ETSI TS 129 512 V15.0.0 (2018-06)

5G;
5G System;
Session Management Policy Control Service;
Stage 3
(3GPP TS 29.512 version 15.0.0 Release 15)

Reference
DTS/TSGC-0329512vf00

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

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 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".

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
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
QoS	Quality of Service
SDF	Service Data Flow
SMF	Session Management Function
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.

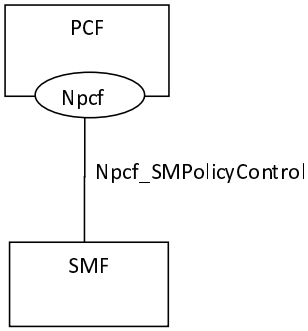

Figure 4.1.2-1: Reference Architecture for the Npcf_SMPolicyControl Service; SBI representation

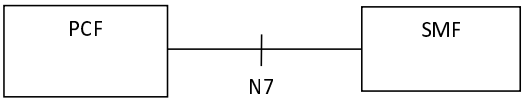

Figure 4.1.2-2: Reference Architecture for the Npcf_SMPolicyControl Service; reference point representation

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 OCS; 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 the PCF, related to service flow detection, QoS, charging, gating, traffic usage reporting and traffic steering

The SMF shall support:

- 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];
- deleting policy rules on the user plane;
- sending usage reports to the PCF;
- handling event notification requests;
- sending event notification towards the PCF; and
- sending charging related information to the PCF.

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 or application identifiers (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.

SessionRule is defined in subclause 4.1.4.3. PccRule is defined in subclause 4.1.4.2.

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.

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
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
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
	Charging	
Charging key	The charging system (OCS or OFCS) 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	
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 RAN when the GFBR can no longer (or again) be fulfilled 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 maximum bitrate authorized for the service data flow.	Optional
GBR (UL/DL)	The downlink maximum 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
	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
Data Network Access Change report	Indicates whether a notification in case of change of DNAI at addition/change/removal of the UPF is requested, as well as the destination(s) for where to provide the notification. The notification information includes the target DNAI and an indication of early and/or late notification.	Optional

Editor's note: The above table is FFS and will be further revised (elements added and/or removed). This table needs to be aligned with the grouping of decision data and PCC rule content as defined in subclause 5.6.2.6.

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 SessionRule

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.

4.1.4.4 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.

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 may include:

- Traffic Control Data ID;
- Dnai;
- Flow Action;
- Redirect Information;
- Mute Notification;
- Traffic Steering Policy ID UL; and
- Traffic Steering Policy ID DL.

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 may include:

- QoS Data ID;
- 5QI;
- 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;
- Allocation Retention Priority; 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 may include:

- Charging Data ID;
- Metering Method;
- Charging Method (online/offline);
- Rating Group;
- 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 may include:

- Usage Monitoring ID;
- Volume Threshold (UL,DL);
- Time Threshold;
- Monitoring Time;
- Next Volume Threshold (UL, DL);
- Next Time Threshold; and
- Inactivity Time Threshold.

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.

Editor's note: Further descriptions are needed for the independent policy control request triggers.

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 corresponding triggers shall be included in the request.

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.

4.1.7 Requested Usage data

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

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.

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.

4.2.2.2 SMPolicyControl_Create

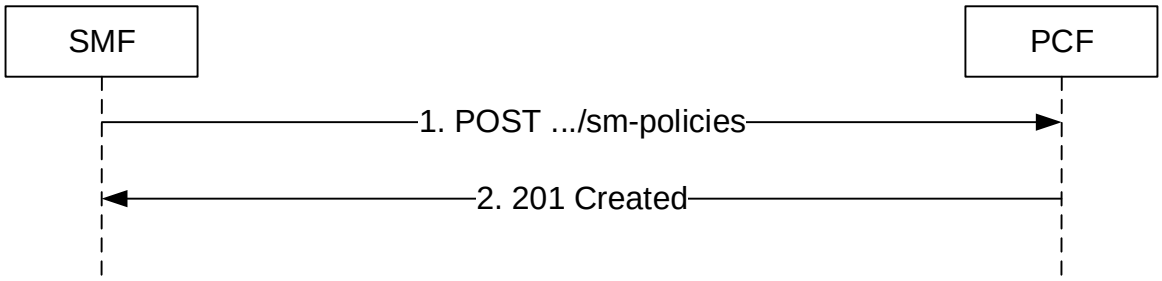

Figure 4.2.2.2-1: SMPolicyControl_Create

When the SMF receives the Nsmf_PDUSession_CreateSMContext Request as defined in subclause 5.2.2.2 of 3GPP TS 29.502 [2], 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 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":

- 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 "smPoliciesUpdateNotificationUrl" attribute;
- PEI within the "pei" 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 "subscribedSessionAmbr" attribute;
- subscribed Default QoS Information within "subscribedDefaultQoSInformation" attribute;
- user location information within the "userLocationInformation" attribute; and
- identifier of the serving network within the "servingNetwork" attribute.

Editor's note: Other information included in the POST message is FFS.

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; and
- (optionally also containing policy control request triggers) encoded 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.

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

Editor's note: Description of failure cases is FFS.

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 to the SMF during the initial interaction with the SMF defining the charging function respectively. In order to do so, the PCF shall include a chargingData attribute and a sessionRule attribute within the "sMPolicyControl" attribute in the response of HTTP POST message. The PCF shall include the CHF addresses within a "chargingInformation" attribute of the "chargingData" attribute and included the "decisionId" attribute of "chargingData" in the sessionRule. 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, respectively, shall not be considered as an error since such PCC rules may be provided in later provisioning.

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 PCF 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 chargingMethod attribute embedded directly within the "smPolicyContextData" attribute 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, the PCF shall include a "chargingData" attribute and a "sessionRule" attribute within the "sMPolicyControl" attribute in the response of HTTP POST message. The PCF shall include the offline attribute set to true, if offline charging applies and/or online attribute set to true, if online charging applies within the "chargingData" attribute and included the "decisionId" attribute of "chargingData" in the sessionRule. The default charging method provided by the PCF shall overwrite any predefined default charging method at the SMF.

4.2.2.4 Provisioning of revalidation time

The SMF 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.

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 4.2.6.4.3.

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.

4.2.3.2 SM Policy Association Notification request

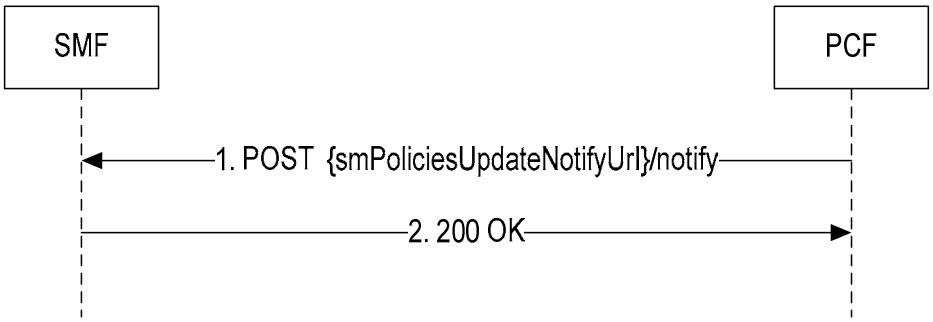

Figure 4.2.3.2-1: SMPolicyControl UpdateNotify Update Service Operation

1. The PCF shall send a POST request to the NF Service Consumer (SMF) (../{smPoliciesUpdateNotifyUri}/notify). The payload body of the message shall contain an SmPolicyNotification data structure that contains 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.
2. In case of a successful update of PCC rule(s) a "200 OK" shall be returned in the response.

