served UE is camping.	RAN-NAS-Cause, NetLoc
ranNasRelCauses	array(RanNasRelCause)	O	1..N	indicates the RAN or NAS release cause code information	RAN-NAS-Cause
accuUsageReports	array(AccuUsageReport)	O	1..N	Contains the usage report	UMC

5.6.2.16 Type QosCharacteristics

Table 5.6.2.16-1: Definition of type QosCharacteristics

Attribute name	Data type	P	Cardinality	Description	Applicability
5qi	5Qi	M	1	Identifier for the authorized QoS parameters for the service data flow. Applies to PCC rule and PDU session level.	
resourceType	QosResourceType	M	1	Indicates whether the resource type is GBR, delay critical GBR, or non-GBR.	
priorityLevel	5QiPriorityLevel	M	1	Unsigned integer indicating the 5QI Priority Level, within a range of 1 to 127.	
packetDelayBudget	PacketDelBudget	M	1	Unsigned integer indicates the packet delay budget. Packet Delay Budget expressed in milliseconds	
packetErrorRate	PacketErrRate	M	1	Unsigned integer indicating the packet error rate. Examples: Packer Error Rate 10^{-6} shall be encoded as "6". Packer Error Rate 10^{-2} shall be encoded as"2".	
averagingWindow	AverWindow	C	0..1	Indicates the averaging window. This IE shall be present only for a GBR QoS flow or a Delay Critical GBR QoS flow.	
maxDataBurstVol	MaxDataBurstVol	C	0..1	Unsigned Integer.Indicates the maximum data burst volume. This IE shall be present for a Delay Critical GBR QoS flow.	

5.6.2.17 Type ChargingInformation

Table 5.6.2.17-1: Definition of type ChargingInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
primaryChfAddress	Uri	M	1	Contains the primary CHF address.	
secondaryChfAddress	Uri	M	1	Contains the secondary CHF address.	

5.6.2.18 Type AccuUsageReport

Table 5.6.2.18-1: Definition of type AccuUsageReport

Attribute name	Data type	P	Cardinality	Description	Applicability
refUmIds	string	M	1	An id referencing UsageMonitoringData objects associated with this usage report.	
volUsage	Volume	O	0..1	Indicates a total accumulated volume usage.	
volUsageUplink	Volume	O	0..1	Indicates an accumulated volume usage in uplink.	
volUsageDownlink	Volume	O	0..1	Indicates an accumulated volume usage in downlink.	
timeUsage	DurationSec	O	0..1	Indicates an accumulated time usage.	
nextVolUsage	Volume	C	0..1	Indicates an accumulated volume usage after the Monitoring Time.	
nextVolUsageUplink	Volume	O	0..1	Indicates an accumulated volume usage in uplink after the Monitoring Time.	
nextVolUsageDownlink	Volume	O	0..1	Indicates an accumulated volume usage in downlink after the Monitoring Time.	
nextTimeUsage	DurationSec	C	0..1	Indicates an accumulated time usage after the Monitoring.	

5.6.2.19 Type SmPolicyUpdateContextData

Table 5.6.2.19-1: Definition of type SmPolicyUpdateContextData

Attribute name	Data type	P	Cardinality	Description	Applicability
repPolicyCtrlReqTriggers	array(PolicyControlRequestTrigger)	C	1..N	The policy control reqeust triges which are met. It is omitted if no triggers are met such as in subclauses 4.2.4.7 and 4.2.4.15.	
accNetChIds	array(AccNetChId)	O	1..N	Indicates the access network charging identifier for the PCC rule(s) or whole PDU session.	
accessType	AccessType	O	0..1	The Access Type where the served UE is camping.	
ratType	RatType	O	0..1	The RAT Type where the served UE is camping.	
servingNetwork	NetworkId	O	0..1	The serving network where the served UE is camping.	
userLocationInfo	UserLocation	O	0..1	The location of the served UE is camping.	
ueTimeZone	TimeZone	O	0..1	The time zone where the served UE is camping.	
ipv4Address	Ipv4Addr	O	0..1	The IPv4 Address of the served UE.	
relIpv4Address	Ipv4Addr	O	0..1	Indicates the released IPv4 Address of the served UE.	
ipv6AddressPrefix	Ipv6Prefix	O	0..1	The Ipv6 Address Prefix of the served UE.	
relIpv6AddressPrefix	Ipv6Prefix	O	0..1	Indicates the released IPv6 Address Prefix of the served UE in multi-homing case.	
relUeMac	MacAddr48	O	0..1	Indicates the released MAC Address of the served UE.	
ueMac	MacAddr48	O	0..1	The MAC Address of the served UE.	
subsSessAmbr	Ambr	O	0..1	Subscribed Session-AMBR.	
subsDefQos	SubscribedDefaultQos	O	0..1	Subscribed Default QoS Information.	
numOfPackFilter	integer	O	0..1	Contains the number of supported packet filter for signalled QoS rules. (NOTE)	numOfPackFilter
accuUsageReports	array(AccuUsageReport)	O	1..N	Accumulate usage report.	
3gppPsDataOffStatus	boolean	O	0..1	If it is included and set to true, the 3GPP PS Data Off is activated by the UE.	
appDetectionInfos	array(AppDetectionInfo)	O	1..N	Reports the start/stop of the application traffic and detected SDF descriptions if applicable.	ADC
ruleReports	array(RuleReport)	O	1..N	Used to report the PCC rule failure.	
qncReports	array(QosNotificationControlInfo)	O	1..N	QoS Notification Control information.	
userLocationInfoTime	DateTime	O	0..1	Contains the NTP time at which the UE was last known to be in the location.	
repPraInfos	map(PresenceInfo)	O	1..N	Reports the changes of presence reporting area. The "praId" attribute within the PresenceInfo data type shall also be the key of the map. The "presenceState" attribute within the PresenceInfo data type shall be supplied.	PRA
ueInitResReq	UeInitiatedResourceRequest	O	0..1	Indicates a UE requests specific QoS handling for selected SDF.	
refQosIndication	boolean	O	0..1	If it is included and set to true, the reflective QoS is supported by the UE. If it is included and set to false, the reflective QoS is revoked by the UE.	
qosFlowUsage	QosFlowUsage	O	0..1	Indicates the required usage for default QoS flow	

| traceReq | TraceData | C | 0..1 | It shall be included if trace is required to be activated, modified or deactivated (see 3GPP TS 32.422 [24]). For trace modification, it shall contain a complete replacement of trace data. For trace deactivation, it shall contain the Null value. | |
| NOTE: This attribute is only applicable to the 5GS and EPC/E-UTRAN interworking scenario as defined in Annex A. | | | | | |

5.6.2.20 Type UpPathChgEvent

Table 5.6.2.10-1: Definition of type UpPathChgEvent

Attribute name	Data type	P	Cardinality	Description	Applicability
notificationUri	Uri	M	1	Notification address of AF receiving the event notification.	TSC
notifCorreId	string	M	1	It is used to set the value of Notification Correlation ID in the notification sent by the SMF.	TSC
dnaiChgType	DnaiChangeType	M	1	Indicates the type of DNAI change.	TSC

5.6.2.21 Type TerminationNotification

Table 5.6.2.21-1: Definition of type TerminationNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
resourceUri	Uri	M	1	The resource URI of the individual SM policy related to the notification.	
cause	PolicyAssociationReleaseCause	M	1	The cause why the PCF requests the termination of the policy association.	

5.6.2.22 Type AppDetectionInfo

Table 5.6.2.22-1: Definition of type SmPolicyContextData

Attribute name	Data type	P	Cardinality	Description	Applicability
appId	string	M	1	A reference to the application detection filter configured at the UPF	
instanceId	string	O	1	Identifier dynamically assigned by the SMF in order to allow correlation of application Start and Stop events to the specific service data flow description, if service data flow descriptions are deducible.	
sdfDescriptions	array(FlowInformation)	O	1..N	Contains the detected service data flow descriptions if they are deducible.	

5.6.2.23 Type AccNetChId

Table 5.6.2.23-1: Definition of type AccNetChId

Attribute name	Data type	P	Cardinality	Description	Applicability
accNetChaIdValue	ChargingId	M	1	Contains a charging identifier	
refPccRuleIds	array(string)	O	1..N	Contains the identifier of the PCC rule(s) associated to the provided Access Network Charging Identifier.	
sessionChScope	boolean	O	0..1	When it is included and set to true, indicates the Access Network Charging Identifier applies to the whole PDU Session	

5.6.2.24 Type RequestedRuleData

Table 5.6.2.24-1: Definition of type RequestedRuleData

Attribute name	Data type	P	Cardinality	Description	Applicability
refPccRuleIds	array(string)	M	1..N	An array of PCC rule id references to the PCC rules associated with the control data.	
reqData	array(RequestedRuleDataType)	M	1..N	Array of requested rule data type elements indicating what type of rule data is requested for the corresponding referenced PCC rules.	

5.6.2.25 Type RequestedUsageData

Table 5.6.2.25-1: Definition of type RequestedUsageData

Attribute name	Data type	P	Cardinality	Description	Applicability
refUmIds	array(string)	C	1..N	An array of usage monitoring data id references to the usage monitoring data instances for which the PCF is requesting a usage report. This attribute shall only be provided when allUmIds is not set to true.	
allUmIds	boolean	C	0..1	This boolean indicates whether requested usage data applies to all usage monitoring data instances. When it's not included, it means requested usage data shall only apply to the usage monitoring data instances referenced by the refUmIds attribute.	

5.6.2.26 Type UeCampingRep

Table 5.6.2.26-1: Definition of type UeCampingRep

Attribute name	Data type	P	Cardinality	Description	Applicability
accessType	AccessType	O	0..1	The Access Type where the served UE is camping.	
ratType	RatType	O	0..1	The RAT Type where the served UE is camping.	
servingNetwork	NetworkId	O	0..1	The serving network where the served UE is camping.	
userLocationInfo	UserLocation	O	0..1	The location of the served UE is camping.	
ueTimeZone	TimeZone	O	0..1	The time zone where the served UE is camping.	

5.6.2.27 Type RuleReport

Table 5.6.2.27-1: Definition of type RuleReport

Attribute name	Data type	P	Cardinality	Description	Applicability
pccRuleIds	array(string)	M	1..N	Contains the identifier of the affected PCC rule(s).	
ruleStatus	RuleStatus	M	1	Indicates the status of the PCC rule(s).	
contVers	array(ContentVersion)	C	1..N	Indicates the version of the PCC rule. If rule versioning feature is supported, the content version shall be included if it was included when the corresponding PCC rule was installed or modified.	RuleVersioning
failureCode	FailureCode	C	0..1	Indicates the reason that the PCC Rule is being reported. It shall be included when the SMF reports the enforcement failure of the PCC rule(s).	
finUnitAct	FinalUnitAction	O	0..1	Contains the related filter parameters and redirect address parameters (if available), when the user's account cannot cover the service cost.	
ranNasRelCauses	array(RanNasRelCause)	O	1..N	Indicates the RAN or NAS release cause code information.	RAN-NAS-Cause

5.6.2.28 Type RanNasRelCause

Table 5.6.2.28-1: Definition of type RanNasRelCause

Attribute name	Data type	P	Cardinality	Description	Applicability
ngApCause	NgApCause	O	0..1	Indicates the cause value of NGAP protocol.	RAN-NAS-Cause
5gMmCause	5GMmCause	O	0..1	Indicates the cause value of 5GMM protocol.	RAN-NAS-Cause
5gSmCause	5GSmCause	O	0..1	Indicates the cause value of 5GSM protocol.	RAN-NAS-Cause

5.6.2.29 Type UeInitiatedResourceRequest

Table 5.6.2.29-1: UeInitiatedResourceRequest

Attribute name	Data type	P	Cardinality	Description	Applicability
packFiltOp	PacketFilterOperation	M	1	Indicates a UE requests specific QoS handling for selected SDF	
packFiltInfo	array(PacketFilterInfo)	M	1..N	Contains the information from a single packet filter sent from the SMF to the PCF.	
reqQos	RequestedQos	O	0..1	Contains the QoS information requested by the UE	

5.6.2.30 Type PacketFilterInfo

Table 5.6.2.30-1: PacketFilterInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
packFiltId	string	O	0..1	An identifier of packet filter.	
precedence	integer	O	0..1	The requested order for the PCC rule generated from the packet fitler information.	
packFiltCont	PacketFilterContent	O	0..1	Contains the content of the packet filter as requested by the UE and required by the PCF to create the PCC rules.	
tosTrafficClass	string	O	0..1	Contains the Ipv4 Type-of-Service and mask field or the Ipv6 Traffic-Class field and mask field.	
spi	string	O	0..1	The security parameter index of the IPSec packet.	
flowLabel	string	O	0..1	The Ipv6 flow label header field.	
flowDirection	FlowDirection	O	0..1	Indicates the direction/directions that a filter is applicable, downlink only, uplink only or both down- and uplink (bidirectional).	

5.6.2.31 RequestedQos

Table 5.6.2.31-1: RequestedQos

Attribute name	Data type	P	Cardinality	Description	Applicability
5qi	5Qi	M	1	Identifier for the authorized QoS parameters for the service data flow.	
gbrUl	BitRate	O	0..1	Indicates the guaranteed bandwidth in uplink requested by the UE.	
gbrDl	BitRate	O	0..1	Indicates the max guaranteed in downlink requested by the UE.	