Editor's note: If a body is being sent in the response and the content is FFS.

4.2.3.3 SM Policy Association termination request

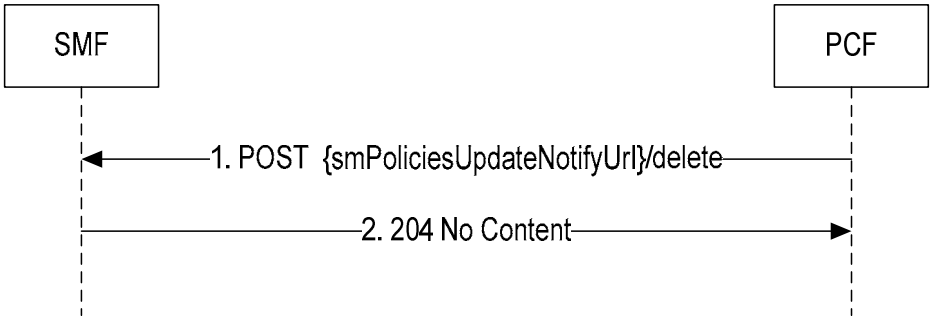

Figure 4.2.3.3-1: SMPolicyControl UpdateNotify Service Operation

1. The PCF shall send a POST request to the NF Service Consumer (SMF) (../{smPoliciesUpdateNotifyUri}/delete). The PCF shall provide in the body of the HTTP POST request the identifier of the individual SM policy resource and the PDU session termination request.
2. If the SMF accepted received POST request the SMF shall send "204 No Content" response.

Editor's note: Additional encoding details will be added when they are agreed.

Editor's note: Description of failure cases is FFS.

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.

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 4.2.6.2.1 and 4.2.6.2.2.

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 in the QoS information within the PCC Rule shall be assigned a priority 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). If the "accessType" attribute is assigned to "3GPP-ACCESS" and the "preemptCap" attribute and "preemptVuln" attribute were received within the "arp" attribute in the "subsDefQos" attribute in the HTTP POST message, the values of the "preemptCap" attribute and "preemptVuln" attribute shall also be assigned as required by local operator policies.

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 running.

Any SMF-initiated request for PCC Rules for an IMS Emergency service triggered by "authPolicyConReqTrigger" assigned to "RES_MO_RE" (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 default QoS flow 5QI or the 5QI used for IMS signalling were removed from the PDU session restricted to Emergency Services. 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

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 [17], 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.

4.2.3.11 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 4.2.6.4.3 to reques 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.

Editor's note: It is FFS how the PCF indicates which rules are applicable to a specific Ipv6 prefix and how the SMF derives the policies and provisions them to the corresponding PDU session Anchor. It is FFS how the usage monitoring is performed in this case.

4.2.4 Npcf_SMPolicyControl_Update Service Operation

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.

Figure 4.2.4-1 illustrates a requesting the update of the Session Management related policies.

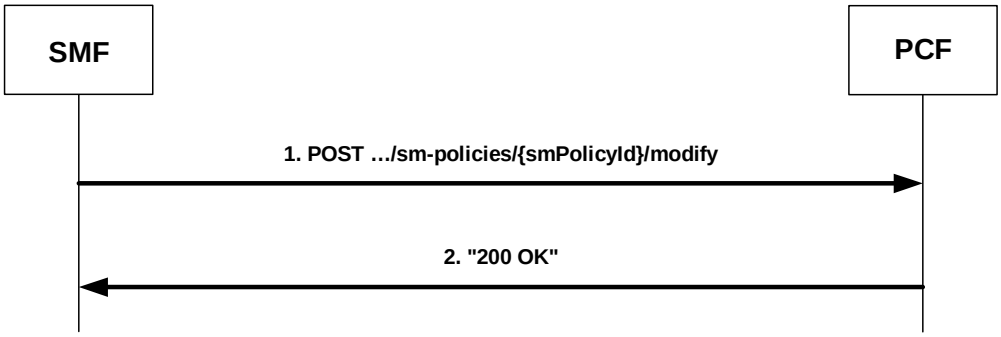

Figure 4.2.4-1: Requesting the update of the Session Management related policies

1. The NF Service Consumer 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.

2. 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.

Editor's note: This text needs to be enhanced with encoding details such as attribute names once they are defined.

4.2.4.1 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 SmPolicyContextData 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.

4.2.4.2 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.

4.2.4.3 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 4.2.6.2.1 and 4.2.6.2.2.

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.

4.2.4.4 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.

4.2.4.5 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 "userLocationInformation" 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 "ranNasRelCause" 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].

4.2.4.6 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.

4.2.4.7 Report of Access Network Information

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.

4.2.4.8 Reporting Accumulated Usage

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.

4.2.4.9 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.

Editor's note: It is FFS how the PCF indicates which rules are applicable to a specific Ipv6 prefix and how the SMF derives the policies and provisions them to the corresponding PDU session Anchor. It is FFS how the usage monitoring is performed in this case.

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.

4.2.5.2 SM_Policy Association Delete

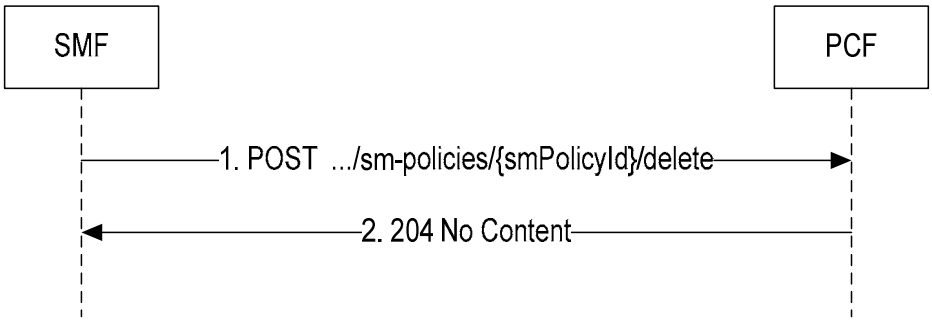

Figure 4.2.5.2-1: SMPolicyControl Delete

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 in the body:

- optional volume usage information "accuUsageReport".

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.

If the HTTP POST request from the SMF is rejected by the PCF, the PCF shall indicate the cause for the rejection in the response to the SMF. Further details of error handling are described in subclause 5.7.

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
- Last requested rule data
- Last requested usage data

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.

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.

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, 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.

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, installing or modifying a 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 install a new PCF-provisioned PCC rule, the PCF shall further set other attributes within the PccRule data structure as follows:

- it shall include the precedence within the "precedence" attribute;
- it shall include the flow information within the "flowInfos" attribute(s) or application identifier within the "appId" attribute;
- it may 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 been provided;
- it may 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 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 SmPoliciesDecision data structure if it has 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 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 been provided;

In order to modify an existing 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).