5.6.2.32 Type QosNotificationControlInfo

Table 5.6.2.32-1: Definition of type QosNotificationControlInfo

Attribute name	Data type	P	Cardinality	Description	Applicability
refPccRuleIds	array(string)	M	1..N	An array of PCC rule id references to the PCC rules associated with the QosNotificationControlInfo.	
notifType	QosNotifType	M	1	Indicates whether the GBR targets for the indicated SDFs are "NOT_GUARANTEED" or "GUARANTEED" again.	
contVers	array(Content Version)	C	1..N	Indicates the version of the PCC rule. If rule versioning feature is supported, the content version shall be included if it was included when the corresponding PCC rule was installed or modified.	RuleVersioning

5.6.2.33 Type PartialSuccessReport

Table 5.6.2.33-1: Definition of type PartialSuccessReport

Attribute name	Data type	P	Cardinality	Description	Applicability
failureCause	FailureCause	M	1	Application error cause specific to this report.	
ruleReports	array(RuleReport)	M	1	Information about the PCC rules provisioned by the PCF not successfully installed/activated.	
ueCampingRep	UeCampingRep	O	0..1	Includes the current applicable values corresponding to the provisioned policy control request triggers.	

5.6.2.34 Type AuthorizedDefaultQos

Table 5.6.2.34-1: Definition of type AuthorizedDefaultQos

Attribute name	Data type	P	Cardinality	Description	Applicability
5qi	5Qi	C	0..1	5G QoS Identifier. It shall be included when the Authorized Default QoS is initially provisioned.	
arp	Arp	C	0..1	Indicates the allocation and retention priority. It shall be included when the Authorized Default QoS is initially provisioned.	
priorityLevel	5QiPriorityLevelRm	O	0..1	Unsigned integer indicating the 5QI Priority Level, within a range of 1 to 127.	
averWindow	AverWindowRm	O	0..1	Indicates the averaging window. This IE can be present only for GBR QoS flow or a Delay Critical GBR QoS flow.	
maxDataBurstVol	MaxDataBurstVolRm	O	0..1	Unsigned integer indicating the maximum data burst volume. This IE can be present for a Delay Critical GBR QoS flow.	

5.6.2.35 Type AccNetChargingAddress

Table 5.6.2.35-1: Definition of type AccNetChargingAddress

Attribute name	Data type	P	Cardinality	Description	Applicability
anChargIpv4Addr	Ipv4Addr	O	0..1	Includes the IPv4 address of network entity within the access network performing charging.	
anChargIpv6Addr	Ipv6Addr	O	0..1	Includes the IPv6 address of network entity within the access network performing charging.	
NOTE: At least one address of the access network entity (the IPv4 address or the IPv6 address or both if both addresses are available) shall be included.					

5.6.2.36 Type ErrorReport

Table 5.6.2.36-1: Definition of type ErrorReport

Attribute name	Data type	P	Cardinality	Description	Applicability
error	ProblemDetails	M	1	More information on the error shall be provided in the "cause" attribute of the "ProblemDetails" structure.	
ruleReports	array(RuleReport)	O	1..N	Used to report the PCC rule failure.	

5.6.3 Simple data types and enumerations

5.6.3.1 Introduction

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

5.6.3.2 Simple data types

The simple data types defined in table 5.6.3.2-1 shall be supported. For additional simple data types see 3GPP TS 29.571 [11].

Table 5.6.3.2-1: Simple data types

Type Name	Type Definition	Description	Applicability
5GSmCause	Uinteger	Indicates the 5GSM cause code value as defined in subclause 9.10.4.2 of 3GPP TS 24.501 [20].	RAN-NAS-Cause
FlowDescription	string	Defines a packet filter for an IP flow. Refer to subclause 5.4.2 of 3GPP TS 29.212 [23] for encoding.	
PacketFilterContent	string	Defines a packet filter for an IP flow. Refer to subclause 5.3.54 of 3GPP TS 29.212 [23] for encoding.	

5.6.3.3 Enumeration: FlowDirection

Table 5.6.3.3-1: Enumeration FlowDirection

Enumeration value	Description	Applicability
DOWNLINK	The corresponding filter applies for traffic to the UE.	
UPLINK	The corresponding filter applies for traffic from the UE.	
BIDIRECTIONAL	The corresponding filter applies for traffic both to and from the UE.	
UNSPECIFIED	The corresponding filter applies for traffic to the UE (downlink), but has no specific direction declared. The service data flow detection shall apply the filter for uplink traffic as if the filter was bidirectional. The PCF shall not use the value UNSPECIFIED in filters created by the network in NW-initiated procedures. The PCF shall only include the value UNSPECIFIED in filters in UE-initiated procedures if the same value is received from the SMF.	

5.6.3.4 Enumeration: ReportingLevel

Table 5.6.3.4-1: Enumeration ReportingLevel

Enumeration value	Description	Applicability
SER_ID_LEVEL	Indicates that the usage shall be reported on service id and rating group combination level.	
RAT_GR_LEVEL	Indicates that the usage shall be reported on rating group level.	
SPON_CON_LEVEL	Indicates that the usage shall be reported on sponsor identity and rating group combination level.	

5.6.3.5 Enumeration: MeteringMethod

Table 5.6.3.5-1: Enumeration MeteringMethod

Enumeration value	Description	Applicability
DURATION	Indicates that the duration of the service data flow traffic shall be metered.	
VOLUME	Indicates that volume of the service data flow traffic shall be metered.	
DURATION_VOLUME	Indicates that the duration and the volume of the service data flow traffic shall be metered.	
EVENT	Indicates that events of the service data flow traffic shall be metered.	

5.6.3.6 Enumeration: PolicyControlRequestTrigger

Table 5.6.3.6-1: Enumeration PolicyControlRequestTrigger

Enumeration value	Description	Applicability
PLMN_CH	PLMN Change	
RES_MO_RE	A request for resource modification has been received by the SMF. (NOTE)	
AC_TY_CH	Access Type Change	
UE_IP_CH	UE IP address change. (NOTE)	
UE MAC_CH	A new UE MAC address is detected or a used UE MAC address is inactive for a specific period	
AN_CH_COR	Access Network Charging Correlation Information	
US_RE	The PDU Session or the Monitoring key specific resources consumed by a UE either reached the threshold or needs to be reported for other reasons.	UMC
APP_STA	The start of application traffic has been detected.	ADC
APP_STO	The stop of application traffic has been detected.	ADC
AN_INFO	Access Network Information report	NetLoc
CM_SES_FAIL	Credit management session failure	
PS_DA_OFF	The SMF reports when the 3GPP PS Data Off status changes. (NOTE)	3GPP-PS-Data-Off
DEF_QOS_CH	Default QoS Change. (NOTE)	
SE_AMBR_CH	Session AMBR Change. (NOTE)	
QOS_NOTIF	The SMF notify the PCF when receiving notification from RAN that QoS targets of the QoS Flow cannot be guaranteed or can be guaranteed.	
NO_CREDIT	Out of credit	
PRA_CH	Change of UE presence in Presence Reporting Area	PRA
SAREA_CH	Location Change with respect to the Serving Area	
SCNN_CH	Location Change with respect to the Serving CN node	
RE_TIMEOUT	Indicates the SMF generated the request because there has been a PCC revalidation timeout (i.e. Enforced PCC rule request defined in table 6.1.3.5.-1 of 3GPP TS 29.503 [6]).	
RES_RELEASE	Indicates that the SMF can inform the PCF of the outcome of the release of resources for those rules that require so.	RAN-NAS-Cause
SUCC_RES_ALLO	Indicates that the SMF shall inform the PCF of the successful resource allocation for those rules that requires so.	
RAT_TY_CH	RAT type change.	
REF_QOS_IND_CH	Reflective QoS indication Change	
NOTE: The SMF always reports to the PCF.		

The PCF may provision the values of policy control request trigger which are not always reported by the SMF as defined in subclause 4.2.6.4.

When the SMF detects the corresponding policy control request trigger(s), the SMF shall report the detected trigger(s) to the PCF as defined in subclause 4.2.4.1 with the additional information for different independent policy control request triggers as follows:

If the "PLMN_CH" is provisioned, when the SMF detectes a change of PLMN, the SMF shall include the "PLMN_CH" within the "repPolicyCtrlReqTriggers" attribute and the current identifier of the serving network within the "servingNetwork" attribute.

When the SMF receives the resource modification request from the UE, the SMF shall include the "RES_MO_RE" within the "repPolicyCtrlReqTriggers" attribute and the information for requesting the PCC rule as defined in subclause 4.2.4.17.

If the "AC_TY_CH" is provisioned, when the SMF detectes a change of access type, the SMF shall include the "AC_TY_CH" within the "repPolicyCtrlReqTriggers" attribute and the current access type within the "accessType" attribute.

When the SMF detects an IPv4 address and/or an IPv6 prefix is allocated or released, the SMF shall include the "UE_IP_CH" within the "repPolicyCtrlReqTriggers" attribute and new allocated UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "ipv6AddressPrefix" attribute or the released UE Ipv4 address within the "ipv4Address" attribute and/or the UE Ipv6 prefix within the "relIpv6AddressPrefix" attribute.

When the SMF detects a new UE MAC address or a used UE MAC address is not used any more, the SMF shall include the "UE_MAC_CH" within the "repPolicyCtrlReqTriggers" attribute and new detected UE MAC address within the "ueMac" attribute or the not used UE MAC address within the "relUeMac" attribute.If the "AN_CH_COR" is provisioned, when the SMF is provisioned with the PCC rule as defined in subclause 4.2.6.5.1, the SMF shall notify the PCF of access network charging identifier associated with the PCC rules as defiend in subclause 4.2.4.13.

If the "US_RE" is provisioned, when the SMF receives the usage report from the UPF, the SMF shall notify the PCF of the accumulated usage as defined in subclause 4.2.4.10. Applicable to functionality introduced with the UMC feature as described in subclause 5.8.

If the "APP_STA" is provisioned, when the SMF receives the application start report from the UPF, the SMF shall notify the PCF of the application start report as defined in subclause 4.2.4.6. Applicable to functionality introduced with the ADC feature as described in subclause 5.8.

If the "APP_STO" is provisioned, when the SMF receives the application stop report from the UPF, the SMF shall notify the PCF of the application stop report as defiend in subclause 4.2.4.6. Applicable to functionality introduced with the ADC feature as described in subclause 5.8.

If the "AN_INFO" is provisioned, when the SMF receives the reported access network information from the access network, the SMF shall notify the PCF of the access network information as defiend in subclause 4.2.4.9. Applicable to functionality introduced with the NetLoc feature as described in subclause 5.8.

If the "PS_DA_OFF" is provisioned, when the SMF receives a change of 3GPP PS Data Off status from the UE, the SMF shall notify the PCF as defined in subclause 4.2.4.8. Applicable to functionality introduced with the 3GPP-PS-Data-Off feature as described in subclause 5.8.

When the SMF detects a change of subscribed default QoS, the SMF shall include the "DEF_QOS_CH" within the "repPolicyCtrlReqTriggers" attribute and the new subscribed default QoS within the "subsDefQos" attribute.

When the SMF detects a change of subscribed Session-AMBR, the SMF shall include the "SE_AMBR_CH" within the "repPolicyCtrlReqTriggers" attribute and the new subscribed Session-AMBR within the "subsSessAmbr" attribute.

If the "QOS_NOTIF" is provisioned, when the SMF receives a notification from access network that QoS targets of the QoS Flow cannot be guaranteed or can be guaranteed again, the SMF shall send the notification as defined in subclause 4.2.4.x.

If the "NO_CREDIT" is provisioned, when the SMF detects the credit for the PCC rule(s) is no longer available, the SMF shall include the "NO_CREDIT" within the "repPolicyCtrlReqTriggers" attribute and the affected PCC rules within the "ruleReports" attribute.

If the "PRA_CH" is provisioned, the SMF is provisioned the presence reporting area information as defined in subclause 4.2.6.5.6. When the SMF receives the presence reporting area information from the serving node, the SMF shall notify the PCF of the reported presence area information as defined in subclause 4.2.4.16. Applicable to functionality introduced with the PRA feature as described in subclause 5.8.

If the "SAREA_CH" is provisioned, when the SMF detects a change of serving area (i.e. tracking area), the SMF shall include the "SAREA_CH" within the "repPolicyCtrlReqTriggers" attribute and the current TAI within the "userLocationInfo" attribute.

If the "RE_TIMEOUT" is provisioned, the SMF is provisioned the revalidation time by the PCF. The SMF shall request the policy before the indicated the revalidation time as defined in subclause 4.2.4.13.

If the "RES_RELEASE" is provisioned, when the SMF receives the request of PCC rule removal as defined in subclause 4.2.6.5.2, the SMF shall report the outcome of resource release as defined in subclause 4.2.4.12. Applicable to functionality introduced with the RAN-NAS-Cause feature as described in subclause 5.8.

When "SUCC_RES_ALLO" is provisioned and PCC rules are provisioned according to subclause 4.2.6.5.5, the SMF shall inform the PCF of the successful resource allocation as defined in subclause 4.2.4.14.

If the "RAT_TY_CH" is provisioned, when the SMF detects a change of the RAT type, the SMF shall include the "RAT_TY_CH" within the "repPolicyCtrlReqTriggers" attribute and the current RAT type within the "ratType" attribute.