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

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 "flowAction" 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 a dynamic PCC rule to the SMF. The Provisioning shall be performed using the PCC rule provisioning procedure as defined in subclause 4.2.6.2.1. The redirect instruction shall be encoded using a "redirectInfo" attribute within the TrafficControlData data structure which the dynamic PCC rule refers to.

For a dynamic PCC rule, the redirect address may be provided as part of the dynamic PCC rule 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 for this PCC rule.

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 "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 remove the reference to the Traffic Control Data decision if this is no valid attribute within the Traffic Control Data decision;
- update the PCC rule to modify the reference to a new Traffic Control Data decision which does not have the "redirectInfo";
- update the Traffic Control Data decision which the PCC rule refers to with the "redirectSupport" attribute set to false if no other PCC rule refers to this Traffic Control Data decision and there are still valid attributes within the Traffic Control Data decision; or

remove the Traffic Control Data decision which the PCC rule refers to if no other PCC rule refers to this Traffic Control Data decision and there are no valid attributes within the 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 [12] applicable for any UE or Internal Group Id if received in the SMF request.

Then the PCF authorizes the request 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.

For impacted PDU Session that corresponds to the AF request, the PCF shall provide the SMF with PCC rules that are generated based on the AF request. In order to do so, the PCF shall within the PccRule data instance(s) include the information to identify the traffic within the "flowInfos" attribute or "appId" attribute, and/or within the Traffic Control Data data decision which the PCC rule refers to include the DNAI change report information within the "dnaiReport" attribute, and/or the information about the DNAI(s) towards which the traffic routing should apply within the "dnais" attribute, and/or a list of traffic steering policy IDs within the "trafficSteeringPolIdDl" attribute and/or "trafficSteeringPolIdUl" attribute. Within the "dnaiReport" attribute, the PCF shall include the "earlyNotification" attribute set to true or "lateNotification" attribute set to true to indicate the notification on AF subscription (type of notifications) and the notification address within the "notificationUri" attribute. The PCF may provide the PCC rule as defined in subclause 4.2.6.2.1.

Editor's note: It is FFS whether or how indication of application relocation possibility is supported.

Editor's note: It is FFS how the SMF notify the DNAI change.

If the temporal validity condition is received, the PCF shall evaluates 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). 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 by triggering a PDU Session Modification. When the SMF becomes aware that the UE left the area subscribed by the PCF, the SMF notifies the PCF and the PCF provides updated PCC rules by triggering a PDU Session Modification. SMF notifications to the PCF about UE location in or out

of the subscribed area of interest are triggered by UE location change notifications received from the AMF or by UE location information received during a Service Request or Handover procedure.

Editor's note: Above description needs to be reviewed when PRA procedure is defined.

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.

Editor's note: It is FFS how to update the conditioned PCC rule.

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 bearer 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 [17] 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 [17], 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 [17], 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 [17] 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 [17] 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 [17] . 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 [17] 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 [10] 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 [17].

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 [10].

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 [17], 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 [17]. 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.

Editor's note: A 5QI can either be a standard 5QI, standard 5QI with 5QI Priority Level, or non-standard 5QI (with flexible QoS characteristics). Therefore, the specific use of 5QI terminology needs to be clarified for each 5QI reference made within this specification and across other specifications.

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 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 subsclause 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 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 change) and, if applicable, shall initiate an HPPT POST message as defined in subcluase 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 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 of the default 5QI 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 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 requires 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 in clause 4.2.y. 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 4.2.6.5.

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:

- set the ARP of the default QoS flow as appropriate for the prioritized service;
- if required, set the ARP and 5QI 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 of these PCC Rules based on the information received over N7/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;
- set the ARP of the default QoS flow as appropriate for the IMS Multimedia Priority set to inactive;
- replace the ARP 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 [17] subclauses 4.4.1 and 4.4.2 or 3GPP TS 29.514 [10] 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 "chgDecs" attribute which the PCC rule refers to. The application service provider identity shall be set using the "appSvcProvId" attribute within the "chgDecs" attribute which the PCC rule refers to. The "sponsorId" attribute and "appSvcProvId" shall be included if the "reportingLevel" attribute 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 structure and request usage monitoring control for the monitoring key by following the procedures specified in subclauses 4.2.6.4.3.

When the AF disables sponsoring a service (See 3GPP TS 29.514 [10] 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 structure 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.

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.

4.2.6.3 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 authorized default QoS within the "authDefaultQoS" attribute;;
- 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.

Editor's note: It is FFS how to update the conditioned session rule.

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].

4.2.6.4 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.

4.2.6.4.1 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 inlcude 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.

4.2.6.4.2 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 RAN_NAS_REL within the "reqData" attribute and reference of the removed PCC rule wthin the "refPccRuleIds" attribute.

Editor's note: Definition of RAN_NAS_REL is FFS.

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.

4.2.6.4.3 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 an 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 an 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 PUD 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 PCRF may requests 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 "authPolicyCtrlReqTriggesr" 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 "usageMonitoringData" attribute within the coppresponding parent attribute.

Threshold levels, monitoring time if applicable and inactive time if application for each usage monitoring control instance may be provisionged 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 "inactiveTime" 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.

Editor's note: It is FFS how to exclude one or several SDF from PDU session level usage monitoring.

Editor's note: It is FFS how to perform the usage monitoring control in the multi-homing case.

If the PCF wishes to modify the threshold level for one or more monitoring keys, the PCRF shall provide the thresholds for all the different levels applicable 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 subcluase 7.5.2 or PFCP Session Modification Request as defined in subcluase 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 conatin the "allUmIds" set to true.

4.2.6.5 Authorized QoS

4.2.6.5.1 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 4.2.6.5.2.
- 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 a explicitly signalled QoS Characteristics, it shall be provisionedas defined in subclause 4.2.6.4.2.
- When the authorized QoS applies to the Reflective QoS, it shall be provisioned as defined in subclause 4.2.6.2.x.

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 PCC Rule Error handling.

Editor's note: PCC Rule Error handling is FFS.

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.

4.2.6.5.2 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, the PCF shall include the authorized GBR 5QI 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. The PCF may request a notification when authorized GBR cannot be fulfilled or can be fulfilled 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 and "reflectiveQos" attribute set to true to enable the Reflective QoS control to the service data flow. 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 during the PDU session establishment.

At reception of the service information from the AF, if configured through policy, the PCF may determine the Maximum Packet Loss Rate for UL and DL based on the service information. In this case, the PCF shall include the Maximum Packet Loss Rate value within the "maxPacketLossRate" attribute.

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

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

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 4.2.8.5.

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 3: 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 an 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.

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.

4.2.6.5.3 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 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 QosCharacteristics 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 Packet Loss Rate value within the "packetLossRate" attribute, the Averaging Window value within the "averagingWindow" attribute if applicable and the Maximum Data Burst Volume value within the "maximumDataBurstVolume" attribute if applicable.

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.

4.2.7 Reporting Result of Policy Enforcement

4.2.7.1 Report of Access Network Charging Identifier

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 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 "accNetChId" attribute with the "accNetChaIdValue" containing the Access Network Charging Identifier and one or more "pccRuleId" attribute containing corresponding PCC rule identifier(s) within the SmPolicyContextData data structure.

4.2.7.2 RAN NAS Cause Support

When RAN-NAS-Cause feature is supported, the PCEF shall maintain locally the removed PCC rules that were referred by the RequestedRuleData instance containing te "reqData" attribute with the RAN_NAS_REL until it reports RES_RELEASE policy control request trigger upon reception of the resource release outcome from the network.

If the RAN-NAS-Cause feature is supported and 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 RAN_NAS_REL 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 "userLocationInformation" attribute (if available), "userLocationInfoTime" attribute (if available) and "ueTimezone" attribute (if available).

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 [2], 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 [2].
- 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].

5.2.3 HTTP custom headers

5.2.3.1 General

5.3 Resources

5.3.1 Resource Structure

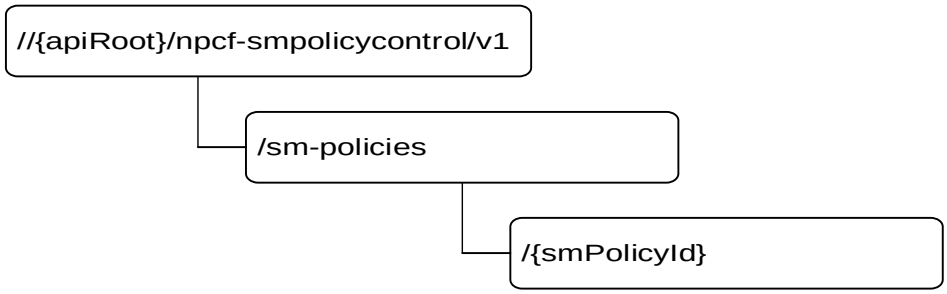

Figure 5.3.1-1: Resource URI structure of the Npcf_SMPolicyControl API

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 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}/modify	Modify (POST)	Update the Individual SM Policies resource when a policy control request event is met.

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		An individual SM Policy resources for the SUPI and PDU session id are created successfully.

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.
			FFS(error case)	

Editor's Note: The description of failure cases is FFS

5.3.3.3.2 DELETE

This method shall support the URI query parameters specified in table 5.3.3.3.2-1.

Table 5.3.3.3.2-1: URI query parameters supported by the DELETE method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 5.3.3.3.2-2 and the response data structures and response codes specified in table 5.3.3.3.2-3.

Table 5.3.3.3.2-2: Data structures supported by the DELETE Request Body on this resource

Data type	P	Cardinality	Description
n/a			

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

Data type	P	Cardinality	Response codes	Description
n/a			204 No Content	The SM Policy resource for the PDU session in the request URI was removed.

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}/modify	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.

5.3.3.4.3 Operation: modify

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.

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

URI: **{Notification URI}/update**

The operation shall support the URI variables defined in table 5.5.4.2-1.

Table 5.3.4.2-1: URI variables

Name	Definition
NotificationUrl	reference provided by the SMF during the initial retrieval of the SM Policies.

This method shall support the URI query parameters specified in table 5.5.2-2.

Table 5.3.4.3.1-1: URI query parameters supported by the POST method on this resource

Name	Data type	P	Cardinality	Description
n/a				

This method shall support the request data structures specified in table 5.5.2-3 and the response data structures and response codes specified in table 5.3.4.3.1-3.

Table 5.5.2-3: 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 5.5.2-4: 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.
			FFS(error case)	

Editor's note: The description of failure cases is FFS.

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.

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

Data type	Section defined	Description	Applicability
AccuUsageReport	5.6.2.18		
ChargingData	5.6.2.11	Contains charging related parameters. Inherits all parameters from DecisionData.	
ChargingInformation	5.6.2.17		
ConditionData	5.6.2.9	Contains conditions for applicability of a rule.	
FlowDirection	5.6.3.3		
FlowInformation	5.6.2.14	Contains the flow information.	
FlowStatus	FFS	Indicates the flow status.	
MeteringMethod	5.6.3.5	Indicates the metering method.	
PccRule	5.6.2.6	Contains the PCC rule information.	
PolicyControlRequestTrigger	5.6.3.6		
QosCharacteristics	5.6.2.16	Contains QoS characteristics for a non standard 5QI.	
QoSData	5.6.2.8	Contains the QoS parameters.	
RedirectAddressType	FFS	Indicates the redirect address type.	
RedirectInformation	5.6.2.13	Contains the redirect information.	
ReportingLevel	5.6.3.4	Indicates the reporting level.	
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.	
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		
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). Inherits all parameters from DecisionData.	
UsageMonitoringData	5.6.2.12	Contains usage monitoring related control information. Inherits all parameters from DecisionData.	

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
5qi	3GPP TS 29.571 [11]	Unsigned integer representing a 5G QoS Identifier (see subclause 5.7.2.1 of 3GPP TS 23.501 [8]), within the range 0 to 255. In an OpenAPI Specification [3] schema, the format shall be designated as "5qi".	
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 [8]), 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. In an OpenAPI Specification [3] schema, the format shall be designated as "5qiPriorityLevel".	
AccessType	3GPP TS 29.571 [11]	The identification of the type of access network.	
AfSignallingProtocol	FFS		
Ambr	3GPP TS 29.571 [11]	Session AMBR	
AverWindow	3GPP TS 29.571 [11]	Averaging Window	
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" In an OpenAPI Specification [3] schema, the format shall be designated as "BitRate".	
ChargingInformation	3GPP TS 29.571 [11]		
DefaultQosInformation	3GPP TS 29.571 [11]	Identifies the information of the default QoS.	
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.	
Ipv4Addr	3GPP TS 29.571 [11]	The Ipv4 address allocated for the user.	
Ipv6Prefix	3GPP TS 29.571 [11]	The Ipv6 prefix allocated for the user.	
MaxDataBurstVol	3GPP TS 29.571 [11]	Maximum Data Burst Volume	
NetworkId	3GPP TS 29.571 [11]	The identification of the Network.	
PacketDelBudget	3GPP TS 29.571 [11]	Packet Delay Budget	
PacketErrRate	3GPP TS 29.571 [11]	Packet Error Rate	
PduSessionId	3GPP TS 29.571 [11]	The identification of the PDU session.	
Pei	3GPP TS 29.571 [11]	The Identification of a Permanent Equipment.	
RatType	3GPP TS 29.571 [11]	The identification of the RAT type.	
ResourceType(FFS)	3GPP TS 29.571 [11]	Indicates whether the resource type is GBR, delay critical GBR, or non-GBR.	
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.	
UeTimeZone	3GPP TS 29.571 [11]		
Uri	3GPP TS 29.571 [11]		
UserLocation	3GPP TS 29.571 [11]		

5.6.2 Structured data types

5.6.2.1 Introduction

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

Allowed structures are: array, object.