If the "REF_QOS_IND_CH" is provisioned, when the SMF receives a change of reflective QoS indication from the UE, the SMF shall include the "REF_QOS_IND_CH" within the "repPolicyCtrlReqTriggers" attribute and the indication within the "refQosIndication" attribute.

5.6.3.7 Enumeration: RequestedRuleDataType

Table 5.6.3.7-1: Enumeration RequestedRuleDataType

Enumeration value	Description	Applicability
CH_ID	Indicates that the requested rule data is the charging identifier.	
MS_TIME_ZONE	Indicates that the requested access network info type is the UE's timezone.	
USER_LOC_INFO	Indicates that the requested access network info type is the UE's location.	
RES_RELEASE	Indicates that the requested rule data is the result of the release of resource.	
SUCC_RES_ALLO	Indicates that the requested rule data is the successful resource allocation.	

5.6.3.8 Enumeration: RuleStatus

Table 5.6.3.8-1: Enumeration RuleStatus

Enumeration value	Description	Applicability
ACTIVE	Indicates that the PCC rule(s) are successfully installed (for those provisioned from PCF) or activated (for those pre-defined in SMF), or the session rule(s) are successfully installed.	
INACTIVE	Indicates that the PCC rule(s) are removed (for those provisioned from PCF) or inactive (for those pre-defined in SMF) or the session rule(s) are removed.	

5.6.3.9   Enumeration: FailureCode

Table 5.6.3.9-1: Enumeration FailureCode

Enumeration value	Description	Applicability
UNK_RULE_ID	Indicates that the pre-provisioned PCC rule could not be successfully activated because the PCC rule identifier is unknown to the SMF.	
RA_GR_ERR	Indicates that the PCC rule could not be successfully installed or enforced because the Rating Group specified within the Charging Data policy decision which the PCC rule refers to is unknown or, invalid.	
SER_ID_ERR	Indicates that the PCC rule could not be successfully installed or enforced because the Service Identifier specified within the Charging Data policy decision which the PCC rule refers to is invalid, unknown, or not applicable to the service being charged.	
NF_MAL	Indicates that the PCC rule could not be successfully installed (for those provisioned from the PCF) or activated (for those pre-defined in SMF) or enforced (for those already successfully installed) due to SMF/UPF malfunction.	
RES_LIM	Indicates that the PCC rule could not be successfully installed (for those provisioned from PCF) or activated (for those pre-defined in SMF) or enforced (for those already successfully installed) due to a limitation of resources at the SMF/UPF.	
MAX_NR_QOS_Flow	Indicates that the PCC rule could not be successfully installed (for those provisioned from PCF) or activated (for those pre-defined in SMF) or enforced (for those already successfully installed) due to the fact that the maximum number of QoS flows has been reached for the PDU session.	
MISS_FLOW_INFO	Indicates that the PCC rule could not be successfully installed or enforced because the Flow Information AVP is not specified within the "pccRule" attribute by the PCF during the first install request of the PCC rule.	
RES_ALLO_FAIL	Indicates that the PCC rule could not be successfully installed or maintained since the QoS flow establishment/modification failed, or the QoS flow was released.	
UNSUCC_QOS_VAL	This value is used to: - indicate that the QoS validation has failed or, - Indicate when Guaranteed Bandwidth > Max-Requested-Bandwidth.	
INCOR_FLOW_INFO	Indicates that the PCC rule could not be successfully installed or modified at the SMF because the provided flow information is not supported by the network (e.g. the provided IP address(es) or Ipv6 prefix(es) do not correspond to an IP version applicable for the PDU session).	
PS_TO_CS_HAN	Indicates that the PCC rule could not be maintained because of PS to CS handover.	
APP_ID_ERR	Indicates that the PCC rule could not be successfully installed or enforced because the Application Identifier is invalid, unknown, or not applicable to the application required for detection.	
NO_QOS_FLOW_BOUND	Indicates that there is no QoS flow which the SMF can bind the PCC rule(s) to.	
FILTER_RES	Indicates that the Flow Information cannot be handled by the SMF because any of the restrictions was not met.	
MISS_REDI_SER_ADDR	Indicates that the PCC rule could not be successfully installed or enforced at the SMF because there is no valid Redirect Server Address within the Traffic Control Data policy decision which the PCC rule refers to, provided by the PCF, and no preconfigured redirection address for this PCC rule at the SMF.	
CM_END_USER_SER_DENIED	Indicates that the charging system denied the service request due to service restrictions (e.g. terminate rating group) or limitations related to the end-user, for example the end-user's account could not cover the requested service.	
CM_CREDIT_CON_NOT_APP	Indicates that the charging system determined that the service can be granted to the end user but no further credit control is needed for the service (e.g. service is free of charge or is treated for offline charging).	
CM_AUTH_REJ	Indicates that the charging system denied the service request in order to terminate the service for which credit is requested.	

CM_USER_UNK	Indicates that the specified end user could not be found in the charging system.	
CM_RAT_FAILED	Indicates that the charging system cannot rate the service request due to insufficient rating input, incorrect AVP combination or due to an attribute or an attribute value that is not recognized or supported in the rating.	
SESS_AMBR_FAILURE	Indicates that the session AMBR update is failure.	
DEF_QOS_FAILURE	Indicates that the default QoS update is failure.	

5.6.3.10 Enumeration: AfSigProtocol

Table 5.6.3.10-1: Enumeration AfSigProtocol

Enumeration value	Description	Applicability
NO_INFORMATION	Indicate that no information about the AF signalling protocol is being provided.	ProvAFsignalFlow
SIP	Indicate that the signalling protocol is Session Initiation Protocol.	ProvAFsignalFlow

5.6.3.11 Enumeration: PacketFilterOperation

Table 5.6.3.11-1: Enumeration PacketFilterOperation

Enumeration value	Description	Applicability
DELETION	Indicates that the resources reserved for the provided packet filter identifiers are to be deleted and are no longer used by the UE.	
ADDITION	Indicates that the UE requests resources allocated for the provided packet filters.	
MODIFICATION	Indicates that the reserved QoS, the filter, the precedence, or any of the fields for the provided packet filter identifiers are being modified.	

5.6.3.12 Enumeration: RedirectAddressType

Table 5.6.3.12-1: Enumeration RedirectAddressType

Enumeration value	Description	Applicability
IPV4_ADDR	Indicates that the address type is in the form of "dotted-decimal" IPv4 address.	
IPV6_ADDR	Indicates that the address type is in the form of IPv6 address.	
URL	Indicates that the address type is in the form of Uniform Resource Locator.	
SIP_URI	Indicates that the address type is in the form of SIP Uniform Resource Identifier.	

5.6.3.13 Enumeration: QosFlowUsage

Table 5.6.3.13-1: Enumeration QosFlowUsage

Enumeration value	Description	Applicability
GENERAL	Indicates no specific QoS flow usage information is available.	
IMS_SIG	Indicates that the QoS flow is used for IMS signalling only.	

5.6.3.14 Enumeration: FailureCause

Table 5.6.3.14-1: Enumeration FailureCause

Enumeration value	Description	Applicability
PCC_RULE_EVENT	The PCC rules provisioned by the PCF in the request cannot be installed/activated. It is used to inform the PCF that the request failed and should not be attempted again.	
PCC_QOS_FLOW_EVENT	For some reason the PCC rules provisioned by the PCF in the request cannot be enforced or modified successfully in a network initiated procedure. It is used to inform the PCF that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future.	

5.6.3.15 Enumeration: FlowDirectionRm

This data type is defined in the same way as the "FlowDirection" data type, but with the OpenAPI "nullable: true" property.

5.7 Error handling

5.7.1 General

HTTP error handling shall be supported as specified in subclause 5.2.4 of 3GPP TS 29.500 [4].

For the Npcf_SMPolicyControl API, HTTP error responses shall be supported as specified in subclause 4.8 of 3GPP TS 29.501 [5]. Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [4] 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 [4]. In addition, the requirements in the following subclauses shall apply.

5.7.2 Protocol Errors

In this Release of the specification, there are no additional protocol errors applicable for the Npcf_SMPolicyControl API.

5.7.3 Application Errors

The application errors defined for the Npcf_SMPolicyControl API are listed in table 5.7.3-1 and 5.7.3-2. The PCF shall include in the HTTP status code a "ProblemDetails" data structure with the "cause" attribute indicating the application error as listed in table 5.7.3-1 when PCF acts as a server. The SMF shall include in the HTTP status code a "ProblemDetails" data structure with the "cause" attribute indicating the application error as listed in table 5.7.3-2 when SMF acts as a server.

Table 5.7.3-1: Application errors when PCF acts as a server

Application Error	HTTP status code	Description
USER_UNKNOWN	400 Bad Request	The HTTP request is rejected because the end user specified in the request is unknown to the PCF.
ERROR_INITIAL_PARAMETERS	400 Bad Request	The HTTP request is rejected because the set of session or subscriber information needed by the PCF for rule selection is incomplete or erroneous or not available for the decision to be made. (E.g. QoS, , RAT type, subscriber information)
ERROR_TRIGGER_EVENT	400 Bad Request	The HTTP request is rejected because the set of session information sent the message originated due to a trigger been met is incoherent with the previous set of session information for the same session. (E.g. trigger met was RAT changed, and the RAT notified is the same as before)
TRAFFIC_MAPPING_INFO_REJECTED	403 Forbidden	The HTTP request is rejected because the PCF does not accept one or more of the traffic mapping filters provided by the SMF in a PCC Request.
ERROR_CONFLICTING_REQUEST	403 Forbidden	The HTTP request is rejected because the PCF cannot accept the UE-initiated resource request as a network-initiated resource allocation is already in progress that has packet filters that cover the packet filters in the received UE-initiated resource request. The SMF shall reject the attempt for UE-initiated resource request.
POLICY_CONTEXT_DENIED	403 Forbidden	The HTTP request is rejected because the PCF does not accept the SMF request due to operator policies and/or local configuration.

Table 5.7.3-2: Application errors when SMF acts as a server

Application Error	HTTP status code	Description
PCC_RULE_EVENT	400 Bad Request	The HTTP request is rejected because all the PCC rules provisioned by the PCF in the request cannot be installed/activated. It is used to inform the PCF that the request failed, and should not be attempted again.
PCC_QOS_FLOW_EVENT	400 Bad Request	The HTTP request is rejected because for some reason all the PCC rules provisioned by the PCF in the request cannot be enforced or modified successfully in a network initiated procedure. It is used to inform the PCF that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future.

5.8 Feature negotiation

The optional features in table 5.8-1 are defined for the Npcf_SMPolicyControl API. They shall be negotiated using the extensibility mechanism defined in subclause 6.6 of 3GPP TS 29.500 [4].

Table 5.8-1: Supported Features

Feature number	Feature Name	Description
1	TSC	This feature indicates support for traffic steering control in the (S)Gi-LAN or routing of the user traffic to a local Data Network identified by the DNAI per AF request. If the SMF supports this feature, the PCF shall behave as described in subclause 4.2.6.2.20.
2	ResShare	This feature indicates the support of service data flows that share resources. If the SMF supports this feature, the PCF shall behave as described in subclause 4.2.7.4.
3	3GPP-PS-Data-Off	This feature indicates the support of 3GPP PS Data off status change reporting.
4	ADC	This feature indicates the support of application detection and control.
5	UMC	Indicates that the usage monitoring control is supported.
6	NetLoc	This feature indicates the support of the Access Network Information Reporting for 5GS.
7	RAN-NAS-Cause	This feature indicates the support for the detailed release cause code information from the access network.
8	ProvAFsignalFlow	This feature indicates support for the feature of IMS Restoration as described in subclause 4.2.3.17. If SMF supports this feature the PCF may provision AF signalling IP flow information.
9	PCSCF-Restoration-Enhancement	This feature indicates support of P-CSCF Restoration Enhancement. It is used for the SMF to indicate if it supports P-CSCF Restoration Enhancement.
10	PRA	This feature indicates the support of presence reporting area change reporting.
11	RuleVersioning	This feature indicates the support of PCC rule versioning as defined in subclause 4.2.6.7.
12	SponsoredConnectivity	This feature indicates support for sponsored data connectivity feature. If the SMF supports this feature, the PCF may authorize sponsored data connectivity to the subscriber.
13	RAN-Support-Info	This feature indicates the support of maximum packet loss rate value(s) for uplink and/or downlink voice service data flow(s).

5.9 Security

As indicated in 3GPP TS 33.501 [27], the access to the Npcf_SMPolicyControl API shall be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [28]), using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [29]) plays the role of the authorization server.

An NF Service Consumer, prior to consuming services offered by the Npcf_SMPolicyControl API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [29], subclause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF Service Consumer used for discovering the Npcf_SMPolicyControl service.

The Npcf_SMPolicyControl API defines a single scope "npcf-smpolicycontrol" for OAuth2 authorization (as specified in 3GPP TS 33.501 [27]) for the entire API, and it does not define any additional scopes at resource or operation level.

Annex A (normative): OpenAPI specification

A.1 General

The present Annex contains an OpenAPI [10] specification of HTTP messages and content bodies used by the Npcf_SMPolicyControl API.