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 charing identifier for the PCC rule(s) or whole PDU session.	
gpsi	Gpsi	O	0..1	Gpsi shall contain either an External Id or an MSISDN.	
supi	Supi	M	1	Subscription Permanent Identifier	
pduSessionId	PduSessionId	M	1	PDU session Id	
dnn	Dnn	M	1	The DNN of the PDU session.	
smPoliciesUpdateNotificationUrl	Uri	M	1	Identifies the recipient of SM policies update notifications sent by the PCF.	
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.	
userLocationInformation	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.	
subSessAmbr	Ambr	O	0..1	Subscribed Session-AMBR.	
subscribedDefaultQosInformation	DefaultQosInformation	O	0..1	Subscribed Default QoS Information.	
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.	
3gppPsDataOffStatus	boolean	O	0..1	If it is included and set to true, the 3GPP PS Data Off is activated by the UE.	
supportedFeatures	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 request the creation of an individual SM policy resource and by the PCF in the related response, respectively.	

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	0..N	A map of Sessionrules with the content being the SessionRule as described in subclause 5.6.2.7.	
pccRules	map(PccRule)	O	0..N	A map of PCC rules with the content being the PCCRule as described in subclause 5.6.2.6.	
qosDecs	map(QoSData)	O	0..N	Map of QoS data policy decisions.	
ChgDecs	map(ChargingData)	O	0..N	Map of Charging data policy decisions.	
chargingInfo	ChargingInformation	O	0..1	Contains the CHF addresses of the PDU session.	
traffContDecs	map(TrafficControlData)	O	0..N	Map of Traffic Control data policy decisions.	
umDecs	map(UsageMonitoringData)	O	0..N	Map of Usage Monitoring data policy decisions.	
qosChars	map(QosCharacteristics)	C	0..N	Map of QoS characteristics for non standard 5QIs. This map uses the 5QI values as keys.	
reflectiveQoSTimer	DurationSec	O	0..1	Defines the lifetime of a UE derived QoS rule belonging to the PDU Session for reflective QoS.	
conds	map(ConditionData)	O	0..N	A map of condition data with the content being as described in subclause 5.6.2.9.	
revalidationTime	DateTime	O	0..1	Defines the time before which the SMF shall have to re-request PCC rules.	
policyCtrlReqTriggers	array(PolicyControlRequestTrigger)	O	0..N	Defines the policy control request triggers subscribed by the PCF.	
lastReqRuleData	array(RequestedRuleData)	O	0..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.	

5.6.2.5 Type SmPolicyNotification

Table 5.6.2.5-1: Definition of type SmPolicyNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
supi	Supi		1	Subscription Permanent Identifier	
pduSessionId	PduSessionId		1	PDU session id	
smPolicyDecision	SmPolicyDecision		1	Session management policy (see subclause 5.6.2.4).	

Editor's note: The use of smPolicyDecision is FFS.

Editor's note: The indication of the presence of the attributes is FFS.

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	0..N	An array of IP flow pac information.
appId	string	C	0..1	A reference to the app detection filter configu UPF.
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.
refQosData	array(string)	O	0..N	A reference to the QoS type decision type. It is described in subclause (NOTE)
refTcData	array(string)	O	0..N	A reference to the TrafficControlData poli type. It is the tcId desc subclause 5.6.2.10. (NOTE)
refChgData	array(string)	O	0..N	A reference to the Cha policy decision type. It described in subclause (NOTE)
refUmData	array(string)	O	0..N	A reference to UsageMonitoringData decision type. It is the described in subclause (NOTE)
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

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	
authDefaultQos	DefaultQosInformation	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	integer	M	1	Identifier for the authorized QoS parameters for the service data flow.	
maxbrUl	BitRate	O	0..1	Indicates the max bandwidth in uplink.	
maxbrDl	BitRate	O	0..1	Indicates the max bandwidth in downlink.	
gbrUl	BitRate	O	0..1	Indicates the guaranteed bandwidth in uplink.	
gbrDL	BitRate	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 RAN when the GFBR can no longer (or again) be fulfilled for a QoS Flow during the lifetime of the QoS Flow.	
reflectiveQos	boolean	O	0..1	Indicates whether the QoS information is reflective for the corresponding service data flow.	
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.	
maxPacketLossRate	PacketLossRate(FFS)	O	0..1	Indicates the maximum rate for lost packets that can be tolerated for the service data flow.	
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	

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	DateTime	O	0..1	The time when the decision data shall be activated.	
deactivationTime	DateTime	O	0..1	The time when the decision data shall be deactivated.	

Editor's note: It is FFS whether other conditional information such as ratType, ipCanType can be part of this type.

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.	
flowAction	FFS			Enum determining what action to perform on traffic. Possible values are: [enable, disable, enable_uplink, enable_downlink, redirect]	
redirectInfo	RedirectInformation	C	0..1	It indicates whether the detected application traffic should be redirected to another controlled address	
muteNotif	boolean	O	0..1	Indicates whether applicat'on's start or stop notification is to be muted.	
trafficSteeringPolIdDl	string	O	0..1	Reference to a pre-configured traffic steering policy for downlink traffic at the SMF.	
trafficSteeringPolIdUl	string	O	0..1	Reference to a pre-configured traffic steering policy for uplink traffic at the SMF.	
dnais	array(string)	O	0..N	Identifier of the target Data Network Access	
dnaiReport	DnaiReport	O	0..1	Contains the information about the AF subscriptions of the DNAI change.	

Editor's note: It is FFS if sub types of TrafficControlData should be created to handle redirect, traffic steering, etc.

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.	
offline	boolean	O	0..1	Indicates the online charging is applicable to the PDU session or PCC rule.	
online	boolean	O	0..1	Indicates the offline charging is applicable to the PDU session or PCC rule.	
ratingGroup	string	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.	
serviceId	string	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.	
appSvcProvId	string	O	0..1	Indicates the application service provider identity.	
afChargingIdentifier	string	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.	
charingInformation	CharingInformation(FFS)	O	0..1	Contains the CHF addresses of the PDU session.	

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	FFS	O	0..1	Indicates the total volume threshold.	
volumeThresholdUplink	FFS	O	0..1	Indicates a volume threshold in uplink.	
volumeThresholdDownlink	FFS	O	0..1	Indicates a volume threshold in downlink.	
timeThreshold	DurationSec	O	0..1	Indicates a time threshold.	
monitoringTime	DateTime	O	0..1	Indicates the time at which the UP function is expected to reapply the next thresholds (e.g. nextVolThreshold)	
nextVolThreshold	FFS	C	0..1	Indicates a volume threshold after the Monitoring Time.	
nextVolThresholdUplink	FFS	O	0..1	Indicates a volume threshold in uplink after the Monitoring Time.	
nextVolThresholdDownlink	FFS	O	0..1	Indicates al volume threshold in downlink after the Monitoring Time.	
nextTimeThreshold	DurationSec	C	0..1	Indicates a time threshold after the Monitoring.	
inactivityTime	DurationSec	O	0..1	Defines the period of time after which the time measurement shall stop, if no packets are received.	

Editor's note: It is FFS how to handle transient control data such as requesting usage. Note that disabling usage monitoring can be done by removing the usage monitoring data from the session level map.

5.6.2.13 Type RedirectInformation

Table 5.6.2.13-1: Definition of type RedirectInformation

Attribute name	Data type	P	Cardinality	Description	Applicability
redirectSupport	boolean	M	1	Indicates the redirect is enable.	
redirectAddressType	RedirectAddressType(FFS)	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..N	Contains the packet filters of the IP flow(s).	
packetFilterUsage	boolean	O	0..1	The packet shall be sent to the UE.	
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).	
sourceMacAddress	string	O	0..1	Contains the source MAC address	
destinationMacAddress	string	O	0..1	Contains the destination MAC address	
ethertype	Ethertype(FFS)	O	0..1	Indicates the type of Ethernet.	
vid	string	O	0..2	Contains the VID of C-TAG or S-TAG.	
pcpdei	string	O	0..2	Contains the PCP/DEI of C-TAG or S-TAG.	

5.6.2.15 Type SmPolicyDeleteData

Table 5.6.2.15-1: Definition of type SmPolicyDeleteData

Attribute name	Data type	P	Cardinality	Description	Applicability
userLocationInformation	UserLocation		0..1	The location of the served UE is camping.	
ueTimeZone	TimeZone		0..1	The time zone where the served UE is camping.	
accuUsageReports	array(AccuUsage Report)	O	0..N	Contains the usage report	

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	integer	M	1	Identifier for the authorized QoS parameters for the service data flow. Applies to PCC rule and PDU session level.	
resourceType	ResourceType(FFS)	M	1	Indicates whether the resource type is GBR, delay critical GBR, or non-GBR.	
priorityLevel	ArpPriorityLevel	M	1	Unsigned integer indicating the ARP Priority Level, within the range 1 to 15. Values are ordered in decreasing order of priority, i.e. with 1 as the highest priority and 15 as the lowest priority.	
packetDelayBudget	PacketDelBudg et	M	1	Unsigned 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 GBR QoS flows.	
maximumDataBurst Volume	MaxDataBurstV ol	C	0..1	Unsigned Integer.Indicates the maximum data burst. This IE shall be present when the packet delay budget is equal to or lower than 20 msec.	

Editor's note: It is FFS if DurationSec granularity is enough to express time values or if finer granularity is needed.

Editor's note: Maximum Data Burst Volume, Averaging Window and Priority Level apply to standardized 5QI too. It is FFS how this can be reflected in the TS.

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(FFS)	O	0..1	Indicates a total accumulated volume usage.	
volUsageUplink	Volume(FFS)	O	0..1	Indicates an accumulated volume usage in uplink.	
volUsageDownlink	Volume(FFS)	O	0..1	Indicates an accumulated volume usage in downlink.	
timeUsage	DurationSec	O	0..1	Indicates an accumulated time usage.	
nextVolUsage	Volume(FFS)	C	0..1	Indicates an accumulated volume usage after the Monitoring Time.	
nextVolUsageUplink	Volume(FFS)	O	0..1	Indicates an accumulated volume usage in uplink after the Monitoring Time.	
nextVolUsageDownlink	Volume(FFS)	0	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)	M	1..N	The policy control reqeust trigges which are met.	
accNetChId	AccNetChId	O	0..1	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.	
userLocationInformation	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.	
relIpv6AddressPrefix	Ipv6Prefix	O	0..1	Indicates the released IPv6 Address Prefix of the served UE in multi-homing case.	
subscribedSessionAmbr	Ambr	O	0..1	Subscribed Session-AMBR.	
subscribedDefaultQosInformation	DefaultQosInformation	O	0..1	Subscribed Default QoS Information.	
accuUsageReports	array(AccuUsageReport)	O	0..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	0..N	Reports the start/stop of the application traffic and detected SDF descriptions if applicable.	ADC

'5.6.2.20 Type DnaiReport

Table 5.6.2.10-1: Definition of type DnaiReport

Attribute name	Data type	P	Cardinality	Description	Applicability
notificationUri	Uri	M	1	Notification address of the DNAI change.	
earlyNotification	boolean	O	0..1	When it is included and set to true, indicates the early notification is required.	
lateNotification	boolean	O	0..1	When it is included and set to true, indicates the late notification is required.	
NOTE: Either earlyNotification or lateNotification or both shall be included					

5.6.2.21 Type TerminationNotification

Table 5.6.2.21-1: Definition of type TerminationNotification

Attribute name	Data type	P	Cardinality	Description	Applicability
supi	Supi	M	1	Subscription Permanent Identifier	
pduSessionId	PduSessionId	M	1	PDU session id	

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	0..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	string	M	1	Contains a charging identifier	
pccRuleId	array(string)	O	0..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	0..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.	

5.6.3 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
ArpPriorityLevel	integer	Unsigned integer indicating the ARP Priority Level (see subclause 5.7.2.2 of 3GPP TS 23.501 [8]), within the range 1 to 15. Values are ordered in decreasing order of priority, i.e. with 1 as the highest priority and 15 as the lowest priority. In an OpenAPI Specification [3] schema, the format shall be designated as "ArpPriorityLevel".	
PreEmpCap	boolean	Pre-emption-Capability where 0 indicates that assigned resources of another IP flow can be assigned to the P flow, while 1 indicates that assigned resources of other IP flows cannot be assigned to the IP flow.	
PreEmpVul	boolean	Pre-emption-Vulnerability where 0 indicates pre-emption on the IP flow cannot be done, while 1 indicates that pre-emption on the IP flow can be done.	

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.	

Editor's note: An Unspecified value would be required if the data type is used to report filter information received from the UE.

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. 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.	
PCC_RMV	The SMF reports when the PCC rule is removed. The SMF always reports to the PCF.	
QOS_STO	The SMF notify the PCF when receiving notification from RAN that QoS targets of the QoS Flow cannot be fulfilled	
QOS_STA	The SMF notify the PCF when receiving notification from RAN that QoS targets of the QoS Flow can be fulfilled 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	
ENF_PCC_RUL	Enforced PCC rule request where the SMF is performing a PCC rules request as instructed by the PCF.	
RE_TIMEOUT	Indicates the SMF generated the request because there has been a PCC revalidation timeout	

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.	

5.7 Error handling

This subclause will include a reference to the general error handling principles specified in TS 29.501, and further specify any general error handling aspect specific to the API, if any Error handling specific to each method (and resource) is specified in subclauses 5.3 and 5.4.

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.

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.

Editor's note: The Npcf_SMPolicyControl API as defined in A.2 is based on the current version of the specification and needs to be updated in later versions.

A.2 Npcf_SMPolicyControl API

Editor's note: HTTP Error responses need to be alligned with updates to Table 5.2.7.1-1 of 3GPP TS 29.500 [].