A.2 Npcf_SMPolicyControl API

```
openapi: 3.0.0
info:
  description: Session Management Policy Control Service
  version: "1.0.0"
  title: Npcf_SMPolicyControl
externalDocs:
  description: 3GPP TS 29.512 V15.2.0; 5G System; Session Management Policy Control Service.
  url: 'http://www.3gpp.org/ftp/Specs/archive/29_series/29.512/'
security:
  - {}
  - oAuth2Clientcredentials:
    - npcf-smpolicycontrol
servers:
  - url: '{apiRoot}/npcf-smpolicycontrol/v1'
    variables:
      apiRoot:
        default: https://example.com
        description: apiRoot as defined in subclause 4.4 of 3GPP TS 29.501
paths:
  /sm-policies:
    post:
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/SmPolicyContextData'
      responses:
        '201':
          description: Created
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/SmPolicyDecision'
          headers:
            Location:
              description: 'Contains the URI of the newly created resource'
              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':
          description: Not Found
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
```

```
                  $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      callbacks:
        SmPolicyUpdateNotification:
          '{$request.body#/notificationUri}/update':
            post:
              requestBody:
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/SmPolicyNotification'
              responses:
                '200':
                  description: OK. The current applicable values corresponding to the policy control
request trigger is reported
                  content:
                    application/json:
                      schema:
                        oneOf:
                          - $ref: '#/components/schemas/UeCampingRep'
                          - type: array
                            items:
                              $ref: '#/components/schemas/PartialSuccessReport'
                            minItems: 1
                '204':
                  description: No Content, Notification was succesfull
                  content:
                    application/json:
                      schema:
                        $ref: '#/components/schemas/RuleReport'
                '400':
                  description: Bad Request.
                  content:
                    application/json:
                      schema:
                        $ref: '#/components/schemas/ErrorReport'
                '401':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/401'
                '403':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/403'
                '404':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/404'
                '411':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/411'
                '413':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/413'
                '415':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/415'
                '429':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/429'
                '500':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/500'
                '503':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/503'
                default:
                  $ref: 'TS29571_CommonData.yaml#/components/responses/default'
        SmPolicyControlTerminationRequestNotification:
          '{$request.body#/notificationUri}/terminate':
            post:
              requestBody:
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/TerminationNotification'
              responses:
                '204':
                  description: No Content, Notification was succesful
                '400':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/400'
                '401':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/401'
                '403':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/403'
                '404':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/404'
                '411':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/411'
```

```
                       '413':
                         $ref: 'TS29571_CommonData.yaml#/components/responses/413'
                       '415':
                         $ref: 'TS29571_CommonData.yaml#/components/responses/415'
                       '429':
                         $ref: 'TS29571_CommonData.yaml#/components/responses/429'
                       '500':
                         $ref: 'TS29571_CommonData.yaml#/components/responses/500'
                       '503':
                         $ref: 'TS29571_CommonData.yaml#/components/responses/503'
                       default:
                         $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  /sm-policies/{smPolicyId}:
    get:
      parameters:
        - name: smPolicyId
          in: path
          description: Identifier of a policy association
          required: true
          schema:
            type: string
      responses:
        '200':
          description: OK. Resource representation is returned
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/SmPolicyControl'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '406':
          $ref: 'TS29571_CommonData.yaml#/components/responses/406'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  /sm-policies/{smPolicyId}/update:
    post:
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/SmPolicyUpdateContextData'
      parameters:
        - name: smPolicyId
          in: path
          description: Identifier of a policy association
          required: true
          schema:
            type: string
      responses:
        '200':
          description: OK. Updated policies are returned
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/SmPolicyDecision'
        '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'
```

```yaml
                '413':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/413'
                '415':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/415'
                '429':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/429'
                '500':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/500'
                '503':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/503'
                default:
                  $ref: 'TS29571_CommonData.yaml#/components/responses/default'
  /sm-policies/{smPolicyId}/delete:
    post:
      requestBody:
        required: true
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/SmPolicyDeleteData'
      parameters:
        - name: smPolicyId
          in: path
          description: Identifier of a policy association
          required: true
          schema:
            type: string
      responses:
        '204':
          description: No content
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '401':
          $ref: 'TS29571_CommonData.yaml#/components/responses/401'
        '403':
          $ref: 'TS29571_CommonData.yaml#/components/responses/403'
        '404':
          $ref: 'TS29571_CommonData.yaml#/components/responses/404'
        '411':
          $ref: 'TS29571_CommonData.yaml#/components/responses/411'
        '413':
          $ref: 'TS29571_CommonData.yaml#/components/responses/413'
        '415':
          $ref: 'TS29571_CommonData.yaml#/components/responses/415'
        '429':
          $ref: 'TS29571_CommonData.yaml#/components/responses/429'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        '503':
          $ref: 'TS29571_CommonData.yaml#/components/responses/503'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
components:
  securitySchemes:
    oAuth2ClientCredentials:
      type: oauth2
      flows:
        clientCredentials:
          tokenUrl: '{nrfApiRoot}/oauth2/token'
          scopes:
            npcf-smpolicycontrol: Access to the Npcf_SMPolicyControl API
  schemas:
    SmPolicyControl :
      type: object
      properties:
        context:
          $ref: '#/components/schemas/SmPolicyContextData'
        policy:
          $ref: '#/components/schemas/SmPolicyDecision'
      required:
        - context
        - policy
    SmPolicyContextData:
      type: object
      properties:
        accNetChId:
          $ref: '#/components/schemas/AccNetChId'
        chargEntityAddr:
```

```
            $ref: '#/components/schemas/AccNetChargingAddress'
          gpsi:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
          supi:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
          interGrpIds:
            type: array
            items:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/GroupId'
            minItems: 1
          pduSessionId:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PduSessionId'
          pduSessionType:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/PduSessionType'
          chargingcharacteristics:
            type: string
          dnn:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
          notificationUri:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
          accessType:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
          ratType:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
          servingNetwork:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/NetworkId'
          userLocationInfo:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
          ueTimeZone:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
          pei:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Pei'
          ipv4Address:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
          ipv6AddressPrefix:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
          ipDomain:
            type: string
            description: Indicates the IPv4 address domain
          subsSessAmbr:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
          subsDefQos:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/SubscribedDefaultQos'
          numOfPackFilter:
            type: integer
            description: Contains the number of supported packet filter for signalled QoS rules.
          online:
            type: boolean
            description: If it is included and set to true, the online charging is applied to the PDU
session.
          offline:
            type: boolean
            description: If it is included and set to true, the offline charging is applied to the PDU
session.
          3gppPsDataOffStatus:
            type: boolean
            description: If it is included and set to true, the 3GPP PS Data Off is activated by the
UE.
          refQosIndication:
            type: boolean
            description: If it is included and set to true, the reflective QoS is supported by the UE.
          traceReq:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/TraceData'
          sliceInfo:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Snssai'
          qosFlowUsage:
            $ref: '#/components/schemas/QosFlowUsage'
          suppFeat:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
        required:
          - supi
          - pduSessionId
          - pduSessionType
          - dnn
          - notificationUri
          - sliceInfo
    SmPolicyDecision:
      type: object
```

```
      properties:
        sessRules:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/SessionRule'
          minProperties: 1
          description: A map of Sessionrules with the content being the SessionRule as described in
subclause 5.6.2.7.
        pccRules:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/PccRule'
          minProperties: 1
          description: A map of PCC rules with the content being the PCCRule as described in
subclause 5.6.2.6.
          nullable: true
        pcscfRestIndication:
          type: boolean
          description: If it is included and set to true, it indicates the P-CSCF Restoration is
requested.
        qosDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/QosData'
          minProperties: 1
          description: Map of QoS data policy decisions.
        chgDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/ChargingData'
          minProperties: 1
          description: Map of Charging data policy decisions.
          nullable: true
        chargingInfo:
          $ref: '#/components/schemas/ChargingInformation'
        traffContDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/TrafficControlData'
          minProperties: 1
          description: Map of Traffic Control data policy decisions.
        umDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/UsageMonitoringData'
          minProperties: 1
          description: Map of Usage Monitoring data policy decisions.
          nullable: true
        qosChars:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/QosCharacteristics'
          minProperties: 1
          description: Map of QoS characteristics for non standard 5QIs. This map uses the 5QI
values as keys.
        reflectiveQoSTimer:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        conds:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/ConditionData'
          minProperties: 1
          description: A map of condition data with the content being as described in
subclause 5.6.2.9.
          nullable: true
        revalidationTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        offline:
          type: boolean
          description: Indicates the offline charging is applicable to the PDU session or PCC rule.
        online:
          type: boolean
          description: Indicates the online charging is applicable to the PDU session or PCC rule.
        policyCtrlReqTriggers:
          type: array
          items:
            $ref: '#/components/schemas/PolicyControlRequestTrigger'
          minItems: 1
```

```
              description: Defines the policy control request triggers subscribed by the PCF.
              nullable: true
            lastReqRuleData:
              type: array
              items:
                $ref: '#/components/schemas/RequestedRuleData'
              minItems: 1
              description: Defines the last list of rule control data requested by the PCF.
            lastReqUsageData:
              $ref: '#/components/schemas/RequestedUsageData'
            praInfos:
              type: object
              additionalProperties:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfoRm'
              minProperties: 1
              description: Map of PRA information.
              nullable: true
            ipv4Index:
              $ref: 'TS29519_Policy_Data.yaml#/components/schemas/IpIndex'
              description: Information that identifies which IP pool or external server is used to
allocate the IPv4 address.
            ipv6Index:
              $ref: 'TS29519_Policy_Data.yaml#/components/schemas/IpIndex'
              description: Information that identifies which IP pool or external server is used to
allocate the IPv6 address.
            qosFlowUsage:
              $ref: '#/components/schemas/QosFlowUsage'
            suppFeat:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      SmPolicyNotification:
        type: object
        properties:
          resourceUri:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
          smPolicyDecision:
            $ref: '#/components/schemas/SmPolicyDecision'
      PccRule:
        type: object
        properties:
          flowInfos:
            type: array
            items:
              $ref: '#/components/schemas/FlowInformation'
            minItems: 1
            description: An array of IP flow packet filter information.
          appId:
            type: string
            description: A reference to the application detection filter configured at the UPF.
          contVer:
            $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/ContentVersion'
          pccRuleId:
            type: string
            description: Univocally identifies the PCC rule within a PDU session.
          precedence:
            type: integer
            description: Determines the order in which this PCC rule is applied relative to other PCC
rules within the same PDU session.
          afSigProtocol:
            $ref: '#/components/schemas/AfSigProtocol'
            nullable: true
          appReloc:
            type: boolean
            description: Indication of application relocation possibility.
          refQosData:
            type: array
            items:
              type: string
            minItems: 1
            maxItems: 1
            description: A reference to the QoSData policy type decision type. It is the qosId
described in subclause 5.6.2.8. (NOTE)
          refTcData:
            type: array
            items:
              type: string
            minItems: 1
            maxItems: 1
```

```
              description: A reference to the TrafficControlData policy decision type. It is the tcId
          described in subclause 5.6.2.10. (NOTE)
                  refChgData:
                    type: array
                    items:
                      type: string
                    minItems: 1
                    maxItems: 1
                    description: A reference to the ChargingData policy decision type. It is the chgId
          described in subclause 5.6.2.11. (NOTE)
                    nullable: true
                  refUmData:
                    type: array
                    items:
                      type: string
                    minItems: 1
                    maxItems: 1
                    description: A reference to UsageMonitoringData policy decision type. It is the umId
          described in subclause 5.6.2.12. (NOTE)
                    nullable: true
                  refCondData:
                    type: string
                    description: A reference to the condition data. It is the condId described in
          subclause 5.6.2.9.
                    nullable: true
                required:
                  - pccRuleId
                nullable: true
            SessionRule:
              type: object
              properties:
                authSessAmbr:
                  $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
                authDefQos:
                  $ref: '#/components/schemas/AuthorizedDefaultQos'
                sessRuleId:
                  type: string
                  description: Univocally identifies the session rule within a PDU session.
                refUmData:
                  type: string
                  description: A reference to UsageMonitoringData policy decision type. It is the umId
          described in subclause 5.6.2.12.
                  nullable: true
                refCondData:
                  type: string
                  description: A reference to the condition data. It is the condId described in
          subclause 5.6.2.9.
                  nullable: true
                required:
                  - sessRuleId
                nullable: true
            QosData:
              type: object
              properties:
                qosId:
                  type: string
                  description: Univocally identifies the QoS control policy data within a PDU session.
                5qi:
                  $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'

                maxbrUl:
                  $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
                maxbrDl:
                  $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
                gbrUl:
                  $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
                gbrDl:
                  $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRateRm'
                arp:
                  $ref: 'TS29571_CommonData.yaml#/components/schemas/Arp'
                qnc:
                  type: boolean
                  description: Indicates whether notifications are requested from 3GPP NG-RAN when the GFBR
          can no longer (or again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow.
                priorityLevel:
                  $ref: 'TS29571_CommonData.yaml#/components/schemas/5QiPriorityLevelRm'
                averWindow:
                  $ref: 'TS29571_CommonData.yaml#/components/schemas/AverWindowRm'
```

```
      maxDataBurstVol:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/MaxDataBurstVolRm'
      reflectiveQos:
        type: boolean
        description: Indicates whether the QoS information is reflective for the corresponding
service data flow.
      sharingKeyDl:
        type: string
        description: Indicates, by containing the same value, what PCC rules may share resource in
downlink direction.
      sharingKeyUl:
        type: string
        description: Indicates, by containing the same value, what PCC rules may share resource in
uplink direction.
      maxPacketLossRateDl:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketLossRateRm'
      maxPacketLossRateUl:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketLossRateRm'
      defQosFlowIndication:
        type: boolean
        description: Indicates that the dynamic PCC rule shall always have its binding with the
QoS Flow associated with the default QoS rule
    required:
      - qosId
    nullable: true
  ConditionData:
    type: object
    properties:
      condId:
        type: string
        description: Uniquely identifies the condition data within a PDU session.
      activationTime:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTimeRm'
      deactivationTime:
        $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTimeRm'
    required:
      - condId
    nullable: true
  TrafficControlData:
    type: object
    properties:
      tcId:
        type: string
        description: Univocally identifies the traffic control policy data within a PDU session.
      flowStatus:
        $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/FlowStatus'
      redirectInfo:
        $ref: '#/components/schemas/RedirectInformation'
      muteNotif:
        type: boolean
        description: Indicates whether applicat'on's start or stop notification is to be muted.
      trafficSteeringPolIdDl:
        type: string
        description: Reference to a pre-configured traffic steering policy for downlink traffic at
the SMF.
        nullable: true
      trafficSteeringPolIdUl:
        type: string
        description: Reference to a pre-configured traffic steering policy for uplink traffic at
the SMF.
        nullable: true
      routeToLocs:
        type: array
        items:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RouteToLocation'
        minItems: 1
        description: A list of location which the traffic shall be routed to for the AF request
      upPathChgEvent:
        $ref: '#/components/schemas/UpPathChgEvent'
    required:
      - tcId
    nullable: true
  ChargingData:
    type: object
    properties:
      chgId:
        type: string
        description: Univocally identifies the charging control policy data within a PDU session.
```

```
        meteringMethod:
          $ref: '#/components/schemas/MeteringMethod'
          nullable: true
        offline:
          type: boolean
          description: Indicates the offline charging is applicable to the PDU session or PCC rule.
        online:
          type: boolean
          description: Indicates the online charging is applicable to the PDU session or PCC rule.
        ratingGroup:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatingGroup'
        reportingLevel:
          $ref: '#/components/schemas/ReportingLevel'
          nullable: true
        serviceId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ServiceId'
flow in a PCC rule relates to.
        sponsorId:
          type: string
          description: Indicates the sponsor identity.
        appSvcProvId:
          type: string
          description: Indicates the application service provider identity.
        afChargingIdentifier:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ChargingId'
      required:
        - chgId
      nullable: true
    UsageMonitoringData:
      type: object
      properties:
        umId:
          type: string
          description: Univocally identifies the usage monitoring policy data within a PDU session.
        volumeThreshold:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        volumeThresholdUplink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        volumeThresholdDownlink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        timeThreshold:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSecRm'
        monitoringTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTimeRm'
        nextVolThreshold:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        nextVolThresholdUplink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        nextVolThresholdDownlink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/VolumeRm'
        nextTimeThreshold:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSecRm'
        inactivityTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSecRm'
        exUsagePccRuleIds:
          type: array
          items:
            type: string
          minItems: 1
          description: Contains the PCC rule identifier(s) which corresponding service data flow(s)
shall be excluded from PDU Session usage monitoring. It is only included in the UsageMonitoringData
instance for session level usage monitoring.
          nullable: true
      required:
        - umId
      nullable: true
    RedirectInformation:
      type: object
      properties:
        redirectEnabled:
          type: boolean
          description: Indicates the redirect is enable.
        redirectAddressType:
          $ref: '#/components/schemas/RedirectAddressType'
        redirectServerAddress:
          type: string
          description: Indicates the address of the redirect server.
    FlowInformation:
```

```
        type: object
        properties:
          flowDescription:
            $ref: '#/components/schemas/FlowDescription'
          ethFlowDescription:
            $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/EthFlowDescription'
            description: Defines a packet filter for an Ethernet flow. "fDir" attribute is not
applicable.
          packFiltId:
            type: string
            description: An identifier of packet filter.
          packetFilterUsage:
            type: boolean
            description: The packet shall be sent to the UE.
          tosTrafficClass:
            type: string
            description: Contains the Ipv4 Type-of-Service and mask field or the Ipv6 Traffic-Class
field and mask field.
            nullable: true
          spi:
            type: string
            description: the security parameter index of the IPSec packet.
            nullable: true
          flowLabel:
            type: string
            description: the Ipv6 flow label header field.
            nullable: true
          flowDirection:
            $ref: '#/components/schemas/FlowDirectionRm'
    SmPolicyDeleteData:
      type: object
      properties:
        userLocationInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        ueTimeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
        servingNetwork:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NetworkId'
        userLocationInfoTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
        ranNasRelCauses:
          type: array
          items:
            $ref: '#/components/schemas/RanNasRelCause'
          minItems: 1
          description: Contains the RAN and/or NAS release cause.
        accuUsageReports:
          type: array
          items:
            $ref: '#/components/schemas/AccuUsageReport'
          minItems: 1
          description: Contains the usage report
    QosCharacteristics:
      type: object
      properties:
        5qi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'
        resourceType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/QosResourceType'
        priorityLevel:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/5QiPriorityLevel'
        packetDelayBudget:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketDelBudget'
        packetErrorRate:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketErrRate'
        averagingWindow:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AverWindow'
        maxDataBurstVol:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MaxDataBurstVol'
      required:
        - 5qi
        - resourceType
        - priorityLevel
        - packetDelayBudget
        - packetErrorRate
    ChargingInformation:
      type: object
      properties:
```

```
          primaryChfAddress:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
          secondaryChfAddress:
            $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        required:
          - primaryChfAddress
          - secondaryChfAddress
    AccuUsageReport:
      type: object
      properties:
        refUmIds:
          type: string
          description: An id referencing UsageMonitoringData objects associated with this usage
report.
        volUsage:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        volUsageUplink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        volUsageDownlink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        timeUsage:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        nextVolUsage:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        nextVolUsageUplink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        nextVolUsageDownlink:
          $ref: 'TS29122_CommonData.yaml#/components/schemas/Volume'
        nextTimeUsage:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        required:
          - refUmIds
    SmPolicyUpdateContextData:
      type: object
      properties:
        repPolicyCtrlReqTriggers:
          type: array
          items:
            $ref: '#/components/schemas/PolicyControlRequestTrigger'
          minItems: 1
          description: The policy control reqeust trigges which are met.
        accNetChIds:
          type: array
          items:
            $ref: '#/components/schemas/AccNetChId'
          minItems: 1
          description: Indicates the access network charging identifier for the PCC rule(s) or whole
PDU session.
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
        servingNetwork:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NetworkId'
        userLocationInfo:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        ueTimeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
        relIpv4Address:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ipv4Address:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ipv6AddressPrefix:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        relIpv6AddressPrefix:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        relUeMac:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
        ueMac:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/MacAddr48'
        subsSessAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        subsDefQos:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SubscribedDefaultQos'
        numOfPackFilter:
          type: integer
          description: Contains the number of supported packet filter for signalled QoS rules.
        accuUsageReports:
```

```
              type: array
              items:
                $ref: '#/components/schemas/AccuUsageReport'
              minItems: 1
              description: Contains the usage report
            3gppPsDataOffStatus:
              type: boolean
              description: If it is included and set to true, the 3GPP PS Data Off is activated by the
UE.
            appDetectionInfos:
              type: array
              items:
                $ref: '#/components/schemas/AppDetectionInfo'
              minItems: 1
              description: Report the start/stop of the application traffic and detected SDF
descriptions if applicable.
            ruleReports:
              type: array
              items:
                $ref: '#/components/schemas/RuleReport'
              minItems: 1
              description: Used to report the PCC rule failure.
            qncReports:
              type: array
              items:
                $ref: '#/components/schemas/QosNotificationControlInfo'
              minItems: 1
              description: QoS Notification Control information.
            userLocationInfoTime:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
            repPraInfos:
              type: object
              additionalProperties:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/PresenceInfo'
              minProperties: 1
              description: Reports the changes of presence reporting area.
            ueInitResReq:
              $ref: '#/components/schemas/UeInitiatedResourceRequest'
              description: Indicates a UE requests specific QoS handling for selected SDF.
            refQosIndication:
              type: boolean
              description: If it is included and set to true, the reflective QoS is supported by the UE.
If it is included and set to false, the reflective QoS is revoked by the UE.
            qosFlowUsage:
              $ref: '#/components/schemas/QosFlowUsage'
            traceReq:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/TraceData'
    UpPathChgEvent:
      type: object
      properties:
        notificationUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        notifCorreId:
          type: string
          description: It is used to set the value of Notification Correlation ID in the
notification sent by the SMF.
        dnaiChgType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DnaiChangeType'
      required:
        - notificationUri
        - notifCorreId
        - dnaiChgType
      nullable: true
    TerminationNotification:
      type: object
      properties:
        resourceUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        cause:
          $ref:
'TS29507_Npcf_AMPolicyControl.yaml#/components/schemas/PolicyAssociationReleaseCause'
      required:
        - resourceUri
        - cause
    AppDetectionInfo :
      type: object
      properties:
        appId:
```

```
            type: string
            description: A reference to the application detection filter configured at the UPF
          instanceId:
            type: string
            description: Identifier dynamically assigned by the SMF in order to allow correlation of
application Start and Stop events to the specific service data flow description, if service data
flow descriptions are deducible.
          sdfDescriptions:
            type: array
            items:
              $ref: '#/components/schemas/FlowInformation'
            minItems: 1
            description: Contains the detected service data flow descriptions if they are deducible.
        required:
          - appId
    AccNetChId:
      type: object
      properties:
        accNetChaIdValue:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ChargingId'
        refPccRuleIds:
          type: array
          items:
            type: string
          minItems: 1
          description: Contains the identifier of the PCC rule(s) associated to the provided Access
Network Charging Identifier.
        sessionChScope:
          type: boolean
          description: When it is included and set to true, indicates the Access Network Charging
Identifier applies to the whole PDU Session
      required:
        - accNetChaIdValue
    AccNetChargingAddress:
      description: Describes the network entity within the access network performing charging
      type: object
      anyOf:
        - required: [anChargIpv4Addr]
        - required: [anChargIpv6Addr]
      properties:
        anChargIpv4Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        anChargIpv6Addr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Addr'
    RequestedRuleData:
      type: object
      properties:
        refPccRuleIds:
          type: array
          items:
            type: string
          minItems: 1
          description: An array of PCC rule id references to the PCC rules associated with the
control data.
        reqData:
          type: array
          items:
            $ref: '#/components/schemas/RequestedRuleDataType'
          minItems: 1
          description: Array of requested rule data type elements indicating what type of rule data
is requested for the corresponding referenced PCC rules.
      required:
        - refPccRuleIds
        - reqData
    RequestedUsageData:
      type: object
      properties:
        refUmIds:
          type: array
          items:
            type: string
          minItems: 1
          description: An array of usage monitoring data id references to the usage monitoring data
instances for which the PCF is requesting a usage report. This attribute shall only be provided when
allUmIds is not set to true.
        allUmIds:
          type: boolean
```

```
              description: Th119ooleanean indicates whether requested usage data applies to all usage
    monitoring data instances. When it's not included, it means requested usage data shall only apply to
    the usage monitoring data instances referenced by the refUmIds attribute.
          UeCampingRep:
            type: object
            properties:
              accessType:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
                description: The Access Type where the served UE is camping
              ratType:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
              servingNetwork:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/NetworkId'
              userLocationInfo:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
              ueTimeZone:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
          RuleReport:
            type: object
            properties:
              pccRuleIds:
                type: array
                items:
                  type: string
                minItems: 1
                description: Contains the identifier of the affected PCC rule(s).
              ruleStatus:
                $ref: '#/components/schemas/RuleStatus'
                description: Indicates the status of the PCC rule(s).
              contVers:
                type: array
                items:
                  $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/ContentVersion'
                minItems: 1
                description: Indicates the version of a PCC rule.
              failureCode:
                $ref: '#/components/schemas/FailureCode'
                description: Indicates the reason tha the PCC Rule is being reported.
              finUnitAct:
                $ref: 'TS32291_Nchf_ConvergedCharging.yaml#/components/schemas/FinalUnitAction'
                description: Contains the related filter parameters and redirect address parameters (if
    available), when the user's account cannot cover the service cost.
              ranNasRelCauses:
                type: array
                items:
                  $ref: '#/components/schemas/RanNasRelCause'
                minItems: 1
                description: indicates the RAN or NAS release cause code information.
            required:
              - pccRuleIds
              - ruleStatus
              - failureCode
          RanNasRelCause:
            type: object
            properties:
              ngApCause:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/NgApCause'
                description: Indicate the cause value for NGAP protocol.
              5gMmCause:
                $ref: 'TS29571_CommonData.yaml#/components/schemas/5GMmCause'
                description: Indicate the cause value for 5GMM protocol.
              5gSmCause:
                $ref: '#/components/schemas/5GSmCause'
                description: Indicate the cause value for 5GSM protocol.
          UeInitiatedResourceRequest:
            type: object
            properties:
              packFiltOp:
                $ref: '#/components/schemas/PacketFilterOperation'
                description: Indicates a UE requests specific QoS handling for selected SDF.
              packFiltInfo:
                type: array
                items:
                  $ref: '#/components/schemas/PacketFilterInfo'
                  description: Contains the information from a single packet filter sent from the SMF to
    the PCF.
                minItems: 1
              reqQos:
```

```
                  $ref: '#/components/schemas/RequestedQos'
                  description: Contains the QoS information requested by the UE.
            required:
              - packFiltOp
              - packFiltInfo
        PacketFilterInfo:
          type: object
          properties:
            packFiltId:
              type: string
              description: An identifier of packet filter.
            precedence:
              type: integer
              description: The requested order for the PCC rule generated fromt the packet fitler
information.
            packFiltCont:
              $ref: '#/components/schemas/PacketFilterContent'
              description: Contains the content of the packet filter as requested by the UE and required
by the PCF to create the PCC rules.
            tosTrafficClass:
              type: string
              description: Contains the Ipv4 Type-of-Service and mask field or the Ipv6 Traffic-Class
field and mask field.
            spi:
              type: string
              description: The security parameter index of the IPSec packet.
            flowLabel:
              type: string
              description: The Ipv6 flow label header field.
            flowDirection:
              $ref: '#/components/schemas/FlowDirection'
              description: Indicates the direction/directions that a filter is applicable, downlink
only, uplink only or both down- and uplink (bidirectional).
        RequestedQos:
          type: object
          properties:
            5qi:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'
              description: Identifier for the authorized QoS parameters for the service data flow.
            gbrUl:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
              description: Indicates the guaranteed bandwidth in uplink requested by the UE.
            gbrDl:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
              description: Indicates the guaranteed bandwidth in downlink requested by the UE.
          required:
            - 5qi
        QosNotificationControlInfo:
          type: object
          properties:
            refPccRuleIds:
              type: array
              items:
                type: string
              minItems: 1
              description: An array of PCC rule id references to the PCC rules associated with the QoS
notification control info.
            notifType:
              $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/QosNotifType'
            contVer:
              $ref: 'TS29514_Npcf_PolicyAuthorization.yaml#/components/schemas/ContentVersion'
          required:
            - refPccRuleIds
            - notifType
        PartialSuccessReport:
          type: object
          properties:
            failureCause:
              type: string
              description: Application error cause specific to this report.
            ruleReports:
              type: array
              items:
                $ref: '#/components/schemas/RuleReport'
                minItems: 1
                description: Information about the PCC rules provisioned by the PCF not successfully
installed/activated.
            ueCampingRep:
```

```
              $ref: '#/components/schemas/UeCampingRep'
              description: Includes the current applicable values corresponding to the provisioned
      policy control request triggers.
          required:
            - failureCause
            - ruleReports
        AuthorizedDefaultQos:
          type: object
          properties:
            5qi:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/5Qi'
              description: Identifier for the 5QI.
            arp:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/Arp'
            priorityLevel:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/5QiPriorityLevelRm'
            averWindow:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/AverWindowRm'
            maxDataBurstVol:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/MaxDataBurstVolRm'
        ErrorReport:
          type: object
          properties:
            error:
              $ref: 'TS29571_CommonData.yaml#/components/schemas/ProblemDetails'
            ruleReports:
              type: array
              items:
                $ref: '#/components/schemas/RuleReport'
              minItems: 1
              description: Used to report the PCC rule failure.
        5GSmCause:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uinteger'
          description: Indicating the cause value of 5GSM protocol.
        PacketFilterContent:
          type: string
          description: Defines a packet filter for an IP flow.Refer to subclause 5.3.54 of
      3GPP TS 29.212 [23] for encoding.
        FlowDescription:
          type: string
          description: Defines a packet filter for an IP flow.Refer to subclause 5.4.2 of
      3GPP TS 29.212 [23] for encoding.
        FlowDirection:
          anyOf:
          - type: string
            enum:
              - DOWNLINK
              - UPLINK
              - BIDIRECTIONAL
              - UNSPECIFIED
          - type: string
            description: >
              This string provides forward-compatibility with future
              extensions to the enumeration but is not used to encode
              content defined in the present version of this API.
          description: >
            Possible values are
            - DOWNLINK: The corresponding filter applies for traffic to the UE.
            - UPLINK: The corresponding filter applies for traffic from the UE.
            - BIDIRECTIONAL: The corresponding filter applies for traffic both to and from the UE.
            - UNSPECIFIED: The corresponding filter applies for traffic to the UE (downlink), but has no
      specific direction declared. The service data flow detection shall apply the filter for uplink
      traffic as if the filter was bidirectional. The PCF shall not use the value UNSPECIFIED in filters
      created by the network in NW-initiated procedures. The PCF shall only include the value UNSPECIFIED
      in filters in UE-initiated procedures if the same value is received from the SMF.
        FlowDirectionRm:
          anyOf:
          - type: string
            enum:
              - DOWNLINK
              - UPLINK
              - BIDIRECTIONAL
              - UNSPECIFIED
          - type: string
            description: >
              This string provides forward-compatibility with future
              extensions to the enumeration but is not used to encode
              content defined in the present version of this API.
```

```
      description: >
        Possible values are
        - DOWNLINK: The corresponding filter applies for traffic to the UE.
        - UPLINK: The corresponding filter applies for traffic from the UE.
        - BIDIRECTIONAL: The corresponding filter applies for traffic both to and from the UE.
        - UNSPECIFIED: The corresponding filter applies for traffic to the UE (downlink), but has no
specific direction declared. The service data flow detection shall apply the filter for uplink
traffic as if the filter was bidirectional. The PCF shall not use the value UNSPECIFIED in filters
created by the network in NW-initiated procedures. The PCF shall only include the value UNSPECIFIED
in filters in UE-initiated procedures if the same value is received from the SMF.
      nullable: true
    ReportingLevel:
      anyOf:
      - type: string
        enum:
          - SER_ID_LEVEL
          - RAT_GR_LEVEL
          - SPON_CON_LEVEL
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - SER_ID_LEVEL: Indicates that the usage shall be reported on service id and rating group
combination level.
        - RAT_GR_LEVEL: Indicates that the usage shall be reported on rating group level.
        - SPON_CON_LEVEL: Indicates that the usage shall be reported on sponsor identity and rating
group combination level.
    MeteringMethod:
      anyOf:
      - type: string
        enum:
          - DURATION
          - VOLUME
          - DURATION_VOLUME
          - EVENT
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - DURATION: Indicates that the duration of the service data flow traffic shall be metered.
        - VOLUME: Indicates that volume of the service data flow traffic shall be metered.
        - DURATION_VOLUME: Indicates that the duration and the volume of the service data flow
traffic shall be metered.
        - EVENT: Indicates that events of the service data flow traffic shall be metered.
    PolicyControlRequestTrigger:
      anyOf:
      - type: string
        enum:
          - PLMN_CH
          - RES_MO_RE
          - AC_TY_CH
          - UE_IP_CH
          - UE_MAC_CH
          - AN_CH_COR
          - US_RE
          - APP_STA
          - APP_STO
          - AN_INFO
          - CM_SES_FAIL
          - PS_DA_OFF
          - DEF_QOS_CH
          - SE_AMBR_CH

          - QOS_NOTIF
          - NO_CREDIT
          - PRA_CH
          - SAREA_CH
          - SCNN_CH
            - RE_TIMEOUT
          - RES_RELEASE
          - SUCC_RES_ALLO
          - RAT_TY_CH
```

```
              - REF_QOS_IND_CH
          - type: string
            description: >
              This string provides forward-compatibility with future
              extensions to the enumeration but is not used to encode
              content defined in the present version of this API.
        description: >
          Possible values are
          - PLMN_CH: PLMN Change
          - RES_MO_RE: A request for resource modification has been received by the SMF. The SMF
always reports to the PCF.
          - AC_TY_CH: Access Type Change
          - UE_IP_CH: UE IP address change. The SMF always reports to the PCF.
          - UE_MAC_CH: A new UE MAC address is detected or a used UE MAC address is inactive for a
specific period
          - AN_CH_COR: Access Network Charging Correlation Information
          - US_RE: The PDU Session or the Monitoring key specific resources consumed by a UE either
reached the threshold or needs to be reported for other reasons.
          - APP_STA: The start of application traffic has been detected.
          - APP_STO: The stop of application traffic has been detected.
          - AN_INFO: Access Network Information report
          - CM_SES_FAIL: Credit management session failure
          - PS_DA_OFF: The SMF reports when the 3GPP PS Data Off status changes. The SMF always
reports to the PCF.
          - DEF_QOS_CH: Default QoS Change. The SMF always reports to the PCF.
          - SE_AMBR_CH: Session AMBR Change. The SMF always reports to the PCF.
          - QOS_NOTIF: The SMF notify the PCF when receiving notification from RAN that QoS targets of
the QoS Flow cannot be guranteed or gurateed again.
          - NO_CREDIT: Out of credit
          - PRA_CH: Change of UE presence in Presence Reporting Area
          - SAREA_CH: Location Change with respect to the Serving Area
          - SCNN_CH: Location Change with respect to the Serving CN node
          - RE_TIMEOUT: Indicates the SMF generated the request because there has been a PCC
revalidation timeout
          - RES_RELEASE: Indicate that the SMF can inform the PCF of the outcome of the release of
resources for those rules that require so.
          - SUCC_RES_ALLO: Indicates that the requested rule data is the successful resource
allocation.
          - RAT_TY_CH: RAT Type Change.
          - REF_QOS_IND_CH: Reflective QoS indication Change
    RequestedRuleDataType:
      anyOf:
      - type: string
        enum:
          - CH_ID
          - MS_TIME_ZONE
          - USER_LOC_INFO
          - RES_RELEASE
          - SUCC_RES_ALLO
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - CH_ID: Indicates that the requested rule data is the charging identifier.
        - MS_TIME_ZONE: Indicates that the requested access network info type is the UE's timezone.
        - USER_LOC_INFO: Indicates that the requested access network info type is the UE's location.
        - RES_RELEASE: Indicates that the requested rule data is the result of the release of
resource.
        - SUCC_RES_ALLO: Indicates that the requested rule data is the successful resource
allocation.
    RuleStatus:
      anyOf:
      - type: string
        enum:
          - ACTIVE
          - INACTIVE
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
```

```
            - ACTIVE: Indicates that the PCC rule(s) are successfully installed (for those provisioned
from PCF) or activated (for those pre-defined in SMF), or the session rule(s) are successfully
installed
            - INACTIVE: Indicates that the PCC rule(s) are removed (for those provisioned from PCF) or
inactive (for those pre-defined in SMF) or the session rule(s) are removed.
    FailureCode:
      anyOf:
      - type: string
        enum:
            - UNK_RULE_ID
            - RA_GR_ERR
            - SER_ID_ERR
            - NF_MAL
            - RES_LIM
            - MAX_NR_QoS_FLOW
            - MISS_FLOW_INFO
            - RES_ALLO_FAIL
            - UNSUCC_QOS_VAL
            - INCOR_FLOW_INFO
            - PS_TO_CS_HAN
            - APP_ID_ERR
            - NO_QOS_FLOW_BOUND
            - FILTER_RES
            - MISS_REDI_SER_ADDR
            - CM_END_USER_SER_DENIED
            - CM_CREDIT_CON_NOT_APP
            - CM_AUTH_REJ
            - CM_USER_UNK
            - CM_RAT_FAILED
            - SESS_AMBR_FAILURE
            - DEF_QOS_FAILURL
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
        description: >
          Possible values are
            - UNK_RULE_ID: Indicates that the pre-provisioned PCC rule could not be successfully
activated because the PCC rule identifier is unknown to the SMF.
            - RA_GR_ERR: Indicate that the PCC rule could not be successfully installed or enforced
because the Rating Group specified within the Charging Data policy decision which the PCC rule
refers to is unknown or, invalid.
            - SER_ID_ERR: Indicate that the PCC rule could not be successfully installed or enforced
because the Service Identifier specified within the Charging Data policy decision which the PCC rule
refers to is invalid, unknown, or not applicable to the service being charged.
            - NF_MAL: Indicate that the PCC rule could not be successfully installed (for those
provisioned from the PCF) or activated (for those pre-defined in SMF) or enforced (for those already
successfully installed) due to SMF/UPF malfunction.
            - RES_LIM: Indicate that the PCC rule could not be successfully installed (for those
provisioned from PCF) or activated (for those pre-defined in SMF) or enforced (for those already
successfully installed) due to a limitation of resources at the SMF/UPF.
            - MAX_NR_QoS_FLOW: Indicate that the PCC rule could not be successfully installed (for
those provisioned from PCF) or activated (for those pre-defined in SMF) or enforced (for those
already successfully installed) due to the fact that the maximum number of QoS flows has been
reached for the PDU session.
            - MISS_FLOW_INFO: Indicate that the PCC rule could not be successfully installed or
enforced because the Flow Information AVP is not specified within the "pccRule" attribute by the PCF
during the first install request of the PCC rule.
            - RES_ALLO_FAIL: Indicate that the PCC rule could not be successfully installed or
maintained since the QoS flow establishment/modification failed, or the QoS flow was released.
            - UNSUCC_QOS_VAL: indicate that the QoS validation has failed or when Guaranteed Bandwidth
> Max-Requested-Bandwidth.
            - INCOR_FLOW_INFO: Indicate that the PCC rule could not be successfully installed or
modified at the SMF because the provided flow information is not supported by the network (e.g. the
provided IP address(es) or Ipv6 prefix(es) do not correspond to an IP version applicable for the PDU
session).
            - PS_TO_CS_HAN: Indicate that the PCC rule could not be maintained because of PS to CS
handover.
            - APP_ID_ERR: Indicate that the rule could not be successfully installed or enforced
because the Application Identifier is invalid, unknown, or not applicable to the application
required for detection.
            - NO_QOS_FLOW_BOUND: Indicate that there is no QoS flow which the SMF can bind the PCC
rule(s) to.
            - FILTER_RES: Indicate that the Flow Information cannot be handled by the SMF because any
of the restrictions was not met.
            - MISS_REDI_SER_ADDR: Indicate that the PCC rule could not be successfully installed or
enforced at the SMF because there is no valid Redirect Server Address within the Traffic Control
```

Data policy decision which the PCC rule refers to provided by the PCF and no preconfigured
redirection address for this PCC rule at the SMF.
     - CM_END_USER_SER_DENIED: Indicate that the charging system denied the service request due
to service restrictions (e.g. terminate rating group) or limitations related to the end-user, for
example the end-user's account could not cover the requested service.
     - CM_CREDIT_CON_NOT_APP: Indicate that the charging system determined that the service can
be granted to the end user but no further credit control is needed for the service (e.g. service is
free of charge or is treated for offline charging).
     - CM_AUTH_REJ: Indicate that the charging system denied the service request in order to
terminate the service for which credit is requested.
     - CM_USER_UNK: Indicate that the specified end user could not be found in the charging
system.
     - CM_RAT_FAILED: Indicate that the charging system cannot rate the service request due to
insufficient rating input, incorrect AVP combination or due to an attribute or an attribute value
that is not recognized or supported in the rating.
     - SESS_AMBR_FAILURE: Indicate that the session AMBR update is failure.
     - DEF_QOS_FAILURL: Indicate that the default QoS update is failure.
    AfSigProtocol:
      anyOf:
      - type: string
        enum:
          - NO_INFORMATION
          - SIP
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - NO_INFORMATION: Indicate that no information about the AF signalling protocol is being
provided.
        - SIP: Indicate that the signalling protocol is Session Initiation Protocol.
    PacketFilterOperation:
      anyOf:
      - type: string
        enum:
          - DELETION
          - ADDITION
          - MODIFICATION
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - DELETION: Indicates that the resources reserved for the provided packet filter identifiers
are to be deleted and are no longer used by the UE.
        - ADDITION: Indicates that the UE requests resources allocated for the provided packet
filters.
        - MODIFICATION: Indicates that the reserved QoS, the filter, the precedence, or any of the
fields for the provided packet filter identifiers are being modified.
    RedirectAddressType:
      anyOf:
      - type: string
        enum:
          - IPV4_ADDR
          - IPV6_ADDR
          - URL
          - SIP_URI
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - IPV4_ADDR: Indicates that the address type is in the form of "dotted-decimal" IPv4
address.
        - IPV6_ADDR: Indicates that the address type is in the form of IPv6 address.
        - URL: Indicates that the address type is in the form of Uniform Resource Locator.
        - SIP_URI: Indicates that the address type is in the form of SIP Uniform Resource Identifier.
    QosFlowUsage:
      anyOf:
      - type: string
        enum:
          - GENERAL

```
          - IMS_SIG
      - type: string
        description: >
          This string provides forward-compatibility with future
          extensions to the enumeration but is not used to encode
          content defined in the present version of this API.
      description: >
        Possible values are
        - GENERAL: Indicate no specific QoS flow usage information is available.
        - IMS_SIG: Indicate that the QoS flow is used for IMS signalling only.
    FailureCause:
      anyOf:
      - type: string
        enum:
          - PCC_RULE_EVENT
          - PCC_QOS_FLOW_EVENT
      - type: string
```