Editor's note: The Open API file needs to be updated to incorporate the changes agreed in CT3#97.

```
openapi: 3.0.0
info:
  description: Session Management Policy Control Service
  version: "1.R15.0.0"
  title: Npcf_SMPolicyControl
externalDocs:
  description: 3GPP TS 29.512 V0.6.0 (2018-05) 5G System; Session Management Policy Control Service;
Stage 3 version 15.0.0
  url: http://www.3gpp.org/ftp/Specs/archive/29_series/29.512/
servers:
  - url: https://{apiRoot}/npcf-sm-policy-control/v1
    variables:
      apiRoot:
        default: demohost.com
        description: apiRoot as defined in subclause subclause 4.4 of 3GPP TS 29.501, excluding the
http:// part
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'
        '400':
          $ref: 'TS29571_CommonData.yaml#/components/responses/400'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      callbacks:
        SmPolicyUpdateNotification:
          '{$request.body#/smPoliciesUpdateNotificationUrl}/update':
            post:
              requestBody:
                required: true
                content:
                  application/json:
                    schema:
                      $ref: '#/components/schemas/SmPolicyNotification'
              responses:
                '204':
                  description: No Content, Notification was succesfull
                '400':
                  $ref: 'TS29571_CommonData.yaml#/components/responses/400'
```

```
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              default:
                $ref: 'TS29571_CommonData.yaml#/components/responses/default'
      SmPolicyContolTerminationRequestNotification:
        '{$request.body#/smPoliciesUpdateNotificationUrl}/terminate':
          post:
            requestBody:
              required: true
              content:
                application/json:
                  schema:
                    $ref: '#/components/schemas/TerminationNotification'
            responses:
              '204':
                description: No Content, Notification was succesfull
              '400':
                $ref: 'TS29571_CommonData.yaml#/components/responses/400'
              '404':
                $ref: 'TS29571_CommonData.yaml#/components/responses/404'
              '500':
                $ref: 'TS29571_CommonData.yaml#/components/responses/500'
              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'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        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'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        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'
        '500':
          $ref: 'TS29571_CommonData.yaml#/components/responses/500'
        default:
          $ref: 'TS29571_CommonData.yaml#/components/responses/default'
components:
  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'
        gpsi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Gpsi'
    # Editor's note: FFS. Defined in TS 29.571, but not listed as reused data type.

        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        pduSessionId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PduSessionId'
        dnn:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Dnn'
        smPoliciesUpdateNotificationUrl:
          $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'
        userLocationInformation:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        ueTimeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
    # Editor's note: FFS. Defined in TS 29.571, but not listed as reused data type.

        pei:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Pei'
        ipv4Address:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ipv6AddressPrefix:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        subSessAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        subscribedDefaultQosInformation:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DefaultQosInformation'
        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.
        supportedFeatures:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/SupportedFeatures'
      required:
        - supi
        - pduSessionId
        - dnn
        - smPoliciesUpdateNotificationUrl
    SmPolicyDecision:
      type: object
      properties:
        sessRules:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/SessionRule'
          minProperties: 0
          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: 0
          description: A map of PCC rules with the content being the PCCRule as described in
subclause 5.6.2.6.
        qosDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/QoSData'
          minProperties: 0
          description: Map of QoS data policy decisions.
        ChgDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/ChargingData'
          minProperties: 0
          description: Map of Charging data policy decisions.
        chargingInfo:
          $ref: '#/components/schemas/ChargingInformation'
    # Editor's note: FFS. Also listed as reused data type from TS 29.571, but not defined there.

        traffContDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/TrafficControlData'
          minProperties: 0
          description: Map of Traffic Control data policy decisions.
        umDecs:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/UsageMonitoringData'
          minProperties: 0
          description: Map of Usage Monitoring data policy decisions.
        qosChars:
          type: object
          additionalProperties:
            $ref: '#/components/schemas/QosCharacteristics'
          minProperties: 0
          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: 0
          description: A map of condition data with the content being as described in
subclause 5.6.2.9.
        revalidationTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
    # Editor's note: FFS. Defined in TS 29.571, but not listed as reused data type.
```

```
        policyCtrlReqTriggers:
          type: array
          items:
            $ref: '#/components/schemas/PolicyControlRequestTrigger'
          minItems: 0
          description: Defines the policy control request triggers subscribed by the PCF.
        lastReqRuleData:
          type: array
          items:
            $ref: '#/components/schemas/RequestedRuleData'
          minItems: 0
          description: Defines the last list of rule control data requested by the PCF.
        lastReqUsageData:
          $ref: '#/components/schemas/RequestedUsageData'
    SmPolicyNotification:
      type: object
      properties:
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        pduSessionId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PduSessionId'
        smPolicyDecision:
          $ref: '#/components/schemas/SmPolicyDecision'
    PccRule:
      type: object
      properties:
        flowInfos:
          type: array
          items:
            $ref: '#/components/schemas/FlowInformation'
          minItems: 0
          description: An array of IP flow packet filter information.
        appId:
          type: string
          description: A reference to the application detection filter configured at the UPF.
        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.
        refQosData:
          type: array
          items:
            type: string
          minItems: 0
          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: 0
          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: 0
          description: A reference to the ChargingData policy decision type. It is the chgId
described in subclause 5.6.2.11. (NOTE)
        refUmData:
          type: array
          items:
            type: string
          minItems: 0
          description: A reference to UsageMonitoringData policy decision type. It is the umId
described in subclause 5.6.2.12. (NOTE)
        refCondData:
          type: string
          description: A reference to the condition data. It is the condId described in
subclause 5.6.2.9.
      required:
        - pccRuleId
    SessionRule:
      type: object
```

```
      properties:
        authSessAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        authDefaultQos:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DefaultQosInformation'
        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.
        refCondData:
          type: string
          description: A reference to the condition data. It is the condId described in
subclause 5.6.2.9.
      required:
        - sessRuleId
    QoSData:
      type: object
      properties:
        qosId:
          type: string
          description: Univocally identifies the QoS control policy data within a PDU session.
        5qi:
          type: integer
          description: Identifier for the authorized QoS parameters for the service data flow.
        maxbrUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        maxbrDl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        gbrUl:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        gbrDL:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/BitRate'
        arp:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Arp'
    # Editor's note: FFS. Defined in TS 29.571, but not listed as reused data type.

        qnc:
          type: boolean
          description: Indicates whether notifications are requested from 3GPP RAN when the GFBR can
no longer (or again) be fulfilled for a QoS Flow during the lifetime of the QoS Flow.
        reflectiveQos:
          type: boolean
          description: Indicates whether the QoS information is reflective for the corresponding
service data flow.
        maxPacketLossRate:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        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
        - 5qi
        - arp
    ConditionData:
      type: object
      properties:
        condId:
          type: string
          description: Uniquely identifies the condition data within a PDU session.
        activationTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
    # Editor's note: FFS. Defined in TS 29.571, but not listed as reused data type.

        deactivationTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
    # Editor's note: FFS. Defined in TS 29.571, but not listed as reused data type.

      required:
        - condId
    TrafficControlData:
      type: object
```

```
      properties:
        tcId:
          type: string
          description: Univocally identifies the traffic control policy data within a PDU session.
        flowAction:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        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.
        trafficSteeringPolIdUl:
          type: string
          description: Reference to a pre-configured traffic steering policy for uplink traffic at
the SMF.
        dnais:
          type: array
          items:
            type: string
          minItems: 0
          description: Identifier of the target Data Network Access
        dnaiReport:
          $ref: '#/components/schemas/DnaiReport'
      required:
        - tcId
    ChargingData:
      type: object
      properties:
        chgId:
          type: string
          description: Univocally identifies the charging control policy data within a PDU session.
        meteringMethod:
          $ref: '#/components/schemas/MeteringMethod'
        offline:
          type: boolean
          description: Indicates the online charging is applicable to the PDU session or PCC rule.
        online:
          type: boolean
          description: Indicates the offline charging is applicable to the PDU session or PCC rule.
        ratingGroup:
          type: string
          description: The charging key for the PCC rule used for rating purposes.
        reportingLevel:
          $ref: '#/components/schemas/ReportingLevel'
        serviceId:
          type: string
          description: Indicates the identifier of the service or service component the service data
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:
          type: string
          description: An identifier, provided from the AF, correlating the measurement for the
Charging key/Service identifier values in this PCC rule with application level reports.
        charingInformation:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

      required:
        - chgId
    UsageMonitoringData:
      type: object
      properties:
        umId:
          type: string
          description: Univocally identifies the usage monitoring policy data within a PDU session.
        volumeThreshold:
          type: string
```

```
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        timeThreshold:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        monitoringTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DateTime'
    # Editor's note: FFS. Defined in TS 29.571, but not listed as reused data type.

        nextVolThreshold:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        nextTimeThreshold:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        inactivityTime:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
      required:
        - umId
    RedirectInformation:
      type: object
      properties:
        redirectSupport:
          type: boolean
          description: Indicates the redirect is enable.
        redirectAddressType:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        redirectServerAddress:
          type: string
          description: Indicates the address of the redirect server.
      required:
        - redirectSupport
    FlowInformation:
      type: object
      properties:
        flowDescription:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        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.
        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'
        sourceMacAddress:
          type: string
          description: Contains the source MAC address
        destinationMacAddress:
          type: string
          description: Contains the destination MAC address
        ethertype:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        vid:
          type: string
          description: Contains the VID of C-TAG or S-TAG.
        pcpdei:
          type: string
          description: Contains the PCP/DEI of C-TAG or S-TAG.
    SmPolicyDeleteData:
      type: object
      properties:
        userLocationInformation:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        ueTimeZone:
```

```
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
    # Editor's note: FFS. Defined in TS 29.571, but not listed as reused data type.

        accuUsageReports:
          type: array
          items:
            $ref: '#/components/schemas/AccuUsageReport'
          minItems: 0
          description: Contains the usage report
    QosCharacteristics:
      type: object
      properties:
        5qI:
          type: integer
          description: Identifier for the authorized QoS parameters for the service data flow.
Applies to PCC rule and PDU session level.
        resourceType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/ResourceType'
    # Editor's note: ResourceType is not yet defined in TS 29.571.

        priorityLevel:
          $ref: '#/components/schemas/ArpPriorityLevel'
        packetDelayBudget:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketDelBudget'
        packetErrorRate:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PacketErrRate'
        averagingWindow:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AverWindow'
        maximumDataBurst Volume:
          $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:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        volUsageUplink:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        volUsageDownlink:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        timeUsage:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DurationSec'
        nextVolUsage:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        nextVolUsageUplink:
          type: string
    # Editor's note: Type is FFS. String only used to pass Syntax check.

        nextVolUsageDownlink:
          type: string
```