Annex A (normative): 5GS and EPC/E-UTRAN interworking scenario support

A.1 Scope

This annex defines procedures for 5GS and EPC/E-UTRAN interworking scenario to support UEs that can be handed over between the EPC/E-UTRAN and 5GS.

A.2 Npcf_SMPolicyControl Service

A.2.1 Service Description

A.2.1.1 Overview

Session Management Policy Control Service applies to the cases where the SMF+PGW-C interacts with the PCF in the non-roaming scenario, the V-SMF+V-PGW-C interacts with the V-PCF in the local breakout roaming scenario and the H-SMF+H-PGW-C interacts with the H-PCF in the home-routed scenario.

A.2.1.2 Service Architecture

The Session Management Policy Control Service is provided by the PCF as shown in the SBI representation model in figure A.2.1.2-1 and in the reference point representation model in figure A.2.1.2.2.

In this scenario the NF Service Consumer is a combined SMF and PGW-C.

Figure A.2.1.2-1: Reference Architecture for the Npcf_SMPolicyControl Service for 5GS and EPC/E-UTRAN interworking scenario; SBI representation

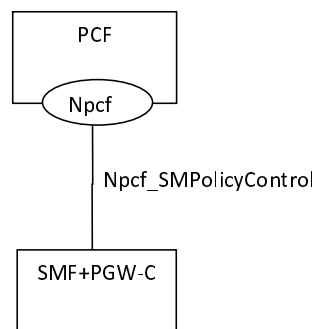**Figure A.2.1.2-2: Reference Architecture for the Npcf_SMPolicyControl Service or 5GS and EPC/E-UTRAN interworking scenario; reference point representation**

NOTE: The SMF+PGW-C represents the V-SMF+V-PGW-C and the PCF represents the V-PCF in the local breakout scenario. The SMF+PGW-C represents the H-SMF+H-PGW-C and the PCF represents the H-PCF in the home routed scenario.

A.3 Service Operation

A.3.1 Introduction

This subclause defines the specific service operations for the 5GS and EPC/E-UTRAN interworking scenario to support UE that can be handed over between EPC/E-UTRAN and 5GS. In addition, the service operations defined in subclause 4.2 shall be applicable.

NOTE: For brevity reason, the combined SMF and PGW-C is denoted as SMF in what follows.

A.3.2 Npcf_SMPolicyControl_Create Service Operation

A.3.3 Npcf_SMPolicyControl_UpdateNotify Service Operation

A.3.4 Npcf_SMPolicyControl_Update Service Operation

A.3.4.a1 Number of Supported Packet Filters Report

When the UE handed over from the EPC/E-UTRAN to the 5GS and the number of supported packet filters for signalled QoS rules is received from the UE, the SMF shall include the number of supported packet filters for signalled QoS rules within the "numOfPackFilter".

A.3.5 Npcf_SMPolicyControl_Delete Service Operation

A.3.6 Provisioning and Enforcement of Policy Decisions

A.3.6.a3 QoS mapping perfomed by the SMF+PGW-C

When the UE is served by the 5GC, during PDU Session establishment and GBR QoS flow establishment, SMF+ PGW-C performs EPS QoS mappings, from the 5G QoS parameters obtained from the PCF, and allocates TFT with the PCC rules obtained from the PCF. If a TFT is to be allocated for a downlink unidirectional EPS bearer mapped from a downlink only QoS Flow, the SMF+ PGW-C shall allocate a TFT packet filter that effectively disallows any useful uplink packet as described in subclause 15.3.3.4 of 3GPP TS 23.060 [26]. The SMF+PGW-C sends the mapped QoS parameters and TFT to the UE via PCO.

When the UE is served by the EPC, during PDN Connection establishment and dedicated bearer establishment/modification, SMF+ PGW-C performs EPS QoS mappings, from the 5G QoS parameters obtained from the PCF, and allocates TFT with the PCC rules obtained from the PCF. Other 5G QoS parameters corresponding to the PDN connection, e.g. Session AMBR, and QoS rules and QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s), are sent to UE in PCO.

The SMF+PGW-C shall perform EPS QoS mappings as follows:

- ignore the QNC and reflective QoS indication if received;

- map the authorized 5QI including the non-standardized 5QI to the authorized QCI;

- map the subscribed default QCI to the subscribed default 5QI;

NOTE: Details of the mapping between the 5QI and QCI are not defined in this release.

- set the subscribed Session-AMBR to the value of subscribed APN-AMBR; and

- set the authorized APN-AMBR to the value of authorized Session-AMBR.

Annex B (informative):
Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2017-10						TS skeleton of Session Management Policy Control Services specification	0.0.0
2017-10	CT3#92					Inclusion of C3-175237, C3-175353 and editorial changes from Rapporteur	0.1.0
2017-12	CT3#93					Inclusion of C3-176145, C3-176248, C3-176252, C3-176254, C3-176255, C3-176256, C3-176257, C3-176319, C3-176320, C3-176321, C3-176322, C3-176323 and editorial changes from Rapporteur	0.2.0
2018-01	CT3#94					Inclusion of C3-180035, C3-180198, C3-180097, C3-180342, C3-180303, C3-180343, C3-180202, C3-180305, C3-180307, C3- 180308, C3-180306, C3-180309, C3-180310, C3-1801311, C3-180312	0.3.0
2018-03	CT3#95					Inclusion of C3-181355, C3-181345, C3-181222, C3-181223, C3-181226, C3-181227	0.4.0
2018-04	CT3#96	C3-182515				Inclusion of C3-182056, C3-182318, C3-182322, C3-182463, C3-182325, C3-182327, C3-182330, C3-182331, C3-182132, C3-182332, C3-182324, C3-182482.	0.5.0
2018-05	CT3#97	C3-183868				Inclusion of C3-183811, C3-183889, C3-183748, C3-183749, C3-183845, C3-183461, C3-183846, C3-183847, C3-183884, C3-183850, C3-183851, C3-183852, C3-183853, C3-183470, C3-183855, C3-183854, C3-183760, C3-183885, C3-183736, C3-183848, C3-183857, C3-183858, C3-183765, C3-183766, C3-183486, C3-183886, C3-183859, C3-183887, C3-183488, C3-183489, C3-183888, C3-183815, C3-183769, C3-183793, C3-183816, C3-183763, C3-183509, C3-183865, C3-183866, C3-183771, C3-183867, C3-183772, C3-183818, C3-183255, C3-183868, C3-183284	0.6.0
2018-06	CT#80	CP-181036				TS sent to plenary for approval	1.0.0
2018-06	CT#80	CP-181036				TS approved by plenary	15.0.0
2018-09	CT#81	CP-182015	0001	5	F	Updates for TS 29.512 structure	15.1.0
2018-09	CT#81	CP-182015	0002	4	F	Update of Npcf_SMPolicyControl_Create Service Operation	15.1.0
2018-09	CT#81	CP-182015	0003	5	F	Update of Npcf_SMPolicyControl_UpdateNotify Service Operation	15.1.0
2018-09	CT#81	CP-182015	0004	3	F	Update of Npcf_SMPolicyControl_Update Service Operation	15.1.0
2018-09	CT#81	CP-182015	0005	4	F	Update of Npcf_SMPolicyControl_Delete Service Operation	15.1.0
2018-09	CT#81	CP-182015	0006	5	F	Multi-homing support	15.1.0
2018-09	CT#81	CP-182015	0007	2	F	Access Network Charging Identifier request and report	15.1.0
2018-09	CT#81	CP-182015	0008	3	F	Request result of PCC rule removal	15.1.0
2018-09	CT#81	CP-182015	0009	3	F	Request the successful resource allocation notification	15.1.0
2018-09	CT#81	CP-182168	0010	6	F	HTTP error handling procedure	15.1.0
2018-09	CT#81	CP-182169	0011	7	F	PCC Rule Error Handling	15.1.0
2018-09	CT#81	CP-182015	0012	2	F	Failure cases of Npcf_SMPolicyControl_Create Service Operation	15.1.0
2018-09	CT#81	CP-182015	0013	5	F	Failure cases of Npcf_SMPolicyControl_UpdateNotify Service Operation	15.1.0
2018-09	CT#81	CP-182015	0014	2	F	Failure cases of Npcf_SMPolicyControl_Update Service Operation	15.1.0
2018-09	CT#81	CP-182015	0015	1	F	Update of PCF and SMF function descriptions	15.1.0
2018-09	CT#81	CP-182015	0016	3	F	Rules, Session rules, PCC rules definition updates	15.1.0
2018-09	CT#81	CP-182015	0017	2	F	Policy Decision types Updates	15.1.0
2018-09	CT#81	CP-182015	0018	4	F	Policy control request trigger definition update	15.1.0
2018-09	CT#81	CP-182015	0019	2	F	Conditioned PCC rule update	15.1.0
2018-09	CT#81	CP-182015	0020	2	F	Conditioned session rule update	15.1.0
2018-09	CT#81	CP-182015	0021	2	F	IMS restoration support	15.1.0
2018-09	CT#81	CP-182015	0022	9	F	PRA support	15.1.0
2018-09	CT#81	CP-182015	0023	5	F	Update of steering the traffic to a local access of the data network	15.1.0
2018-09	CT#81	CP-182015	0024	2	F	Support for Ethernet PDU type	15.1.0
2018-09	CT#81	CP-182015	0025	6	F	Update of Provisioning of charging related information for PDU session	15.1.0
2018-09	CT#81	CP-182015	0026	4	F	UE requests specific QoS handling for selected SDF	15.1.0
2018-09	CT#81	CP-182015	0027	6	F	Provisioning of IP index information	15.1.0
2018-09	CT#81	CP-182015	0028	1	F	Update of Multimedia Priority Services	15.1.0
2018-09	CT#81	CP-182015	0029	3	F	Exclude the traffic from the session level usage monitoring	15.1.0
2018-09	CT#81	CP-182015	0030	3	F	Provisioning of specific QoS parameters together with 5QI	15.1.0
2018-09	CT#81	CP-182015	0031	1	F	Add Unspecified value to the FlowDirection data type	15.1.0
2018-09	CT#81	CP-182015	0032	2	F	Completion of definitions of UsageMonitoringData and AccuUsageReport	15.1.0
2018-09	CT#81	CP-182015	0033	4	F	Definition of FlowStatus data type	15.1.0
2018-09	CT#81	CP-182015	0034	1	F	Definition of RedirectAddressType data type	15.1.0

2018-09	CT#81	CP-182015	0035	1	F	Mandate the TrafficControlData decision	15.1.0
2018-09	CT#81	CP-182015	0036	2	F	Reflective QoS support	15.1.0
2018-09	CT#81	CP-182015	0037	1	F	Remove the DELETE method	15.1.0
2018-09	CT#81	CP-182015	0038	1	F	Remove the Packet Loss Rate from the QoS characteristics	15.1.0
2018-09	CT#81	CP-182015	0039	1	F	Re-use the ARP data type from 29.571	15.1.0
2018-09	CT#81	CP-182015	0043	1	F	Definition of DNAI	15.1.0
2018-09	CT#81	CP-182015	0044	1	F	Completion of ConditionData	15.1.0
2018-09	CT#81	CP-182015	0045	1	F	Completion of TrafficControlData data type	15.1.0
2018-09	CT#81	CP-182023	0046	1	B	Trace activation	15.1.0
2018-09	CT#81	CP-182015	0047	2	F	Corrections on the notification URIs defined for the UpdateNotify	15.1.0
2018-09	CT#81	CP-182015	0048	4	F	Corrections on attributes and data types	15.1.0
2018-09	CT#81	CP-182015	0049	-	F	Corrections on Supported Features	15.1.0
2018-09	CT#81	CP-182015	0050	1	F	Update custom operation for Npcf_SMPolicyControl_Update	15.1.0
2018-09	CT#81	CP-182015	0051	-	F	Missing Slice Information	15.1.0
2018-09	CT#81	CP-182015	0052	1	F	Solution to IPv4 overlapping	15.1.0
2018-09	CT#81	CP-182015	0053	1	F	Description of Structured data types	15.1.0
2018-09	CT#81	CP-182104	0054	1	B	Support of PCC rule versioning	15.1.0
2018-09	CT#81	CP-182015	0055	1	F	Update of Sponsored data connectivity support	15.1.0
2018-09	CT#81	CP-182015	0056	1	F	Update of resource structure	15.1.0
2018-09	CT#81	CP-182015	0057	1	F	Correction on cardinality of array and map	15.1.0
2018-09	CT#81	CP-182015	0058	-	F	Update of PccRule data type	15.1.0
2018-09	CT#81	CP-182015	0059	1	F	Open issues on Reused data types	15.1.0
2018-09	CT#81	CP-182015	0060	-	F	DNAI report	15.1.0
2018-09	CT#81	CP-182015	0061	-	F	Definition of maxPacketLossRate	15.1.0
2018-12	CT#82	CP-183205	0063	6	F	Correction to the AF influence traffic steering control	15.2.0
2018-12	CT#82	CP-183205	0064	2	F	Some corrections to the OpenAPI file	15.2.0
2018-12	CT#82	CP-183205	0065	3	F	Backgroud data transfer support	15.2.0

2018-12	CT#82	CP-183205	0066	4	F	Clarification of default QoS	15.2.0
2018-12	CT#82	CP-183205	0067	3	F	Clarification of Maximum Packet Loss Rate authorization	15.2.0
2018-12	CT#82	CP-183205	0068	1	F	Clarification of PCC rule enforcement	15.2.0
2018-12	CT#82	CP-183205	0069		F	Clarification of service data flow template	15.2.0
2018-12	CT#82	CP-183205	0070		F	Correction to name of maximumDataBurstVolume attribute	15.2.0
2018-12	CT#82	CP-183205	0071	1	F	Correction to the QoS notification control authorization	15.2.0
2018-12	CT#82	CP-183205	0072	3	F	IMS dedicated signalling QoS flow	15.2.0
2018-12	CT#82	CP-183205	0073	2	F	Internal Group Id during the PDU session establishment	15.2.0
2018-12	CT#82	CP-183205	0074	3	F	Number of packet filters sent to the UE	15.2.0
2018-12	CT#82	CP-183205	0075	2	F	Packet filter identifier	15.2.0
2018-12	CT#82	CP-183205	0076	1	F	Remove two values of policy control request triggers in OpenAPI	15.2.0
2018-12	CT#82	CP-183205	0077	1	F	SM policy association termination	15.2.0
2018-12	CT#82	CP-183205	0078	3	F	The procedure of QoS notification control	15.2.0
2018-12	CT#82	CP-183205	0079	4	F	Architecture of 5GS and EPS interworking scenario support	15.2.0
2018-12	CT#82	CP-183205	0083	2	F	QoS mapping in 5GS and EPS interworking scenario	15.2.0
2018-12	CT#82	CP-183205	0084		F	PCC Rules for MPS	15.2.0
2018-12	CT#82	CP-183205	0086	2	F	ExternalDocs field	15.2.0
2018-12	CT#82	CP-183205	0089	1	F	Correction of SMPolicyControl resource URI structure	15.2.0
2018-12	CT#82	CP-183205	0089	2	F	Correction of SMPolicyControl resource URI structure	15.2.0
2018-12	CT#82	CP-183205	0090	1	F	Definition on map keys in SmPolicyDecision	15.2.0
2018-12	CT#82	CP-183205	0091	1	F	Security field	15.2.0
2018-12	CT#82	CP-183205	0092	1	F	Correction of datatypes related to QoS	15.2.0
2018-12	CT#82	CP-183205	0093	1	F	Correction of 404 error information	15.2.0
2018-12	CT#82	CP-183205	0094		F	Correction of API name	15.2.0

2018-12	CT#82	CP-183205	0095	1	F	Corrections of external references in OpenAPI	15.2.0
2018-12	CT#82	CP-183205	0096	4	F	Corrections on IP index provisioning	15.2.0
2018-12	CT#82	CP-183205	0097	1	F	Corrections misused data types, attributes and error definitions	15.2.0
2018-12	CT#82	CP-183205	0098	2	F	Application Error POLICY_CONTEXT_DENIED	15.2.0
2018-12	CT#82	CP-183205	0099	2	F	Corrections on RAN-NAS-Cause feature	15.2.0
2018-12	CT#82	CP-183205	0100	1	F	Missing Policy Control Request trigger for RAT Type Change	15.2.0
2018-12	CT#82	CP-183205	0101	2	F	Corrections on rule versioning	15.2.0
2018-12	CT#82	CP-183205	0102	1	F	Corrections for Npcf_SMPolicyControl_UpdateNotify service operation.	15.2.0
2018-12	CT#82	CP-183205	0103		F	Default value for apiRoot	15.2.0
2018-12	CT#82	CP-183205	0104	1	F	Correction to RAN-NAS-Cause feature	15.2.0
2018-12	CT#82	CP-183205	0105	1	F	a new PolicyControlRequestTrigger for refQosIndication	15.2.0
2018-12	CT#82	CP-183205	0106	1	F	PCC rule error report triggerconvention	15.2.0
2018-12	CT#82	CP-183205	0108	1	F	Missing SponsoredConnectivity feature	15.2.0
2018-12	CT#82	CP-183205	0109	2	F	Correct DNAI change type in OpenAPI	15.2.0
2018-12	CT#82	CP-183205	0110	3	F	Selection of Predefined PCC Rule Base	15.2.0
2018-12	CT#82	CP-183205	0111	3	F	Correction to treatment of subscribed default QoS and authorized default QoS	15.2.0
2018-12	CT#82	CP-183123	0113	1	F	Address attribute for the network entity performing charging	15.2.0
2018-12	CT#82	CP-183205	0115	1	F	Status code update for Npcf_SMPolicyControl API	15.2.0
2018-12	CT#82	CP-183205	0116	1	F	CHF discovery and selection	15.2.0
2018-12	CT#82	CP-183205	0117	1	F	Condition Data	15.2.0
2018-12	CT#82	CP-183205	0119		F	Correction to authDefaultQos attribute	15.2.0
2018-12	CT#82	CP-183205	0120	1	F	Correction to error handling	15.2.0
2018-12	CT#82	CP-183205	0121		F	Correction to Partial Success handling	15.2.0
2018-12	CT#82	CP-183205	0122	2	F	Correction to precedence of the PCC rule	15.2.0

2018-12	CT#82	CP-183205	0123	2	F	Correction to pre-defined PCC rule activation	15.2.0
2018-12	CT#82	CP-183205	0124		F	Correction to the terminology of QoS notification control	15.2.0
2018-12	CT#82	CP-183205	0125	1	F	Correction to the general descriptions of Provisioning and Enforcement of Policy Decisions	15.2.0
2018-12	CT#82	CP-183205	0126	3	F	Correction to the PCC rule defintion	15.2.0
2018-12	CT#82	CP-183205	0128	1	F	Correction to the policy decision data definition	15.2.0
2018-12	CT#82	CP-183205	0129	1	F	Correction to the resource URI	15.2.0
2018-12	CT#82	CP-183205	0130		F	Correction to the RuleReport data type	15.2.0
2018-12	CT#82	CP-183205	0131	1	F	Delay critical GBR resrouce type	15.2.0
2018-12	CT#82	CP-183205	0132	1	F	Correction to the specific data type table	15.2.0
2018-12	CT#82	CP-183205	0133	1	F	HTTP custom headers	15.2.0
2018-12	CT#82	CP-183205	0134	1	F	Inactivity timer for emergency session	15.2.0
2018-12	CT#82	CP-183205	0135	1	F	Provisioning and deletion of the policy decision data	15.2.0
2018-12	CT#82	CP-183205	0136	1	F	QoS authorization for the emergency service	15.2.0
2018-12	CT#82	CP-183205	0137	1	F	Reference number alignment	15.2.0
2018-12	CT#82	CP-183205	0138		F	Supported content types	15.2.0
2018-12	CT#82	CP-183205	0140	2	F	Adding "nullable" property to data types	15.2.0
2018-12	CT#82	CP-183205	0141	2	F	VolumeRm data type	15.2.0
2018-12	CT#82	CP-183205	0142		F	Re-use PresenceInfoRm data type	15.2.0
2018-12	CT#82	CP-183205	0143	1	F	Re-use PacketLossRateRm data type	15.2.0
2018-12	CT#82	CP-183205	0144	1	F	Re-use MaxDataBurstVolRm data type	15.2.0
2018-12	CT#82	CP-183205	0145		F	Re-use DurationSecRm data type	15.2.0
2018-12	CT#82	CP-183205	0146		F	Re-use DateTimeRm data type	15.2.0
2018-12	CT#82	CP-183205	0147		F	Re-use BitRateRm data type	15.2.0
2018-12	CT#82	CP-183205	0148		F	Re-use AverWindowRm data type	15.2.0

2018-12	CT#82	CP-183205	0150		F	Re-use 5QiPriorityLevelRm data type	15.2.0
2018-12	CT#82	CP-183205	0151		F	FlowDirectionRm data type	15.2.0
2018-12	CT#82	CP-183205	0152	1	F	Correction to TrafficControlData data type	15.2.0
2018-12	CT#82	CP-183205	0153	1	F	Correction to the redirect function	15.2.0
2018-12	CT#82	CP-183205	0154		F	Correction to the modification of an attribute with a value of type map	15.2.0
2018-12	CT#82	CP-183205	0155	3	F	Correction to SmPolicyDection data type	15.2.0
2018-12	CT#82	CP-183205	0157	1	F	Correction to request rule data and requuest usage data	15.2.0
2018-12	CT#82	CP-183205	0158	1	F	Correction to QosData data structure	15.2.0
2018-12	CT#82	CP-183205	0159	2	F	Correction to Qos Characteristics	15.2.0
2018-12	CT#82	CP-183205	0160	1	F	Correction to PccRule data type	15.2.0
2018-12	CT#82	CP-183205	0161		F	Correction to FlowInformation data type	15.2.0
2018-12	CT#82	CP-183205	0162	1	F	Correction to ChargingData data type	15.2.0
2018-12	CT#82	CP-183205	0163		F	Correct the minProperties of the attributes	15.2.0
2018-12	CT#82	CP-183205	0164	1	F	Correct the minItems of the attributes	15.2.0
2018-12	CT#82	CP-183205	0166	1	F	delete UsageMonitoring in pccRule	15.2.0
2018-12	CT#82	CP-183205	0167		F	rename the heading	15.2.0
2018-12	CT#82	CP-183205	0168		F	incorrect description of online and offline	15.2.0
2018-12	CT#82	CP-183205	0169		F	Location header	15.2.0
2018-12	CT#82	CP-183205	0170	1	F	API Version Update	15.2.0
2018-12	CT#82	CP-183205	0172		F	Corrections to OpenAPI file	15.2.0
2018-12	CT#82	CP-183205	0173	1	F	Corrections of user location and session AMBR attributes	15.2.0
2018-12	CT#82	CP-183205	0174	1	F	Common data types	15.2.0
2018-12	CT#82	CP-183205	0176	2	F	Presence Info removal	15.2.0
2018-12	CT#82	CP-183205	0177	2	F	Correction of SmPolicyUpdateContext data type in OpenAPI	15.2.0

History

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