Editor's note: Type is FFS. String only used to pass Syntax check.

```
        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.
        accessType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/AccessType'
        ratType:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/RatType'
        servingNetwork:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/NetworkId'
        userLocationInformation:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/UserLocation'
        ueTimeZone:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/TimeZone'
```

Editor's note: FFS. Defined in TS 29.571, but not listed as reused data type.

```
        pei:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Pei'
        ipv4Address:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv4Addr'
        ipv6AddressPrefix:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        relIpv6AddressPrefix:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ipv6Prefix'
        subscribedSessionAmbr:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Ambr'
        subscribedDefaultQosInformation:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/DefaultQosInformation'
        accuUsageReport:
          $ref: '#/components/schemas/AccuUsageReport'
        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: 0
          description: Report the start/stop of the application traffic and detected SDF
descriptions if applicable.
      required:
        - repPolicyCtrlReqTriggers
    DnaiReport:
      type: object
      properties:
        notificationUri:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'
        earlyNotification:
          type: boolean
          description: When it is included and set to true, indicates the early notification is
required.
        lateNotification:
          type: boolean
          description: When it is included and set to true, indicates the late notification is
required.
      required:
        - notificationUri
    TerminationNotification:
      type: object
      properties:
        supi:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/Supi'
        pduSessionId:
          $ref: 'TS29571_CommonData.yaml#/components/schemas/PduSessionId'
      required:
        - supi
```

```
        - pduSessionId
    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: 0
          description: Contains the detected service data flow descriptions if they are deducible.
      required:
        - appId
    AccNetChId:
      type: object
      properties:
        accNetChaIdValue:
          type: string
          description: Contains a charging identifier
        pccRuleId:
          type: array
          items:
            type: string
          minItems: 0
          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
    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: 0
          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: Th77ooleanean 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.
    ArpPriorityLevel:
      type: integer
```

```
      description: Unsigned integer indicating the ARP Priority Level (see subclause 5.7.2.2 of
3GPP TS 23.501 [8]), within the range 1 to 15. Values are ordered in decreasing order of priority,
i.e. with 1 as the highest priority and 15 as the lowest priority. In an OpenAPI Specification [3]
schema, the format shall be designated “s "ArpPriorityLe”el".
    # Editor's note: ArpPriorityLevel is also defined in TS 29.571.

    PreEmpCap:
      type: boolean
      description: Pre-emption-Capability where 0 indicates that assigned resources of another IP
flow can be assigned to the P flow, while 1 indicates that assigned resources of other IP flows
cannot be assigned to the IP flow.
    # Editor's note: Data type not used.

    PreEmpVul:
      type: boolean
      description: Pre-emption-Vulnerability where 0 indicates pre-emption on the IP flow cannot be
done, while 1 indicates that pre-emption on the IP flow can be done.
    # Editor's note: Data type not used.

    FlowDirection:
      anyOf:
      - type: string
        enum:
          - DOWNLINK
          - UPLINK
          - BIDIRECTIONAL
      - 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.
    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
          - PCC_RMV
          - QOS_STO
          - QOS_STA
          - NO_CREDIT
          - PRA_CH
          - SAREA_CH
          - SCNN_CH
          - ENF_PCC_RUL
          - RE_TIMEOUT
      - 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.
        - PCC_RMV: The SMF reports when the PCC rule is removed. The SMF always reports to the PCF.
        - QOS_STO: The SMF notify the PCF when receiving notification from RAN that QoS targets of
the QoS Flow cannot be fulfilled
        - QOS_STA: The SMF notify the PCF when receiving notification from RAN that QoS targets of
the QoS Flow can be fulfilled 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
        - ENF_PCC_RUL: Enforced PCC rule request where the SMF is performing a PCC rules request as
instructed by the PCF.
        - RE_TIMEOUT: Indicates the SMF generated the request because there has been a PCC
revalidation timeout
    RequestedRuleDataType:
      anyOf:
      - type: string
        enum:
          - CH_ID
          - MS_TIME_ZONE
          - USER_LOC_INFO
      - 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.

Annex A (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

History

Document history		
V15.0.0	June 2018	Publication